Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technology

Master's Thesis

Investigating security vulnerabilities in E-Commerce web applications and designing countermeasures to improve their security

Prashant Gadhiya

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Prashant Ghanshyambhai Gadhiya

Informatics

Thesis title

Investigating security vulnerabilities in E-Commerce web applications and designing countermeasures to improve their security

Objectives of thesis

The key objective of the thesis is to investigate the types of vulnerabilities in e-commerce web applications, such as injection attacks, cross-site scripting, and cross-site request forgery, Broken Authentication and Session Management, Information Leakage, Insecure Direct Object References, Insecure Cryptographic Storage.
Partial objectives are as follows:
To identify the root causes of these vulnerabilities, such as insufficient input validation, improper access control, and weak authentication mechanisms.
To propose countermeasures to address these vulnerabilities, such as using secure coding practices, implementing access controls, and improving authentication mechanisms.
To evaluate the effectiveness of the proposed countermeasures by testing their impact on e-commerce web applications.

Methodology

The elaboration of the theoretical part will be based on the study of professional materials and specialized Internet sources regarding web security. The practical part of the thesis will be based on the information obtained in the theoretical part. It will also focus on the analysis and the collection of data on the e-commerce web application to analyze existing security practices, such as access controls, authentication mechanisms, and encryption protocols. Then a combination of automated and manual techniques, such as web vulnerability scanners and penetration testing, will be used to identify vulnerabilities in the e-commerce web application. The identified vulnerabilities will be prioritized and classified based on their severity and potential impact. Based on the identified vulnerabilities, design and implementation of countermeasures will be addressed. The effectiveness of the applied countermeasures in addressing the identified vulnerabilities and improving the overall security of the e-commerce web application will be analyzed.

Based on the conducted research and the practical part of the thesis, the conclusions of the thesis will be formulated.

The proposed extent of the thesis

60 – 80 pages

Keywords

Web application security, E-Commerce, Security vulnerabilities, Cyber security

Recommended information sources

FOWLER, Susan L.; STANWICK, Victor R. *Web application design handbook : best practices for web-based software.* Amsterdam ; Boston: Morgan Kaufmann Publishers, 2004. ISBN 1558607528.

GRIGORESCU, Octavian, NICA, Andreea, DASCALU, Mihai and RUGHINIS, Razvan. CVE2ATT&CK: BERT-Based Mapping of CVEs to MITRE ATT&CK Techniques. Algorithms [online]. 31 August 2022. Vol. 15, no. 9, p. 314. DOI 10.3390/a15090314. Available from: http://dx.doi.org/10.3390/a15090314

GUTMANN, Peter. *Cryptographic security architecture : design and verification.* Berlin: Springer, 2004. ISBN 978-1-4419-2980-8.

HERRMANN, Debra S. *Complete guide to security and privacy metrics : measuring regulatory compliance, operational resilience, and ROI.* Boca Raton (Florida): Auerbach Publications, 2007. ISBN 0-8493-5402-1.

CHAFFEY, Dave. *Digital business and e-commerce management : strategy, implementation and practice.* Harlow: Prentice Hall, 2015. ISBN 978-0-273-78654-2.

KUMMEROW, André, SCHÄFER, Kevin, GUPTA, Parul, NICOLAI, Steffen and BRETSCHNEIDER, Peter. Combined Network Intrusion and Phasor Data Anomaly Detection for Secure Dynamic Control Centers. Energies [online]. 9 May 2022. Vol. 15, no. 9, p. 3455. DOI 10.3390/en15093455. Available from: http://dx.doi.org/10.3390/en15093455

LAUDON, Kenneth C.; TRAVER, Carol Guercio. *E-commerce 2015 : business, technology, society.* Harlow: Pearson Education Limited, 2015. ISBN 978-1292076317.

SCOTT, David; SHARP, Richard. Abstracting Application-Level Web Security. New York, NY, USA [online]. 2022. p. 396–407. DOI 10.1145/511446.511498. Available from: https://doi.org/10.1145/511446.511498

SONG, Xuyan, ZHANG, Ruxian, DONG, Qingqing and CUI, Baojiang. Grey-Box Fuzzing Based on Reinforcement Learning for XSS Vulnerabilities. Applied Sciences [online]. 15 February 2023. Vol. 13, no. 4, p. 2482. DOI 10.3390/app13042482. Available from: http://dx.doi.org/10.3390/app13042482

Expected date of thesis defence

2023/24 SS – PEF

The Diploma Thesis Supervisor

Ing. Petr Benda, Ph.D.

Supervising department

Department of Information Technologies

Electronic approval: 29. 6. 2023

doc. Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 3. 11. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Dean

Prague on 05. 12. 2023

Declaration

I declare that I have worked on my master's thesis titled "**Investigating security vulnerabilities in E-Commerce web applications and designing countermeasures to improve their security**" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the master's thesis, I declare that the thesis does not break any copyrights.

In Prague on 13-02-2024

_____

Prashant Gadhiya

Acknowledgement

Thanks from my heart go to Ing. Petr Benda, my thesis adviser, for their guidance, aid, and sharp input throughout my research project. Their insight and prowess have significantly impacted the course and quality of my thesis.

A big thank you goes to my respected professors, dear classmates, and the hardworking admin team at the Informatics department in the Czech University of Life Sciences, Prague. Their constant support over the last two years truly enhanced my academic journey. Their support and shared wisdom inflated my understanding of the subjects and boosted cooperation and collective learning. I'm grateful for every effort that helped me grow, and I owe a lot to the academic community for enriching my education.

In the end, I thank my family and friends for their endless patience, understanding, and backing throughout my academic adventure.

Investigating security vulnerabilities in E-Commerce web applications and designing countermeasures to improve their security

Abstract

The ease of e-commerce is indisputable in the ever changing world of online commerce, but it comes with a worrying weakness: the security of e-commerce websites. In order to fortify the resilience of online shopping platforms, this thesis sets out to conduct a thorough investigation of the security issues that are common in these platforms. The first few chapters expose the common security vulnerabilities that e-commerce websites face and highlight the possible threats listed in the OWASP Top Ten. The research looks over several online purchasing platforms to find flaws and vulnerabilities, much like a detective investigating a crime scene. The main goal is to strengthen the digital fortifications of e-commerce and prevent sensitive data from being stolen, rather than just identifying these problems and moving on with them.

The thesis introduces a complex technique as we delve further. It introduces the strategic use of Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) as tools for examining code vulnerabilities and simulating real-world assaults, therefore improving the security of e-commerce websites.

The goals go beyond simple identification; they include a continuous commitment to defense and monitoring. The deployment of Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) systems functions as a constant watchdog, quickly identifying and addressing any cyberthreats from both a macro and micro viewpoint. It provides a strong protection against ever-evolving cyber dangers and is akin to a watchful security guard and a complex network of security cameras.

This thesis acknowledges the significance of choosing suitable security tools and suppliers. Making your way through this complex procedure is similar to carefully choosing the right tools for a certain task, it's like trying to find your way through a labyrinth while keeping your budget in mind. The study actively develops countermeasures in addition to identifying vulnerabilities as the chapters go. It introduces a process for designing

customized protections, ranking their implementation according to the seriousness of vulnerabilities, and thoroughly testing each defense's effectiveness.

The research findings include the challenges encountered and opportunities identified over the course of this study excursion. This thesis contributes to the ongoing discourse around the protection of e-commerce platforms by analyzing the OWASP Top Ten vulnerabilities and effectively using security tools like as SAST, DAST, SIEM, and EDR. In order to enhance their digital presence, safeguard customer information, and cultivate trust in the online realm, it provides valuable insights for organizations. The objective of this thesis is to enhance the safety of the digital realm by focusing on the establishment of secure e-commerce websites. This is particularly significant in the current era when digital platforms play a crucial role in facilitating trade.

Keywords: E-commerce Security, Online Shopping, Cybersecurity, OWASP Top Ten, Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), Vulnerability Assessment, Countermeasures, Digital Resilience, Cyber Threats, Risk Mitigation, Secure Transactions, Customer Data Protection, Security Tools, Vendor Selection, Online Threat Detection, Security Best Practices, Digital Trust

Zkoumání bezpečnostních slabin ve webových aplikacích elektronického obchodování a navrhování protiopatření ke zlepšení jejich zabezpečení

Abstrakt

Snadnost elektronického obchodování je nesporná v neustále se měnícím světě online obchodu, ale přichází se znepokojivou slabinou: zabezpečení webových stránek elektronického obchodu. Za účelem posílení odolnosti platforem pro online nakupování si tato práce klade za cíl provést důkladné prozkoumání bezpečnostních problémů, které jsou na těchto platformách běžné. Prvních několik kapitol odhaluje běžné bezpečnostní chyby, kterým čelí webové stránky elektronického obchodování, a upozorňuje na možné hrozby uvedené v OWASP Top Ten. Výzkum zkoumá několik online nákupních platforem, aby našel nedostatky a zranitelnosti, podobně jako detektiv vyšetřující místo činu. Hlavním cílem je spíše posílit digitální opevnění elektronického obchodu a zabránit krádeži citlivých dat, než jen tyto problémy identifikovat a pokračovat v nich.

Práce představuje složitou techniku, jak se ponoříme dále. Představuje strategické využití statického testování zabezpečení aplikací (SAST) a dynamického testování zabezpečení aplikací (DAST) jako nástrojů pro zkoumání zranitelnosti kódu a simulaci útoků v reálném světě, čímž zlepšuje zabezpečení webových stránek elektronického obchodování.

Cíle přesahují prostou identifikaci; zahrnují neustálý závazek k obraně a monitorování. Nasazení systémů Endpoint Detection and Response (EDR) a Security Information and Event Management (SIEM) funguje jako stálý hlídač, který rychle identifikuje a řeší jakékoli kybernetické hrozby z makro i mikro hlediska. Poskytuje silnou ochranu proti neustále se vyvíjejícím kybernetickým nebezpečím a je podobný bdělému hlídači a složité síti bezpečnostních kamer.

Tato práce uznává důležitost výběru vhodných bezpečnostních nástrojů a dodavatelů. Probojovat se tímto složitým postupem je podobné jako pečlivý výběr správných nástrojů pro určitý úkol, je to jako snažit se najít cestu v labyrintu a přitom mít na paměti svůj rozpočet. Studie v průběhu kapitol aktivně vyvíjí protiopatření kromě identifikace

zranitelností. Zavádí proces navrhování přizpůsobených ochran, řazení jejich implementace podle závažnosti zranitelností a důkladné testování účinnosti každé obrany.

Výsledky výzkumu zahrnují výzvy a příležitosti identifikované v průběhu této studijní exkurze. Tato práce přispívá k pokračujícímu diskurzu o ochraně platforem elektronického obchodování analýzou OWASP Top Ten zranitelnosti a efektivním využitím bezpečnostních nástrojů, jako jsou SAST, DAST, SIEM a EDR. S cílem zlepšit jejich digitální přítomnost, chránit informace o zákaznících a pěstovat důvěru v online sféře poskytuje organizacím cenné informace. Cílem této diplomové práce je zvýšit bezpečnost digitální sféry zaměřením na zřízení bezpečných webových stránek elektronického obchodu. To je zvláště významné v současné době, kdy digitální platformy hrají zásadní roli při usnadňování obchodu.

Klíčová slova: Zabezpečení elektronického obchodu, Online nakupování, Kybernetická bezpečnost, OWASP Top Ten, Statické testování zabezpečení aplikací (SAST), Dynamické testování zabezpečení aplikací (DAST), Bezpečnostní informace a správa událostí (SIEM), Detekce a reakce koncových bodů (EDR), Zranitelnost Posouzení, protiopatření, digitální odolnost, kybernetické hrozby, zmírňování rizik, bezpečné transakce, ochrana zákaznických dat, nástroje zabezpečení, výběr dodavatele, online detekce hrozeb, osvědčené postupy zabezpečení, digitální důvěra

Table of Contents

1. Introduction

Buying and selling items online, or e-commerce, is popular today. It's used for purchasing items, getting food delivered, and conducting business. But there's an issue. Some websites used for e-commerce aren't secure (Rungsrisawat, Sriyakul, and Jermsittiparsert, 2019; Gao et al., 2020; Hassan, Shukur, and Hasan, 2020; Kaushik, Gupta, and Gupta, 2020). Weak spots exist on these websites. Vulnerabilities that can be taken advantage of and cause harm.

This research focuses on these concerns. The aim is to understand what's wrong with e-commerce sites and figure out how to make them more secure. It's similar to finding cracks in a wall and patching them up for better defense.

Let's picture having an online store. Wouldn't it be horrible if someone accessed your customers' credit card info illegally? Hence, it's vital to understand these security challenges thoroughly. We'll inspect different online shopping sites to identify possible weaknesses.

The goal here is to grasp the specific issues and weaknesses in varying types of sites. We're not only spotting the problems but also finding ways to amplify security measures. It's like examining different locks on doors and getting better ones if required. The mission is to enhance the trustworthiness of these websites for businesses and customers alike. However, we won't stop at just problem-detection. We aim to make e-commerce platforms safer, establishing a sense of security for everyone involved.

This thesis aims to uncover issues in e-commerce sites, then seeks solutions to bolster their strength and security. It's like being a builder and investigator concurrently, safeguarding a digital space we heavily depend upon. As we dive deeper in forthcoming chapters, we'll unravel the intriguing process of pinpointing flaws and contriving measures to secure e-commerce for everyone.

2. Objectives and Methodology

2.1 Objectives

- **Exploring security weaknesses**

In this study, I intend to examine two ways for increasing the safety of E-Commerce web pages: static application security testing (SAST) as well as Dynamic Application Security Testing (DAST). I will analyse their efficacy and identify any difficulties they may have. Subsequently, I will employ both of these strategies to strengthen the security of E-Commerce websites among online consumers.

My major purpose is to increase the safety of online commerce. By integrating these two approaches and figuring out how to handle any security issues, I hope to accomplish this. This will eventually offer a safer and more delightful buying experience for consumers on E-Commerce websites.

- **Security enhancement through advanced assessments**

In this research, we wish to learn about two techniques to make E-Commerce websites safer: static application security testing (SAST) along with Dynamic Application Security Testing (DAST). We will assess their performance and identify any issues. Then, in order to make websites that sell goods safer for online shoppers, we will combine the two approaches.

Increasing the security of online buying is our aim. In order to do this, we wish to combine these two techniques and look for solutions to any security flaws. This will help customers have a safer and better shopping experience on E-Commerce websites.

- **Keeping a watchful eye**

In E-Commerce, we're constantly on the lookout for online threats. Our tools? Systems for managing information about security and events (also known as SIEM) along with systems for detecting and responding to endpoint threats (known as EDR). SIEM helps us gather and check lots of data from all over the E-Commerce world, like a big radar for finding security issues right away. EDR keeps an eye on individual

devices and tells us if something seems strange. Together, they help us be ready to act fast when there's a problem (Dijesh, Babu and Vijayalakshmi, 2020).

- **Building strong defences**

We collect information to make things safer for E-Commerce. We don't just find problems; we fix them, like repairing holes in a leaky boat. Our goal is to create smart plans and solutions (countermeasures) to make E-Commerce websites safer. This way, businesses and customers can trust that their online shopping and transactions are safe from cyber problems.

2.2 Methodology

- **To exploring security weaknesses**

To delve into this aspect, I will begin by extensively reviewing various E-Commerce websites. This process will involve a meticulous examination to uncover any potential security weaknesses and vulnerabilities. Additionally, I will closely investigate the security issues listed in the OWASP Top Ten, a widely recognized compilation of critical threats to web applications. My aim is to gain an in-depth understanding of these security issues and their implications for both online retailers and their customers. By amalgamating this knowledge, I hope to contribute to the enhancement of E-Commerce security.

- **To security enhancement through advanced assessments**

This stage revolves around enhancing the protection of online shopping sites. We'll use superior safety examination strategies for this. We'll first look at Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST). SAST finds source code vulnerabilities, while DAST simulates real-world assaults to find runtime vulnerabilities. I want to evaluate these strategies' efficacy, drawbacks, and combined performance. I use SAST and DAST to create effective online purchasing safety solutions.

- **To Keeping a watchful eye on cloud and private network**

To fulfil this objective, I will consistently monitor E-Commerce environments for potential cyber issues. We'll boost safety with Security Information and Event

Management (SIEM) systems, alongside Endpoint Detection and Response (EDR) tools. SIEM will be our watchtower. It takes data from many sources in E-Commerce and examines it, just like a radar picks up on possible safety issues right when they happen. In parallel, EDR will scrutinize individual devices, promptly alerting us to any suspicious activities. The integration of SIEM and EDR will fortify our ability to respond quickly to emerging security incidents(Dijesh, Babu and Vijayalakshmi, 2020).

- **To Building strong defences**

  To achieve this goal, the methodology will focus on creating robust defenses for E-Commerce. The approach will encompass not only the identification of security vulnerabilities but also the formulation of effective countermeasures. I will identify vulnerabilities and develop tailored countermeasures for each issue. Subsequently, I will prioritize the implementation of these countermeasures based on the severity of vulnerabilities. Pilot testing and validation will be conducted to assess the effectiveness of the proposed countermeasures in a controlled E-Commerce environment. Evaluation and adjustments will be made as necessary to strengthen the security of online shopping platforms.

3. Literature review

3.1 Understanding E-Commerce security

E-Commerce, which is buying and selling things online, is a big part of life today. It means getting stuff and paying for it on the internet. Because more and more people shop online and use digital money, we really worry about how safe E-Commerce websites are (Hassan, Shukur and Hasan, 2020). Lots of studies have looked at the problems and dangers with these websites. These problems include things like hackers getting into customer info, fake payments, and data leaks (Akour et al., 2022). Experts have thought a lot about how these dangers are changing and why we need strong security to keep important information safe in the world of E-Commerce (Gao et al., 2020; Kaushik, Gupta and Gupta, 2020).

So, the main focus of this research is to find these problems and come up with ways to make E-Commerce websites safer. We want to make special plans to fix the issues we find, like patching up holes in a leaky boat. Our goal is to make E-Commerce websites safer for businesses and customers. We hope this will give people peace of mind when they shop online and do transactions because they'll know their information is protected from cyber threats.

3.2 The OWASP top ten vulnerabilities

The Open Web Application Security Project (OWASP) is important for finding and sorting out security problems in web apps. The OWASP Top Ten is a well-recognised list of the top ten critical security flaws in online applications. These difficulties include cross-site scripting (XSS) and SQL injection attacks, as well as issues with improper security configuration and inadequate methods for determining who is authorised to do what. Numerous research works have examined these problems, their impact on E-Commerce applications, and solutions (Rungsrisawat, Sriyakul and Jermsittiparsert, 2019; Ungerer et al., 2020). The OWASP Top Ten serves as a basic reference for identifying and resolving security issues with e-commerce websites. So, the main idea here is that we use OWASP's knowledge to make E-Commerce websites safer. We want to find these problems and figure out how

to make them go away. This will help businesses and customers feel more secure when they shop online, knowing that their information is safe from cyber threats.

Let's deep dive in some of common vulnerabilities

- **Injection**

I want to talk about a big problem in online stores called "Injection." Injection is like when a bad person tries to put bad stuff into a good thing. In our case, the good thing is an online shopping website, and the bad stuff is computer code that can hurt it.

Think of it like this: When you shop online and add things to your cart, the website talks to a database to get information about the products and your payment. Sometimes, hackers try to mess with this talk between the website and the database. They send in harmful code, like a virus, hoping it will do bad things.

One common type of injection is called SQL Injection. It's like a secret language the website and the database use to talk (Dijesh, Babu and Vijayalakshmi, 2020). Hackers try to sneak in bad words or commands in this language. If they succeed, they can steal data or even control the website.

To make online stores safer, we need to find and fix these problems. One way is to check all the stuff you put in on the website, like what you type in the search box or your credit card details. If we make sure they are clean and safe, we can stop the bad code from getting in.

In my thesis, I will look at different ways hackers try to use injection to hurt online shops. I will also study how we can build better defences to protect these websites. By doing this, we can make sure that when you shop online, your personal information stays safe and secure.

- **Common injection**

Our journey to find and fix problems in E-Commerce websites starts with something called "Injection" attacks. These attacks are like sneaky intruders trying to

break the website's security. In our investigation, we'll look at five different types of Injection attacks, each with its own way of doing things.

1.   SQL Injection - The data manipulator

SQL Injection operates like a cunning code trickster. It manipulates the way the application communicates with its database (Galhotra and Dewan, 2020). Attackers insert malicious SQL queries into input fields, potentially gaining unauthorized access or tampering with sensitive data. SQL Injection can lead to data breaches, loss of customer information, and a tarnished reputation.

2.   LDAP Injection - The directory invader

It's like a sneaky intruder playing with the app's directory service. Bad guys mess with LDAP searches, maybe getting in and changing directory info without permission. LDAP Injection can mess up important directory info and how the app works.

3.   SQL Injection - The data manipulator

It's a troublemaker that messes with the app's NoSQL database. Bad guys play with NoSQL questions, maybe taking important data or breaking into the database. NoSQL Injection can cause data leaks and let unauthorized people in, making the app unsafe.

4.   SQL Injection - The data manipulator

Now, let's talk about a problem called "Broken Authentication" in online stores. Imagine it's like having a front door lock that doesn't work properly, and anyone can walk in, even if they shouldn't.

What's Broken Authentication? It's when the online shop doesn't do a good job of checking if it's really you when you log in. For example, even if you log out, sometimes you can still get back in without showing your ID, like your username and password. This can be a big problem because someone else might pretend to be you and do bad things, like using your money.

Why is it important to fix it? Fixing Broken Authentication is crucial because it helps make sure that only the right people can access their accounts on online shopping sites. If it's not fixed, bad folks might get in and cause trouble for customers. In this thesis, we'll take a closer look at the Broken Authentication issue in online shops. We'll try to find better ways to make sure only the right people can access their accounts. By doing this, we aim to make online shopping safer for everyone.

- **Sensitive data exposure**

It's a bit like when accidentally drop an important letter in the mailbox, and someone sees it. Sensitive Data Exposure happens when online shops don't keep your secret information safe, like your credit card number or personal details. If bad folks get this info, they can do bad things, like taking your money or pretending to be you.

Why is this a big problem? Well, it can hurt customers. If their private info isn't safe, it can lead to identity theft or losing money. In this thesis, we'll take a closer look at this issue in online shops and try to find better ways to keep your sensitive info safe from bad folks. Our goal is to make online shopping safer for everyone.

- **XML External Entities (XXE)**

Let's talk about XXE, which is a bit like when a website accidentally listens to someone's private information it shouldn't be hearing. XXE happens when a website trusts the wrong source and ends up getting information from an unauthorized person. It's like sharing your personal secrets with a stranger instead of keeping them safe.

This can be a big problem because it could allow bad actors to access information they shouldn't have (Zhu et al., 2021). They might learn important things about the website or even steal data, similar to giving your house keys to someone you don't know. In my thesis, I will explore the issue of XXE in online shopping platforms. My goal is to find more effective methods to ensure that websites only communicate with trusted sources and prevent unauthorized access. Through these efforts, I aim to enhance online shopping security for everyone.

- **Broken access control**

Broken Access Control is similar to when a door doesn't lock, allowing people to enter even if they shouldn't be able to. This issue arises when an online shop doesn't effectively manage access to its resources, much like a library that doesn't regulate who can access specific books (Galhotra and Dewan, 2020).

The significance of Broken Access Control lies in its potential to grant unauthorized individuals access to information or the ability to make changes they shouldn't. For example, someone might access private information or manipulate prices to steal money.

In my thesis, I will thoroughly examine the problem of Broken Access Control in online shops. My objective is to discover improved methods to ensure that only authorized individuals can perform the right actions on the website. Through these efforts, I aim to enhance the safety of online shopping for everyone.

- **Security misconfigurations**

Now, let's talk about another issue in online stores called "Security Misconfigurations." It's a bit like when you open a shop but forget to lock the back door.

So, what are Security Misconfigurations? They happen when the online shop doesn't set up its security properly. It's a bit like leaving your bike unlocked and easy for someone to take.

Why is this a problem? Well, it can be a big issue because it gives bad people a chance to get in. They might find important stuff or even take control of the website.

In this thesis, we'll take a closer look at Security Misconfigurations in online shops. We'll try to find better ways to set up security so that bad people can't easily get in. Our goal is to make online shopping safer for everyone.

- **Cross-Site Scripting (XSS)**

  Now, let's talk about another worry in online stores called "Cross-Site Scripting" or XSS. It's a bit like leaving hidden messages for visitors on a website, but sometimes, those messages can be harmful.

  So, what is XSS? It's when sneaky folks leave secret messages on a website. When visitors come to the site, they might see these hidden messages and get tricked. Bad people use XSS to grab personal info or spread nasty computer stuff.

  Why is this a problem? Well, it's a big issue because it can lead to data theft or session hijacking. When attackers put bad code into web pages, they can mess up the security and privacy of website visitors.

  In this thesis, we'll look closely at XSS in online shops. Our goal is to find better ways to protect against these hidden messages and make sure online shopping is safer for everyone.

- **Insecure deserialization**

  Now, let's talk about another worry in online stores known as "Insecure Deserialization." It's a bit like opening a mysterious package without knowing what's inside – it might cause trouble.

  So, what's Insecure Deserialization? It happens when online shops aren't careful when they open packages of data they receive, just like opening a mysterious package. If it's not done right, it can lead to problems.

  Insecure Deserialization can cause remote code execution or other security issues. If the website doesn't handle incoming data correctly, it can create opportunities for bad folks to take control or cause harm.

  In this thesis, we'll closely examine Insecure Deserialization in online shops. Our goal is to find better ways to handle data safely, just like opening packages carefully, to ensure that online shopping is secure for everyone.

- **Using components with known vulnerabilities**

Let's talk about another worry in online stores, known as "Using Components with Known Vulnerabilities." It's a bit like having old, broken tools in your toolbox that can make your work harder.

So, what's Using Components with Known Vulnerabilities? It happens when online shops use old or broken parts in their website-building toolbox. These parts may have known problems or weaknesses, just like old tools that can break easily.

Utilizing Components with Known Vulnerabilities can open up security vulnerabilities in a website. Similar to how outdated and corroded tools may not function correctly, these susceptible components can be targeted by attackers, potentially resulting in security breaches.

In my thesis, I will delve deeper into the problem of Using Components with Known Vulnerabilities in online stores. My objective is to identify more effective approaches to maintain the website's toolkit current and free from outdated and weak elements. Through these efforts, my aim is to enhance the safety of online shopping for all users.

- **Injection**

Let's discuss another concern in online stores, known as "Insufficient Logging and Monitoring." It's a bit like not keeping an eye on your shop when you're not around, making it difficult to detect if anything is going wrong.

So, what exactly is Insufficient Logging and Monitoring? It's when online shops don't maintain proper records or watch for unusual activities. It's similar to not having security cameras in a physical store, which means you can't see what's happening when you're not there.

Insufficient Logging and Monitoring can make it challenging to identify security issues. It's similar to not having security cameras and not knowing whether someone

sneaked inside the store. Malicious activity may be carried out by attackers, and we might not even be aware of it.

We'll examine the problem of inadequate logging and monitoring throughout online stores in more detail in this thesis. Our objective is to develop more effective methods for monitoring events and maintaining accurate data. By doing this, we want to increase everyone's safety while purchasing online, even when no one is always keeping an eye on things.

3.3 Static and Dynamic Application Security Testing

Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) are two important ways to check if web stores are safe. SAST looks at the code or program files to find problems early when making the website. DAST checks how the website works while it's running, like testing it with pretend attacks. Experts say it's best to use both SAST and DAST to make sure online shops are really secure. These tests help find and fix problems, making online stores safer for shoppers (Zhu et al., 2021).

3.3.1 SAST

SAST tools are like smart detectives for computer code. They carefully examine the website's code to find mistakes and problems that could be used by bad folks.Their Job in Code Security: The job of SAST tools is to make sure the code is built in a safe way. They search for things that could lead to security troubles, like unlocked doors in a house.

In this part of the thesis, we've learned about SAST tools and how they work like detectives to keep the code safe in E-Commerce websites. They help find problems early, so online shopping can be safer for everyone.

- **Challenges in integrating SAST into E-Commerce development**

Integrating SAST into E-Commerce development is like making SAST tools work smoothly with the process of creating an online store. It's a bit like adding extra safety checks when building a house. It's important because SAST helps find problems

in the code before the website goes live. But making it fit well with the development process can be a challenge.

- **Balancing speed and security**

    One challenge is finding the right balance between developing the website quickly and making sure it's secure. If we slow down too much for security checks, it might take longer to open the online store.

    E-Commerce websites often have deadlines, like opening for a big sale. Balancing speed and security means making sure the website is safe without missing important dates.

    In this part of the thesis, we've explored the challenges of fitting SAST into E-Commerce development. It's like finding the right balance so that the website can be both secure and open on time for customers to shop safely.

- **Effectiveness of SAST in protecting customer data**

    It's vital to evaluate real-life instances where SAST has proved beneficial. Valuable lessons may be gleaned from examples where SAST effectively guarded client data from theft.

    SAST performs a critical function in avoiding data breaches. By identifying and fixing flaws, it works as a deterrent, preventing hostile persons from entering the website to grab client information.

    In this portion of the thesis, researchers have investigated the usefulness of SAST in securing consumer data. Similar to a solid lock on your door, SAST adds to the protection of critical information, therefore boosting the safety of online purchasing for everybody.

- **Real-world success stories**

It is important to look at real-world examples where SAST has worked. Cases where SAST effectively prevented client data theft may provide us with valuable information.

SAST is essential for preventing data breaches. It serves as an obstacle to stop malevolent people from breaking into the website and stealing consumer data by locating and fixing flaws.

I have examined SAST's efficacy in protecting client data in this portion of the thesis. Comparable to having a sturdy lock on the door, SAST helps safeguard private data, making internet buying safer for everyone.

3.3.2 DAST

DAST is like a website detective. It examines the online store like a treasure hunt to find secret traps or weaknesses.DAST tries to use tricks and tactics to see if it can find any hidden problems. If it does, it helps us fix them before bad folks can find them.

Uncovering Hidden Issues: DAST is important because it looks for problems that might not be easy to see. Just like a hidden treasure, these issues need to be uncovered and fixed.

Preventing Sneaky Attacks: By finding and fixing hidden weaknesses, DAST helps prevent sneaky attacks that could harm the website and its customers.

In this part of the thesis, we've learned about DAST and how it works like a detective to uncover secret traps in E-Commerce websites. It's an important tool for making online shopping safer for everyone.

- **Integration of DAST into E-Commerce development process**

Integrating means making DAST tools a part of creating an online store. Think of it as getting a new teammate to assist in the project. Why It's a Big Deal: Integrating

DAST is important because it helps find issues in the website's code while it's still in the making. This way, we can fix things early and avoid headaches later on.

- **Speed vs. Safety**

The Challenge We Face: One tricky part is finding the right balance between building the website quickly and making sure it's super secure. We don't want to slow things down, but we definitely want it to be safe.

Sticking to the Schedule: E-Commerce websites often have deadlines, like launching for a big sale. We've got to ensure that integrating DAST doesn't mess up our important dates.

In this part of the thesis, we've explored how to bring DAST tools into the E-Commerce development process. It's kind of like having a new helper on the team to build a fantastic online store that's both speedy and safe, without missing any important deadlines.

- **DAST and secure E-Commerce transactions**

DAST is like a vigilant guard for online shops. It checks the website to ensure that everything is safe for customers when they make purchases (Achmad, 2023).

Protecting Customer Transactions: DAST helps keep customer transactions secure by searching for hidden dangers in the website's code. It's like checking every corner to make sure it's safe for shoppers.

- **Real-Life stories of success**

To truly understand, we can look at real stories where DAST played a crucial role in protecting E-Commerce transactions. These stories show how it keeps bad folks away from sensitive customer data.

Preventing Data Theft: DAST's job is to prevent bad people from stealing customer information during transactions. It's like having a trusted bouncer at the door who only allows the right people inside.

In this part of the thesis, we've explored how DAST contributes to ensuring that E-Commerce transactions are safe and sound. It's like having a watchful guard to make sure everything runs smoothly, and customers can shop securely online.

3.4 SIEM and EDR

Security Information and Event Management (SIEM) systems are like important security helpers for online shops. They watch out for problems and respond quickly. These systems collect and connect information from different places, so we can find and check security issues right away (González-Granadillo, González-Zarzosa and Diaz, 2021).

In addition, there are special tools called Endpoint Detection and Response (EDR) solutions. EDR tools are like guards for each computer in the online shop. They keep a close eye on things and can spot advanced threats (Arfeen et al., 2021). People have looked at how to use both SIEM and EDR tools together to make online shops safer. This helps organizations act fast if there might be any trouble.

3.4.1 SIEM - A watchful eye

SIEM stands for Security Information and Event Management. It's like a guardian for the online store. SIEM tools collect information about what's happening in the website and look for anything suspicious (Radoglou-Grammatikis et al., 2021). SIEM helps protect the website from bad folks who might want to break in or steal information. It's like a security guard who keeps an eye on the store 24/7.

- **Monitoring and alerts**

SIEM tools monitor the website for unusual activities, like someone trying to get in without permission. If they spot something fishy, they send an alert to the website's protectors (Radoglou-Grammatikis et al., 2021). SIEM can help stop issues before they become big problems. It's like catching a leak in a boat before it sinks. In this part of the thesis, we've learned about SIEM, which acts as a watchful eye, helping to keep E-Commerce websites safe and secure. Just like a diligent guardian, SIEM is always on the lookout for trouble to protect the online store and its customers.

3.4.2 EDR - The computer hero

EDR stands for Endpoint Detection and Response. It's similar to a superhero for your computer. EDR tools help protect individual devices (like computers and servers) from bad things (Pourni, 2022). EDR is very important because it keeps a close watch on the devices that connect to the website. Think of it as a guardian that ensures these devices stay safe and don't do anything harmful.

- **Protecting endpoints**

I, as the author, would like to emphasize that EDR tools are diligent in monitoring individual devices. These tools diligently scan for any indications of problems, such as viruses or unusual activities, and they promptly respond when detecting any malicious activities.

Think of EDR as a superhero in the digital world, actively combatting cyber threats. EDR's role is to proactively prevent attacks on the website by identifying and addressing potential threats at an early stage.

In this section of my thesis, I've delved into the world of EDR, likening it to a computer hero that plays a crucial role in ensuring the safety of individual devices connected to E-Commerce websites. In much the same way that superheroes come to the rescue, EDR is there to uphold safety and security in the digital realm.

3.4.3 Why we need both

- **Comprehensive coverage**

SIEM keeps an eye on the overall network, keeping tabs on all the different events and actions that happen. On the other hand, EDR concentrates on each individual device, making sure they remain secure from any potential threats (Radoglou-Grammatikis et al., 2021). With both of these tools, I cover all aspects, from broad network-wide concerns to the finer details of each device's safety.

- **Faster threat detection**

The collaboration between SIEM and EDR enhances our ability to swiftly and effectively detect threats. SIEM identifies suspicious activities across the network,

while EDR focuses on pinpointing issues on individual devices (Radoglou-Grammatikis et al., 2021).

When we combine their capabilities, we can identify and respond to threats more rapidly, thereby decreasing the likelihood of a successful attack.

- **Detailed investigations:**

SIEM aids in identifying the possible location of a security problem within the network. Meanwhile, EDR offers detailed insights into the activities occurring on particular devices (Yudhianto, 2023).

When used together, they support comprehensive investigations, which are crucial for comprehending and mitigating security incidents.

- **Protecting customer Data:**

E-Commerce websites handle sensitive customer data like payment information and personal details (Marchany and Tront, 2002). SIEM and EDR working in tandem help ensure that this valuable data remains secure, preventing data breaches and protecting customer trust (Radoglou-Grammatikis et al., 2021).

- **A Balanced approach:**

SIEM and EDR create a well-rounded security strategy. SIEM focuses on the broader perspective, while EDR deals with the finer aspects (Younus and Alanezi, 2023). This equilibrium is crucial because cyber threats vary in their forms and magnitudes, demanding a comprehensive defense.

To sum it up, the presence of both SIEM and EDR is vital because they enhance each other's strengths, offer swift threat detection, enable thorough investigations, protect customer data, and establish a well-balanced approach to cybersecurity. Together, they establish a sturdy defense system for E-Commerce websites.

3.4.4 Future of security

The future holds more complex and sophisticated cyber threats. Attackers are continually evolving their tactics (Choi and Lee, 2019). SIEM and EDR provide the advanced capabilities needed to detect, respond to, and mitigate these evolving threats effectively.

- **Data protection and privacy regulations:**

Data protection laws and regulations are tightening globally, increasing the demands on organizations to safeguard customer information. SIEM and EDR play a pivotal role in assisting businesses in complying with these regulations by furnishing strong security measures and effective incident response capabilities (Achmad, 2023).

- **Real-time threat intelligence:**

In the coming years, immediate threat intelligence will be indispensable for promptly recognizing and countering threats. SIEM and EDR offer real-time surveillance and analysis, enabling organizations to proactively address emerging threats.

- **Endpoint security becomes paramount:**

Endpoints (devices like computers, smartphones, and IoT devices) will continue to be a prime target for cyberattacks. EDR's role in securing endpoints will grow in importance as more devices connect to networks (Arfeen et al., 2021).

- **Cloud and remote workforce challenges:**

As businesses increasingly adopt cloud services and remote work, securing these environments will be critical. SIEM and EDR solutions are adaptable and can extend their protection to cover cloud-based and remote work scenarios.

- **Integration and automation:**

The future of security will rely on seamless integration between different security tools and automation of routine tasks. SIEM and EDR can integrate with other security solutions and automate incident response, reducing the burden on cybersecurity teams.

In summary, SIEM and EDR are at the forefront of the future of security due to their capabilities in combating advanced threats, ensuring compliance with regulations, providing real-time threat intelligence, securing endpoints, addressing cloud and remote work challenges, and facilitating integration and automation (Arfeen et al., 2021). As the cybersecurity landscape continues to evolve, these tools will remain indispensable in safeguarding E-Commerce web applications and customer data.

3.5 Threat modelling

Threat modelling is like being a detective for computer security. It helps find problems in E-Commerce websites and stops bad people from doing harm. Imagine it's like making a plan before going on a trip. It helps us see where we might face trouble and how to avoid it (Dijesh, Babu and Vijayalakshmi, 2020).

In threat modelling, we look at E-Commerce websites and figure out where the weak spots are. These weak spots are like open doors for bad people to sneak in. We don't want that!

- **Threat modelling helps us:**

Be smart and stay ahead of bad folks. Fix problems early, like finding a leak in a boat before it sinks. Save money because fixing things later can be super expensive. It's important to know where problems might pop up so we can stop them and keep E-Commerce websites safe.

The STRIDE Model helps you think about different ways bad folks might try to harm your e-commerce website. It stands for Spoofing (when someone pretends to be someone else), Tampering (messing with your website's data), Repudiation (denying they did something bad), Information Disclosure (stealing info), Denial of Service (making your website crash), and Elevation of Privilege (getting more access than they should) (Jiang, Chen and Deng, 2010). It's like having a guide to understand and prevent problems that could happen to your website, making it safer for your customers.

3.5.1 STRIDE model

In this section, let's talk about something called the STRIDE Model. It's like a tool to discover issues in E-Commerce websites and make them more secure.

Championing the STRIDE model in the thesis is rooted in its effectiveness in threat modeling, supported by recognition in industry reports from esteemed sources such as NIST and MITRE. The model's adoption enjoys wide acknowledgment, earning approval from large enterprises and validation in various surveys. The thesis underscores its applicability across diverse sectors, positioning it as a versatile and reliable approach to threat modeling.

The STRIDE model has six things to watch out for:

S - Spoofing identity: This is when an individual pretends to be someone else, such as a hacker posing as a legitimate customer. To prevent this, web developers must verify the identity of the person logging in to ensure it's the genuine user.

T - Tampering with data: This happens when nefarious people change or falsify the data on the website. To prevent this, websites must employ robust encryption to safeguard data from unauthorized modifications (Jiang, Chen and Deng, 2010).

R - Repudiation: This happens when someone engages in improper activities on the website but later denies their involvement. To prevent this, the website should maintain records of actions taken and their responsible parties.

I - Information disclosure: This is about keeping confidential information secret. Web developers must ensure that only authorized people can access sensitive data.

D - Denial of service: Bad folks may try to make the website stop working so customers can't use it. Web developers need to prepare for this and have backup plans in case the website gets attacked and stops working (Younus and Alanezi, 2023).

E - Elevation of privilege: This is when a person gets more power on the website than they should have. To prevent this, web developers need to ensure that everyone has the right level of access.

So, the STRIDE Model helps people find these issues in E-Commerce websites, and then they can fix them to make the website safer for all the customers.

3.5.2 Attack trees

Let's discuss Attack Trees for the thesis. They are a bit like a map to figure out how bad people might try to harm a shopping website. It's similar to planning your moves in a game.

Think of an Attack Tree like an upside-down tree. At the very top, there's the main goal of the bad person, like stealing customer information. Then, it splits into different ways they could try to achieve it. These branches keep splitting until you see all the things they need to do to make it work.

For example, if someone wants to steal passwords from the website, the Attack Tree might show they first need to find a way in, maybe by guessing a weak password. Then, they have to locate where the passwords are stored, and finally, they can steal them.

Attack Trees help the people building the website think about all the ways an attacker might try to harm it. This way, they can create defenses to stop these bad things from happening (Rungsrisawat, Sriyakul and Jermsittiparsert, 2019).

So, Attack Trees are like a treasure map, but instead of hunting for treasure, you're hunting for problems in the website's security. They help you plan how to keep the website safe from bad folks.

3.5.3 Agile threat modelling

Imagine you're at the beach building a sandcastle. You don't create the whole castle at once. Instead, you start with a bit of sand, adding more and shaping it as you go.

Agile Threat Modeling is a bit like that. Instead of waiting until the very end to check if the online store is safe, you search for problems bit by bit while working on different parts of the website (Bernsmed et al., 2022).

So, while you're working on one part of the website, you also think about how bad people might try to harm it. You discuss these possible issues with your team and figure out how to stop them. It's like ensuring your sandcastle walls are strong as you build them, not waiting until they're all finished and hoping they don't collapse.

Agile Threat Modeling is a way to make sure security is a part of everything you do when creating a website (De, 2020). It's like fastening your seatbelt before driving, not after an accident. This helps keep the website safer right from the beginning, instead of trying to fix it later.

3.5.4 DREAD model

The DREAD Model is like a map to understand how bad things can happen to your website. It helps you figure out which problems are the most important to fix first. DREAD stands for five things: Damage (how bad the problem could be), Reproducibility (how easy it is to do the bad thing again and again), Exploitability (how likely it is that the bad people can actually do the bad thing), Affected Users (how many people could be in trouble because of the problem), and Discoverability (how easy it is for someone to find the problem) (Story et al., 2013). It's like having a checklist to make your website safer from the bad folks out there.

DREAD represents five things that are like potential dangers to the website:

D - Damage: This indicates the severity of the issue, whether it's a minor concern or a major catastrophe.

R - Reproducibility: This pertains to how easily malicious individuals can repeatedly carry out the same harmful action.

E - Exploitability: It measures the likelihood that malicious actors can successfully execute the harmful action.

A - Affected Users: It informs us about the number of individuals who could face trouble due to the issue.

D - Discoverability: This relates to how easy it is for someone to detect the problem.

By employing the DREAD Model, one can assess each of these factors and determine which issues should be addressed first. It aids in making the website safer for customers.

In essence, the DREAD Model serves as a practical checklist that assists website developers in comprehending and mitigating issues intelligently. It's akin to knowing which components of a car need repair to ensure its smooth operation.

3.5.5 PASTA model

The PASTA Model helps us understand and fix problems in cybersecurity. It's like a recipe that checks how bad folks might try to harm a website. We use it to find weak spots, test how strong the website is, and figure out which problems are most likely to happen. It's like checking our house for places where burglars might break in and making those spots stronger. This way, we can keep our E-Commerce website safer from online threats (Castro, Cabrero and Heimgärtner, 2022).

PASTA stands for a few important things that aid in and fixing problems:

P - Process for attack simulation and threat analysis: Think of this as a recipe for checking how bad people might try to harm the website (Hassan, Shukur and Hasan, 2020).

S - Security testing and assessment: This involves testing the website to see if it's strong enough to stop bad people.

T: Threat intelligence and attack patterns: Similar to knowing how hackers access websites.

A-Risk assessment: Determine which concerns are most likely and riskiest.

By using the PASTA Model, you can look at each of these things and create a plan to make the website safer. It's like checking your house for places where burglars might break in and then making those spots stronger.

So, the PASTA Model is like a helpful guide that assists people in making websites safer by identifying and fixing problems. It's similar to ensuring your bike is in good shape before you go for a ride to keep yourself safe.

3.5.6 Kill chain model

The Kill Chain Model shows how bad folks attack a website step by step. They start by gathering information about the website, then create tools to break in, send those tools, break into the website, control it, and finally, do the bad things they planned. It helps us understand where the bad folks might strike and how to stop them at each step, like setting up defenses to protect a castle from enemy attacks (Khan, Siddiqui and Ferens, 2018).

The Kill Chain Model has several steps that show how bad folks attack a website:

- **Reconnaissance:** This is when the bad people gather information about the website. They sort of spy on it to find weak spots.

- **Weaponization:** After they identify the weak spots, they create their tools or "weapons" to attack the site.

- **Delivery:** They send their weapons to the website, like a sneak attack.

- **Exploitation:** This is when they use their weapons to break into the website.

- **Installation:** Once they're inside, they might put more bad stuff on the website to control it.

- **Command and control:** They take over the website and give it orders, like a puppeteer with strings.

- **Actions on objectives:** Finally, they do the bad things they planned, like stealing information or messing up the site.

The Kill Chain Model helps people see where the bad folks might strike and figure out how to stop them at each step. It's like knowing where the enemy might attack your castle and setting up defenses to protect it (Khan, Siddiqui and Ferens, 2018).

So, the Kill Chain Model is like a strategy guide that helps make websites safer by understanding and blocking the moves of bad people. It's like a shield to keep your website safe from attackers.

3.5.7 Attack surface analysis

Attack Surface Analysis is like making a list of all the doors and windows in a house.

You want to know where bad folks could get in:

- **Find the doors and windows:** To start, you assess the website and pinpoint all the potential entry points that someone might use to gain access, such as login pages or areas where personal information is entered (Maple et al., 2019).

- **Check for weak spots:** Afterward, you scrutinize these areas meticulously to determine if they possess the strength necessary to fend off malicious individuals. If any vulnerabilities are found, it's akin to having a window that doesn't lock, leaving an opening for potential security breaches (Alwaheidi, Islam and Papastergiou, 2022).

- **Make it stronger:** Finally, you come up with ways to make those weak spots stronger. It's like adding locks to your doors and windows to keep burglars away.

So, Attack Surface Analysis ensures that all the ways into the website are safe and secure. It's like checking all the paths to your house and making sure they're protected from intruders. This keeps everyone who accesses the website safer.

3.5.8 Attack library

An Attack Library is similar to a collection of data on different techniques that malevolent people may use to damage a website. Consider it a list of possible ruses they may use. Website developers may better understand the types of threats that might

be experienced by using this library (Pinchinat, Schwarzentruber, and Lê Cong, 2020). It's similar to knowing all the many card and dice games that can be played.

You may learn more about how these bad actors could try to get into a website or steal data by using the Attack Library (Jhawar et al., 2018). It's like trying to figure out a winning strategy in a game by watching your opponent's actions.

Essentially, the Attack Library serves as a reference that facilitates comprehension of every possible problem and danger that a website may encounter. It functions similarly to a book of tactics for protecting the website from attacks from malevolent parties.

3.5.9 Abuse case modelling

Initially, we search for any potential threats, such as someone attempting to steal data or manipulate the system.We compile an overview of all these negative actions, such as attempting to hack a website or displaying an incorrect pricing on a shopping website.

Then, we think about how to protect the website from these bad things. It's like making sure your house has good locks and alarms to keep burglars away.So, Abuse Case Modeling helps us understand what could go wrong with the website and how to stop it (Whitmore, 1984). It's like being a detective, looking for clues to prevent problems and make the website safer for everyone.

3.6 Vendor comparison for cybersecurity technologies

Choosing the right companies for cybersecurity tools is an important decision for organizations, especially if they have a limited budget. Research in this area looks at how well different cybersecurity tool providers work and how much they cost (Khan et al., 2022). Comparing these providers helps organizations make smart choices that match their security needs and budget, making sure that the security tools are not only good but also affordable.

3.6.1 Vendor feature evaluation

Vendor Feature Evaluation is like comparing different tools or products when choosing what's best for protecting E-Commerce websites (Keskin et al., 2021). It's a bit like comparing different gadgets to see which one suits your needs best.

- **Understanding vendor feature evaluation:**

Vendor Feature Evaluation is like checking what special things different cybersecurity tools or products can do from different companies. We need it to figure out which tool or product is the best for our E-Commerce website. It's like picking the right superhero for a specific job.

- **Comparing the features:**

Vendor Feature Evaluation involves creating a checklist of the capabilities of each tool or product. For instance, one tool may excel in preventing viruses, while another is proficient at detecting unusual activities. I assess which features hold the utmost significance for my website's security. It's akin to selecting the appropriate tools from a toolbox for a specific task.

- **Making informed choices:**

By evaluating vendor features, we make smart choices about what to use. It's like making sure we have the right tools to protect our cybersecurity.

- **Staying secure:**

This process helps make sure our E-Commerce website stays safe and protected from threats and problems.

In this part of the thesis, we've explored Vendor Feature Evaluation, which is like comparing the powers of different superheroes to find the best one to protect our E-Commerce website. It's all about making smart choices to keep the website safe and sound.

3.6.2 Performance benchmarking

Performance Benchmarking is similar to assessing the speed and effectiveness of various cybersecurity tools to gauge their performance. It's somewhat akin to

evaluating how swiftly different superheroes can react to crises and how robust they are.

- **Understanding performance benchmarking:**

Performance Benchmarking is like checking how fast and strong different cybersecurity tools are to see how well they work. We need it to find out which tool can protect our E-Commerce website without making it slow.

- **Measuring speed and efficiency:**

I evaluate how rapidly a cybersecurity tool can detect and resolve issues. Generally, a faster response is preferable. Additionally, I examine a tool's ability to function effectively without consuming excessive computer resources. It's akin to having a powerful superhero who can endure for an extended period without getting fatigued quickly.

- **Making the right choice:**
  1. **Choosing wisely:** By doing Performance Benchmarking, we can pick the cybersecurity tool that's just right for our website.

  2. **Happy customers:** It helps make sure our E-Commerce website runs smoothly, and customers can shop without any delays.

In this part of the thesis, we've explored Performance Benchmarking, which is like comparing the speed and strength of different superheroes to choose the best one to protect our E-Commerce website. It's all about making the right choice to keep the website fast and secure.

3.6.3 Scalability and integration review

Scalability and Integration Review is like checking if a cybersecurity tool can grow and work well with other tools, similar to making sure that different members of a team, like superheroes, can work together.

- **Understanding scalability and integration:**

    Scalability is like asking if the cybersecurity tool can handle a growing website with more users and data. Integration is about whether it can work smoothly with other tools.

    We need to make sure our cybersecurity tools can grow with our E-Commerce website and play nice with others. Scalability asks if the tool can handle more work as our website gets bigger. It's like making sure our superhero can take on more challenges as the city grows.

    Integration checks if the tool can work alongside other tools without causing problems. It's like making sure our superheroes can work together without fighting. By reviewing scalability and integration, we can choose a cybersecurity tool that's ready for the future, even as our website expands. It helps ensure that all our cybersecurity tools can work together smoothly, like a team of heroes saving the day.

    In this part of the thesis, we've explored Scalability and Integration Review, which is like checking if our superheroes can handle more challenges and work together as a team. It's all about making the right choice to keep our E-Commerce website secure and adaptable.

3.6.4 Cost benefit assessment

Cost-Benefit Assessment is like deciding if something is worth the money, just like when you decide if you should buy a new gadget (Butler, 2002).

- **Understanding cost-benefit assessment:**

    Cost-Benefit Assessment is like asking if the cybersecurity tool's benefits are worth the money it costs (Butler, 2002). Why Do We Need It? We need it to make sure we're spending our budget wisely on tools that truly protect our E-Commerce website.

- **Weighing the costs and benefits:**

    Counting the Costs: We look at how much money we'll spend on the tool, like buying it and maintaining it. We also see what the tool brings to the table, like how well it protects our website and if it helps prevent costly security breaches.

- **Making a smart choice:**

  Balancing Act: Cost-Benefit Assessment helps us balance the cost of the tool with the benefits it provides.

- **Investing wisely:**

  It ensures that we invest our budget in tools that offer real value and protection for our E-Commerce website.

  In this part of the thesis, we've explored Cost-Benefit Assessment, which is like deciding if a new gadget is worth buying. It's all about making a smart choice to use our budget wisely and keep our website safe and secure.

3.6.5 Customer feedback examination

User feedback examination resembles hearing user reviews of a cybersecurity technology (Finch, 2007). We need to know whether users enjoyed and found the product useful.

- **Understanding customer feedback examination:**

  Inspecting customer feedback entails examining cybersecurity tool users' comments. This is crucial for understanding how well the product works in practise and if clients like it.

- **Listening to customers:**

  We take into consideration the opinions of those who have used the tool. Are they fond of it? Does it suit them well? Customer feedback gives us insights into how the tool performs in real situations, just like reading reviews to know if a gadget lives up to its promises.

- **Making informed decisions:**

  Customer Feedback Examination helps us make informed decisions about whether the cybersecurity tool is a good fit for our E-Commerce website.

- **Avoiding surprises:**

This process helps me steer clear of unexpected issues and guarantees that I opt for a tool with a favorable history among other users. In this segment of my thesis, I've delved into Customer Feedback Examination, which is akin to perusing product reviews before purchasing a new device.

It's all about making smart decisions based on what others have experienced with the cybersecurity tool to keep our E-Commerce website safe and secure.

4. Practical part

4.1 Overview of network architecture

Imagine an e-commerce website as a big store. In this store, you have different sections: the front entrance, the cash register, the shelves with products, and the back room where you keep stock. These sections need to work together, just like parts of a network. Like a well-orchestrated symphony, various components work seamlessly together to bring forth the websites we interact with daily. This intricate dance involves the Front-End, Back-End, Servers, Database, and the underlying backbone, the Internet. In this exploration, we'll delve into the metaphorical analogy of a store, unravelling the roles each component plays in shaping the user's journey.

Front-End: Imagine the Front-End as the inviting storefront of a physical store. It's the first impression, the visual appeal that captivates and guides customers. In web development, the Front-End encompasses everything a user interacts with – from web pages and buttons to forms and visual elements. The user-friendly and attractive design is paramount, creating an environment that encourages seamless navigation and engagement. HTML, CSS, and javascript are the artisans of the Front-End, sculpting the visual and interactive aspects that lure users into the digital store.

Back-End: As the customers explore the captivating storefront, the Back-End quietly operates in the hidden engine room of the store. This is where the magic happens, where all the information about products, customers, and transactions is stored and processed. Comparable to the back room of a physical store, the Back-End ensures the website's functionality, managing the data and executing operations beyond the user's sight. Server-side languages like Python, Ruby, and Node.js are the craftsmen shaping the logic and functionality that power the Back-End.

Servers: Analogous to the cash registers in a physical store, servers handle the requests made by customers and process transactions. These powerful computers store and manage the website's data, ensuring that every interaction is swift and secure. The server's role is dynamic, responding to users' requests, managing resources, and

facilitating communication between the Front-End and the Back-End. The reliability and efficiency of servers are crucial for a smooth and enjoyable user experience.

Database: Think of the database as the organized storage shelves in a store, neatly containing all the essential information. It is here that product details, customer data, and order history find their structured place. The database is not just a storage space; it is the backbone of the Back-End, providing a systematic structure for data retrieval and manipulation. Technologies like MySQL, PostgreSQL, and MongoDB shape and manage this crucial repository, ensuring data integrity and security.

Internet: In the vast mall of the digital world, the Internet serves as the interconnected network of roads linking stores and customers. It is the conduit through which user's access websites, and the speed and reliability of this connection are paramount. The Internet facilitates the seamless flow of data between the user's device, the Front-End, the Back-End, servers, and databases. Its infrastructure, including protocols like HTTP and HTTPS, ensures a stable and secure environment for users to traverse.

The Synchronized Dance: Now, envision the entire web development process as a synchronized dance within the store. The Front-End attracts customers with its appealing design, guiding them through the digital aisles. Simultaneously, the Back-End orchestrates the behind-the-scenes operations, ensuring that every user interaction is met with a seamless response. Servers act as the digital cash registers, processing transactions and managing the flow of data. The database, akin to organized storage shelves, holds the vital information in a structured manner. All of this is made possible by the interconnected web of the Internet, the roads connecting users to the digital storefront.

So, in the intricate tapestry of web development, each component plays a pivotal role, contributing to the seamless and engaging online experiences we've come to expect. The Front-End, Back-End, Servers, Database, and the Internet collaboratively shape the digital landscape, creating a harmonious symphony of technology. As we continue to traverse the boundless realms of the online world, understanding these

components unveils the complexity and beauty behind the websites we interact with daily. The store metaphor provides a tangible framework to comprehend the interplay of these elements, ultimately highlighting the craftsmanship that goes into creating the digital storefronts we explore with a click.

Now, let's talk about security in this setup. Just like in a physical store, you need security measures to protect online store from thieves and troublemakers. In the digital world, these measures include things like strong passwords, firewalls, and encryption. These are like locks on store's doors and alarms to alert you if something's wrong.

In thesis, you'll investigate the weak points in this network architecture – places where cyber attackers might try to break in or steal information. Then, you'll come up with ways to make these areas more secure. It's like adding extra locks and security cameras to store to keep it safe. In the world of e-commerce, security is super important. People trust website with their personal and payment information, and it's job to make sure it stays safe. That's what thesis is all about – finding ways to make e-commerce websites more secure for everyone.

4.1.1 Small E-Commerce network insights

In a small e-commerce business, they have lots of things to help them work on the internet safely (Marchany and Tront, 2002). The network architecture plays a crucial role in ensuring a safe and seamless online shopping experience for both the business and its customers. This discussion will delve into the various components of a small e-commerce network, exploring their functions and highlighting the importance of cybersecurity measures. It's like having tools for their online shop. I created illustrative diagram for understanding purpose.
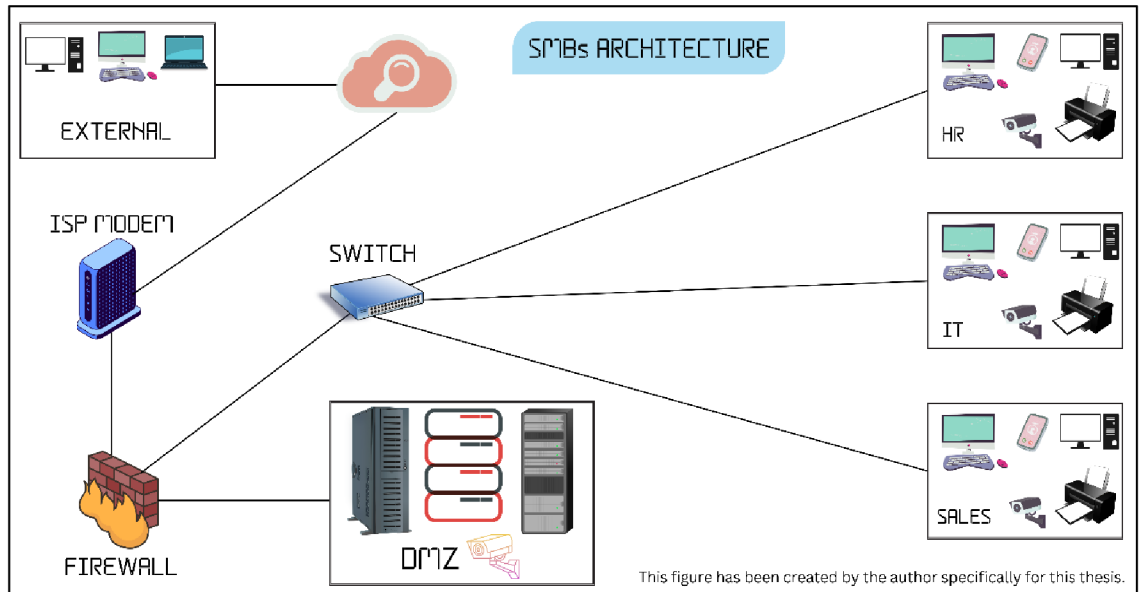
Figure 1: Small E-Commerce Network Architecture

[**Source:** This figure has been created by the author specifically for this thesis]

Let's discuss each of the parts in high level:

Component	Analogy	Description
Internet	Road Leading to Online Shop	Serves as the gateway for the e-commerce business, providing the foundation for its virtual presence. Connects with customers and facilitates transactions in the expansive digital space.
Router Modem	Central Connector	Acts as the central connector, bridging the internal network and the external internet. Enables the establishment of a reliable online presence, facilitating communication and data exchange. Crucial for making the online shop accessible to potential customers.
Firewall	Vigilant Guard	Monitors incoming and outgoing traffic, preventing malicious entities from infiltrating the network. Ensures the integrity and security of the online shop's operations by allowing legitimate transactions and interactions to proceed smoothly.

Component	Analogy	Description
DMZ (Demilitarized Zone)	Showcase for Online Shop	Specialized area within the network architecture, accessible from the outside but separated from the main secure zone. Functions as a showcase for the online shop, containing elements like website images and information that need external visibility. Critical for maintaining a balance between accessibility and security.
Switching	Wiring in a House	Interconnects various devices within the network, facilitating seamless communication between different components. Enhances the overall functionality of the e-commerce network, ensuring efficient transmission of relevant information when customers place orders.
Human Resources (HR)	Human Element	Represents the human element in the network. HR personnel rely on the network for tasks such as order tracking and customer management. Secure access to the network is essential for the smooth functioning of internal processes related to human resources.
IT and DEV Team	Tech Experts	Comprising IT and development teams, they play a pivotal role in maintaining and advancing the e-commerce network. Responsible for ensuring proper functioning, addressing issues promptly, and potentially developing new features to enhance the online shop's capabilities.
Sales	Sales Team	The sales team utilizes the network for customer interactions, order handling, and overall business transactions. Effective use of the network is crucial for providing a seamless shopping experience and

Component	Analogy	Description
		reinforcing the significance of a secure and well-maintained e-commerce network.
Camera Setup	Surveillance System	Represents the eyes watching over the physical office space. The surveillance system adds an additional layer of security, safeguarding the physical premises. It complements the digital defenses in place for the online network, contributing to an overall secure environment for the e-commerce business.

Table: 1 Small E-Commerce network insights

[**Source:** This table has been created by the author specifically for this thesis. The Small E-Commerce network insights under the ownership of the author of the thesis.]

So, the small e-commerce network architecture is a complex ecosystem with various interconnected components. Each element plays a unique role in ensuring the business's secure presence on the internet and facilitating smooth operations. This thesis aims to identify and address potential vulnerabilities within this network, with the ultimate goal of enhancing cybersecurity measures. By comprehensively analyzing the network architecture and proactively addressing any issues, the online shop can thrive in a secure digital environment, providing customers with a trustworthy and reliable platform for their shopping needs.

4.1.2 Budget friendly network security tools and path

In the dynamic world of e-commerce, safeguarding the online store from potential threats is paramount. Small businesses often face budget constraints, making it challenging to invest in high-end security tools. However, there are cost-effective strategies and tools available that can significantly enhance the security posture of a small e-commerce store. This discussion explores various affordable cybersecurity measures, emphasizing their importance and practical implementation. Free Antivirus Software: A cornerstone of digital security, free antivirus software serves as a reliable digital guard for protecting computers from malicious entities. While some may

associate effective antivirus solutions with high costs, there are reputable free options that provide robust protection. These programs act as a first line of defense, detecting and neutralizing potential threats before they can compromise the integrity of the online shop.

Firewall: Reiterating its significance, the firewall acts as a virtual barrier, warding off unauthorized access and potential threats. Free firewall solutions are available and can be instrumental in fortifying the digital perimeter of the e-commerce store. These tools help regulate incoming and outgoing network traffic, ensuring that only legitimate transactions and interactions are allowed, while malicious activities are promptly intercepted.

Regular Updates: One of the most cost-effective yet impactful cybersecurity measures is maintaining regular updates for both operating systems and software applications. Updates often include patches and fixes for known security vulnerabilities, reducing the risk of exploitation by cybercriminals. This practice, which comes at no additional cost, is essential in building a resilient defense against emerging threats.

Strong Passwords: The human element remains a significant factor in cybersecurity, and using strong, unique passwords is a fundamental aspect of online safety. Free password managers offer a practical solution for creating and securely storing complex passwords. By utilizing these tools, small e-commerce businesses can enhance the security of their accounts and prevent unauthorized access, mitigating the risk of data breaches.

Security Scanners: Cost should not be a deterrent to proactive security measures. Free security scanners are valuable tools that can scan a website for potential vulnerabilities and security issues. Identifying and addressing these issues before malicious actors exploit them is crucial for maintaining the integrity of the e-commerce store. These scanners provide an additional layer of defense, ensuring that the website remains secure and trustworthy for customers.

Learning: Knowledge is a powerful and cost-free resource in the realm of cybersecurity. By investing time in learning about online safety and sharing this

knowledge with the team, small e-commerce businesses can build a resilient human firewall. Training employees to recognize potential threats, phishing attempts, and best practices for secure online behavior contributes significantly to the overall security posture of the organization.

In conclusion, securing a small e-commerce store on a tight budget is feasible through a strategic combination of affordable cybersecurity measures. Utilizing free antivirus software, implementing firewalls, prioritizing regular updates, employing strong passwords with the assistance of free password managers, leveraging security scanners, and fostering a culture of continuous learning are all integral components of a robust cybersecurity strategy. By adopting these practical measures, small e-commerce businesses can fortify their online defenses, protecting both their digital assets and the trust of their customers. It's akin to putting effective locks on the doors of the online shop without incurring substantial costs, ensuring a safer and more secure e-commerce environment.

4.2   Advanced networking for large e-store

In the dynamic landscape of e-commerce, where transactions happen at the speed of a click, the foundation of a large-scale e-store is crucial for ensuring seamless operations, security, and scalability. This thesis delves into the intricacies of advanced networking for a large e-commerce setup, emphasizing the components that play a pivotal role in maintaining a robust digital infrastructure.

As we navigate the expansive landscape of Security Information and Event Management (SIEM), Splunk naturally emerges as the undisputed choice for my thesis. Going beyond the accolades in Gartner and Forrester reports, I embark on a detailed comparison with fellow SIEM tools, including LogRhythm and IBM QRadar. Among these options, Splunk shines brightly, boasting unparalleled versatility, user-friendliness, and scalability. Its user-centric design and adaptability make it my top pick, with a proven track record of adeptly handling diverse data sources and delivering actionable insights. Unlike LogRhythm, Splunk's ecosystem extends seamlessly, integrating with a broader range of technologies. Similarly, when weighed against IBM QRadar, Splunk's agility and flexibility take center stage, making it a

pragmatic choice—especially vital for large enterprises and the dynamic e-commerce sector. In essence, Splunk's exceptional functionality, user experience, and adaptability position it as the quintessential SIEM solution for a robust and practical cybersecurity approach.
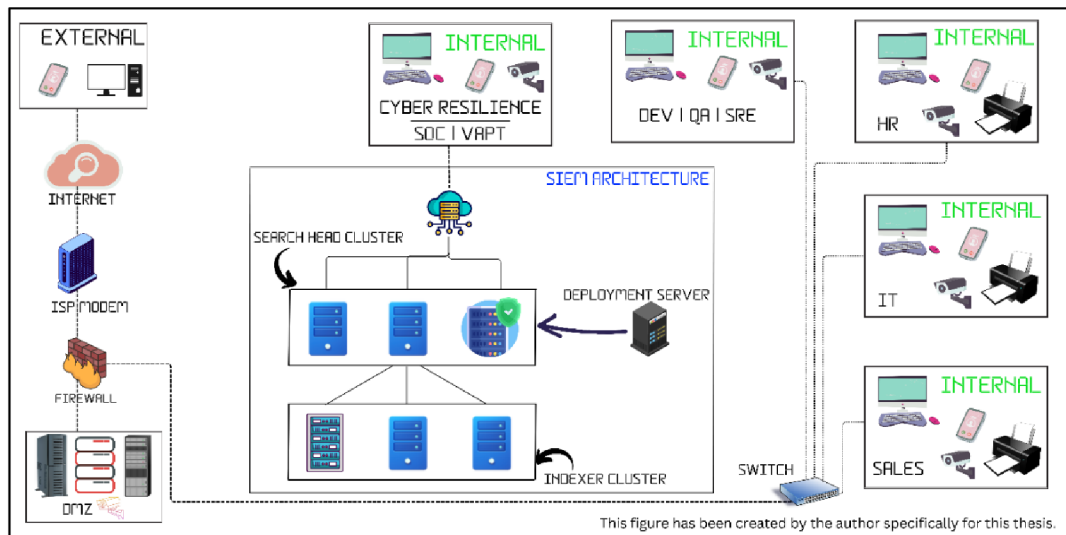

Figure 2: Advanced Networking for large e-store Architecture

[**Source:** This figure has been created by the author specifically for this thesis]

Component	Analogy	Description
Internet	World of Opportunities	The internet serves as the expansive marketplace for e-commerce, connecting customers to the e-store. The connection is facilitated through an Internet Service Provider (ISP) modem, serving as a gateway to the vast online world.
Firewall	Digital Bouncer for Security	Acts as a digital bouncer, safeguarding the e-store's network by scrutinizing incoming and outgoing traffic. Only authorized and secure data is allowed to pass through, ensuring the integrity and confidentiality of sensitive customer information.

41

Component	Analogy	Description
Switch	Wiring the Digital House	Similar to house wiring, a switch connects computers within the network, enabling seamless communication. In a large e-store, an efficient switch is crucial for collaboration between various departments and systems, contributing to a smooth operational flow.
DMZ	Securing External Visibility	The Demilitarized Zone (DMZ) is a special area housing elements that need external visibility, such as the store's website pictures. It ensures accessibility for users while isolating them from the core network, enhancing security by minimizing potential attack vectors.
Load Balancer	Ensuring Smooth Traffic Flow	Functions like a traffic cop, evenly distributing incoming website traffic to prevent server overload. Essential in large e-commerce environments with common traffic fluctuations, a load balancer ensures every user receives prompt service, contributing to optimal performance.
Splunk Search Heads	Detectives of Data	Act as detectives extracting insights from the vast sea of data generated by the e-store. The captain oversees the investigation, while search heads and indexers work together to organize and analyze data, uncovering patterns, and identifying potential issues.
Splunk Deployment Server	Orchestrating the Investigation	Acts as the orchestrator, ensuring cohesion among detectives (search heads) and their assistants (indexers). Dictates tasks, keeps the investigative process streamlined, and plays a central role in maintaining a synchronized and effective data analysis system.

Table 2: Advanced networking for large e-store

[**Source:** This table has been created by the author specifically for this thesis. The Advanced networking for large e-store under the ownership of the author of the thesis.]

By integrating these components into the architecture of a large e-store, the aim is to address potential vulnerabilities and enhance overall system security and scalability. The thesis focuses on identifying and resolving issues that may compromise the confidentiality, integrity, and availability of customer data and the e-commerce platform as a whole.

In conclusion, the advanced networking architecture outlined above is not just about connecting computers and facilitating data flow; it's about fortifying the e-store against cyber threats, ensuring optimal performance, and providing a seamless experience for customers. Through a meticulous examination of each component and their interactions, this thesis aims to contribute to the ongoing effort to make large e-commerce networks more resilient, secure, and adaptable to the ever-evolving digital landscape.

4.2.1 Ensuring network resilience for e-store

In the realm of e-commerce, where transactions occur in the blink of an eye and customer expectations are at an all-time high, the stability and resilience of the network supporting an online store are paramount. The analogy of building a strong and sturdy house aptly captures the essence of fortifying the computer infrastructure of an e-store. This thesis explores strategies and measures to ensure network resilience, focusing on components analogous to backup systems, reliable wiring, emergency plans, regular maintenance, software updates, and employee training.

Component	Analogy	Description
Backup Internet	Redundancy Safeguard	Similar to having a backup generator for power outages, maintaining a backup internet connection ensures network resilience. It acts as a crucial element to seamlessly continue operations in the event of unexpected internet

Component	Analogy	Description
		outages, minimizing downtime and potential revenue loss for the e-store.
Good Wiring	Backbone of Data Flow	Just as a house's robust wiring ensures uninterrupted electricity flow, high-quality network cables in an e-store are essential for smooth and uninterrupted data flow. Investing in reliable and durable network infrastructure mitigates the risk of connectivity issues and disruptions, preserving a positive user experience and supporting business operations effectively.
Emergency Plan	Navigating Through Challenges	Analogous to knowing the location of a fire extinguisher in a house, having a well-defined emergency plan is imperative for navigating through network challenges. This plan serves as a guide for the team, detailing specific steps to be taken in the event of network failure or security breach. A well-prepared and practiced emergency plan enables the e-store to respond promptly to incidents, minimizing the impact on business continuity.
Regular Checks	Proactive Maintenance	Similar to keeping an eye on a house for leaks or broken windows, regular network checks are essential for proactive maintenance. Conducting routine assessments of the network infrastructure allows the identification and resolution of potential issues before they escalate. This proactive approach contributes to the overall stability and resilience of the e-store's network, ensuring continuous and efficient operations.
Up-to-date Software	Fortifying Digital Locks	Analogous to ensuring the locks on a house are functional, keeping computer software up-to-date is crucial for fortifying the digital security of the e-store. Regular software updates include patches and security enhancements that protect against emerging threats.

Component	Analogy	Description
		Updating all software components within the network creates a robust defense against cyber threats, safeguarding sensitive customer data and preserving the integrity of the e-commerce platform.
Training	Empowering the Response Team	Like teaching a family how to call for help in an emergency, educating the e-store team is fundamental for an effective response to network issues. Training employees on how to recognize and address common network problems empowers them to act swiftly and confidently. Fostering a culture of awareness and accountability contributes to a collective effort in maintaining network resilience and responding efficiently to challenges.

Table 3: Ensuring network resilience for e-store

[**Source:** This table has been created by the author specifically for this thesis. The Ensuring network resilience for e-store under the ownership of the author of the thesis.]

In conclusion, the analogy of building a strong house serves as a fitting metaphor for ensuring the resilience of an e-store's network. By implementing measures such as backup internet, reliable wiring, emergency plans, regular checks, up-to-date software, and employee training, the e-store can fortify its digital foundation against potential threats and challenges. This thesis aims to delve into each of these components, exploring best practices, emerging technologies, and innovative strategies to further enhance the e-store's readiness to withstand any obstacles that may arise in the dynamic landscape of e-commerce. In doing so, the objective is to contribute to the ongoing discourse on fortifying network resilience in the ever-evolving digital age.

4.2.2 Efficient network monitoring tools

In the expansive and dynamic world of e-commerce, where the success of a business hinges on the seamless operation and security of its online store, effective network monitoring is paramount. Running a big online store requires vigilant

oversight to ensure that everything is not only working well but also safeguarded against potential threats. This thesis explores a set of essential network monitoring tools, each playing a unique role in the collective effort to keep a big online store safe, efficient, and responsive.

Component	Analogy	Description
Watchdog Software	Guard Dog for Your Website	Similar to a guard dog watching over a property, watchdog software serves as the vigilant protector of a website. Continuously monitors the online store, providing real-time alerts at the first sign of irregularities or potential issues. Ensures prompt addressing of anomalies, contributing to the overall security and stability of the e-commerce platform.
Ping Tool	Sending a Friendly "Hello" to the Website	Comparable to a friendly greeting, a ping tool checks if the website is awake and responsive. Sends a signal and waits for a response. If the site fails to acknowledge the greeting, the ping tool signals a potential issue. Serves as an early indicator of connectivity problems or server responsiveness, enabling quick identification and resolution.
Logs Keeper	The Diary for Your Website	Functions as a diary for the website, meticulously recording every event and interaction. Maintains a detailed log of activities, errors, and system events. Becomes a valuable resource for troubleshooting, allowing administrators to retrospectively analyze events, identify patterns, trends, and potential areas for improvement.
Traffic Light Dashboard	Navigating with Colors	Provides a visual representation of the online store's health and performance. Similar to traffic lights, green signals smooth operation, while red indicates a problem requiring attention. Allows for quick

Component	Analogy	Description
		assessments, enabling administrators to prioritize and address issues based on severity.
Reports Machine	The Website's Storyteller	Acts as a storyteller for the website, generating comprehensive reports that provide insights into overall performance and status. Offers a narrative beyond data points, aiding administrators in understanding the e-commerce platform's health, user behavior, and areas for optimization. Instrumental in making informed decisions and strategic adjustments.
Auto-Fixer	The Problem-Solving Robot	Operates like a problem-solving robot in network monitoring. Detects and attempts to resolve minor issues automatically, sparing administrators from manual intervention. Contributes to the efficiency of network monitoring by addressing routine problems swiftly, allowing the team to focus on more complex issues requiring human expertise.

Table 4: Efficient network monitoring tools

[**Source:** This table has been created by the author specifically for this thesis. The: Efficient network monitoring tools under the ownership of the author of the thesis.]

In conclusion, the effective management of a big online store demands a robust network monitoring strategy, supported by a suite of essential tools. The watchful eye of watchdog software, the friendly greeting of the ping tool, the meticulous documentation of the logs keeper, the intuitive insights from the traffic light dashboard, the informative narratives from the reports machine, and the automated troubleshooting capabilities of the auto-fixer collectively form a formidable team. This thesis aims to explore the significance of each tool, evaluating their strengths, potential synergies, and optimal implementation strategies to enhance the security and efficiency of e-commerce websites.

By identifying the best tools and practices for network monitoring, administrators can proactively address challenges, safeguard customer data, and maintain the optimal performance of their online stores. As the digital landscape continues to evolve, the ongoing refinement of network monitoring tools will play a crucial role in the success and longevity of big online stores in the competitive e-commerce arena.

4.3 Deciphering vulnerabilities

E-commerce websites are large online shops where you can purchase items. Since they handle both your financial transactions and personal information, it's extremely vital to ensure their security (Marchany and Tront, 2002). I accomplish this by examining the website's code and its functionality. It's similar to inspecting the architectural plans of a building to uncover concealed entrances or secret passages. Additionally, we conduct tests to identify potential risks, such as attempting to guess your password or manipulating the website into performing unauthorized actions.

Once these vulnerabilities are identified, we can start considering ways to enhance the website's security. It's akin to repairing the unlocked doors and windows in a house. We can add locks and alarms to deter unauthorized access.

So, in this part of my thesis, I'm gonna study how to find these weak spots in e-commerce websites and come up with ways to make them safer. It's important because we want people to feel safe when they shop online and protect their money and information.

4.3.1 HTTPS protocol

The unequivocal recommendation of the HTTPS protocol in the thesis is grounded in its status as the most widely used and trusted method for securing web communications. Surveys from Netcraft and W3Techs affirm the pervasive use of HTTPS across the internet. Its adoption, not solely based on industry standards, is further reinforced by the largest user base in major enterprises and e-commerce platforms, ensuring a secure foundation for web communication.

HTTPS (Hypertext Transfer Protocol Secure) acts as a special shield for websites, particularly crucial in the context of online shopping, as it ensures the safety of customers' sensitive information, including credit card numbers (Callegati, Cerroni, and Ramilli, 2009). The significance lies in the added layer of security HTTPS provides compared to its less secure counterpart, HTTP (Hypertext Transfer Protocol).

In the analogy of online security, HTTP is akin to sending a postcard in the mail information transmitted through it is susceptible to interception and can be read by anyone with the intent to do so. Using HTTP for an online store is comparable to having an insufficient lock on the door, leaving customer data vulnerable to potential threats.

On the other hand, HTTPS employs encryption mechanisms to safeguard data during transmission, ensuring that it remains confidential and secure. This security protocol is analogous to a robust shield, protecting the integrity of online transactions and instilling confidence in customers who entrust their sensitive information to the e-commerce platform.
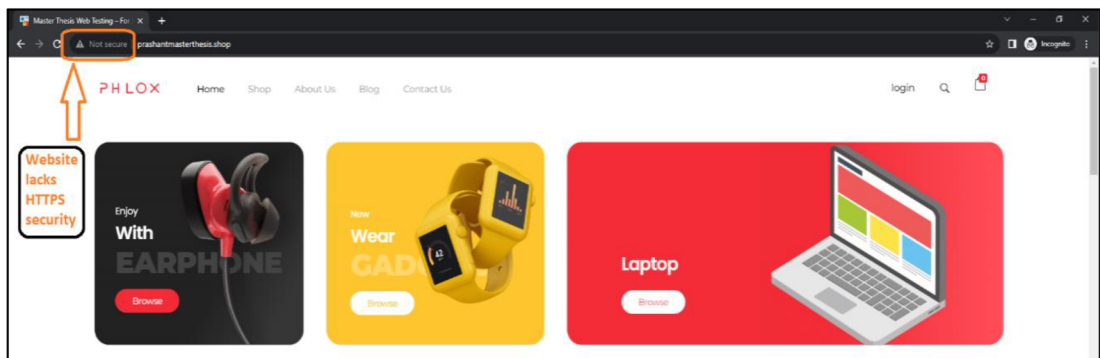
Figure 2: HTTPS protocol Example

[**Source:** This figure has been created by the author specifically for this thesis. The DNS and IP address of the website are registered under the ownership of the author of the thesis.]

Let's breakdown the importace of HTTPS:

Component	Key Advantage	Description
Privacy	HTTPS as a Secret Code	Functions like a secret code understood only by the buyer and the online store. Encrypts sensitive information, ensuring personal details and credit card numbers remain hidden. Establishes a secure communication channel, prioritizing customer privacy in a digitally crucial environment.
Security	HTTPS as a Digital Guard	Acts as a digital guard to prevent malicious actors from stealing information. Provides encryption against cyber threats, ensuring the integrity of transmitted data. Analogous to a vigilant guard checking everyone entering the online store, creating a robust defense against potential breaches.
Trust	HTTPS as an Assurance of Safety	Inspires greater trust among customers, signaling that their information is safe. Comparable to shopping in a physically secure store, visible security measures reassure customers of the business's commitment to prioritizing safety and proactively protecting their data.

Table 5: HTTPS protocol

[**Source:** This table has been created by the author specifically for this thesis. The HTTPS protocol under the ownership of the author of the thesis.]

Conclusion:

In the context of an e-commerce website, implementing HTTPS is akin to putting a strong lock on the door of an online shop. This security measure not only safeguards customer data but also contributes to creating a safe and confident online shopping experience. When customers feel secure, they are more likely to trust the website, make purchases, and become repeat customers. For businesses, the adoption of HTTPS is not just a technical necessity but a strategic move to build a positive online

reputation, enhance customer satisfaction, and ensure the long-term success of the e-commerce venture. In the digital era, where cyber threats are prevalent, HTTPS serves as a crucial tool in fortifying the online shopping ecosystem and fostering a secure and trustworthy environment for both buyers and sellers.

4.3.2 Anti CSRF tokens

An Anti-CSRF token is like a magical shield in the world of online shopping. It's a unique and secret token that only the website can understand. This magical token serves as a powerful defense mechanism, protecting customers from sneaky tricks and malicious activities when they engage in transactions on the website. By requiring users to present this special token, the website ensures that only legitimate customers can perform important actions, creating a secure and trustworthy online shopping experience.
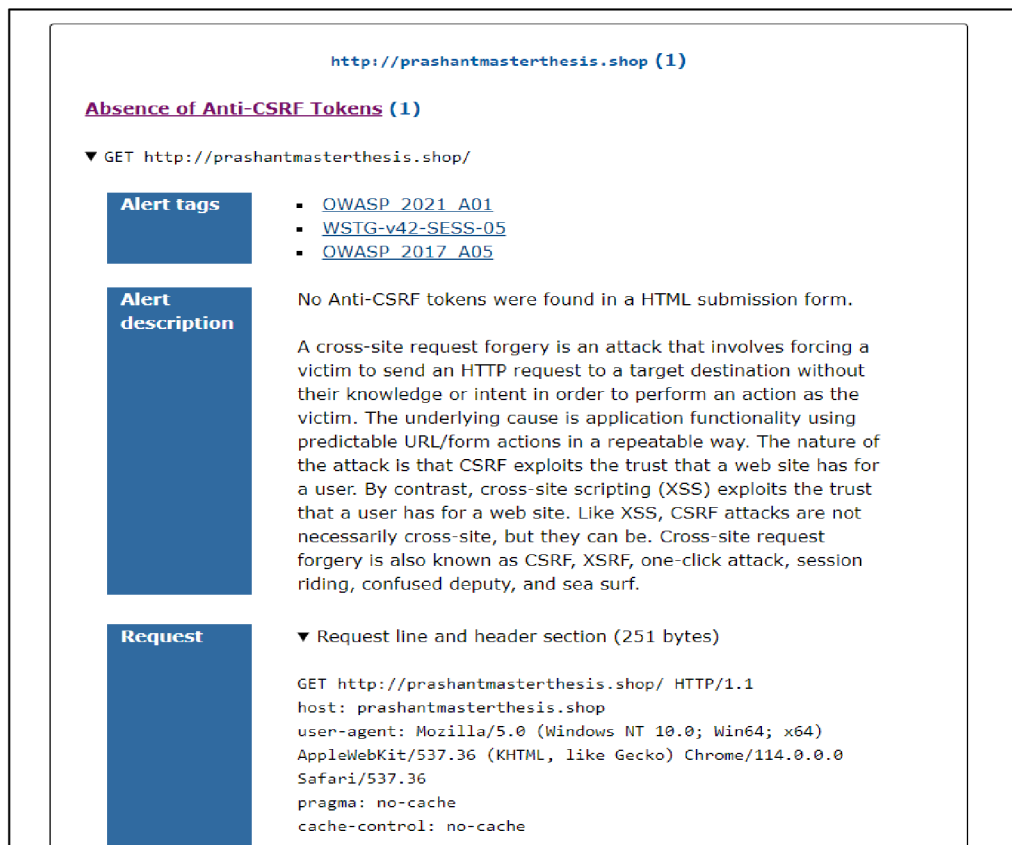
Component	Analogy	Description
Tokens for Safety	Unique Keys for Actions	Website issues unique tokens for significant actions, like purchases or account modifications. Tokens act as unique keys, granting access to specific actions, ensuring only authorized users can initiate important activities.
Token Exchange	Token as Proof of Legitimacy	Customer's present associated tokens for significant actions, similar to a secret handshake. Tokens serve as proof of legitimacy, and if absent, the website won't execute the requested action. This process prevents unauthorized access.
Stop Sneaky Tricks	Anti-CSRF Token as a Vigilant Guard	The Anti-CSRF token acts as a vigilant guard, verifying the authenticity of customer requests. It serves as a barrier against tricks by robots or hackers, ensuring only genuine customers, validated through tokens, can interact with the platform.

Table 6: Anti CSRF tokens

Conclusion

In essence, the utilization of Anti-CSRF Tokens serves as a sophisticated security measure, granting customers a secure online shopping experience. This system is comparable to providing users with a secret key to open the door to a safe and protected digital environment. It not only safeguards the integrity of customer transactions but also fortifies the overall security posture of the e-commerce web application, instilling confidence in users and reinforcing the trustworthiness of the online platform. As online threats continue to evolve, the integration of Anti-CSRF Tokens stands as a critical component in the ongoing effort to create resilient and secure e-commerce ecosystems.

Figure 3: Anti-CSRF Token Example

4.3.3 Authentication request identified

In the intricate world of e-commerce, the process of authentication acts as a virtual gatekeeper, ensuring the security of crucial transactions and safeguarding sensitive customer information. This security measure parallels real-world scenarios where confirming one's identity is a standard practice, such as when a cashier requests identification or a signature at a physical store.

By implementing this authentication mechanism, the website establishes a robust defense against unauthorized access and potential security breaches. Only genuine customers, who successfully confirm their identity, are granted access to perform important actions on the e-commerce site.
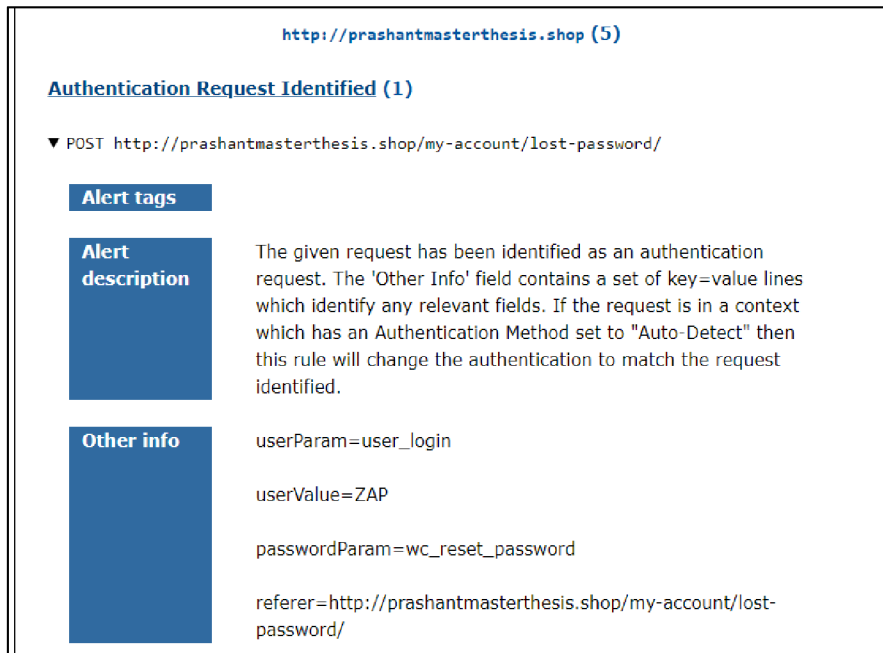

Figure 4: Authentication Vulnerability Example

[**Source:** This figure has been created by the author specifically for this thesis. The DNS and IP address of the website are registered under the ownership of the author of the thesis.]

Component	Key Aspect	Description
Authentication Request	Critical User Action	Occurs when a user initiates a significant action, like making a purchase or updating account information. Similar to approaching a cashier in a physical store,

Component	Key Aspect	Description
		signaling the beginning of a critical interaction on the online store.
Identified	Verification of User's Identity	Following the authentication request, the website diligently checks and verifies the user's identity. This step ensures the authentic customer initiates the request, preventing impostors. Analogous to a cashier confirming a customer's identity through ID or a signature, this verification process is crucial for the security infrastructure.
Trusted Bouncer at the Door	Digital Gatekeeper	Analogous to having a trusted bouncer at the entrance of a physical venue, the authentication process serves as a digital gatekeeper. Its role is to ensure only authorized customers gain entry to sensitive areas of the online store, effectively keeping out unauthorized individuals and maintaining the security and integrity of the shopping environment.
Securing Customer Information	Rigorous Identity Confirmation	By rigorously confirming user identity, the website significantly contributes to keeping customer information safe. This security measure prevents unauthorized access to personal and financial details, fostering a secure and trustworthy online shopping experience. The authentication process acts as a vigilant gatekeeper, ensuring only legitimate customers can undertake important actions, collectively contributing to overall store security.

Table 7: Authentication request identified

[**Source:** This table has been created by the author specifically for this thesis. The Authentication request identified under the ownership of the author of the thesis.]

In essence, the authentication process in the e-commerce web application is akin to having a vigilant gatekeeper at the entrance, ensuring that only legitimate customers can undertake important actions. This meticulous verification not only protects individual users but collectively contributes to the overall security and integrity of the online store, cultivating a safe and reliable environment for customers to engage in their e-commerce activities.

4.3.4 Cookie poisoning

In the digital landscape of e-commerce, cookies play a fundamental role as tiny data files stored on a customer's computer by a website. These digital notes are essential for remembering various user preferences and actions, such as items added to a shopping cart, thereby enhancing the overall user experience (Cahn et al., 2016). However, like any digital element, cookies are susceptible to manipulation, and when bad actors attempt to interfere with these notes, it is referred to as "Cookie Poisoning."

Figure 5: Cookie Poisoning Example

[**Source:** This figure has been created by the author specifically for this thesis. The DNS and IP address of the website are registered under the ownership of the author of the thesis.]

55

Component	Key Aspect	Description
Cookies	Digital Reminders	Similar to little reminders, cookies store information about user interactions on a website, including shopping cart contents and personalized preferences. Enhances the browsing experience with seamless navigation and tailored recommendations.
Poisoning	Cookie Tampering	Cookie Poisoning occurs when malicious individuals tamper with or alter cookie content. Comparable to someone adding fake items to a customer's shopping cart without consent, this act may lead to distorted data, unauthorized access, or other security concerns.
Impact of Cookie Poisoning	Significant Consequences	Successful Cookie Poisoning can lead to unexpected website behavior, showing incorrect items in the shopping cart, or enabling unauthorized access. The manipulation compromises user interactions, erodes trust, and may result in financial or reputational damage.
Protecting Against Cookie Poisoning	Security Measures	To mitigate Cookie Poisoning risks, developers use encryption, data integrity validation, and secure coding practices. Regular security protocol updates fortify defenses against evolving threats, ensuring resilience against potential vulnerabilities related to cookies.

Table 8: Cookie poisoning

[**Source:** This table has been created by the author specifically for this thesis. The Cookie poisoning under the ownership of the author of the thesis.]
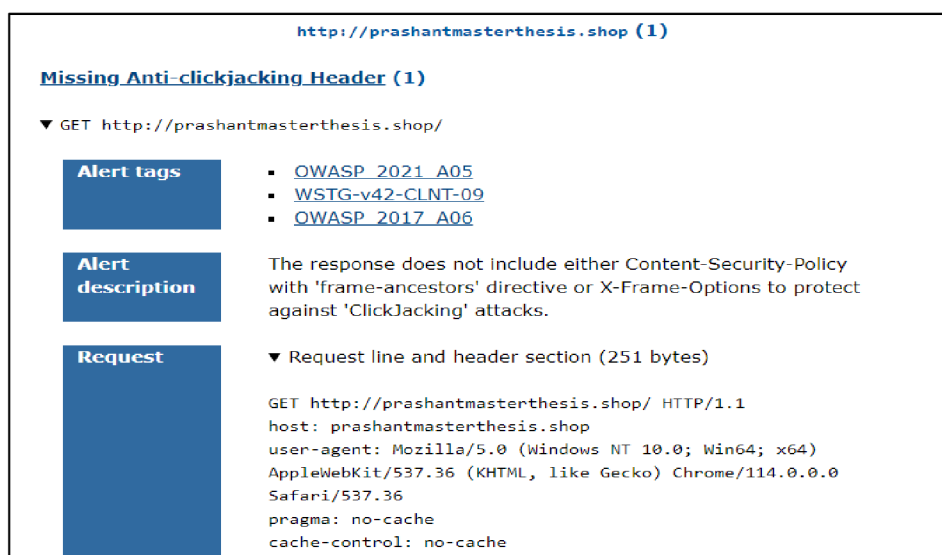
Conclusion

In conclusion, while cookies enhance the user experience in e-commerce by remembering important details, the risk of Cookie Poisoning underscores the need for robust security measures. By understanding and addressing these risks, website

operators can protect against unauthorized manipulations, maintain the integrity of user data, and provide a safe and reliable online shopping environment for customers. Ongoing vigilance, proactive security measures, and user education collectively contribute to a resilient defense against potential cookie-related threats.

4.3.5 Missing anti-clicking header

The absence of an "Anti-clicking Header" on a website can lead to potential abuse where a malicious individual or a computer program repeatedly clicks a "Buy Now" button. In the absence of this protective measure, a single click could result in the purchase of multiple items, exploiting the vulnerability for financial gain or disruption. This unchecked and automated clicking, known as click fraud, can lead to unintended consequences such as inventory issues, financial losses, and a compromised user experience. The implementation of an "Anti-clicking Header" is crucial to prevent such abuses, ensuring that each click corresponds to a legitimate and intentional action, thereby safeguarding the integrity of online transactions and preserving the fairness of the purchasing process.

Figure 6: Anti-Clickjacking Example

[**Source:** This figure has been created by the author specifically for this thesis. The DNS and IP address of the website are registered under the ownership of the author of the thesis.]

Component	Key Aspect	Description
Anti-clicking Header	Click Control Rule	The "Anti-clicking Header" is a rule preventing multiple clicks on the "Buy Now" button for each item. It safeguards against exploitation by individuals or automated programs, preventing unintended consequences such as click fraud.
Missing Rule Consequences	Click Fraud Impact	Without the rule, malicious actors or programs can exploit vulnerabilities, leading to excessive purchases through continuous clicking. Click fraud consequences include quickly selling out of items, inventory issues, and customers being charged for unintended purchases.
Impact on Inventory and Customer Experience	Inventory Depletion Risks	The absence of the "Anti-clicking Header" can adversely affect inventory management and customer satisfaction. Excessive and unintended purchases may deplete stock rapidly, causing unfulfilled orders, disappointing customers, and potential financial losses for both customers and the e-commerce business.
Maintaining Fairness and Security	Online Store Vigilant Bouncer	Implementing the "Anti-clicking Header" is akin to having a vigilant bouncer at the entrance of an online store. It ensures compliance with rules, preventing unfair or disruptive practices. This protective measure safeguards the fairness of the purchasing process, preventing exploitation of vulnerabilities for personal gain or disruption.
Benefits of the "Anti-clicking Header"	Secure and Equitable Environment	The "Anti-clicking Header" creates a secure and equitable environment for all customers. It prevents abuses like click fraud, contributing to a positive customer experience by ensuring transparency,

Component	Key Aspect	Description
		control, and freedom from manipulation in the purchasing process.

Table 9: Missing anti-clicking header

[**Source:** This table has been created by the author specifically for this thesis. The Missing anti-clicking header under the ownership of the author of the thesis.]

Conclusion

In conclusion, the "Anti-clicking Header" is a crucial component in maintaining the integrity of online transactions. By preventing abuses and ensuring fair and secure interactions, this rule serves as a digital bouncer, safeguarding the interests of both customers and the e-commerce business. Its implementation is fundamental to fostering trust, preventing inventory issues, and upholding the principles of fairness and security in the online shopping ecosystem.

4.3.6 SQL Injection

In the digital realm of e-commerce, the website's database is akin to a treasure chest, containing valuable information about products and customers. However, this treasure trove is not immune to nefarious attempts by bad actors who seek to exploit vulnerabilities and trick the website into divulging sensitive data. One such method employed by these malicious individuals is known as SQL Injection.

Component	Key Aspect	Description
SQL	Database Language	SQL (Structured Query Language) is the language understood by the website's database. It is used for retrieving, managing, and interacting with data stored in the database.
Injection	SQL Injection	SQL Injection involves maliciously inserting SQL commands into a website's input fields. This act is

Component	Key Aspect	Description
		analogous to inserting a secret code into a conversation, intending to exploit vulnerabilities in the system.
OR Operator	Tactic in SQL Injection	A common tactic in SQL Injection uses the equals sign (=) or the OR operator. For example, inputting "1=1" or "OR 1=1" into a login field can trick the website, potentially granting unauthorized access.
Security Risk	Risks of SQL Injection	SQL Injection poses a significant security risk by providing malicious actors access to unauthorized parts of the website. This includes sensitive information like customer data or administrative controls, compromising the integrity and confidentiality of the e-commerce platform.

Table 10: SQL Injection

[**Source:** This table has been created by the author specifically for this thesis. The SQL Injection under the ownership of the author of the thesis.]
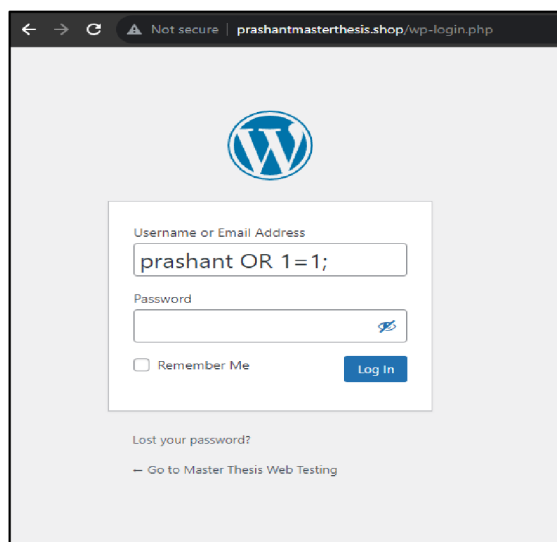
Figure 8: SQL Injection Example

[**Source:** This figure has been created by the author specifically for this thesis. The DNS and IP address of the website are registered under the ownership of the author of the thesis.]

60

Component	Key Aspect	Description
Parameterized Statements	Secure SQL Queries	Utilize parameterized statements in SQL queries to treat user input as data, preventing it from being executed as code. This helps thwart malicious injections by separating data from SQL code.
Input Validation	Rigorous Scrutiny of User Inputs	Implement thorough input validation to examine and filter user inputs. This includes validating length, type, and format to ensure adherence to expected parameters, reducing the risk of malicious inputs.
Escaping User Input	Proper Character Encoding	Use proper escaping mechanisms to neutralize potentially harmful characters in user input. This involves encoding special characters to prevent them from being interpreted as part of the SQL code.
Least Privilege Principle	Minimum Access Levels	Apply the principle of least privilege, granting users and processes the minimum access required. This limits potential damage, even if an SQL Injection attempt is partially successful.
Regular Security Audits	Ongoing Vulnerability Identification	Conduct regular security audits and penetration testing to identify and address potential vulnerabilities in the website's code and database structure. This proactive approach helps enhance overall security.

Table 11: Mitigating SQL Injection:

[**Source:** This table has been created by the author specifically for this thesis. The Mitigating SQL Injection under the ownership of the author of the thesis.]

Conclusion:

In conclusion, preventing SQL Injection is paramount to maintaining the security and integrity of an e-commerce website. By implementing robust security practices, such as parameterized statements, input validation, and regular security audits, the website fortifies its defenses against unauthorized access and data breaches.

The metaphorical smart guard at the treasure chest becomes a critical component in preserving the confidentiality of customer information and securing the overall functionality of the e-commerce platform.

4.4 SIEM: Simplified security management

In the vast and dynamic landscape of online commerce, the Security Information and Event Management (SIEM) system stands as a formidable guardian, akin to a super detective that meticulously watches over an online store. As elucidated by (González-Granadillo, González-Zarzosa, and Diaz) in 2021, SIEM plays a pivotal role in proactively identifying and mitigating potential security threats, functioning as a vigilant security watcher for e-commerce platforms.

Component	Key Aspect	Description
Security Watcher	Vigilant Surveillance	SIEM functions as an astute guard, overseeing all online store activities. It monitors logins, user actions, and detects unusual activities, acting as the eyes and ears of the e-commerce platform for continuous security assessment.
Event Collector	Data Gathering	The SIEM system acts as an event collector, gathering information from various website areas like checkout processes and customer accounts. This comprehensive data collection provides a holistic view for a thorough analysis of potential security incidents.
Analysis	Sophisticated Pattern Recognition	SIEM possesses analytical capabilities to discern patterns, anomalies, and deviations. It identifies potential security threats such as repeated unsuccessful login attempts or unusual traffic surges, enabling proactive intervention before escalation.

Component	Key Aspect	Description
Alerts	Proactive Warning Mechanism	SIEM sends alerts when it identifies suspicious activities, serving as a timely notification system. Similar to a silent alarm in a physical store, these alerts enable swift responses from security teams to potential threats, contributing to a proactive defense mechanism.
Application in E-commerce	Valuable in Large Enterprises	SIEM is particularly valuable in large enterprise e-commerce projects where diverse departments collaborate closely. It facilitates seamless web application functioning, involving logistics, software development, QA automation, site reliability, and IT support teams.
Mitigating Threats	Addressing MITRE and OWASP Threats	SIEM is critical in mitigating threats outlined by MITRE ATT&CK and OWASP Top 10. It aids in detecting and addressing attacks on web and database servers, including common servers like Apache, Tomcat, MongoDB, and SQL, fortifying overall security.

Table 12: SIEM: Simplified security management

[**Source:** This table has been created by the author specifically for this thesis. The SIEM: Simplified security management under the ownership of the author of the thesis.]

Conclusion

In conclusion, the role of SIEM in e-commerce security is akin to deploying a super detective to safeguard the digital assets of an online store. Its multifaceted capabilities, including vigilant surveillance, event collection, sophisticated analysis, and timely alerts, collectively contribute to creating a resilient defense against potential security threats. In the ever-evolving landscape of online commerce, SIEM remains an

indispensable ally, empowering security teams to proactively protect e-commerce platforms and maintain the trust of both businesses and customers alike.
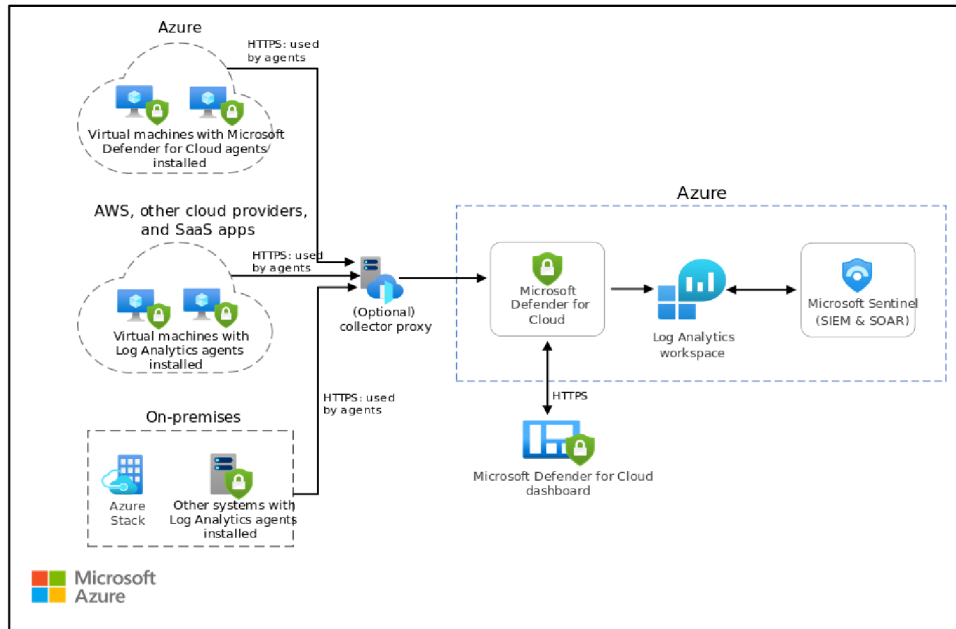

Figure 7: Microsoft Hybrid Security Structure

[**Source:** https://learn.microsoft.com/en-us/azure/architecture/hybrid/hybrid-security-monitoring]

4.4.1 Recommended SIEM tools with justification

Splunk and LogRhythm stand out as highly recommended Security Information and Event Management (SIEM) tools, each offering unique strengths that contribute to robust e-commerce security.

Splunk: Splunk acts as a detective with a magnifying glass, excelling in data analysis and threat detection. Its powerful search and reporting capabilities make it an invaluable asset for e-commerce security. Splunk's ability to efficiently process and analyze vast amounts of data allows it to uncover hidden threats and vulnerabilities. Its versatility and user-friendly interface make it well-suited for handling the complexities of e-commerce environments.

LogRhythm: LogRhythm functions like an extra pair of tireless eyes, specializing in real-time monitoring and alerting. In the fast-paced world of e-commerce, where events unfold rapidly, LogRhythm's capability to provide instantaneous alerts is crucial. It ensures that security teams are promptly notified of any unusual activities, enabling swift responses to potential threats. LogRhythm's emphasis on real-time monitoring aligns well with the need for constant vigilance in securing e-commerce websites.

By employing SIEM tools like Splunk and LogRhythm, it's akin to having a dedicated team of detectives safeguarding the online store 24/7. These tools contribute to the proactive identification and mitigation of security threats, helping to ensure the safety and integrity of the e-commerce platform. Their combined capabilities provide a comprehensive security solution, addressing the dynamic challenges posed by potential bad actors seeking to disrupt or compromise the online shopping experience.

Figure 8: E-Store Web App Logs in Splunk

[**Source:** This figure has been created by the author specifically for this thesis. The IP address of the webpage are registered under the ownership of the author of the thesis.]

4.4.2 Real-Time threat detection for E-Commerce application

In the ever-evolving landscape of e-commerce, the significance of real-time threat detection cannot be overstated. Security Information and Event Management (SIEM) systems, particularly when integrated with powerful tools like Splunk, play a

65

pivotal role in fortifying the security posture of an e-commerce application. This comprehensive overview delves into the functionalities of SIEM with Splunk, highlighting its role as a security helper, the utilization of Splunk forwarder, the alert system, event types, and the management of roles for effective real-time threat detection.

Splunk Forwarder: Splunk Forwarder plays a crucial role in the real-time threat detection process by serving as a data mover. It facilitates the transportation of data from different segments of the e-commerce site to Splunk for in-depth examination. Acting as a secure carrier, Splunk Forwarder ensures that the data travels safely to its destination, analogous to a trusted courier delivering valuable information. This mechanism is integral to the efficient functioning of the SIEM system, enabling the continuous flow of data for real-time analysis.
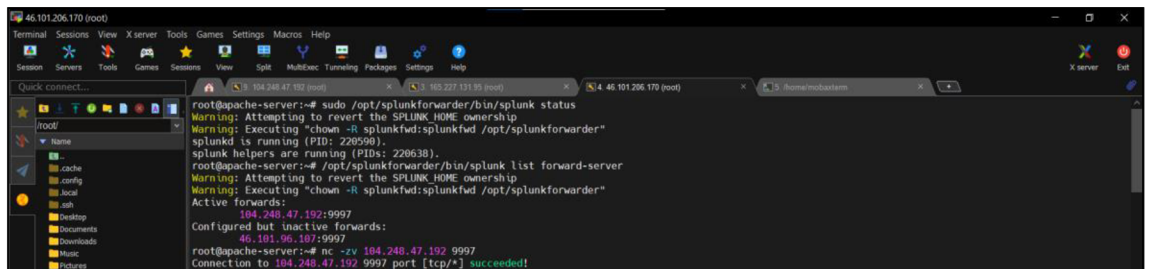

Figure 9: Splunk Universal Forwarder Configuration

[**Source:** This figure has been created by the author specifically for this thesis. The IP address of the webpage are registered under the ownership of the author of the thesis.]

Splunk alert: The Splunk Alert system functions as an integral part of the real-time threat detection mechanism. Similar to an alarm in a physical store, Splunk Alert sends out warnings whenever it identifies something unusual or potentially harmful. These alerts serve as notifications to the website owner, providing timely information about potential security incidents. The alerts act as a notification sender, conveying messages that prompt swift action to mitigate threats and safeguard the e-commerce platform.
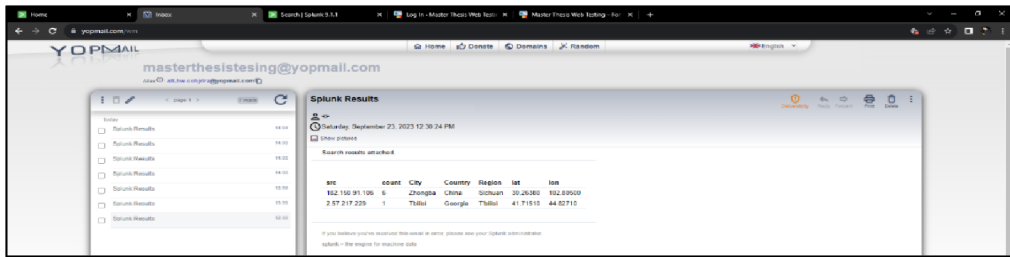
Figure 10: Splunk Incident Alerts on E-Mail Example

[**Source:** This screenshot has been captured by the author specifically for this thesis.]
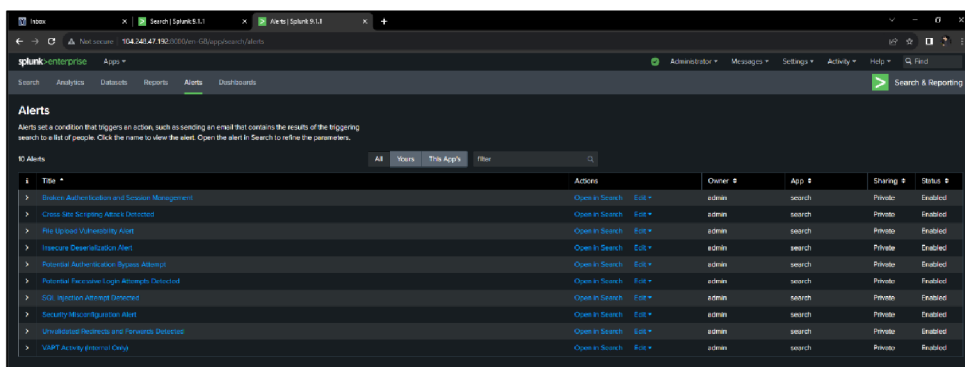

Figure 11: Splunk Alert Use Case

[**Source:** This figure has been created by the author specifically for this thesis. The IP address of the webpage are registered under the ownership of the author of the thesis.]

Splunk event types: Splunk Event Types are instrumental in organizing and categorizing various activities that occur on the e-commerce website. These event groups help in structuring and labeling different types of activities for easier analysis. Custom event types can be created to track specific actions, such as customer logins, product purchases, or order updates. This customization is akin to giving names to different types of customer actions, enhancing the granularity of threat detection.

Splunk Event Types also serve as a search helper, making it easier for website owners to sift through and analyze the vast amount of data generated by the e-commerce platform. By categorizing events into different groups, it becomes analogous to sorting items into different boxes, facilitating quicker and more efficient searches.
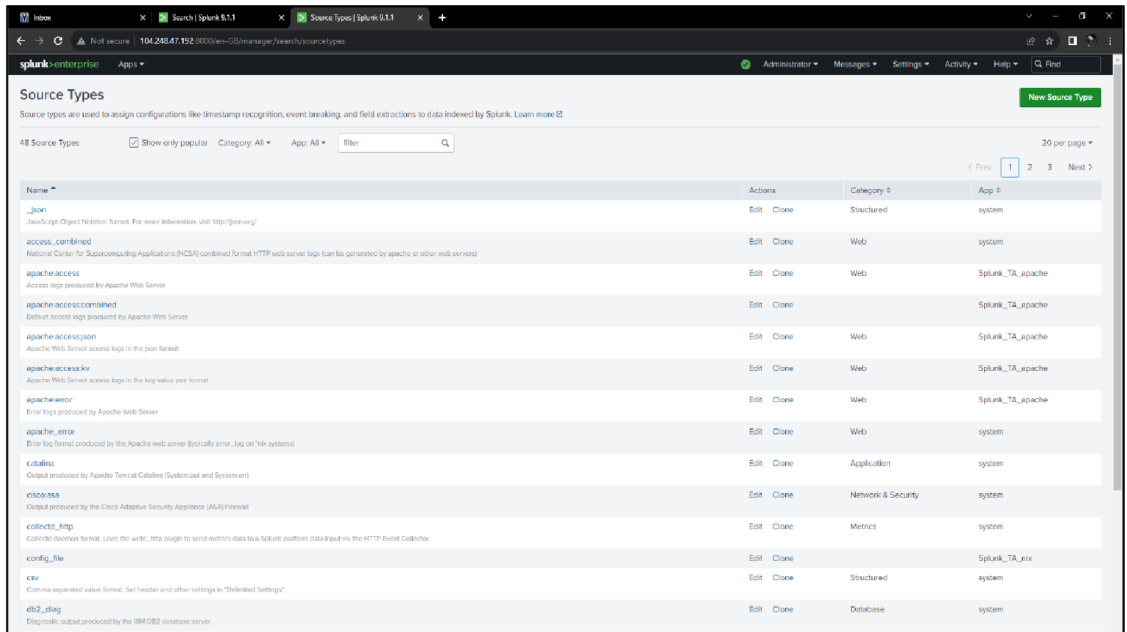
67

Figure 12: Splunk Source Types on Cloud Instance

[**Source:** This figure has been created by the author specifically for this thesis. The IP address of the webpage are registered under the ownership of the author of the thesis.]

Custom labels: I can create custom event types to track specific actions, like customer logins, product purchases, or order updates. It's like giving names to different types of customer actions.

Search helper: These event types make it easier for me to search and analyze what's happening on e-commerce site. It's like sorting items into different boxes to find them quickly.
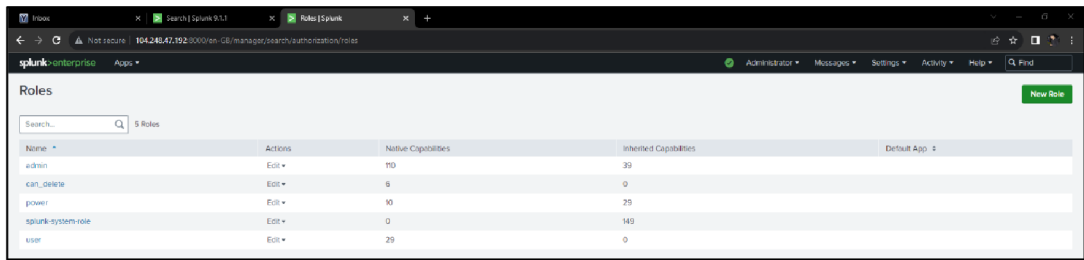
Splunk roles: Splunk Roles play a pivotal role in user responsibilities within the SIEM system. Assigning roles is akin to delineating specific responsibilities for different users on the website. For example, Admins may be responsible for managing the Splunk system, while Analysts review security data. This role assignment is comparable to having different employees with distinct roles and responsibilities within a physical store.

Component	Key Aspect	Description
Splunk Forwarder	Data Mover for Threat Detection	Splunk Forwarder plays a vital role in real-time threat detection by transporting data from various e-commerce site segments to Splunk for in-depth analysis. It ensures secure data transportation, acting as a trusted courier delivering valuable information, crucial for the continuous flow of data in the SIEM system.
Splunk Alert	Real-time Warning System	The Splunk Alert system functions as an integral part of real-time threat detection, sending warnings similar to alarms in a physical store. These alerts notify the website owner promptly about potential security incidents, prompting swift action to mitigate threats and safeguard the e-commerce platform.
Splunk Event Types	Organizing and Categorizing Activities	Splunk Event Types are instrumental in organizing and categorizing various e-commerce website activities. Custom event types can be created to track specific actions, enhancing threat detection granularity. They serve as a search helper, facilitating easier data analysis by categorizing events into different groups, similar to sorting items into boxes.
Splunk Roles	User Responsibilities and Access Management	Splunk Roles play a pivotal role in delineating user responsibilities within the SIEM system. Assigning roles, such as Admins for managing Splunk and Analysts for reviewing security data, is comparable to defining distinct roles and responsibilities for different users, ensuring effective access management within the digital environment.

Table 13: Real-Time threat detection for E-Commerce application
[**Source:** This table has been created by the author specifically for this thesis. The Real-Time threat detection for E-Commerce application under the ownership of the author of the thesis.]

Access control is a crucial aspect of Splunk Roles, governing who can see and do what within the Splunk system. For instance, certain settings may only be accessible to Admins, ensuring that critical configurations remain in the hands of trusted personnel. This access control mechanism is analogous to providing store keys only to employees with specific roles and responsibilities.

Figure 13: Splunk Roles and Capabilities
[**Source:** This figure has been created by the author specifically for this thesis. The IP address of the webpage are registered under the ownership of the author of the thesis.]

Admins and analysts: I can assign roles like Admins, who manage the Splunk system, and Analysts, who review security data. It's like having different employees with different roles in a store.

Access control: Roles also control who can see and do what in Splunk. For example, I can make sure only Admins have access to certain settings. It's like giving store keys to trusted employees.

Conclusion

In conclusion, the integration of SIEM with Splunk in an e-commerce environment serves as a multi-faceted solution for real-time threat detection. From acting as a security assistant and data collector to serving as a search helper and access control manager, SIEM with Splunk plays a critical role in fortifying the security

70

posture of an online store. The watchful eyes of Splunk, in collaboration with the comprehensive roles and access control mechanisms, contribute to a secure and vigilant environment. By continuously collecting, analyzing, and alerting on potential security threats, SIEM with Splunk ensures that the online store remains resilient against the ever-present challenges posed by cyber threats, safeguarding both the integrity of the platform and the trust of its customers.

4.5 Delving into E-Commerce code for safety checks

An SAST tool for my e-commerce website is like a friendly code checker. It checks the website's code for mistakes and security problems, similar to how a store checks products for defects. It's a user-friendly tool that enhances my online store's security by identifying and repairing code issues, ensuring a safer shopping experience for my customers.

Code checker: An SAST tool is like a code checker for my e-commerce website. It reads through the website's code to find mistakes and security problems, just like checking a recipe for errors.

Automatic detective: It works like an automatic detective, scanning every part of the code to spot issues. It's like having a robot inspector that goes through the store looking for hidden problems.

Easy to use: These tools are simple to use, even if you're not a coding expert. It's like using a tool that's designed for everyday people, not just experts.

Security boost: By using an SAST tool, I can make my website more secure for my customers. It's like adding extra locks and alarms to keep a store safe.

4.5.1 Training teams in code security

In the realm of e-commerce, where the digital landscape is the storefront and the code is the foundation, ensuring the safety and security of the online store is paramount. This involves employing Static Application Security Testing (SAST) tools and providing comprehensive training to e-commerce teams in code security. This dual

approach, likened to a friendly code checker and a team of dedicated guards, fortifies the online store against potential threats and ensures a safer shopping experience for customers.

In delving into Static Application Security Testing (SAST), my thesis adopts a neutral stance, avoiding favoritism towards any specific tool. I present various tools, as highlighted in surveys from reputable sources like OWASP and SANS, focusing on their unique features and use cases. This approach ensures a comprehensive overview, facilitating informed decision-making based on project requirements. Notably, the thesis accentuates the diverse landscape of SAST tools, recognizing that certain tools may gain more prevalence in specific sectors or industries.

SAST Tool for E-Commerce Website:

Code Checker: An SAST tool serves as a friendly code checker for the e-commerce website. Just as a store checks products for defects before putting them on shelves, the SAST tool reads through the website's code to identify mistakes and security problems. This process is akin to scrutinizing a recipe for errors before preparing a dish. The SAST tool acts as a vigilant inspector, ensuring the code meets the required standards for security and functionality.
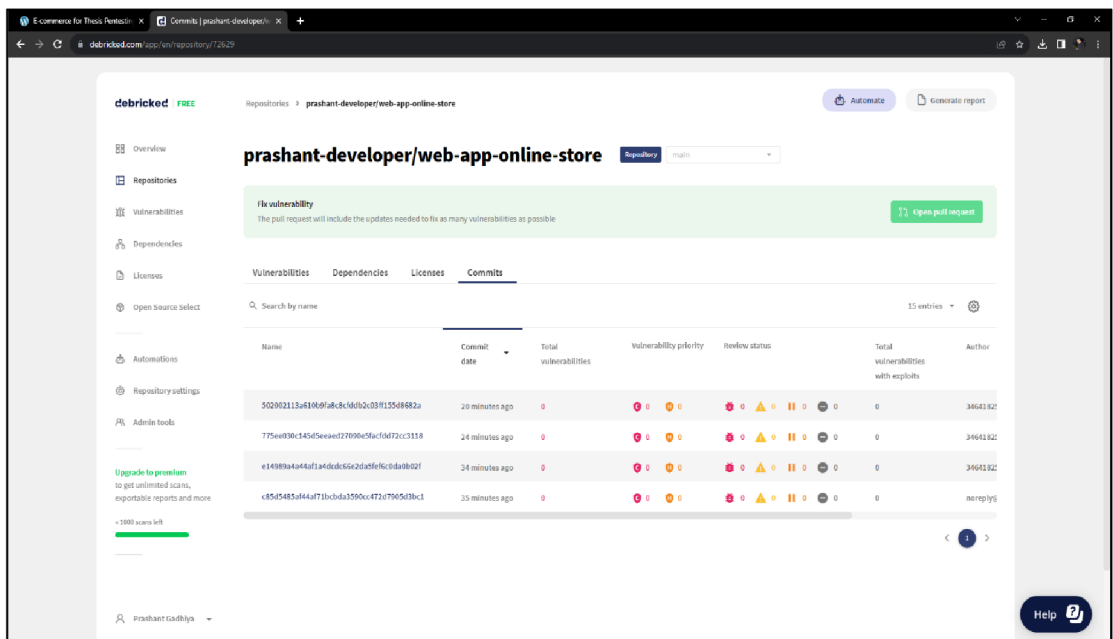

Figure 16: SAST Tool Performance on E-Store

72

Automatic Detective: The AST tool functions as an automatic detective, scanning every part of the code to spot issues. It operates like a robot inspector navigating through the store, diligently looking for hidden problems or vulnerabilities. This automated scrutiny is essential in detecting potential security threats within the codebase, offering a proactive approach to identifying and mitigating risks.

Easy to Use: One of the notable advantages of SAST tools is their user-friendly nature. Even for individuals who may not be coding experts, these tools are designed for simplicity. It's like using a tool that's accessible to everyday people, emphasizing ease of use over technical complexity. This characteristic ensures that security measures are accessible and implementable by a broader range of individuals within the e-commerce team.

Security Boost: By employing an SAST tool, the e-commerce website experiences a significant security boost. This is comparable to adding extra locks and alarms to a physical store to enhance its safety measures. The SAST tool identifies vulnerabilities, potential exploits, and coding errors, allowing developers to address these issues promptly. This proactive approach contributes to building a robust security framework for the online store, instilling confidence in both the business and its customers.

Training Teams in Code Security

Code Safety School: Training teams in code security is likened to establishing a code safety school. This educational initiative serves as a learning platform where teams acquire knowledge and skills to keep the website's code safe. Similar to students learning essential lessons, e-commerce teams gain insights into best practices, secure coding principles, and strategies for mitigating potential security risks.

Guarding the Store: The training equips teams to act as guards for the e-commerce store, with their knowledge serving as the armor and shields against online threats. Instead of uniforms and physical weapons, they utilize their understanding of code security to protect the integrity and safety of the online store. This guarding role extends beyond traditional physical security measures, acknowledging the digital landscape's unique challenges.

Detecting Dangers: The training focuses on empowering teams to detect dangers in the code. This involves the ability to identify hidden problems, weaknesses, and potential vulnerabilities. The analogy here is akin to teaching them how to find hidden treasures in a game – a rewarding process that requires skill, attention to detail, and a thorough understanding of the digital terrain.

Keeping Shoppers Safe: By imparting code security training to e-commerce teams, the overarching goal is to ensure the online store is a safe place for shoppers. This parallels the importance of having robust security measures in a physical store to protect customers. The teams become the guardians of the e-commerce website, actively contributing to its safety and security, and creating an environment where customers can shop with confidence.

Conclusion: In conclusion, the dual strategy of employing SAST tools and providing comprehensive code security training for e-commerce teams creates a formidable defense against potential threats. The SAST tool functions as a friendly code checker and an automatic detective, contributing to the identification and mitigation of security vulnerabilities. Simultaneously, training teams in code security establishes them as the guardians of the online store, equipped with the knowledge and skills needed to maintain a secure digital environment.

This comprehensive approach not only enhances the security posture of the e-commerce website but also instills a culture of vigilance and responsibility within the development teams. It recognizes that safeguarding an online store requires a combination of automated tools and human expertise. By fostering a code safety school, empowering teams to guard the store, and enabling them to detect and address

dangers in the code, the e-commerce platform can provide a safe and secure shopping experience for customers. This proactive and holistic strategy is essential in the dynamic and ever-evolving landscape of digital commerce, where code integrity is fundamental to building and maintaining trust with the online audience.

4.6 Security pipeline in E-Commerce

Advocating for the integration of DevSecOps pipelines, the thesis aligns with industry standards and practices recognized by surveys from Puppet and Sonatype. DevSecOps pipelines are portrayed as a staple in modern development practices, emphasizing their prevalence in large enterprises and e-commerce ecosystems. The recommendation highlights their adaptability across industries, ensuring a holistic and secure approach to software development.

In the expansive realm of e-commerce, safeguarding the online store is akin to fortifying a fortress against potential online robbers. The analogy extends to the concept of a DevSecOps pipeline, where each stage plays a crucial role in ensuring the security of the digital stronghold. This comprehensive exploration will delve into the various components of the Develops pipeline, drawing parallels between the steps involved and the measures taken to protect an online store from virtual intruders.
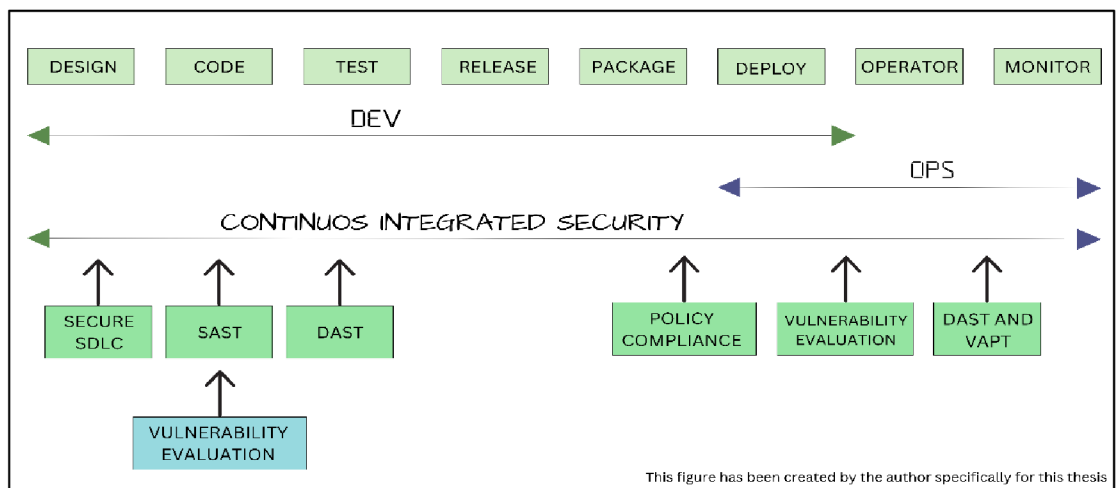

Figure 17: Security pipeline for E-store

[**Source:** This figure has been created by the author specifically for this thesis.]

VAPT - Guards Practicing and Running Drills:

75

Vulnerability Assessment and Penetration Testing (VAPT) can be likened to guards practicing and running drills to ensure they know how to protect the fortress effectively. This phase involves proactive testing to identify potential vulnerabilities and assess the effectiveness of security measures.

Phase	Analogy	Description
Design	Blueprinting the Fortress	The design phase plans the online shop's look and function, equivalent to designing a fortress blueprint. It outlines the security architecture from project inception to preemptively address vulnerabilities.
Code	Building Strong Walls	The code phase involves constructing robust walls for the digital fortress, eliminating secret passages or weak points. Ensuring code integrity and resilience is paramount to create strong defenses against potential exploits.
Test	Ensuring Sturdy and Secure Walls	Testing ensures fortress walls are sturdy and secure, verifying that all elements function as intended. It proactively identifies and rectifies security loopholes to strengthen the overall security posture.
Release	Opening the Doors Safely	The release phase is akin to opening fortress doors to the public. It emphasizes ensuring the online store is safe and ready for public access, highlighting the importance of a meticulous and secure release process.
Package	Securely Packing the Items	Packaging in the DevSecOps pipeline is like securely packing items in the online shop. It ensures nothing escapes or gets tampered with during deployment, emphasizing the integrity and confidentiality of deployed components.
Deploy	Setting up Fortress in a New Location	Deploying is similar to setting up the fortress in a new location, requiring careful execution to avoid potential problems. It translates the digital fortress into a live

Phase	Analogy	Description
		environment while maintaining the highest standards of security.
Operator	Guards Inside the Fortress	Operators serve as guards inside the digital fortress, overseeing operations and ensuring security. Similar to vigilant guards, operators monitor activities and intervene if security concerns arise during the ongoing operations.
Monitor	Watchtowers All Around the Fortress	Monitoring is like having watchtowers strategically positioned around the fortress. These watchtowers maintain constant vigil, scanning for signs of trouble and alerting stakeholders to anything suspicious. It emphasizes continuous surveillance for proactive threat detection.
Security SDLC	Detailed Plan for Security Guards	Security Software Development Life Cycle (SDLC) serves as a detailed plan for security guards, specifying what to look for and how to act at each DevSecOps pipeline stage. It provides a structured approach for a systematic and comprehensive security strategy.
SAST	Scanning Fortress Walls for Weak Points	Static Application Security Testing (SAST) scans fortress walls during construction, identifying potential weak points or vulnerabilities in the code. This proactive scanning ensures the digital fortress foundation is resilient against potential attacks.
DAST	Guard Sneaking into the Fortress	Dynamic Application Security Testing (DAST) simulates a guard attempting to sneak into the fortress, finding hidden vulnerabilities. This dynamic testing approach identifies weaknesses not apparent in static analysis, enhancing the fortress's overall defense.
Policy Compliance	Enforcing Guard Rules	Policy compliance serves as rules for guards, ensuring everyone in the DevSecOps pipeline adheres to the

Phase	Analogy	Description
		established security plan. This phase emphasizes the importance of consistency and adherence to security protocols across all stages of development and operation.
Vulnerability	Finding Hidden Trapdoors	Identifying vulnerabilities is like discovering hidden trapdoors or secret passages in fortress walls. Guards must actively seek out and address these vulnerabilities to fortify the overall security posture of the online store.
VAPT	Guards Practicing and Running Drills	Vulnerability Assessment and Penetration Testing (VAPT) is akin to guards practicing and running drills to protect the fortress effectively. This phase involves proactive testing to identify potential vulnerabilities and assess the effectiveness of security measures in preparation for real-world scenarios.

Table 14: Security pipeline in E-Commerce

[**Source:** This table has been created by the author specifically for this thesis. The Security pipeline in E-Commerce under the ownership of the author of the thesis.]

The scrutiny of Dynamic Application Security Testing (DAST) tools in the thesis draws insights from surveys conducted by OWASP and Acunetix, among others. The analysis emphasizes the plethora of available options, with a focus on tools showcasing prowess in different scenarios. The recommendation adopts a balanced view, acknowledging the varying preferences in the industry while avoiding explicit endorsement of a single tool.

Conclusion - A Strong Fortress for Online Shopping

In amalgamating these security measures, the DevSecOps pipeline constructs a strong fortress for the online shop, safeguarding it from potential online intruders at every step of the way. The thesis presented here is dedicated to discovering and implementing the best practices to fortify e-commerce websites, ensuring a secure and

trustworthy online shopping experience. In an era where digital fortresses are as crucial as physical strongholds, the DevSecOps pipeline emerges as a formidable strategy to protect the integrity of e-commerce platforms and instill confidence in online consumers.

4.7 Simplifying the guardian of cybersecurity

In the dynamic landscape of e-commerce, the concept of endpoints in cybersecurity refers to the devices—such as computers and smartphones—that access our online store. Analogous to ensuring the secure locking of all doors and windows in a physical building, safeguarding these endpoints is paramount to keeping digital intruders at bay. This protection is particularly crucial when customers engage with our website, turning their devices into endpoints that demand dedicated security measures.

Within the realm of Endpoint Detection and Response (EDR), Crowdstrike emerges as the unparalleled choice, celebrated for its status as the most widely used EDR platform, particularly in the expansive domains of large enterprises and e-commerce giants. Insights from reputable sources like Gartner, NSS Labs, and others unequivocally affirm Crowdstrike's dominance. With the largest user base in critical sectors, Crowdstrike stands out for its efficacy in threat detection and response, surpassing competitors. This includes instances where alternatives like Tanium might not achieve the same level of prominence in larger enterprise settings.

Endpoint Detection and Response (EDR) emerges as a critical facet in fortifying these digital entry points. Think of it as the digital equivalent of security cameras and alarms strategically placed to detect and respond to any anomalous activity. This parallels the meticulous security measures implemented to safeguard the entrances and exits of a physical store, fostering a secure and trustworthy online shopping experience.
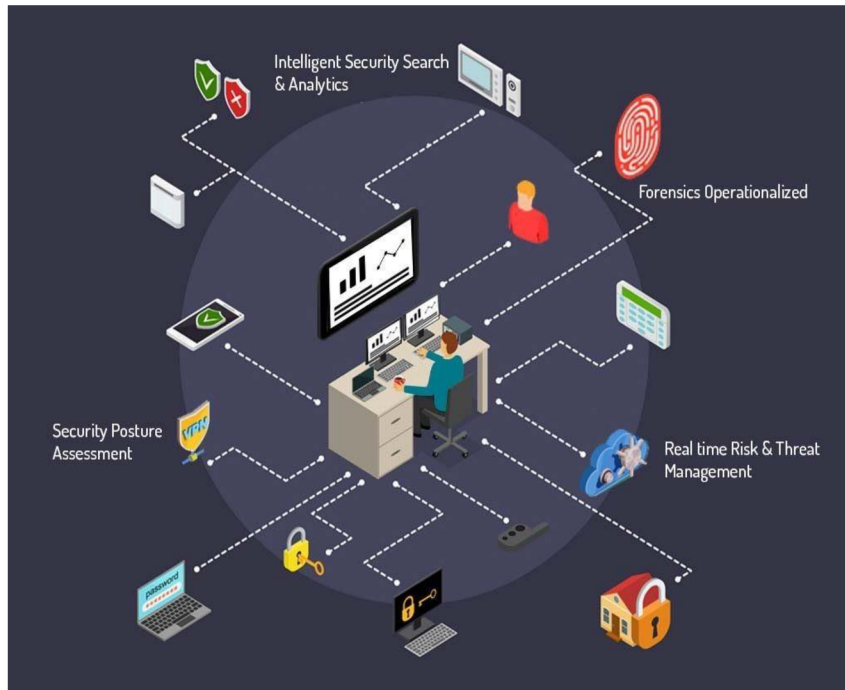
Figure 18: EDR Management

Understanding the Significance of EDR in E-Commerce:

In the realm of e-commerce, where vast amounts of customer data are managed—including personal information and payment details—EDR assumes a pivotal role in safeguarding this sensitive information. It acts as a digital shield against cybercriminals who may attempt to pilfer or misuse customer data, reinforcing the integrity and confidentiality of the online shopping experience.

E-commerce platforms stand as prime targets for a myriad of cyberattacks, ranging from ransomware and phishing to malware. EDR functions as a proactive defines mechanism, detecting and thwarting these threats before they can inflict damage on the website or compromise customer information. By acting as a vigilant gatekeeper, EDR fortifies the digital storefront against potential malicious incursions.
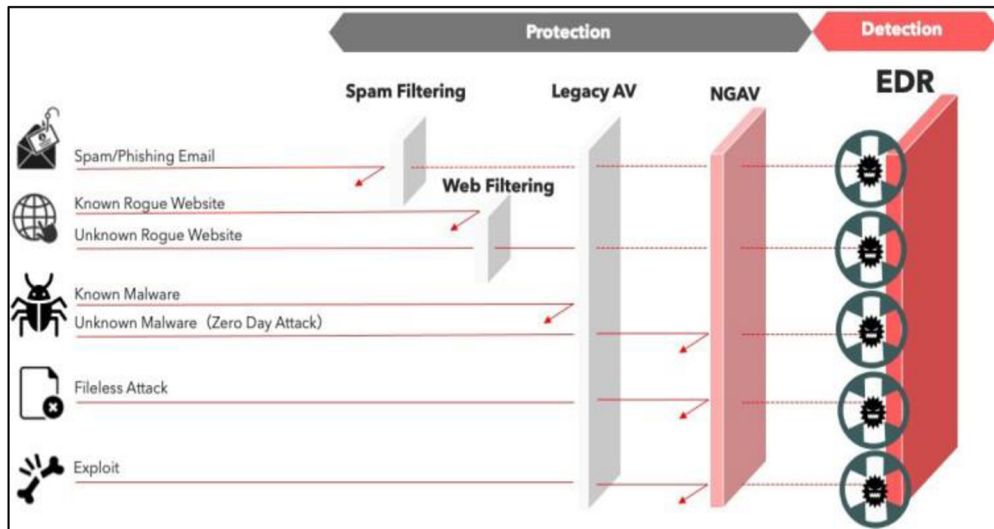
Figure 14: Importance of EDR

[**Source:**

https://www.linkedin.com/pulse/what-edr-why-important-usman-shahzad/]

Aspect	Description
Protecting Customer Data	EDR serves as a digital shield, safeguarding vast amounts of customer data, including personal information and payment details. It acts as a defense against cybercriminals attempting to pilfer or misuse customer data, reinforcing the integrity and confidentiality of the online shopping experience.
Preventing Cyberattacks	EDR functions as a proactive defense mechanism, detecting and thwarting various cyberattacks, including ransomware, phishing, and malware. By acting as a vigilant gatekeeper, EDR fortifies the digital storefront against potential malicious incursions.
Continuous Monitoring	EDR provides ongoing scrutiny of all endpoints, including computers and mobile devices, ensuring prompt identification and resolution of any suspicious activities. This constant vigilance aligns with the dynamic nature of cyber threats, allowing swift responses to emerging challenges.
Quick Response Mechanism	EDR facilitates rapid responses to security issues, mitigating potential threats before escalation. Real-time threat detection and response capabilities minimize the impact on the e-commerce firm

Aspect	Description
	and its consumers, maintaining the resilience of the online shopping environment.
Maintaining Trust	By protecting customer data and ensuring overall security, EDR contributes to fostering trust among customers. A secure digital environment instills confidence, encouraging repeat business and establishing the e-commerce brand as a reliable and secure entity.
Compliance Assurance	EDR plays a crucial and pivotal role in ensuring compliance with regulatory standards such as GDPR and PCI DSS. It verifies the presence and functionality of robust security measures, underscoring the e-commerce business's commitment to adhering to industry standards.
Business Continuity	EDR plays a critical role in maintaining business continuity by preventing disruptions caused by cyber incidents. Its proactive approach to threat detection and response contributes to the overall resilience of the e-commerce operation, preventing downtime and financial losses.

Table 15: Simplifying the guardian of cyber security

[**Source:** This table has been created by the author specifically for this thesis. The Simplifying the guardian of cyber security under the ownership of the author of the thesis.]

In Conclusion

In summary, Endpoint Detection and Response (EDR) stands as a linchpin in the realm of e-commerce security. Its multifaceted contributions, ranging from protecting customer data to ensuring regulatory compliance, collectively reinforce the digital storefront against an array of cyber threats. The continuous monitoring, quick response mechanisms, and trust-building capabilities inherent in EDR position it as an indispensable tool for maintaining the integrity and security of e-commerce platforms.

In an era where online threats are omnipresent, EDR emerges as the digital guardian, tirelessly watching over the digital store, identifying potential risks, and responding with agility to safeguard both the e-commerce business and its customers. As the digital landscape continues to evolve, EDR remains a fundamental component in the arsenal of cybersecurity measures, contributing to the resilience and trustworthiness of the online shopping experience

4.8   Uncovering live threats in online stores

In the realm of e-commerce, getting a team ready to combat real-time threats is akin to providing them with superhero training (Galhotra and Dewan, 2020). It's all about ensuring they are well-prepared to safeguard the online store from cunning cyber adversaries.

Let's explore the training for live threats holds such significance:

In the dynamic landscape of e-commerce, preparing a team to combat real-time threats is analogous to providing them with superhero training. This comprehensive training equips them with the skills and knowledge necessary to safeguard the online store from cunning cyber adversaries. The significance of this training lies in its ability to fortify the digital defenses of an e-commerce website, preserve customer trust, and maintain the uninterrupted functionality of the online store.

Understanding the Enemy: Similar to how superheroes familiarize themselves with their adversaries, your cybersecurity team should possess a deep understanding of the various cyber threats that can target an e-commerce website. From phishing attacks to malware, deceitful tactics come in various forms, and a well-trained team is capable of identifying and thwarting these threats.

Spotting Suspicious Activity: Training is instrumental in assisting a team in detecting uncommon or dubious activities on a website. This keen awareness is akin to having a sharp eye for anything that deviates from the norm. Recognizing unusual login attempts, unanticipated alterations in customer data, or any other anomalies is crucial for early threat detection.

Quick Response: In the face of a detected threat, a well-trained team must act swiftly. Training ensures that team members are well-versed in the steps required to contain and mitigate threats. Whether it involves blocking a suspicious IP address, isolating an infected device, or implementing other countermeasures, a prompt response is essential.

Protecting Customer Data: In the world of e-commerce, customer trust is paramount. Providing training to a team to address threats is instrumental in safeguarding customer data. Guaranteeing the safety and security of customer information is crucial for preserving trust and loyalty. Training ensures that the team employs robust measures to protect sensitive data from cyber threats.

Keeping the Store Open: Cyber threats can disrupt an online store, leading to downtime. Training a team to respond efficiently helps in minimizing downtime and keeping e-commerce operations running smoothly. This is not only essential for business continuity but also for ensuring that customers can access and use the online store without disruptions.

Regular Drills: Just like superheroes practice their skills to stay sharp, a cybersecurity team should regularly participate in threat response drills. These drills are essential for keeping team members prepared and ready to face any situation. Practicing responses to various threat scenarios enhances the team's ability to handle real-time incidents effectively.

Staying Informed: The world of cybersecurity is always evolving, with new threats emerging regularly. Training ensures that a team stays updated on the latest threats and security best practices. It's like providing them with a constantly updated playbook, enabling them to navigate the ever-changing landscape of cyber threats.

Team Coordination: In the face of a threat, teamwork is crucial. Training sessions help a team understand their roles and how to coordinate their efforts for a swift and effective response. Clear communication and collaboration are essential components of an effective cybersecurity strategy.

Customer Confidence: When customers see that a team is well-prepared to handle threats, it boosts their confidence in an e-commerce platform. Knowing that their information is in safe hands encourages trust and loyalty among customers. Customer confidence is a crucial aspect of maintaining a successful e-commerce business.

Continuous Improvement: Training is not a one-time event; it's an ongoing process. A cybersecurity team should continually improve their threat response skills to stay ahead of cybercriminals. This commitment to continuous improvement ensures that the team remains adaptive and resilient in the face of evolving threats.

Conclusion

In conclusion, training a team for live threats is like providing them with the tools and skills they need to be cybersecurity superheroes. It's an ongoing process that ensures an e-commerce website remains safe, customers stay happy, and the business thrives in the digital world. As cyber threats continue to evolve, a well-trained and continuously improving cybersecurity team is the frontline defense, ensuring the security and success of the e-commerce platform.

4.8.1 Continuous improvement in threat detection

In the intricate world of e-commerce, the quest for continuous improvement in threat detection mirrors the journey of a detective committed to refining their skills to apprehend cunning criminals (Chun, 2019). This ongoing endeavor is paramount for staying ahead of cyber adversaries, optimizing security measures, and ensuring the safety of an online store and its customers.

Staying Ahead of Bad Guys: Cybercriminals are notorious for constantly evolving their tactics. Continuous improvement is akin to a detective staying one step ahead of criminals by learning and adapting to new threats. This proactive approach is essential for anticipating and mitigating emerging risks in the ever-changing landscape of cyber threats (Coburn, Leverett, and Woo, 2018).

Reducing False Alarms: Much like a detective striving to eliminate unnecessary distractions, continuous improvement in threat detection allows a security team to enhance their ability to distinguish real threats from false alarms. This refinement saves valuable time and resources that might otherwise be wasted on investigating non-existent or insignificant security incidents.

Learning from Mistakes: Every instance where a threat manages to breach defenses presents an opportunity for learning. Continuous improvement involves a thorough analysis of security lapses, identifying the root causes, and implementing measures to prevent their recurrence. It's a detective's approach to turning setbacks into lessons for future threat mitigation.

Optimizing Security Tools: Security tools, akin to a detective's arsenal, need constant optimization to perform efficiently. Continuous improvement involves fine-tuning security tools, such as antivirus software, to enhance their performance within the unique context of an e-commerce setting. This optimization ensures that the tools remain effective in detecting and neutralizing threats.

Updating Policies: In the world of cybersecurity, policies serve as the rulebook for defenders. Continuous improvement mandates the regular review and updating of security policies to address new risks and challenges. This detective-like scrutiny ensures that security measures align with the evolving threat landscape and compliance requirements.

Sharing Knowledge: Detectives often collaborate and share information to solve cases. Similarly, a cybersecurity team should foster a culture of knowledge-sharing. This involves exchanging insights, experiences, and best practices among team members to enhance collective awareness.

Testing and Simulations: To refine their skills, detectives engage in simulated scenarios. Likewise, a cybersecurity team conducts tests and simulations to enhance their threat detection capabilities. These simulated exercises act as practice sessions,

allowing the team to hone their skills, identify weaknesses, and improve their overall readiness to respond to real-world threats.

Feedback Loop: Continuous improvement relies on a feedback loop. Detectives seek feedback to enhance their investigative techniques. Similarly, a cybersecurity team should encourage the reporting of any suspicious activity. This feedback helps identify areas for improvement, adjust strategies, and fortify defenses against specific threat vectors.

Adapting to E-commerce Changes: As an e-commerce business evolves, so do the associated threats. Continuous improvement ensures that security measures adapt to these changes. Detectives adapt their methods to the changing nature of crime, and similarly, a cybersecurity team must adjust strategies to address new vulnerabilities introduced by changes in the e-commerce environment (Kaushik, Gupta, and Gupta, 2020).

In summary, the journey of continuous improvement in threat detection is comparable to a detective's quest for mastery in the realm of e-commerce security. It involves learning from mistakes, staying well-informed, and refining security measures. By embracing this continuous improvement mindset, an e-commerce business can enhance the protection of its online store and customers from the ever-evolving landscape of cyber threats.

Root Causes of Vulnerabilities Table:

Vulnerability Type	Description
Weak Passwords	Insufficiently strong passwords that can be easily guessed or cracked.
Firewall Misconfigurations	Errors in configuring firewalls that may allow unauthorized access to the network.
Outdated Software	Failure to regularly update and patch software, leaving known vulnerabilities unaddressed.

Lack of Encryption	Absence of encryption measures, making sensitive data susceptible to interception.
Inadequate Access Controls	Poorly defined user access permissions, potentially leading to unauthorized data access or manipulation.
Insufficient Training	Lack of awareness and training among the team, increasing the risk of falling victim to social engineering or phishing.
Cookie Security Issues	Vulnerabilities related to the handling of cookies, such as cookie poisoning or insecure storage.
SQL Injection	Flaws allowing attackers to inject malicious SQL code, potentially compromising the integrity of the database.
Lack of HTTPS	Absence of secure communication protocols, exposing sensitive user data to potential eavesdropping.
CSRF Vulnerabilities	Cross-Site Request Forgery vulnerabilities that may enable attackers to perform unauthorized actions on behalf of users.
Missing Anti-Clicking Header	Absence of mechanisms to prevent abuse, such as repeated clicking, leading to potential disruption of service or fraud.

Table 16: Root Causes of Vulnerabilities Table

[**Source:** This table has been created by the author specifically for this thesis. The Root Causes of Vulnerabilities Table security under the ownership of the author of the thesis.]

The table above outlines various root causes of vulnerabilities within the network architecture of the e-commerce website. Each vulnerability type is accompanied by a brief description to provide clarity on the potential risks and issues associated with it. Identifying and addressing these root causes will be a key focus of the security analysis in this thesis.

5. Results and Discussion

5.1 Discussion

In the pursuit of fortifying the security of e-commerce web applications, this investigation delved into prevalent security flaws, emphasizing issues within the OWASP Top Ten. The study explored various cybersecurity techniques, including Endpoint Detection and Response (EDR), Security Data and Event Management (SIEM), Static Application Security Testing (SAST), and Dynamic Application Security Testing (DAST). Additionally, an assessment of several cybersecurity solution providers, particularly focusing on small and medium-sized enterprises (SMEs), was conducted.

5.1.1 Addressing Risks in Online Shopping

The study verified that e-commerce applications exhibit vulnerabilities outlined in the OWASP Top Ten, posing substantial risks. Issues like injection attacks and authentication errors continue to threaten online businesses. The examination evaluated the effectiveness of various cybersecurity techniques to mitigate these challenges.

5.1.2 Protecting the Online E-Commerce Application

The practical assessment of Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST) highlighted their collaborative effectiveness. While DAST simulates real-world attacks to identify runtime issues, SAST plays a crucial role in uncovering vulnerabilities in the source code. This collaborative approach enhances the resilience of web applications against a broader range of attacks.

5.1.3 Enhancing Online Store Security

Security Information and Event Management (SIEM) systems, when appropriately configured, were acknowledged for their robust real-time security monitoring capabilities. These systems empower organizations to identify security events promptly. The study also recognized the value of Endpoint Detection and

Response (EDR) solutions in augmenting device visibility, providing an additional layer of defense against potential intrusions.

5.1.4 Vendor Comparison

The research underscored the critical role played by the selection of cybersecurity technology providers in shaping the overall security strategy. A detailed vendor comparison, with a focus on cost-effective solutions for SMEs, emphasized the importance of providers offering a balance between functionality and pricing.

5.2 Recommendations

5.2.1 Comprehensive Vulnerability Assessment

Conducting a thorough review to identify any oversights is recommended to maintain the security of the website and the purchasing process. A comprehensive vulnerability assessment ensures a proactive approach to identifying and addressing potential security risks.

5.2.2 Effective Security Monitoring

Emphasizing the importance of constant monitoring, the study recommends regular scans for any signs of problems. Similar to security cameras in a physical store, effective security monitoring is essential for ensuring the safety of online transactions.

5.2.3 Vendor Selection

Choosing top-tier cybersecurity firms for collaboration is crucial. The study draws an analogy between selecting vendors and inviting friends to a party, emphasizing the importance of enjoyable and trustworthy collaborations. SMEs are encouraged to opt for providers offering cost-effective security solutions.

5.2.4 Employee Training and Awareness

Recognizing the significance of ensuring that all staff members possess the necessary skills to protect the online business, the study recommends comprehensive

employee training and awareness programs. Employees are likened to friends learning a new game, with a focus on cybersecurity fundamentals to identify potential threats.

5.2.5 Regular Updates and Patch Management

Highlighting the importance of keeping software up to date, the study recommends proactive measures for regular updates and patch management. Analogous to regular checkups for a car, this approach ensures the timely fixing of vulnerabilities, maintaining a secure online shopping experience for customers.

5.2.6 Incident Response Plan

Drawing parallels between an online store and a ship navigating cyberspace, the study introduces the concept of an "Incident Response Plan." Similar to life jackets and rescue boats on a ship, this plan serves as a safety manual for prompt problem-solving and protection in case of emergencies.

In summary, the study offers practical insights into addressing security risks in online shopping, protecting e-commerce applications, enhancing online store security, and making informed decisions regarding vendors. The recommendations encompass a comprehensive approach to vulnerability assessment, effective security monitoring, vendor selection, employee training, regular updates, and an incident response plan. These recommendations aim to empower e-commerce businesses, especially SMEs, in fortifying their cybersecurity posture and ensuring a secure digital shopping environment.

6. Conclusion

Diving deep into the vulnerabilities of e-commerce web applications, our focus was on understanding the root causes and proposing practical countermeasures. I took a thorough approach, scrutinizing each vulnerability to provide concrete solutions. Here's a breakdown of findings.

- **Identifying Root Causes**

  Our examination went beyond surface-level vulnerabilities, delving into the foundational issues affecting e-commerce platforms. We pinpointed areas such as insufficient input validation, access control weaknesses, and authentication system vulnerabilities.

  Insufficient Input Validation: Our investigation highlighted the risks associated with lax input validation, allowing potential security breaches. Strengthening input validation emerged as a crucial aspect of addressing this vulnerability.

  Improper Access Control: Instances of poorly defined access controls posed risks of unauthorized access and data compromise. Addressing this vulnerability required a nuanced approach, emphasizing the refinement of access control mechanisms.

  Weak Authentication Mechanisms: Weaknesses in authentication mechanisms were identified as potential vulnerabilities. Enhancing password policies, implementing multi-factor authentication, and securing user credentials became imperative to mitigate this risk.

- **Proposed Countermeasures**

  Rather than isolated fixes, our proposed countermeasures were formulated as an integrated strategy. Secure coding practices, meticulous access controls, and strengthened authentication mechanisms were not just solutions; they were

part of an overarching plan to fortify the inherent security of e-commerce web applications.

Secure Coding Practices: Our proposal advocated for the adoption of secure coding practices throughout the development lifecycle. This included robust input validation, secure data handling, and adherence to coding standards to establish a resilient foundation against potential exploits.

Implementing Access Controls: To address vulnerabilities related to improper access control, our proposed countermeasures focused on meticulous implementation. This involved defining and enforcing access policies, regular review of permissions, and adherence to least privilege principles.

Improving Authentication Mechanisms: Recognizing the pivotal role of authentication, our proposal detailed enhancements. This encompassed stringent password policies, multi-factor authentication, and the use of secure protocols to safeguard user credentials during transmission.

- **Effectiveness Evaluation**

  Our commitment extended to practical validation through rigorous testing. Utilizing methodologies like Vulnerability Assessment and Penetration Testing (VAPT), we examined the real-world impact of our countermeasures on e-commerce applications. Advanced tools, including SIEM, EDR, Firewall, SAST, DAST, and Anti-virus solutions, were employed to scrutinize the tangible efficacy of our security measures.

  Testing Their Impact: Rigorous evaluation of the proposed countermeasures was conducted, utilizing methodologies such as Vulnerability Assessment and Penetration Testing (VAPT). Advanced tools like SIEM, EDR, Firewall, SAST, DAST, and Anti-virus tools were deployed to scrutinize their tangible impact on e-commerce web applications.

Strategic Integration of Tools and Systems:

In our pursuit of a comprehensive defense strategy, a variety of tools and systems were strategically integrated:

1. **SIEM, EDR, Firewall:** Providing real-time monitoring, swift threat response, and a robust defense against potential breaches.

2. **SAST, DAST:** Ensuring proactive identification and rectification of vulnerabilities through static and dynamic application security testing.

3. **Anti-virus Tools:** Adding an extra layer of protection against malware and other security threats.

4. **DevSecOps Pipeline:** Integrating security into every stage of the development lifecycle to foster a culture of continuous security improvement.

5. **OWASP Top 10 and HTTPS Protocol:** Adhering to industry standards, systematically addressing common vulnerabilities, and prioritizing the HTTPS protocol for enhanced encryption and communication security during e-commerce transactions.

In conclusion, the comprehensive transcends the identification of vulnerabilities and the proposal of countermeasures. It serves as a testament to our commitment to fortifying e-commerce web applications, providing a detailed account of the practical implementation and thorough evaluation of measures. By integrating advanced tools and adhering to industry standards, our approach ensures a proactive and robust defense mechanism, contributing significantly to creating a safer and more secure digital ecosystem for e-commerce platforms.

7. References

Achmad, W. (2023) 'MSMEs Empowerment through Digital Innovation: The Key to Success of E-Commerce in Indonesia', Daengku: Journal of Humanities and Social Sciences Innovation, 3(3), pp. 469–475. Available at: https://doi.org/10.35877/454RI.daengku1742.

Akour, I. et al. (2022) 'A Conceptual Model for Investigating the Effect of Privacy Concerns on E-Commerce Adoption: A Study on United Arab Emirates Consumers', Electronics, 11(22), p. 3648.

Alwaheidi, M.K.S., Islam, S. and Papastergiou, S. (2022) 'A Conceptual Model for Data-Driven Threat Analysis for Enhancing Cyber Security', in K. Daimi and A. Al Sadoon (eds) Proceedings of the ICR'22 International Conference on Innovations in Computing Research. Cham: Springer International Publishing (Advances in Intelligent Systems and Computing), pp. 365–374. Available at: https://doi.org/10.1007/978-3-031-14054-9_34.

Arfeen, A. et al. (2021) 'Endpoint Detection & Response: A Malware Identification Solution', in 2021 International Conference on Cyber Warfare and Security (ICCWS). 2021 International Conference on Cyber Warfare and Security (ICCWS), pp. 1–8. Available at: https://doi.org/10.1109/ICCWS53234.2021.9703010.

Bernsmed, K. et al. (2022) 'Adopting threat modelling in agile software development projects', Journal of Systems and Software, 183, p. 111090. Available at: https://doi.org/10.1016/j.jss.2021.111090.

Butler, S.A. (2002) 'Security attribute evaluation method: a cost-benefit approach', in Proceedings of the 24th International Conference on Software Engineering. New York, NY, USA: Association for Computing Machinery (ICSE '02), pp. 232–240. Available at: https://doi.org/10.1145/581339.581370.

Cahn, A. et al. (2016) 'An Empirical Study of Web Cookies', in Proceedings of the 25th International Conference on World Wide Web. Republic and Canton of Geneva, CHE: International World Wide Web Conferences Steering Committee (WWW '16), pp. 891–901. Available at: https://doi.org/10.1145/2872427.2882991.

Callegati, F., Cerroni, W. and Ramilli, M. (2009) 'Man-in-the-Middle Attack to the HTTPS Protocol', IEEE Security & Privacy, 7(1), pp. 78–81. Available at: https://doi.org/10.1109/MSP.2009.12.

Castro, L.M., Cabrero, D. and Heimgärtner, R. (2022) Software Usability. BoD – Books on Demand.

Choi, E. and Lee, K.C. (2019) 'Effect of trust in domain-specific information of safety, brand loyalty, and perceived value for cosmetics on purchase intentions in mobile e-commerce context', Sustainability, 11(22), p. 6257.

Chun, S.-H. (2019) 'E-Commerce Liability and Security Breaches in Mobile Payment for e-Business Sustainability', Sustainability, 11(3), p. 715. Available at: https://doi.org/10.3390/su11030715.

Coburn, A., Leverett, E. and Woo, G. (2018) Solving Cyber Risk: Protecting Your Company and Society. John Wiley & Sons.

De, S. (2020) 'A Novel Perspective to Threat Modelling using Design Thinking and Agile Principles', in 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC). 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC), pp. 31–35. Available at: https://doi.org/10.1109/PDGC50313.2020.9315844.

Dijesh, P., Babu, S. and Vijayalakshmi, Y. (2020) 'Enhancement of e-commerce security through asymmetric key algorithm', Computer Communications, 153, pp. 125–134.

Finch, B.J. (2007) 'Customer expectations in online auction environments: An exploratory study of customer feedback and risk', Journal of Operations Management, 25(5), pp. 985–997. Available at: https://doi.org/10.1016/j.jom.2006.10.007.

Galhotra, B. and Dewan, A. (2020) 'Impact of COVID-19 on digital platforms and change in E-commerce shopping trends', in 2020 fourth international conference on I-SMAC (IoT in social, mobile, analytics and cloud)(I-SMAC). IEEE, pp. 861–866.

Available at: https://ieeexplore.ieee.org/abstract/document/9243379/ (Accessed: 11 November 2023).

Gao, X. et al. (2020) 'To buy or not buy food online: The impact of the COVID-19 epidemic on the adoption of e-commerce in China', PloS one, 15(8), p. e0237900.

González-Granadillo, G., González-Zarzosa, S. and Diaz, R. (2021) 'Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures', Sensors, 21(14), p. 4759. Available at: https://doi.org/10.3390/s21144759.

Hassan, M.A., Shukur, Z. and Hasan, M.K. (2020) 'An efficient secure electronic payment system for e-commerce', computers, 9(3), p. 66.

Jhawar, R. et al. (2018) 'Semi-automatically Augmenting Attack Trees Using an Annotated Attack Tree Library', in S.K. Katsikas and C. Alcaraz (eds) Security and Trust Management. Cham: Springer International Publishing (Lecture Notes in Computer Science), pp. 85–101. Available at: https://doi.org/10.1007/978-3-030-01141-3_6.

Jiang, L., Chen, H. and Deng, F. (2010) 'A Security Evaluation Method Based on STRIDE Model for Web Service', in 2010 2nd International Workshop on Intelligent Systems and Applications. 2010 2nd International Workshop on Intelligent Systems and Applications, pp. 1–5. Available at: https://doi.org/10.1109/IWISA.2010.5473445.

Kaushik, D., Gupta, A. and Gupta, S. (2020) 'E-commerce security challenges: A review', in Proceedings of the international conference on innovative computing & communications (ICICC). Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3595304 (Accessed: 11 November 2023).

Keskin, O.F. et al. (2021) 'Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports', Electronics, 10(10), p. 1168. Available at: https://doi.org/10.3390/electronics10101168.

Khan, A.W. et al. (2022) 'Analyzing and Evaluating Critical Cyber Security Challenges Faced by Vendor Organizations in Software Development: SLR Based Approach', IEEE Access, 10, pp. 65044–65054. Available at: https://doi.org/10.1109/ACCESS.2022.3179822.

Khan, M.S., Siddiqui, S. and Ferens, K. (2018) 'A Cognitive and Concurrent Cyber Kill Chain Model', in K. Daimi (ed.) Computer and Network Security Essentials. Cham: Springer International Publishing, pp. 585–602. Available at: https://doi.org/10.1007/978-3-319-58424-9_34.

Maple, C. et al. (2019) 'A Connected and Autonomous Vehicle Reference Architecture for Attack Surface Analysis', Applied Sciences, 9(23), p. 5101. Available at: https://doi.org/10.3390/app9235101.

Marchany, R.C. and Tront, J.G. (2002) 'E-commerce security issues', in Proceedings of the 35th Annual Hawaii International Conference on System Sciences. Proceedings of the 35th Annual Hawaii International Conference on System Sciences, pp. 2500–2508. Available at: https://doi.org/10.1109/HICSS.2002.994190.

martinekuan (2023) Hybrid security monitoring with Microsoft Sentinel - Azure Architecture Center. Available at: https://learn.microsoft.com/en-us/azure/architecture/hybrid/hybrid-security-monitoring (Accessed: 11 November 2023).

Pinchinat, S., Schwarzentruber, F. and Lê Cong, S. (2020) 'Library-Based Attack Tree Synthesis', in H. Eades III and O. Gadyatskaya (eds) Graphical Models for Security. Cham: Springer International Publishing (Lecture Notes in Computer Science), pp. 24–44. Available at: https://doi.org/10.1007/978-3-030-62230-5_2.

Pourni, G.-E. (2022) 'The Depiction of the Loser Teenager in the Film and Television Adaptations of John Green's Young Adult Novels', Journal of Literary Education, (6), pp. 167–179. Available at: https://doi.org/10.7203/JLE.6.25373.

Radoglou-Grammatikis, P. et al. (2021) 'SPEAR SIEM: A Security Information and Event Management system for the Smart Grid', Computer Networks, 193, p. 108008. Available at: https://doi.org/10.1016/j.comnet.2021.108008.

Rungsrisawat, S., Sriyakul, T. and Jermsittiparsert, K. (2019) 'The era of e-commerce & online marketing: risks associated with online shopping', International Journal of Innovation, Creativity and Change, 8(8), pp. 201–221.

Shapsough, S. et al. (2015) 'Smart grid cyber security: Challenges and solutions', in 2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE). 2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE), pp. 170–175. Available at: https://doi.org/10.1109/ICSGCE.2015.7454291.

Story, G.W. et al. (2013) 'Dread and the Disvalue of Future Pain', PLOS Computational Biology, 9(11), p. e1003335. Available at: https://doi.org/10.1371/journal.pcbi.1003335.

Taherdoost, H. (2023) 'Legal, Regulatory, and Ethical Considerations in E-Business', in H. Taherdoost (ed.) E-Business Essentials: Building a Successful Online Enterprise. Cham: Springer Nature Switzerland (EAI/Springer Innovations in Communication and Computing), pp. 379–402. Available at: https://doi.org/10.1007/978-3-031-39626-7_15.

Ungerer, C. et al. (2020) 'Recommendations to leverage e-commerce during the covid-19 crisis'. Available at: https://openknowledge.worldbank.org/handle/10986/33750 (Accessed: 11 November 2023).

Whitmore, R. (1984) 'Modelling the Policy/Implementation Distinction: The Case of Child Abuse', Policy & Politics, 12(3), pp. 241–267. Available at: https://doi.org/10.1332/030557384782628336.

Younus, Z.S. and Alanezi, M. (2023) 'A Survey on Network Security Monitoring: Tools and Functionalities'.

Yudhianto, I. (2023) 'Simple, Fast, and Accurate Cybercrime Detection on E-Government with Elastic Stack SIEM', JEPIN (Jurnal Edukasi dan Penelitian Informatika), 9(2), pp. 263–276. Available at: https://doi.org/10.26418/jp.v9i2.64213.

Zhu, Z. et al. (2021) 'Quality of e-commerce agricultural products and the safety of the ecological environment of the origin based on 5G Internet of Things technology', Environmental Technology & Innovation, 22, p. 101462.

8. List of pictures and abbreviations

8.1 List of pictures

8.2 List of tables

8.3 List of abbreviations

SIEM: Security Information and Event Management

SIEM: Security Information and Event Management

EDR: Endpoint Detection and Response

SAST: Static Application Security Testing

DAST: Dynamic Application Security Testing

OWASP: Open Web Application Security Project

SME: Small and Medium-sized Enterprise

SMB: Small and Medium-sized Business

XXE: XML External Entities

XSS: Cross-Site Scripting

DREAD: Damage, Reproducibility, Exploitability, Affected Users, Discoverability

VAPT: Vulnerability Assessment and Penetration Testing

WASC: Web Application Security Consortium

CWE: Common Weakness Enumeration

AV: Anti-Virus

NGAV: Next Generation Anti-Virus

SRE: Site Reliability Engineer

QA: Quality Assurance

Dev: Developer

HR: Human Resource

LB: Load Balancer

IT: Information Technology

STRIDE: Spoofing Identity, Tampering with Data, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege.

PASTA: Process for Attack Simulation and Threat Analysis, Application for Threat Analysis, Security Testing and Assessment, Threat Intelligence and Attack Patterns, Risk Assessment