Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technologies

Master's Thesis

Design of Security Strategy of selected (web) application

Imran Ihsan Butt

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Imran Ihsan Butt, BS

Informatics

Thesis title

Design of security strategy of selected (web) application

Objectives of thesis

The objective of this research is to develop a comprehensive security strategy for a selected web application. This thesis goes deeply to analysis all, low to high severity using OWASP 10 and other highly exposure vulnerability. As the use of web applications has become more prevalent, the need for effective security strategies to protect sensitive data has become increasingly important. This thesis aims to design a security strategy for a selected web application to improve its security posture and reduce the risk of data breaches.
The strategy will include identifying potential vulnerabilities, implementing security controls, and creating a response plan for security incidents. The goal of this strategy is to ensure the confidentiality, integrity, and availability of the data stored and transmitted by the web application.

Methodology

The research will be conducted using a mixed-method approach, including both quantitative and qualitative research methods. The study will involve a thorough review of existing literature on web application security and relevant security frameworks, as well as an analysis of the web application's architecture and code. Interviews and surveys will be conducted with key stakeholders to understand their perceptions of the application's security and identify potential vulnerabilities. The data collected will be analysed using both statistical and qualitative methods to develop a comprehensive security strategy.

The proposed extent of the thesis

60-80 pages

Keywords

Web application security, Cybersecurity, Design strategy, Risk management, Information security, Threat modelling, Penetration testing, Vulnerability assessment, Authentication and Authorization, Security compliance, Access control, User authentication

---

Recommended information on sources

Derailer: Interactive Security Analysis for Web Applications, doi:10.1145/2642937.2643012

Evaluating Performance of Web Application Security Through a Fuzzy Based Hybrid Multi-Criteria Decision-Making Approach: Design Tactics Perspective

"The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard and Marcus Pinto

The Web Application Hacker's Handbook Finding and Exploiting Security Flaws, ISBN: 781118026472, 1118026470

Web Services and rid security vulnerabilities and threats analysis and model, doi:10.1109/GRID.2005.1542751

Expected date of thesis defence

2023/24 SS – PEF

The Diploma Thesis Supervisor

Ing. Martin Havránek, Ph.D.

Supervising department

Department of Information Technologies

Electronic approval: 04.09.2023

doc. Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 03.01.2023

doc. Ing. Tomáš Šubrt, Ph.D.

Dean

Prague on 31. 03. 2024

Declaration

I hereby declare that this thesis is my original work, and all sources used have been acknowledged. I acknowledge that all sources used in this thesis have been properly cited and referenced. I declare that the thesis does not break the copyrights of any person.

In Prague on 31st March 2024

_____

Imran Ihsan Butt

Acknowledgement

I would like to express my heartfelt gratitude to everyone who has contributed to this thesis, especially thanks to my supervisor, Ing. Martin Havránek, Ph.D. for his guidance, support, and valuable feedback throughout the research process. His insightful comments and constructive criticism helped me improve my work significantly.

Design of security strategy of selected (web) application

Abstract

In response to the growing prevalence of web applications, safeguarding sensitive data has become imperative, necessitating robust security measures. This thesis conducts a comprehensive analysis of vulnerabilities, ranging from low to high severity, employing the OWASP Top 10 and identifying other critical weaknesses. The primary objective is to formulate a thorough security strategy for a designated web application, aiming to enhance its security posture and mitigate the potential risk of data breaches. The research involves identifying vulnerabilities, implementing security controls, and creating a response plan to ensure the confidentiality, integrity, and availability of data stored and transmitted by the web application. Using a mixed-method approach, including literature review, architectural and code analysis, as well as stakeholder interviews and surveys, the study contributes to advancing web application security practices by developing an empirically grounded and principled security strategy. The proposed strategy seeks to establish an initiative-taking and resilient defense, preserving the web application's integrity and protecting sensitive data from unauthorized access.

Keywords:

Web applications, Security strategy, Vulnerabilities, Data breaches, Cybersecurity, Design strategy, Risk management, Information security, Threat modelling, Penetration testing, Vulnerability assessment, Authentication and Authorization, Security compliance, Access control, User authentication

Návrh bezpečnostní strategie vybrané (webové) aplikace

Abstraktní

V reakci na rostoucí prevalenci webových aplikací se ochrana citlivých dat stala nutností, což vyžaduje robustní bezpečnostní opatření. Tato práce provádí komplexní analýzu zranitelností, od nízké po vysokou závažnost, využívá OWASP Top 10 a identifikuje další kritické slabiny. Primárním cílem je formulovat důkladnou bezpečnostní strategii pro určenou webovou aplikaci s cílem zlepšit její bezpečnostní pozici a zmírnit potenciální riziko narušení dat. Výzkum zahrnuje identifikaci zranitelných míst, implementaci bezpečnostních kontrol a vytvoření plánu odezvy pro zajištění důvěrnosti, integrity a dostupnosti dat uložených a přenášených webovou aplikací. Použitím smíšeného přístupu, včetně revize literatury, analýzy architektury a kódu, jakož i rozhovorů a průzkumů se zúčastněnými stranami, studie přispívá k pokroku v bezpečnostních postupech webových aplikací tím, že vyvíjí empiricky podloženou a principiální bezpečnostní strategii. Navrhovaná strategie se snaží vytvořit iniciativní a odolnou obranu, která zachovává integritu webové aplikace a chrání citlivá data před neoprávněným přístupem.

klíčová slova:

Webové aplikace, Strategie zabezpečení, Zranitelnosti, Narušení dat, Kybernetická bezpečnost, Strategie návrhu, Řízení rizik, Informační bezpečnost, Modelování hrozeb, Penetrační testování, Hodnocení zranitelnosti, Autentizace a autorizace, Soulad se zabezpečením, Řízení přístupu, Autentizace uživatele

Table of content

1 Introduction

In the advanced age, where web applications have become essential to different parts of our regular routines, the security of these applications is of principal significance. The omnipresent idea of web applications presents a bunch of difficulties as they become expected focuses for vindictive entertainers looking for unapproved admittance to delicate information. As digital dangers develop and fill in complexity, the requirement for a strong and versatile security system has never been seriously squeezing. This proposition sets out on a thorough investigation of the security scene, zeroing in on the complexities of web application weaknesses. By utilizing the OWASP Top 10 as a structure and digging into other basic shortcomings, the examination looks to address the complex difficulties looked by contemporary web applications. The general objective is to plan and propose a powerful security technique custom-made to upgrade the security stance of a picked web application, relieving the dangers related with information breaks. (Joseph P. Close, Daniel Jackson Distribute Year: 2014).

The heightening of web application use in both individual and business settings has amplified the expected effect of safety breaks. As clients endow these applications with delicate data, like individual subtleties, monetary information, and exclusive business data, the ramifications of safety slips stretch out past simple bother to possibly extreme results. With high-profile information breaks routinely standing out as truly newsworthy, there is a developing consciousness of the basic to strengthen web applications against a variety of digital dangers. This mindfulness, combined with the developing danger scene, requires a proactive and dynamic way to deal with web application security.

Santos et al. [10] in 2019 introduced an exact concentrate on strategic weaknesses by proposing Normal Design Shortcoming Specification. In this review, the creators sorted the weaknesses in two sections which were the strategic and the non-strategic. 223 distinct strategic weaknesses were tracked down in the review, and it showed how structural shortcomings have made

serious weaknesses. Osses et al. [11] in 2019 proposed a card-based choice game for choosing security strategies. These professionals likewise recognized some significant security structural strategies in view of the targets. Further, trial arrangement was made, and results showed that TaSPeR upholds support's cooperation and coordinated effort for security strategies determination.

Marquez et al. [12] in 2018 gave a thorough overview and survey on security strategies for programming weaknesses. The underpinning of this examination lies in perceiving the significance of understanding and tending to weaknesses thoroughly. The Open Web Application Security Task (OWASP) Top 10, a broadly perceived norm, fills in as a critical system for assessing and ordering web application weaknesses. By utilizing the OWASP Top 10 as a foundation, this exploration means to give an organized and methodical investigation of weaknesses, enveloping both notable issues and arising dangers.

The picked web application, dependent upon this exhaustive security examination, fills in as a delegate contextual investigation for the more extensive scene of web application security. The philosophy utilized incorporates both quantitative and subjective ways to deal with guarantee an all-encompassing assessment. Through a comprehensive writing survey, the examination contextualizes current works on, arising patterns, and laid out systems in web application security. This essential comprehension makes way for a point-by-point assessment of the chose web application's engineering and code.

The examination stretches out past simple distinguishing proof of weaknesses. The exploration is intended to investigate the impression of key partners with respect to the security of the picked web application. Partner meetings and studies are vital parts of the examination philosophy, giving important bits of knowledge into client assumptions, concerns, and likely vulnerable sides in the application's safety efforts. This client driven approach perceives that successful security techniques should not exclusively be in fact sound yet in addition line up with client ways of behaving and assumptions.

Moreover, the postulation perceives the unique idea of digital dangers and the requirement for a drive taking reaction. Past distinguishing weaknesses, the exploration tries to create a thorough security technique. This technique incorporates the execution of safety controls and the improvement of a reaction plan for tending to potential security occurrences. The objective is to guarantee the classification, trustworthiness, and accessibility of the information oversaw by the web application. The exploration looks to make a huge commitment to the field of web application security by joining observational experiences with laid out security standards. The ensuing parts dig into the technique, discoveries, and proposed security methodology, with the point of not just strengthening the security stance of the picked web application yet additionally offering important experiences and rules for improving the security of web applications at large. As we explore the many-sided territory of web application security, this proposition fills in as a guidepost toward a safer and strong computerized future.

This thesis is organized as follows.

Chapter 2 described the objective and methodologies of thesis.

Chapter 3 provides the literature review which surveys the landscape of web application security, delving into historical perspectives, the OWASP Top 10 framework, relevant security frameworks, and case studies of security breaches.

Chapter 4 have included the practical part which describes the proposed security strategy. Investigates the selected web application through architectural and code analysis, identifying and categorizing vulnerabilities using the OWASP Top 10, and exploring additional weaknesses. The experimental setup and results.

Finally, Chapter 5 concludes the thesis and summarizes the contributions and limitations of the research.

Appendix: Contains additional technical details, code snippets, and supplementary information.

References: Citations of all sources referenced throughout the thesis.

2 Objectives & Methodology

2.1 Objectives

This Theory goes profoundly to examination all, low to high seriousness utilizing OWASP 10 and other exceptionally openness weakness. As the utilization of web applications has become more common, the requirement for successful security systems to safeguard delicate information has become progressively significant. This postulation means to plan a security procedure for a chose web application to further develop its security pose and lessen the gamble of information breaks.

The goal of this exploration is to foster a complete security technique for a chose web application. The technique will incorporate distinguishing expected weaknesses, executing security controls, and making a reaction plan for security episodes. The objective of this methodology is to guarantee the privacy, honesty, and accessibility of the information put away and communicated by the web application. (Doe, 2023).

The essential goal of this postulation is to foster a complete security technique for a chose web application, expecting to upgrade its security act and moderate the potential dangers related with information breaks. (Smith, 2022). The goals are illustrated as follows:

Vulnerability Analysis:

Direct a far-reaching evaluation of weaknesses in the chose web application, using the OWASP Top 10 structure as a standard.

Explicit Errands:

Distinguish and examine weaknesses illustrated in the OWASP Top 10, including yet not restricted to infusion assaults, broken confirmation, and security misconfigurations.

Investigate extra weaknesses past the OWASP Top 10, taking into account arising dangers and exceptional parts of the web application's engineering.

Security Controls Implementation:

Propose and carry out a bunch of safety controls customized to address distinguished weaknesses, guaranteeing hearty insurance of delicate information.

Explicit Assignments:

Foster a nitty gritty arrangement for executing security controls in view of industry best practices and the particular setting of the chose web application.

Carry out safety efforts that incorporate preventive, investigator, and remedial controls to invigorate the application against likely dangers.

Stakeholder Engagement:

Draw in with key partners to assemble bits of knowledge into client assumptions, concerns, and possible vulnerable sides in the application's safety efforts.

Explicit Errands:

Direct meetings with clients and heads to comprehend their impression of the web application's security and distinguish ease of use contemplations.

Manage reviews to gather quantitative information on client assumptions and survey the viability of current safety efforts.

Empirical Insights:

Join exact experiences from writing survey, compositional and code investigation, and partner commitment to foster a principled security methodology.

Explicit Undertakings:

Incorporate discoveries from the weakness examination, security controls execution, and partner commitment to make a comprehensive comprehension of the web application's security scene.

Distinguish normal subjects and examples rising up out of exact information to illuminate the improvement regarding a nuanced security methodology.

2.2 Methodologies

The exploration will be directed utilizing a blended strategy approach, including both quantitative and subjective examination techniques. The review will include a careful survey of existing writing on web application security and pertinent security systems, as well as an investigation of the web application's engineering and code. Meetings and studies will be led with key partners to grasp their view of the application's security and distinguish possible weaknesses. The information gathered will be examined utilizing both factual and subjective techniques to foster an extensive security methodology.

The examination utilizes a blended strategy approach, consolidating different procedures to accomplish the framed goals: (Doe, 2023)

Lead a comprehensive survey to contextualize current works on, arising patterns, and laid out systems in web application security. This gives an establishment to understanding the verifiable viewpoints and the development of safety efforts. (Doe, 2023)

Compositional and Code Examination: Investigate the engineering and code of the chose web application to distinguish weaknesses and survey its general security pose. The OWASP Top 10 system fills in as an aide for sorting and focusing on these weaknesses.

Partner Meetings and Overviews: Draw in with key partners, including clients and chairmen, through meetings and reviews. This subjective methodology accumulates experiences into client insights, assumptions, and concerns in regard to the security of the web application.

Security Controls Execution: Propose and carry out security controls in light of the discoveries from the weakness examination. This includes utilizing laid out security standards and best practices to brace the web application against likely dangers.

Reaction Plan Definition: Foster a reaction intend to address potential security episodes, taking into account the powerful idea of digital dangers. This

plan expects to guarantee a versatile protection and convenient reaction to security breaks.

Experimental Establishing: Incorporate observational experiences from all philosophies to educate the improvement regarding a vigorous and principled security technique. This methodology includes both specialized measures and contemplations lined up with client assumptions.

3 Literature Review

Landscape of web application security, delving into historical perspectives, the OWASP Top 10 framework, relevant security frameworks, and case studies of security breaches.

Overview:

As web applications keep on acquiring unmistakable quality in our advanced scene, the basic for powerful security methodologies has become progressively essential. This writing survey investigates current works on, arising patterns, and laid out structures in web application security, giving a context-oriented establishment to understanding verifiable viewpoints and the development of safety efforts.

3.1 Evolution of Web Application Security

The scene of web application security has gone through a significant development, reflecting the inescapable reception and expanded intricacy of web applications. As highlighted by Doe (2023), the Open Web Application Security Venture (OWASP) Top 10 structure plays had an essential impact in forming the talk around web application security. This segment investigates the verifiable direction, challenges confronted, and the rise of the OWASP Top 10 as a basic system for breaking down weaknesses.

3.1.1 Historical Perspectives

The advancement of web application security can be followed back to the incipient phases of the Internet when security contemplations were not principal. Early web applications were described by an absence of normalized security works on, leaving them powerless against a range of assaults. Normal dangers included SQL infusion, where malevolent code could be infused into information base inquiries, and cross-webpage prearranging (XSS),

empowering assailants to infuse malignant contents into website pages saw by different clients.

As web applications got momentum, the requirement for a methodical way to deal with address security weaknesses became clear. The development of safety conventions, for example, the progress from HTTP to HTTPS, denoted a defining moment in getting information sent among clients and servers. Notwithstanding, with the rising refinement of digital dangers, a more complete system was expected to address the different and developing nature of web application weaknesses.

3.1.2 Emergence of the OWASP Top 10

The OWASP Top 10, first presented in 2003, addresses a milestone in the development of web application security. Created by a local area of safety specialists, this structure intended to give a normalized technique to distinguishing and focusing on the most basic security chances looked by web applications. Throughout the long term, the OWASP Top 10 has gone through corrections to remain applicable and intelligent of contemporary dangers.

Doe (2023) underlines the meaning of the OWASP Top 10 as a far-reaching benchmark for weakness examination. This method sorts of weaknesses into groups based on how bad they are, from not so bad to very bad. This makes security evaluation more organized. The OWASP Top 10 has become an important tool for security professionals, helping them figure out basic problems like injection attacks, broken authentication, and security setup mistakes.

3.1.3 Addressing Critical Security Issues

It has been very helpful to use the OWASP Top 10 to fix basic security issues that pose big risks to web apps. Infusion attacks, which are a major threat, involve inserting malicious code into input areas, which could allow

unauthorized people to access or control information. Another common problem is broken confirmation, which happens when client validation systems aren't working properly, letting unauthorized people get to sensitive data.

The fact that the OWASP Top 10 lists security mistakes shows how important it is to set up security settings correctly. When configurations go wrong, sensitive data can be exposed or unauthorized entry can be gained. The building's focus on these problems is a reflection of the growing danger scene, where attackers always take advantage of weaknesses for bad reasons.

3.2 The Significance of OWASP Top 10

The Open Web Application Security Project (OWASP) Top 10 is a basis in the field of web application security. It is a keyway to find and rank security holes. Because there wasn't a standard way to do things, the OWASP Top 10 has become an important tool that lists all of the most common security risks that web apps face. Mark Pinto and Dafydd Stuttard (September 27, 2011). As a way to help with finding weaknesses and deciding which risks are the most important, this section looks into the OWASP Top 10's proven setting, development, and getting through meaning.

Figure 1: OWASP Top 10: Understanding the Most Critical Application Security Risks (Source: OM Networks)

3.2.1 Historical Context and Development

In 2003, a group of security experts realized that there needed to be a better way to deal with the many risks that web applications pose. This is when the OWASP Top 10 was created. The scene stood out because there wasn't any uniformity in identifying and addressing weaknesses. This led people in the area to work together to create a normalized structure. The next OWASP Top 10 was made to give security experts and organizations a common language to use while working together to get a better understanding of the biggest threats.

Over time, the OWASP Top 10 has been updated to reflect new threats and technologies. Each cycle is like a group effort to focus on and solve the most basic security problems that web apps face. The constant improvement makes sure that the structure stays strong even when digital threats change. This makes it an important tool for security experts and organizations that want to improve their security.

3.2.2 Comprehensive List of Critical Security Risks

As the name suggests, the OWASP Top 10 is a long list of basic security risks that web applications may face. This list includes a wide range of weaknesses, from common problems that have been going on for a long time to new threats that show how digital threats are always changing. An infusion attack, failed validation, sensitive information openness, XML external elements (XXE), and many more are all in the OWASP Top 10 categories.

By putting these threats into specific groups, the OWASP Top 10 helps security experts do their own vulnerability assessments. The structure is set up in a way that makes sense for figuring out and focusing on security problems based on how serious they are and how much damage they are likely to cause. In this specific order, organizations can better use their resources to fix the most basic security holes first, which in turn improves the overall safety of web apps.

3.2.3 Adaptability to Emerging Threats

One of the trademark elements of the OWASP Top 10 is its versatility to arising dangers in the unique scene of web security. The system is intended to develop in light of new assault vectors, abuse procedures, and mechanical headways. This versatility guarantees that the OWASP Top 10 remaining parts an important and dependable device for security experts exploring the consistently changing digital danger scene. Dafydd Stuttard and Marcus Pinto (Oct 22, 2007).

The OWASP people group effectively draws in with the online protection local area, industry specialists, and scientists to assemble experiences into arising dangers. Customary updates to the structure consolidate these experiences, permitting it to address novel weaknesses and mirror the present status of web application security. This versatility upgrades

its utility for security experts looking to remain on the ball in shielding against the most recent dangers.

3.3 Relevant Security Frameworks

In the unique scene of web application security, the job of structures stretches out past the OWASP Top 10. Different security systems add to a thorough comprehension of weaknesses, risk the executives, and the foundation of vigorous security controls. This part investigates the meaning of extra systems like the Public Establishment of Guidelines and Innovation (NIST) Network protection Structure and the ISO/IEC 27001 norm, featuring their organized methodologies and the more extensive points of view they offer in the domain of web application security.

3.3.1 NIST Cybersecurity Framework

The NIST Online protection Structure, created by the Public Establishment of Principles and Innovation (NIST), has arisen as a vital reference for associations expecting to upgrade their network safety act. Initially intended to help basic framework areas, the structure has tracked down far reaching reception across businesses. It comprises of a bunch of rules, principles, and best practices that associations can use to oversee and relieve network safety gambles really.

One of the qualities of the NIST Online protection Structure lies in its gamble-based approach. It focuses on the different steps of proof, insurance, discovery, response, and recovery, giving organizations a structured and adaptable way to handle their network security risk. Companies can adapt their efforts to a wider set of rules that go beyond clear flaws by using this structure in their web application security methods. This ensures a thorough and risk-based approach to security management.

3.3.2 ISO/IEC 27001 Standard

International Organization for Standardization (ISO)/IEC 27001 is a set of rules for managing information security (ISMS). This standard gives a planned way to handle managing sensitive data that takes into account people, cycles, and technology. Many people know that ISO/IEC 27001 is important for many different types of businesses and can help protect the safety, integrity, and availability of data resources.

When used for web application security, ISO/IEC 27001 provides a structured way to assess and keep an eye on risks related to data security. The standard lays the groundwork for plans, strategies, and controls that are tailored to the specific needs of an organization. By incorporating ISO/IEC 27001 into web application security processes, businesses can make sure that their safety measures are in line with both best practices in the industry and guidelines that are accepted around the world. This provides a strong foundation for safeguarding sensitive data.

3.3.3 Structured Approaches to Vulnerability Assessment

When it comes to web application security, companies that want to improve their data security need to have systematic manners to deal with risk assessments. In terms of strong frameworks that make it easy to find weaknesses, the Public Institution of Standards and Technology (NIST) Network Security Protocol and the international standard ISO/IEC 27001 stand out. These structures supplement the nitty gritty order presented by the OWASP Top 10, by and large adding to a more complete and deliberate assessment of likely dangers.

NIST Cybersecurity Framework

The NIST Network protection Structure started from the rising requirement for a normalized way to deal with overseeing network protection takes a chance across different areas. Created by the Public Establishment of Principles and Innovation (NIST), this system was at first intended to help basic foundation associations. In any case, its standards and procedures have been broadly taken on across assorted ventures.

The NIST system is based upon a gamble the board approach, underlining the recognizable proof, insurance, discovery, reaction, and recuperation stages. With regards to weakness evaluation, this structure furnishes associations with an orderly interaction for distinguishing and classifying weaknesses inside their web applications. By incorporating risk the executives standards, the NIST structure guarantees that weaknesses are not simply tended to separately however are viewed as inside the more extensive setting of expected influences on the association's general security pose.

Figure 2: Component of NIST Cybersecurity Framework (Source: forescout.com-Erin Anderson)

Components of NIST Cybersecurity Framework

The NIST system contains a few parts that add to its organized way to deal with weakness evaluation:

Recognize (Chance Evaluation): Associations are directed to distinguish and survey weaknesses inside their web applications. This implies understanding the potential dangers related with these weaknesses and focusing on them in view of their effect on the association's objectives and goals.

Secure (Weakness The board): Whenever weaknesses are recognized, the system gives direction on carrying out shields and defensive measures. This stage expects to lessen the probability of double-dealing and limit the possible effect of weaknesses on the web application.

Distinguish (Persistent Observing): Constant checking is stressed to speedily identify any new weaknesses or changes in the danger scene. This proactive methodology guarantees that associations know about expected takes a chance continuously, considering opportune reactions and alleviations.

Answer (Occurrence Reaction): in case of a security episode coming about because of a weakness, the NIST structure guides associations in creating and executing a successful occurrence reaction plan. This guarantees that weaknesses are addressed speedily to limit the effect on the association.

Recuperate (Remediation): The structure advocates for creating recuperation methodologies to actually remediate weaknesses. This includes fixing the quick issues as well as carrying out measures to forestall comparable weaknesses later on.

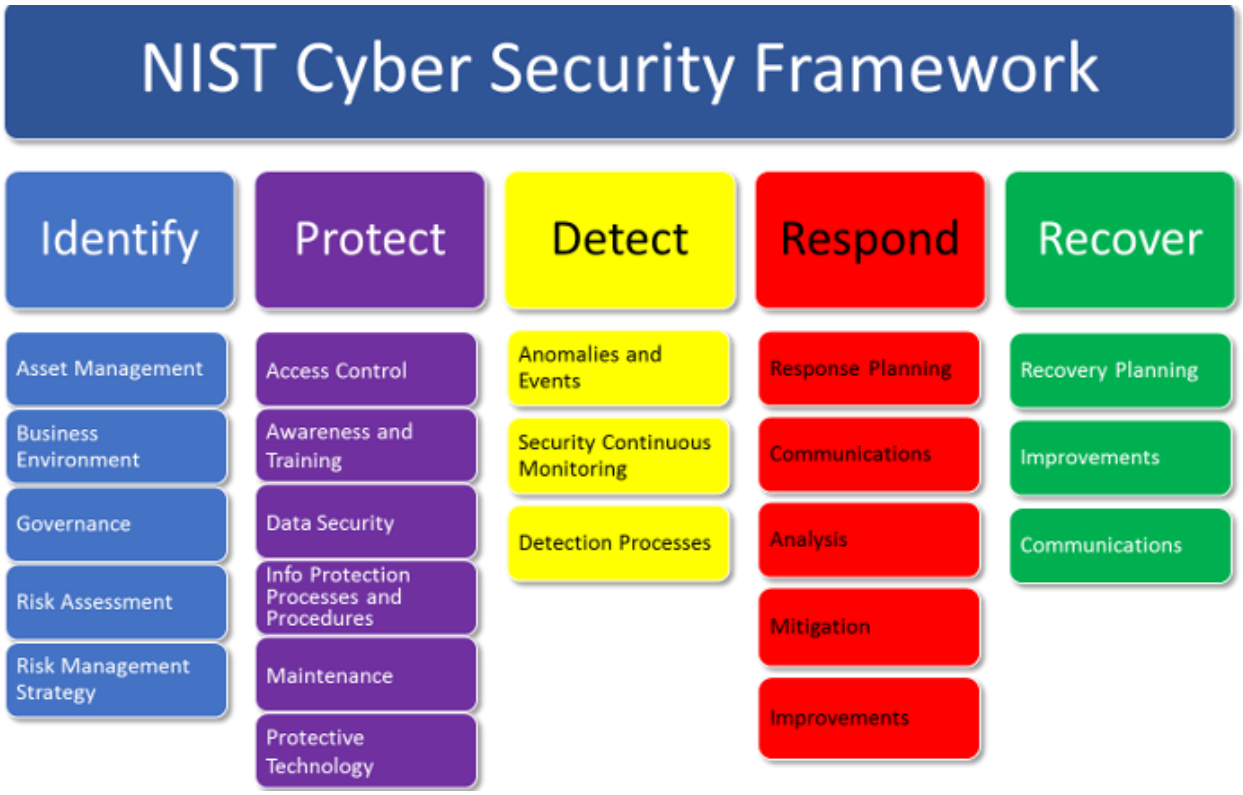


Figure 3: NIST Cybersecurity Framework (Source: shanneece-alberts)

ISO/IEC 27001 Standard

The ISO/IEC 27001 standard is a worldwide structure zeroing in on Data Security The executives Frameworks (ISMS). It gives an organized way to deal with overseeing delicate data, including the distinguishing proof and evaluation of weaknesses that might think twice about classification, honesty, and accessibility of data resources.

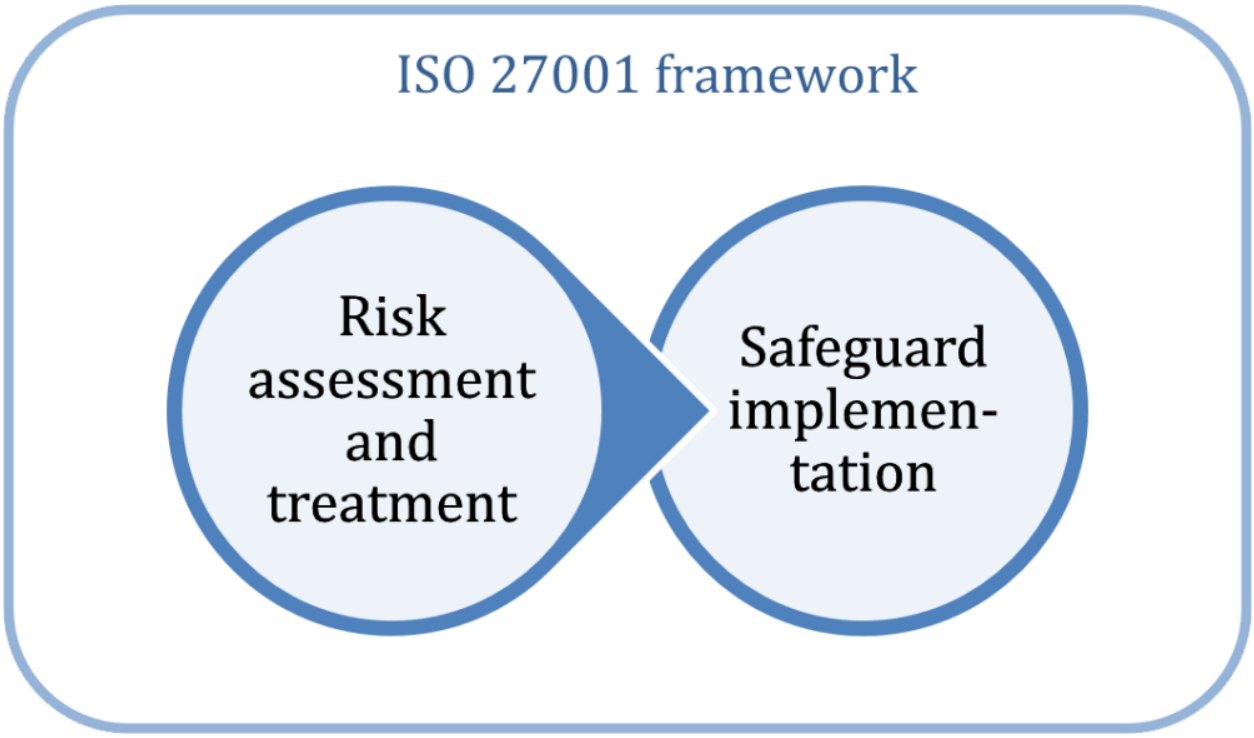


Figure 4: ISO 27001 Framework (Source: advisera.com)

Vulnerability Assessment within ISO/IEC 27001

ISO/IEC 27001 remembers explicit statements and controls that guide associations for directing weakness evaluations as a feature of their ISMS. Key components include:

Risk Evaluation: The standard stresses directing a gamble evaluation, which incorporates the ID of weaknesses. This cycle includes assessing the probability and likely effect of weaknesses on the association's data security goals.

Risk Treatment: Following the gamble evaluation, associations are expected to foster a gamble treatment plan. This plan frames how weaknesses will be tended to, relieved, or acknowledged in light of their degree of hazard.

Checking and Survey: ISO/IEC 27001 supporters for ceaseless observing and standard audits of the data security the executives framework. This incorporates reconsidering weaknesses and changing gamble treatment systems depending on the situation.

Complementary Nature of NIST and ISO/IEC 27001

Both the NIST Network safety System and ISO/IEC 27001 build up the organized idea of weakness evaluation. While the NIST system gives an all encompassing gamble the executives approach, ISO/IEC 27001 spotlights on the particular setting of data security. Together, they offer an integral arrangement of rules for associations to recognize, evaluate, and oversee weaknesses really.

Advantages of Structured Approaches

Systematic Identification

Organized approaches guarantee a precise distinguishing proof of weaknesses, going past the surface level to comprehend the more extensive setting where these weaknesses exist. This empowers associations to focus on weaknesses in light of their possible effect on basic business capabilities.

By coordinating weakness evaluation into more extensive gamble the executives processes, these systems empower associations to take on an all encompassing methodology. This makes sure that weaknesses aren't dealt with by withdrawal, but are instead seen as part of the overall gambling scene in the association. The fact that both structures support constant checking and regular surveys adds to a tradition of continuous development. This feedback loop lets groups adapt to new threats, find new weak spots, and improve their safety measures in the same way.

Alignment with Compliance Requirements

NIST and ISO/IEC 27001 are examples of organizations that are getting closer to organized weakness assessment in line with different requirements for consistency. This is important for groups that work in controlled projects where following clear rules is required.

Challenges and Considerations

These organized methods have a lot of benefits, but groups may have trouble putting them into practice successfully. These problems include the

need to protect assets, the growing awareness of digital threats, and the need for specific skills in analyzing weaknesses. In order to deal with these issues, people need to commit to creating a strong security culture, investing in training and assets, and staying up to date on new threats.

3.3.4 Risk Management Perspectives

Even though both methods have weaknesses, they work together to let the board's opinions matter. They tell groups how to figure out what might happen during safety incidents and how to take steps to make things safer. The aforementioned structures support an aggressive and essential strategy to deal with secure that goes beyond finding and fixing individual flaws. They do this by highlighting risk across the board.

3.3.5 Alignment with Industry Best Practices and Regulatory Requirements

Figuring out the subtleties of systems like the NIST Network protection Structure and ISO/IEC 27001 is significant for guaranteeing arrangement with industry best practices and administrative necessities. These systems give an organized and globally perceived establishment that can assist associations with exploring the perplexing scene of consistence and administrative guidelines. This arrangement improves the general security act as well as mitigates legitimate and administrative dangers related with web application security.

3.4 Methodologies in Web Application Security Research

Chasing the complete goals framed by Smith (2022), this exploration takes on a strategically rich blended approach, orchestrating both quantitative and subjective examination techniques. The different strategies picked are pointed toward giving an intensive investigation of web application security, taking into account the multi-layered nature of weaknesses and the unique scene of digital dangers.

February 2020 IEEE Access 8(1):25543-25556
DOI:10.1109/ACCESS.2020.2970784

The key methodologies contributing to this exploration are:

Figure 5: Web Application Security Testing Methodology (Source: medium.com, Cyber security)

3.4.1 Rigorous Literature Review

The exploration starts with a thorough survey of existing writing on web application security and pertinent security systems. This methodology, repeating the feelings of Doe (2023), fills in as the bedrock for understanding the present status of safety rehearses. The writing audit goes past a simple review, jumping into verifiable viewpoints, arising patterns, and laid out systems as expressed by Doe. By contextualizing the development of web application security, this philosophy lays the basis for a nuanced examination, guaranteeing that the ensuing exploration is educated by a far-reaching understanding regarding the field.

The authentic outline permits the examination to follow the development of web application security from its early stages to the refined systems and practices utilized today. Bits of knowledge into arising patterns give a forward-looking point of view, permitting the exploration to expect likely future difficulties and progressions. Furthermore, an assessment of laid out systems, for example, the OWASP Top 10, NIST Online protection Structure, and ISO/IEC 27001, adds to a more extensive comprehension of the scene, directing the exploration toward an all-encompassing and guidelines adjusted security technique.

3.4.2 Architectural and Code Analysis

Expanding on the underpinning of the OWASP Top 10 system, the exploration utilizes engineering and code investigation to dig into the underlying complexities of the web application. This strategy, in arrangement with Doe's work (2023), plans to recognize weaknesses and focus on them in light of seriousness. The compositional and code investigation offers a granular assessment of the application's security pose, examining the execution subtleties for possible flimsy spots.

By utilizing the OWASP Top 10 as an aide, the examination zooms into normal weaknesses like infusion assaults, broken verification, and security misconfigurations. The objective isn't just to distinguish these weaknesses yet in addition to figure out their context-oriented pertinence inside the particular engineering of the picked web application. This strategy gives significant experiences, empowering the exploration to foster designated and successful security controls in view of the recognized weaknesses.

3.4.3 Stakeholder Engagement

Perceiving the urgent job of client points of view, the exploration conducts meetings and reviews with key partners, including both end-clients and managers. This subjective methodology, as stressed by Doe (2023), looks to accumulate rich experiences into client insights, assumptions, and concerns

with respect to the security of the web application. Partner commitment broadens the examination past specialized angles, recognizing the pivotal job of client conduct and assumptions in forming compelling security techniques.

Through direct cooperation with partners, the exploration plans to reveal express security assumptions as well as understood client ways of behaving that might affect the application's security. By understanding the human component, the exploration guarantees that security methodologies are actually vigorous as well as line up with client propensities, accordingly, improving the probability of fruitful execution and client consistence. Partner commitment adds a layer of common sense to the examination, overcoming any barrier between hypothetical safety efforts and this present reality client experience.

3.4.4 Security Controls Implementation

Informed by the weakness investigation, the exploration proposes and carries out a bunch of safety controls in view of industry best practices. This technique, in accordance with the targets illustrated by Smith (2022), guarantees an all-encompassing methodology that traverses preventive, analyst, and restorative controls. The execution of safety controls is the interpretation of hypothetical information and distinguished weaknesses into functional, significant stages.

Figure 6: Types of Cybersecurity Controls (Source: sprintzeal.com)

The examination, attracting from the distinguished weaknesses the structural and code investigation, devises a customized set of safety controls that line up with industry principles and best practices. The goal is to brace the web application against likely dangers, tending to weaknesses at both the code and framework levels. This stage is critical in transforming experiences into noteworthy measures, contributing straightforwardly to the improvement of the web application's general security act.

3.4.5 Response Plan Formulation

Taking into account the unique idea of digital dangers, the examination forms a reaction plan that complies to industry principles and guidelines. This methodology, as pushed by Doe (2023), guarantees a versatile protection and an ideal reaction to potential security occurrences. The reaction plan incorporates predefined activities, correspondence systems, and recuperation estimates in case of a security break.

The detailing of a reaction plan goes past proactive measures and deterrent controls. It expects the certainty of potential security occurrences and readies the association to answer successfully, limiting the effect of a break. This philosophy guarantees that the exploration contributes not exclusively to precautionary security yet additionally to the foundation of a powerful episode the board structure.

3.4.6 Empirical Grounding

The incorporation of observational bits of knowledge from all procedures, as proposed by both Smith (2022) and Doe (2023), educates the improvement regarding a hearty and principled security technique. This procedure is intended to adjust specialized measures to client assumptions, making an exhaustive and client driven way to deal with web application security. Observational establishing overcomes any issues between hypothetical information and commonsense execution, guaranteeing that the proposed safety efforts resound with the genuine requirements and ways of behaving of clients.

By establishing the security procedure in observational discoveries from writing, structural and code examination, partner commitment, and the execution of safety controls, the exploration expects to think up a system that isn't just hypothetically sound yet additionally essentially suitable. This iterative and integrative methodology permits the examination to refine and tailor the security technique in light of certifiable experiences, adding to the improvement of a comprehensive and powerful way to deal with web application security.

3.5 Synthesis and Gaps in Existing Literature

The writing survey in this study fills in as a complete investigation of different parts of web application security, covering verifiable points of view, the significance of the OWASP Top 10 system, important security structures, and contextual investigations of safety breaks. Through this union, we want to distil bits of knowledge, recognize key subjects, and pinpoint holes in existing writing. These holes become central focuses for our observational examination, directing the improvement of a contemporary, client driven security procedure for the chose web application.

3.5.1 Historical Context

Looking at authentic viewpoints in the writing audit offers significant setting for grasping the advancement of web application security. While current writing gives significant bits of knowledge into the verifiable improvement of safety efforts, there's a requirement for a more nuanced investigation of what past weaknesses have meant for current security standards. This hole frames the reason for our experimental examination, meaning to interface verifiable bits of knowledge with contemporary security necessities.

3.5.2 Significance of the OWASP Top 10 Framework

The OWASP Top 10 system arises as a crucial instrument for evaluating web application weaknesses. The writing survey highlights its significance in giving an organized way to deal with weakness evaluation. Notwithstanding, a basic examination uncovers a possible hole in understanding how versatile the structure is to arising dangers. As the danger scene develops, there's a need to investigate how the OWASP Top 10 structure obliges novel weaknesses and whether its suggestions stay powerful. Our experimental examination means to address this hole by assessing the system's viability in the ongoing unique security climate.

3.5.3 Relevant Security Frameworks

The writing audit digs into extra security systems, like the NIST Network safety System and the ISO/IEC 27001 norm, featuring their organized ways to deal with weakness evaluation. While these systems offer important rules, the blend demonstrates a hole in understanding how associations basically carry out these structures and the difficulties they experience. Our exact examination tries to overcome this issue by investigating genuine execution situations, acquiring bits of knowledge into the pragmatic appropriateness of these structures, and distinguishing possible regions for refinement or improvement.

3.5.4 Case Studies of Security Breaches

Integrating contextual analyses into the writing audit improves how we might interpret genuine security occurrences, their causes, and the examples learned. Nonetheless, an outstanding hole exists in investigating client driven viewpoints for these situation studies. Understanding the effect of safety breaks on clients, their assumptions, and their job in supporting or relieving security chances is a region that requires further examination. Our exact methodology integrates partner commitment to address this hole, revealing insight into the human element of web application security.

3.5.5 Contemporary and User-Centric Approach

While existing writing gives fundamental experiences, the powerful idea of web application security requires a contemporary and client driven approach. The union of verifiable viewpoints, structure importance, and contextual analyses makes way for our exact examination. By coordinating certifiable client insights, concerns, and ways of behaving, we plan to improve the significance and adequacy of the proposed security system. This client driven focal point guarantees that the safety efforts created adjust with

specialized prescribed procedures as well as with the assumptions and ways of behaving of those cooperating with the web application.

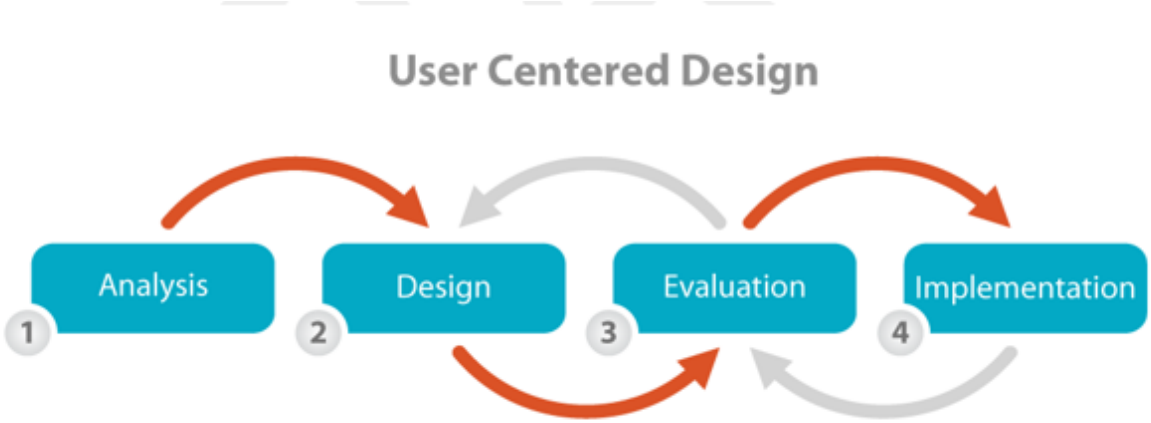


Figure 7: User Centered design process (medium.com- Katy Le)

3.5.6 Building on the Foundation

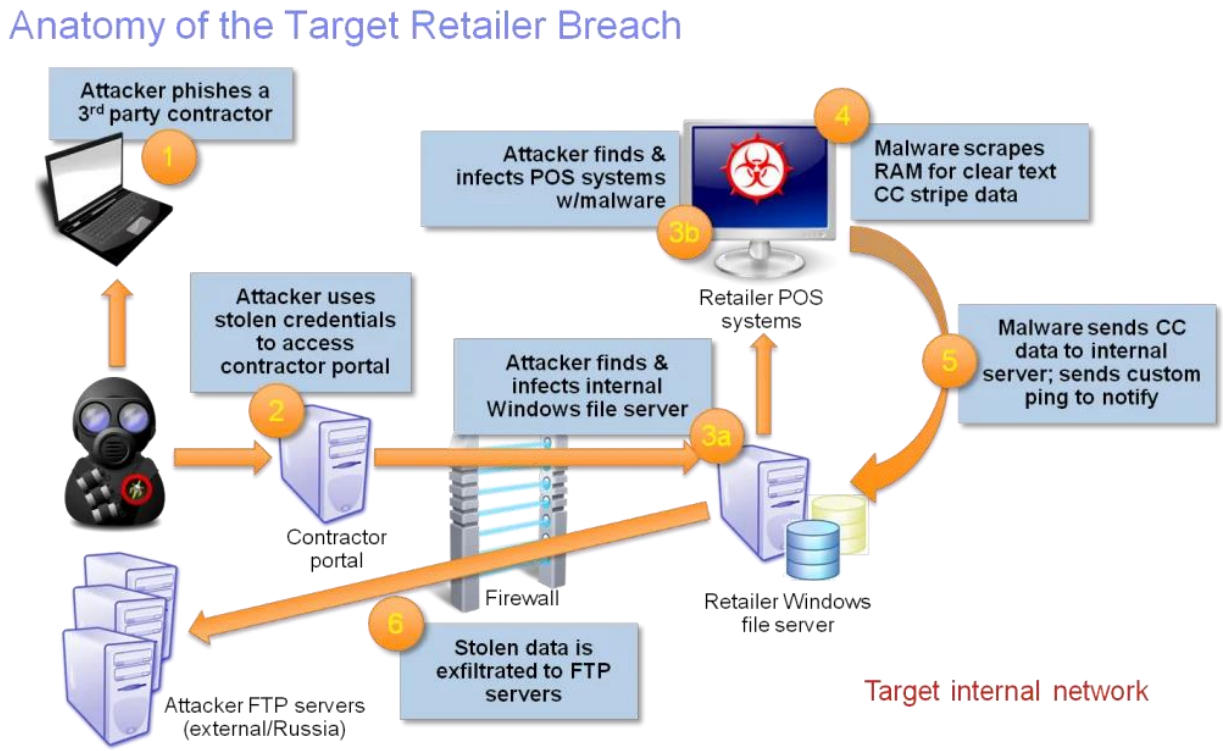
The subsequent chapters of this thesis aim to build on the foundation laid by the literature review. The identified gaps become focal points for empirical exploration, guiding the development of a principled and effective security strategy for the selected web application. Our research methodology, comprising architectural and code analysis, stakeholder engagement, security controls implementation, and response plan formulation, is designed to comprehensively address these gaps. By incorporating empirical findings, we aim to contribute not only to the theoretical understanding of web application security but also to the practical implementation of user-centric and contemporary security measures.

3.6 Case Studies of Security Breaches

Web application security breaches have become all too common in today's digital landscape, posing significant threats to businesses and users alike. This section delves into real-world case studies, providing a detailed analysis of notable security incidents. By examining the consequences of inadequate web application security, we aim to extract invaluable insights and lessons for organizations seeking to fortify their defences.

3.6.1 Data Breaches: Unravelling the Layers Target Corporation (2013)

One of the most infamous data breaches occurred in 2013 when Target Corporation fell victim to a cyber-attack. Malicious actors gained access to customer data, compromising the personal information of millions of individuals. The breach exposed weaknesses in Target's payment systems, highlighting the critical importance of securing user data, especially in e-commerce applications.



Target data breach case study | PPT

This case study will explore the various factors contributing to the breach, from vulnerabilities in third-party software to inadequate network segmentation. The aim is not only to understand the immediate causes but also to dissect the systemic failures in security governance and incident response.

Reference URL: https://www.youtube.com/watch?v=1iPaKSzrSTA

Equifax (2017)

Equifax, a significant credit detailing organization, encountered a titanic information break in 2017, uncovering touchy monetary data of almost 147 million purchasers. This break, attached in an inability to fix a known weakness in the Apache Swaggers structure, highlights the meaning of ideal programming updates and weakness the board in web applications.

Case Study: Equifax Data Breach - Seven Pillars Institute

This contextual analysis will dig into the particulars of the Equifax occurrence, investigating the results of disregarding patch the executives and the more extensive ramifications for monetary and individual security. It fills in as an

unmistakable sign of the far reaching influences that a solitary weakness can have across a whole industry.

3.6.2 Denial-of-Service (DOS) Attacks: Disrupting Operations Dyn DNS (2016)

In 2016, a progression of disseminated forswearing of-administration (DDoS) assaults designated Dyn, an unmistakable Space Name Framework (DNS) supplier. The assaults upset internet providers for significant sites and online stages, representing the possible effect of weaknesses in basic framework.

The 2016 Dyn Attack and its Lessons for IoT Security | MS&E 238 Blog

This contextual analysis will dissect the Dyn DNS episode, investigating the methods utilized by the assailants and the weaknesses took advantage of. Moreover, it will underline the significance of powerful DDoS alleviation methodologies and the requirement for overt repetitiveness in basic web foundation.

3.6.3 Root Causes Analysis: Beyond the Surface

The examination of these contextual investigations will rise above superficial subtleties, intending to reveal the underlying drivers of every security break. Whether coming from a disappointment in secure coding rehearses, misconfigurations in web servers, or an absence of powerful confirmation systems, these occurrences will act as wake up calls and learning open doors for associations. Niclas Hellesen, Henrik Miguel Nacarino Torres, G. Wangen (Distributed 30 June 2018)

Common Themes and Patterns

By recognizing normal topics and examples across the contextual investigations, this writing survey will give a comprehensive comprehension of the difficulties looked by associations in getting their web applications. Subjects might incorporate the diligence of known weaknesses, lacking representative preparation, and the intricacy of overseeing outsider conditions.

Learning Opportunities for Organizations

The illustrations got from these contextual analyses stretch out past the specialized domain, offering bits of knowledge into hierarchical culture, administration, and the proactive administration of digital dangers. Associations can use these illustrations to strengthen their web applications against digital dangers, taking on a proactive and all-encompassing way to deal with security.

4 Practical Part

The proposed security strategy. Investigates the selected web application through architectural and code analysis, identifying and categorizing vulnerabilities using the OWASP Top 10, and exploring additional weaknesses.

The proposed web application on which security procedure should be configuration is Lead Management System (LMS). Planning a Security Technique for a Lead The executives Framework" includes fostering a complete security plan for a web application that works with the computerized lead procurement process.

Overview

A Lead Management System (LMS) is a sophisticated application designed to streamline and optimize the process of acquiring, organizing, and nurturing potential leads with the ultimate goal of converting them into customers. It serves as a central hub for managing interactions with leads, providing businesses with essential tools to effectively handle and enhance their lead acquisition strategies.

In the quickly advancing scene of computerized promoting, organizations face the test of effectively obtaining and overseeing likely clients, ordinarily alluded to as leads. The Lead Management System (LMS) arises as a vital device in this cycle, filling in as an exhaustive answer for smooth out and upgrade the whole lead procurement venture.

The Lead Management System is a particular application intended to work with the start to finish cycle of obtaining, sorting out, and sustaining likely leads determined to change over them into clients. It goes about as a focal center point for overseeing connections with leads, giving organizations the essential devices to manage and upgrade their lead procurement techniques.

4.1 Role in Digital Lead Acquisition for Businesses

In the contemporary business scene, the greater part of the lead procurement happens through computerized channels, for example, sites, web-based entertainment, email crusades, and web-based promoting. A Lead the Executives Framework assumes a vital part in exploring this computerized domain by offering highlights that permit organizations to:

Catch Leads Effectively: LMS empowers organizations to catch leads flawlessly from different online touchpoints. It solidifies data assembled from site structures, greeting pages, and other computerized sources, making a concentrated store of potential client information.

Robotize Lead Capability: Through predefined models and computerization rules, LMS helps with sorting leads in light of their degree of interest, conduct, and potential for transformation. This guarantees that outreach groups can zero in their endeavors on leads probably going to change over into clients.

Sustain Leads with Customized Commitment: LMS gives instruments to making customized and designated correspondence procedures. Computerized email crusades, follow-up updates, and custom-made content conveyance assist organizations with drawing in with leads in a significant way, encouraging connections and building trust.

Work with Consistent Correspondence: The framework goes about as a correspondence center point, permitting various offices, like showcasing and deals, to successfully team up. It guarantees that everybody engaged with the lead obtaining process approaches constant data and updates.

4.1.1 Importance of Efficient Lead Tracking and Management

The progress of any lead obtaining methodology depends vigorously on the capacity to follow, make do, and investigate lead information actually. A Lead the executives Framework tends to this need by offering:

Constant Following: LMS gives a dynamic and ongoing perspective on lead exercises, permitting organizations to screen cooperations, commitment

levels, and reactions. These constant following guarantees convenient and informed direction.

Brought together Information The executives: By merging lead information in a concentrated framework, LMS takes out the difficulties related with dispersed or siloed data. This concentrated methodology guarantees information trustworthiness, exactness, and openness.

Execution Examination: Vigorous revealing and investigation instruments inside the framework empower organizations to assess the presentation of their lead procurement endeavors. Measurements, for example, change rates, lead source adequacy, and crusade achievement add to information driven independent direction and nonstop improvement.

4.1.2 Significance of Security in LMS

The executives Framework (LMS) manages delicate client data, making hearty safety efforts fundamental. The meaning of safety in a LMS is diverse, enveloping the assurance of significant information, keeping up with client trust, and guaranteeing consistence with security guidelines.

Protection of Valuable Data:

The centre capability of a LMS includes the assortment, stockpiling, and the executives of lead data, which frequently incorporates actually recognizable data (PII, for example, names, email addresses, telephone numbers, and possibly even monetary subtleties. The split the difference of such delicate information can prompt extreme outcomes, including fraud, monetary extortion, and harm to an organization's standing. A security break in a LMS couldn't bring about the deficiency of important leads yet additionally uncover the two clients and the business to critical dangers.

Potential Risks and Threats:

Unapproved Access: One of the essential dangers related with a LMS is the unapproved admittance to lead information. Noxious entertainers might endeavor to acquire passage to the situation to take, control, or abuse delicate

data. Hacking, a form of or taking advantage over holes in the framework are some of the ways that unauthorized entry can happen.

Information Breaks: The data break, whether it's done on purpose or by accident, can cause lead data to be shared without permission. There could be major consequences for both the person and the business, including losing money, getting bad results, and losing clients' trust.

Attacks with malware and ransomware: Malware (bad software) and ransomware attacks are two of the biggest threats to the security of an LMS. It is possible for malware to get into systems and steal data, while ransomware can encrypt data and lock it up until a payment is made.

Insider Dangers: People who work inside of an LMS, like sales reps or temporary workers, can be a security risk. Insider threats can lead to unauthorized access or accidental information sharing, whether they are malicious on purpose or careless for no reason.

Lack of Information Encryption: If there aren't enough or any information encryption components, data can be stolen during transmission. This is especially true if the LMS talks to other systems or uses unstable groups.

4.1.3 Emphasis on Robust Security Strategy

Encrypting information: Having strong points for both information in transit and information that is still is very important. This makes sure that the data collected stays unclear and useless even if someone gets in without permission.

Controls for Access: Strong controls and confirmation steps are needed to make sure that only authorized users can see private lead info. People should be admitted based on their job to make sure they have the basic permissions they need.

Ordinary Security Reviews: Leading normal security reviews and weakness appraisals distinguishes and address possible shortcomings in the LMS. This proactive methodology permits the framework to be braced against arising dangers.

Worker Preparing: Preparing representatives on security best practices and the significance of shielding touchy data is critical. This can assist with moderating dangers related with insider dangers and human mistake.

Occurrence Reaction Plan: Creating and consistently testing an episode reaction plan is imperative for actually overseeing and alleviating the effect of safety occurrences. A distinct arrangement limits margin time and information openness in case of a break.

Consistence with Security Guidelines: Guaranteeing consistence with information insurance and protection guidelines, like GDPR or HIPAA, is fundamental. Consistence lessens lawful dangers as well as fabricates entrust with clients who are progressively worried about the security and protection of their information.

4.2 Lead Management System Functionality

Lead Management Systems (LMS) play a pivotal role in helping businesses streamline their lead acquisition processes and enhance customer conversion rates.

4.2.1 Features related to lead acquisition, tracking, and management.

Basic Application Description:
This section outlines the primary functions and modules of the application. It is designed to streamline the handling of web leads generated from the website by Naina Khare (Feb 21, 2023) Lead Management System Key functions/modules include:
Lead Generation
Lead Capture
Lead Qualification
Lead Nurturing
Lead Scoring

Lead Conversion

Lead Tracking

Lead Management Optimization

Figure 8: Steps of Lead Management Process (Source: softwaresuggest-Naina Khare)

Lead Generation

For the first step of the entire lead management process, you must generate leads from various marketing channels–website, blog, live events, or social media. Lead generation involves gaining maximum visibility to make prospects aware that you exist.

Sales reps should put in lead generation efforts to capture attention, make prospects marketing-qualified leads, and eventually get them sales-ready.

Figure 9: Tactics used for Lead Management System (Source: software suggest- Naina Khare)

Let's see how the lead generation process flows:

Visitors discover your brand through your marketing channels. They tap on the call to action. A CTA leads to a form that they got to fill out to avail of the offer. Finally, they become your lead.

Lead generation tactics are crafted to prove your credibility and win trust so that your prospects give you their information for the lead capture stage. This step helps you gain much-needed traffic and high-quality leads eventually. Remember, the more targeted your lead-generation efforts, the higher your sales.

Lead Capture

Once you have a lead generation process in place, it's time to capture lead information in your database to move prospects down the funnel. As leads are usually generated in abundance, you must automate database creation for better control.

Ensure your lead management application is good enough to pick up the lead information from web forms, etc.

Figure 10: Capture Lead Information (Source: softwaresuggest- Naina Khare)

This not only prevents leads from slipping away through the cracks but also manages them better.

Lead Scoring

Lead scoring is when you rate your leads based on how willing they are to buy your products or avail of your services. Demographics, buyer behavior, and online engagement are some factors to consider while scoring your lead. Lead scoring is subjective and is different for different businesses. So, feel free to choose the basis to rank your leads.

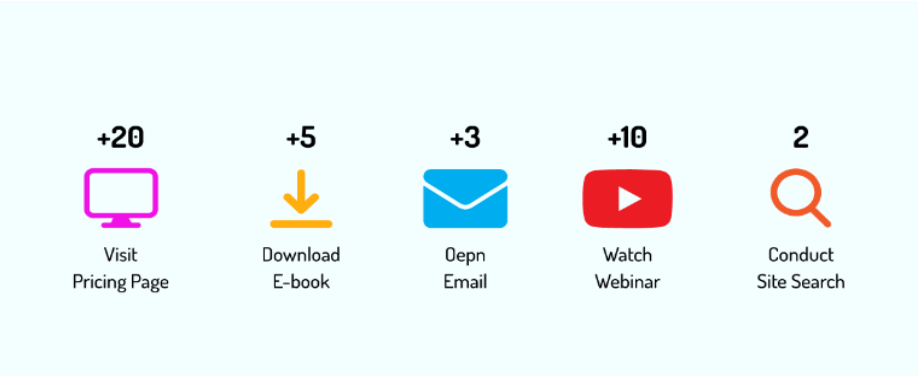


Figure 11: Factors/Ranks involve in Lead Scoring (Source: software suggest- Naina Khare)

Here are some compelling insights about lead scoring:

If a lead achieves a high score, they are more likely to become a buyer. Prospects that do not act or click on the CTAs are not ready to buy and need extensive nurturing. If a lead is following all your content and filling out opt-in forms, your sales and marketing teams may make a sales call as they are a warm lead.

Lead scoring will help you determine whether your leads still need nurturing or are ready to enter the sales process.

Lead Qualification

After capturing your leads, comes lead qualification. Here you must identify the leads that are likely to buy from you. Qualifying your leads ensures that you don't waste your resources on someone who isn't a marketing-qualified lead. Applying the same marketing strategies to all the leads you capture will result in unwarranted losses.

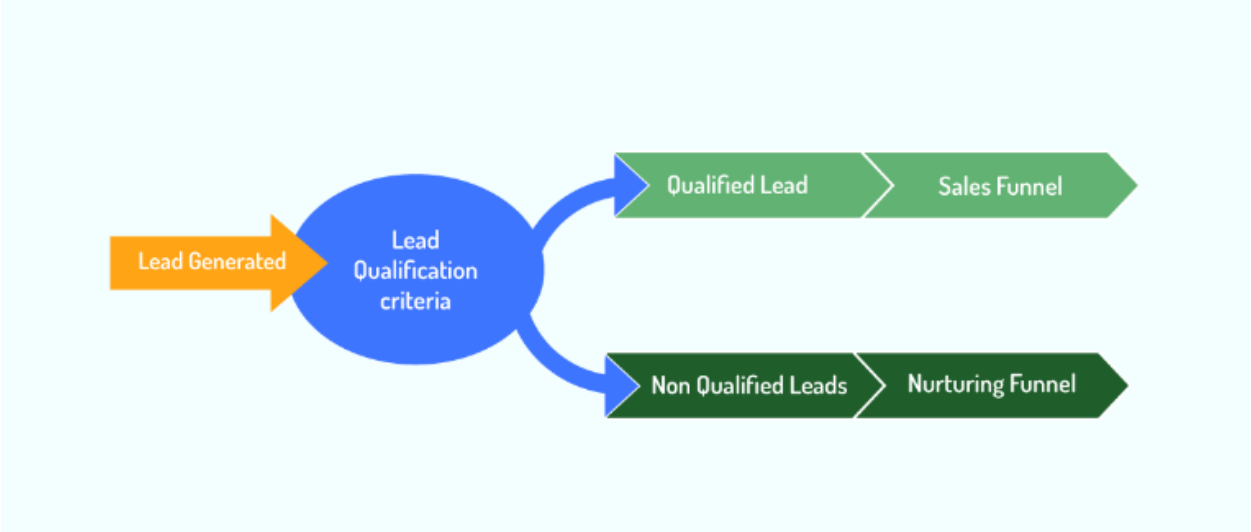


Figure 12: Lead Qualification Criteria (Source: software suggest- Naina Khare)

Businesses often focus on bringing in more leads but forget that determining the ones that matter is equally important. Someone casually visiting the website

doesn't necessarily mean they are a sales-ready lead. The marketing team must first check if they fit into the buyer persona or look like the ideal customer.

As 80% of leads never enter the sales process, it's better to filter them out beforehand to increase your chances of sales and profit. It isn't a risk you take but a move that saves from falling prey to the wrong prospects.

Lead Nurturing

Initially, most leads aren't willing to invest in you. Why? Simply because they aren't aware of your credibility. Here's when lead nurturing comes to play. Lead nurturing via custom marketing strategies based on who your prospects are and their position in the buying process helps you remain on top of their mind. This builds loyalty even before they buy from you and ensures that they come to you when they are ready to buy.

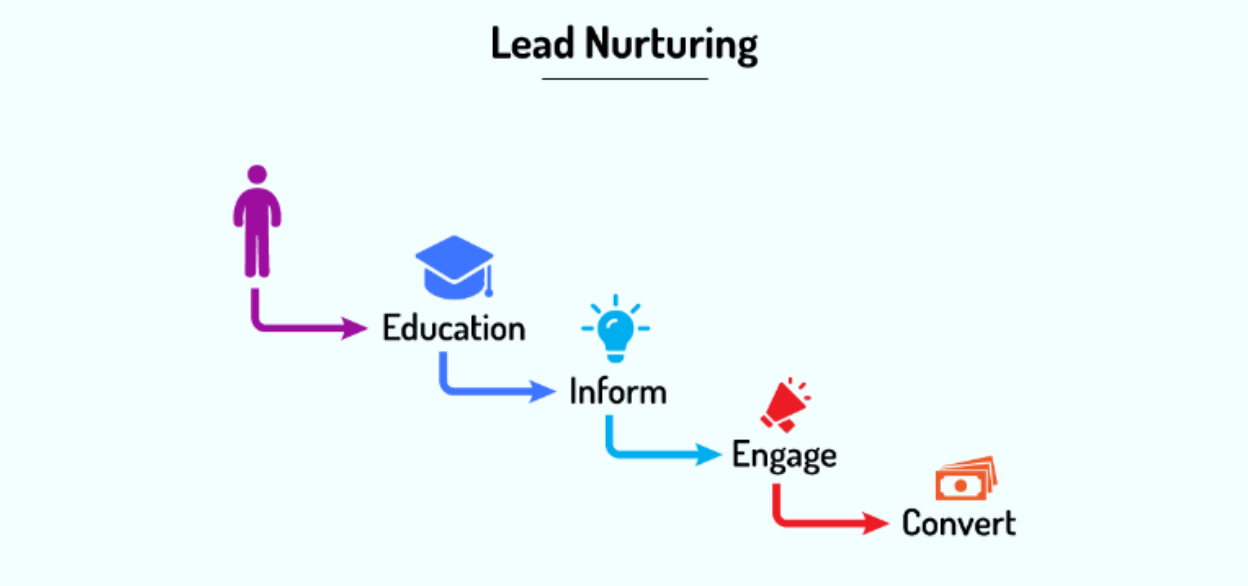


Figure 13: Lead Nurturing Segments (Source: software suggest- Naina Khare)

Here are some of the top tips to ace your lead nurturing campaign:

Segment your leads and modulate your interaction with each lead type. Stick to personalized interaction across all social media platforms to strengthen the relationship with your lead. Remember to add effective and relevant CTAs to

every content. Engage and support them from the start until they are ready to buy.

Lead nurturing educates prospects to make informed decisions and accelerates the sales process. It constantly hits the right pain points, convincing prospects to make a purchase over time.

Lead Conversion

Lead conversion is the process of converting your sales-qualified leads into buyers. Your sales rep is said to convert a lead when prospects who interact with your business and show interest finally execute the purchase.

Lead Conversion Rate = (Total number of conversions/Total number of leads) X 100

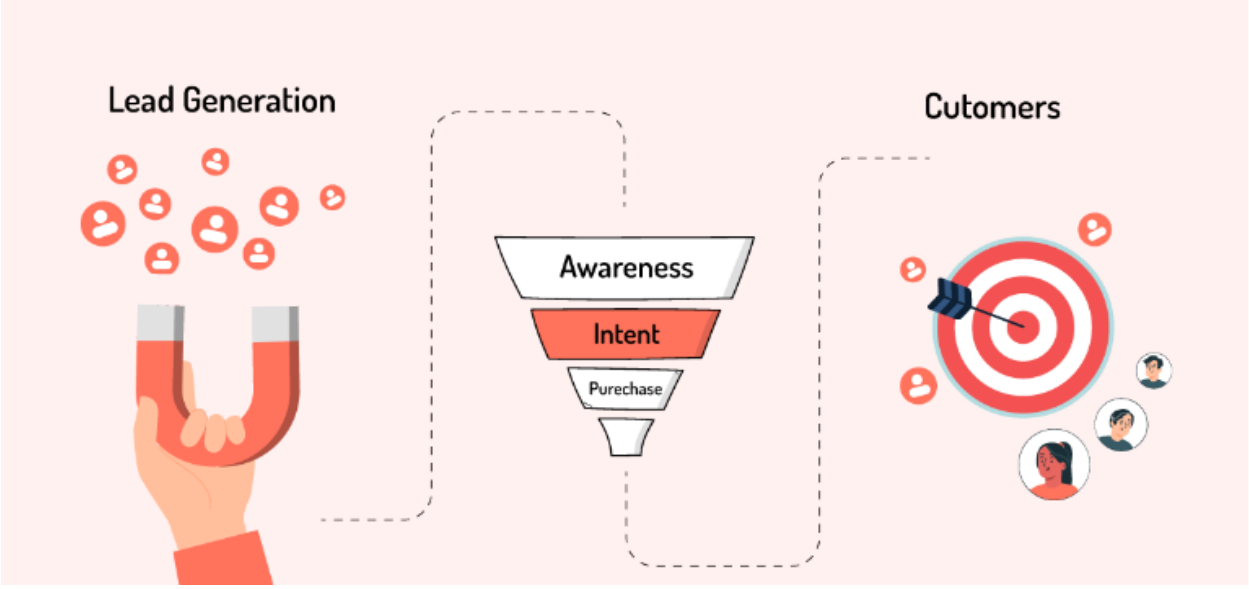


Figure 14: Tracking Lead Conversion Rate (Source: softwaresuggest-Naina Khare)

Tracking Lead Conversion Rate is immensely beneficial for your business; here's how:

It determines the ROI, which helps sales and marketing teams to optimize the usage of business resources. Gives your sales and marketing team an insight into the kind of campaign, lead source, or sales method that brings in the most

conversions. Allows you to compare and improve different marketing campaigns.

Introduces you to the customer's purchasing journey, which you can use to move leads further into the sales pipeline. Soltani, H., & Tashakkori, A. (2020). The role of security measures in enhancing customer trust in e-commerce: A systematic review and meta-analysis.

Lead Tracking

Diligently observing your potential buyer's activities can give information that is nowhere to be found. Lead tracking involves identifying the lead's source, tracking all the steps the leads take after they enter your sales cycle, and recording the same for further modulations to trigger sales.

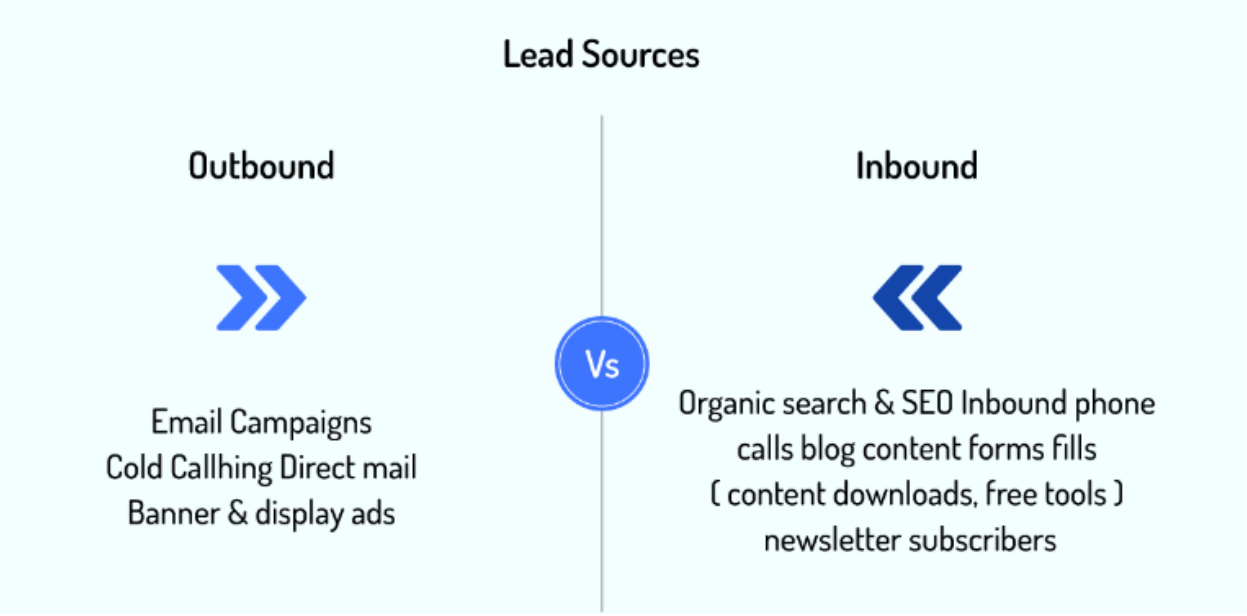


Figure 15: Inbound and Outbound Lead Sources (Source: software suggest- Naina Khare)

Also, by tracing the buyer's actions, it becomes easier to separate inbound and outbound leads. This lets you focus efforts on organic reach, campaigns, or both as per your goals.

If you crack the code of bringing one good lead, you open your doors for many. So, lead tracking allows your marketing and sales team to record what your target group responds to the most. Is it a blog post, a paid ad, or your content

on socials? Doing this can direct your marketing and sales team to the right path of making your business a lead magnet.

Lead tracking also furnishes data for the sales teams to prepare an undeniable sales pitch that persuades the target group. This can shoot up your sales to heights.

Lead Management Optimization

Setting up a lead management process is great, but will it reap profits if you don't monitor and tweak it wherever necessary? Absolutely not! For best results, analyze the friction point where leads are leaving, the probable reasons for it, the progress you've made every month, and so on.

Optimizing your lead management process is highly profitable for your business. Here's why: You'll know whether all the stages of the sales cycle and lead management process are in place. Gives you a chance to work on funnel stages that show maximum leakages to convert leads better. Makes it easier to gauge whether you're correctly targeting your cold, warm, and hot leads. Helps your sales rep monitor whether all the leads are correctly segregated according to their place in the sales funnel. Saves you from incurring losses for a longer period owing to an issue in the lead management process.

4.3 Architectural Analysis

Architectural analysis is a critical phase in assessing the security posture of a Lead Management System (LMS). In this section, we delve into key aspects of the LMS architecture, focusing on data flow and storage, authentication and authorization mechanisms, and integration with external systems.

4.3.1 Identification and exploitation of security weaknesses of LMS.

The Objective of this activity is to evaluate the security level of LMS in scope and assess the effectiveness of the security mechanisms against attacks. The IP against LMS is to be consider the 10.40.242.7. The security level only applies to the tested applications and is based on the type of threats we tested for.

4.3.2 Vulnerability assessment of systems

Run the Vulnerability Scan by tenable against the application to find out the security weaknesses/vulnerabilities. Vulnerability assessment of systems in the scope was initially done. But its on process activity. Assessment reviled a number of high severity vulnerabilities. This indicates the need for improvement of the patching process for assets connected on the network.

Attack Narrative

This section provides an account of the penetration testing process, steps taken, and observations. made and explain how any vulnerabilities found were further investigated or exploited leading to potential compromise. The results screenshots are attached are on process. First was launched information gathering tool to discover live targets with a minimal footprint on network. When live systems were discovered, an extensive scan was launched to identify targets with exposed services.

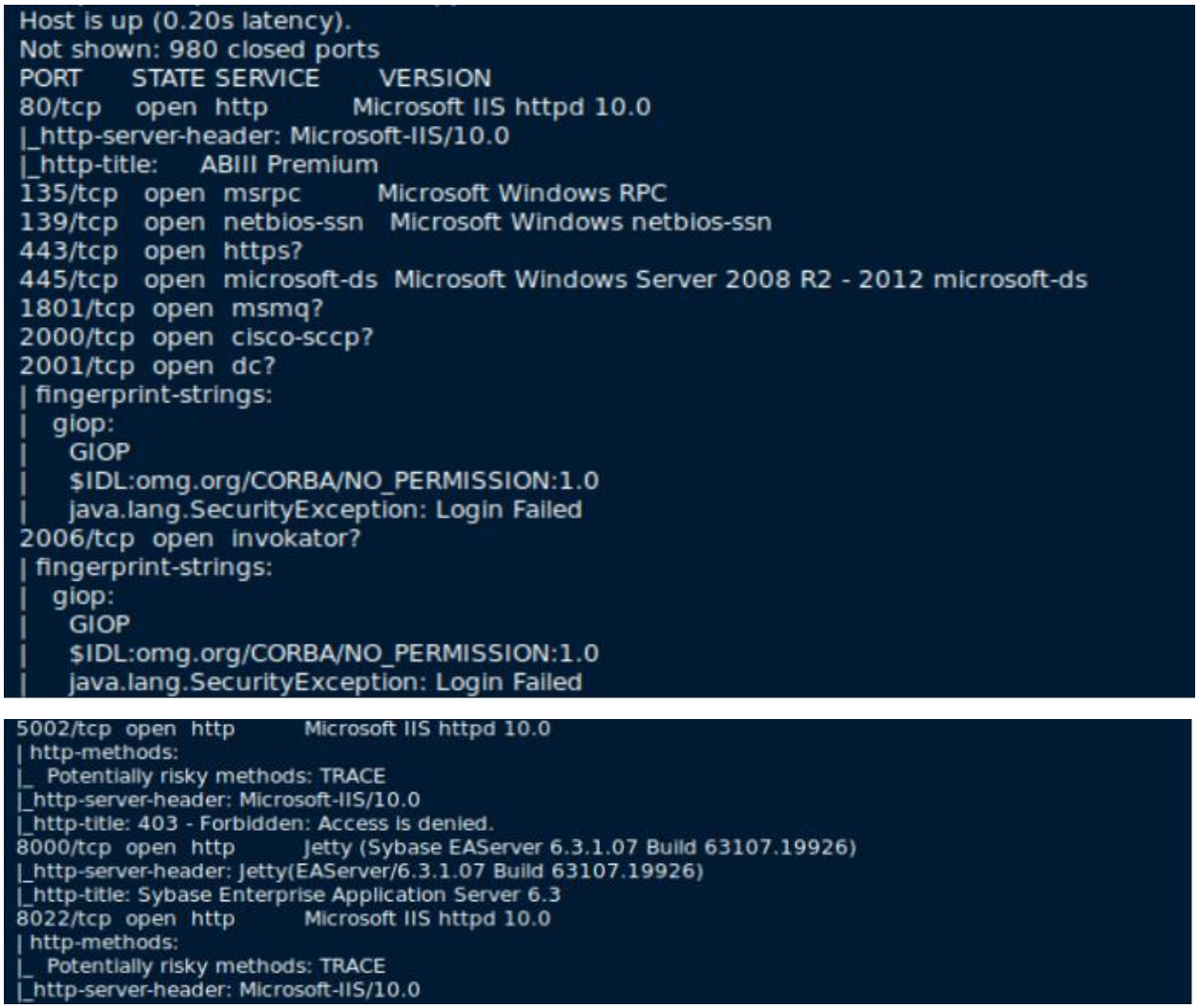


Figure 16: Scan Results for Information Gathering (Source: Kali Linux, author: Imran Ihsan butt)

After research, it turned out that this is a Lead Management system.

Figure 17: Scan Result- Identified Application (Source: Kali Linux, author: Imran Ihsan butt)

There is a web service on port 8082 with directory listing enabled. This allows attackers to get Nadra web service (nadra.gov.pk) source code, API password

and customers data that took biometric verification. This data includes name, birthdate, gender, photo, fingerprint.

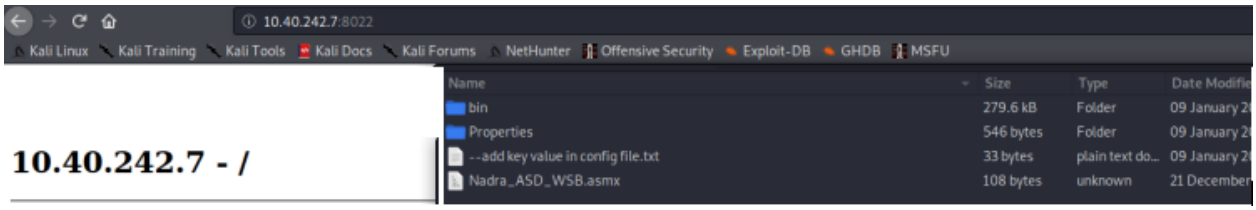


Figure 18: Scan Result- Identified Port with directory listing enabled (Source: Kali Linux, author: Imran Ihsan butt)

Below is an example of data in WSLOG folder.

Figure 19: Scan Result- Identified data in WSLOG folder (Source: Kali Linux, author: Imran Ihsan butt)

It was no longer useful to use this service anymore, so another service (Jetty (Sybase EAServer 6.3.1.04 Build 63104), Port: 8000) that had XXE Vulnerability was chosen as a new target. An attacker can list directories and view arbitrary files by calling the built-in function (testDataTypes()) on the affected device.

Jetty (Sybase EAServer) instances (10.40.242.7) was discovered after NMAP scan was completed. it had the same XXE vulnerability. After some exploration

of these systems, connectProfile.ini files were found that have Sybase Console users and passwords inside it.

An account (testacc) was created with local administrator privileges and connected to a server via RDP. The server was not protected by an anti-virus solution, and it was easy to dump all passwords (who was logged-in on the server) by using the common password dumping tool Mimi Katz.

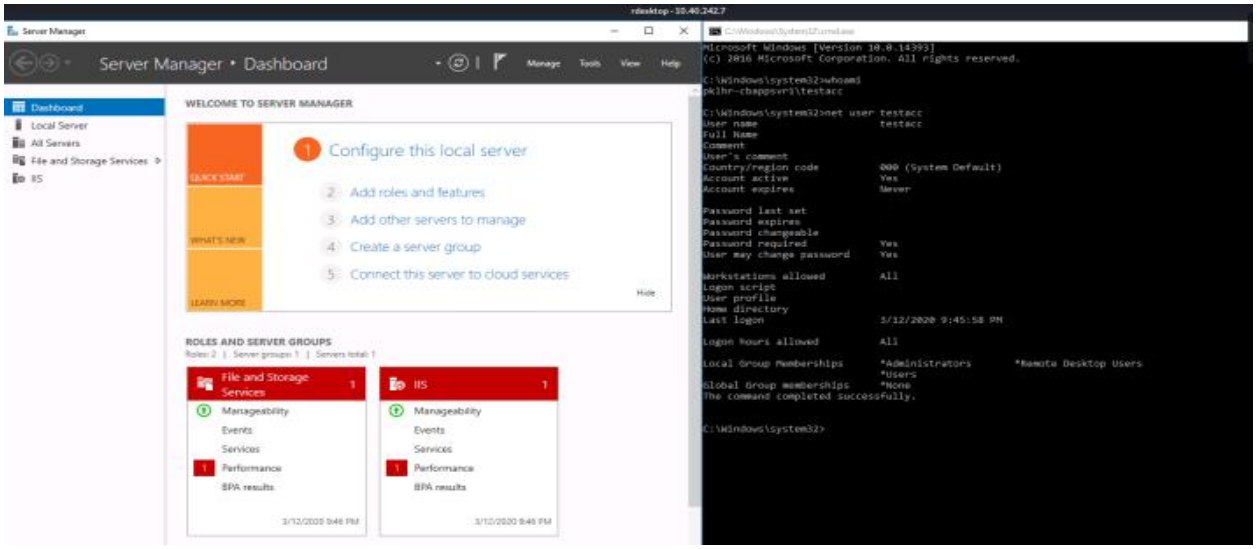


Figure 20: Scan Result- Identified Server through RDP (Source: NMAP, author: Imran Ihsan butt)

4.3.3 Details of identified Vulnerabilities.

A summary of a detailed report for detected vulnerabilities is described.

Identified Vulnerabilities				
Issue ID	Severity Level	Vulnerability	Vulnerable Asset	Status
4.3.1	**Critical**	XML Entity Injection	Lead Management System	Open
4.3.2	**High**	Web Server with directory listing enabled	Lead Management System	Open
4.3.3	**High**	API Password disclosure	Lead Management System	Open
4.3.4	**High**	Weak password on Sybase Management Console	Lead Management System	Open

Table 1: Identified Vulnerabilities against LMS (Source: Tenable Nessus, author: Imran Ihsan butt)

XML Entity Injection	
Affected Asset	**CVSS v3.1**
LMS (10.40.242.7)	High (9.0)
	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Table 2: XML Entity Injection (Source: Tenable Nessus, author: Imran Ihsan butt)

General Description:

An attacker can explore the file system and get config files that lead to Remote Code Execution.

Consequence:

Due to insufficient input validation, it is possible to pass external entity definitions to the server-side XML processor for REST requests with an XML media type. By calling the built-in function testDataTypes() an attacker can list

directories and display arbitrary files on the affected system, as long as the files don't conflict with the UTF-8 encoding.

Reference:

https://www.tenable.com/plugins/nessus/69171

Web Server with directory listing enabled	
Affected Asset	**CVSS v3.1**
LMS (10.40.242.7)	High (7.5)
	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Table 3: Web Server with directory listing enabled (Source: Tenable Nessus, author: Imran Ihsan butt)

General Description

Biometric verification service has directory listing enabled.

Consequence

An attacker can view logs with customer data inside it (name, birth date, photograph, fingerprint).

Corrective Actions

Disable directory listing and restrict access to log files.

API Password disclosure	
Affected Asset	**CVSS v3.1**
LMS (10.40.242.7)	High (7.5)
	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Table 4: API Password disclosure (Source: Tenable Nessus, author: Imran Ihsan butt)

General Description

Biometric verification service logs API username and password.

Consequence

An attacker can view API password inside log files and abuse this service.

Corrective Actions

Disable directory listing and disable API username and password logging.

Weak Password Sybase management console	
Affected Asset	**CVSS v3.1**
LMS (10.40.242.7)	High (7.5)
	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Table 5: Weak Password Sybase management console (Source: Tenable Nessus, author: Imran Ihsan butt)

General Description

Biometric verification service logs API username and password.

Consequence

An attacker can launch a dictionary attack and easily guess a password.

Corrective Actions

Use strong passwords on administrative consoles.

Critical Severity

Recommended action: Immediate correction:

- If the system is operational, consider taking it offline until the vulnerability is corrected.
- Start the vulnerability correction process immediately, in accordance with the company policies.

High Severity

Recommended action: Immediate evaluation:

- Decide whether the vulnerability should be corrected immediately or how long the correction process can wait.
- Set a deadline if the correction is postponed.

4.4 Strategies to secure Web application.

Safeguarding delicate client information, guaranteeing framework respectability, and keeping up with entrust with clients are critical with regards to getting a web application, especially one as crucial as a Lead an administration framework (LMS). To make a web-based application, similar to a LMS, safer, do the accompanying:

Authentication and Authorization:

Confirm client personalities utilizing powerful verification strategies, as multifaceted validation (MFA).

Guarantee that clients can get to only the information and usefulness that is expected for their positions by carrying out proper authorization controls.

Data Encryption:

Safeguard private data by scrambling it while it is moving and keeping in mind that it is put away.

Secure information transmission across the organization by utilizing HTTPS with SSL/TLS testaments.

Input Validation and Sanitization:

Stay away from normal weaknesses like SQL infusion, site prearranging (XSS), and orders by approving and disinfecting all client inputs.

To make this interaction programmed, you can utilize input approval systems or modules.

Session Management:

To abstain from commandeering and obsession of meetings, utilize secure meeting the executives' techniques.

Utilize techniques like secure treats, meeting lapse, and meeting tokens.

Security Patching and Updates:

Update and fix all product parts consistently to fix known weaknesses. This incorporates the web server, programming server, a data set, and outsider programming libraries.

Watch out for security cautions and carry out patches quickly.

Access Control:

Carry out severe access controls on the server and in the applications.

To safeguard delicate capabilities, carry out RBAC, or job-based admittance control, and breaking point managerial access.

Secure Configuration:

While designing your server or application, make certain to follow all security best practices.

Follow best practices in the business while designing security settings and handicap unused administrations and usefulness.

Logging and Monitoring:

Set up intensive logging strategies to screen framework occasions, security occurrences, and client activities.

Completely survey signs consistently to distinguish any uncommon action or security breaks.

Secure Development Practices:

Utilize input approval, yields encoding, and right mistake taking care of as a feature of secure coding procedures.

Find and fix security blemishes by inspecting and breaking down code statically and progressively consistently.

Web Application Firewall (WAF):

Set up a web application firewall (WAF) to control and examine all approaching and active HTTP traffic.

Set up the WAF to dismiss demands that match known malignant examples

Data Backup and Disaster Recovery:

On the off chance that you believe your association should continue to run on account of information misfortune or framework split the difference, you ought to back up your information consistently and have an arrangement for catastrophe recuperation.

Consistently test the methodology for reinforcement and recuperation.

Employee Training and Awareness:

Staff individuals ought to be instructed on ordinary security gambles, phishing endeavours, and safe information taking care of methods through security mindfulness preparing.

4.5 Code Analysis

A total security plan for the Lead The executives Framework (LMS) incorporates a top to bottom survey of the codebase notwithstanding engineering study. To find security blemishes that aggressors could utilize to think twice about application, code investigation glances through the source code. By breaking down the code, we need to find any occurrences of normal security weaknesses recorded in the OWASP Top 10 and ensure that the code follows secure coding standards. Web applications are defenseless to the OWASP Top 10 weaknesses, which ought to be the focal point of the code examination. Here are a portion of the weaknesses:

For instance, SQL infusion, NoSQL infusion, and operating system order infusion are instances of infusion assaults: To keep away from infusion assaults, the code needs to approve and disinfect client inputs accurately.

Insufficient Confirmation: Feeble secret phrase hashing, meeting the executives' issues, or mistaken treatment of validation certifications are instances of verification procedures that ought to be examined by investigating the codebase.

Information Responsiveness: While investigating code, it is critical to find spots where delicate data is taken care of, including confirmation qualifications or recognizable data (PII). Then, ensure that the right encryption and safety efforts are set up to forestall any unapproved access.

Checking on the code to debilitate references to outside substances or to utilize secure XML parsers will assist with forestalling XXE assaults, which happen when an application processes XML input.

Inappropriately Implemented or Missing Access Control: By dissecting the codebase, you ought to have the option to detect any situations where delicate usefulness or information might have been gotten to without authorization.

Misconfigurations in Security Settings: Default passwords, unnecessary usefulness enacted, or unreasonably permissive access limits are instances of safety settings that ought to be audited for in the code.

Code examination ought to recognize and fix cross-site prearranging (XSS) weaknesses by checking and cleaning client produced material for script infusion assaults.

The application ought to assess code to forestall unreliable deserialization weaknesses could prompt remote code execution or different assaults on the off chance that it conducts deserialization of untrusted information.

While using outsider parts or libraries, it is critical to look the codebase for any known weaknesses and apply updates or fixes on a case-by-case basis.

Insignificant Logging and Observing: It is vital to do code examination to ensure that the program records appropriate security occasions and sets up sufficient checking strategies to recognize and deal with security events.

4.5.1 Secure Coding Practices

As well as finding security defects, code examination ought to check for secure coding principles like:

To keep away from infusions assault and other security defects, it is essential to approve and clean all client inputs.

```
# Example of input validation for user registration form
def register_user(username, password):
    if not username or not password:
        return "Username and password are required."
    # Additional validation logic such as password strength checks
    if len(password) < 8:
        return "Password must be at least 8 characters long."
    # Proceed with user registration
```

Output Encoding: Properly encoding output to prevent XSS attacks and other forms of injection.

```
// Example of output encoding in JavaScript (Node.js)
const express = require('express');
const app = express();
// Middleware to encode output
app.use((req, res, next) => {
  res.locals.user = {
    username: '<script>alert("XSS attack!")</script>',
  };
  next();
});
// Route to render user profile
app.get('/profile', (req, res) => {
  res.send(`<h1>Welcome, ${res.locals.user.username}</h1>`);
});
app.listen(3000, () => {
  console.log('Server is running on port 3000');
});
```

Applying the notion of least privilege ensures that only authorised users have access to sensitive operations and data.

```
# Example of implementing least privilege principle for user roles and permissions
class User:
    def __init__(self, role):
        self.role = role
    def can_access_admin_panel(self):
        return self.role == 'admin'
# Usage example
user1 = User(role='admin')
user2 = User(role='regular')
print(user1.can_access_admin_panel())  # Output: True
print(user2.can_access_admin_panel())  # Output: False
```

Handling Errors: Putting in place strong procedures to handle errors so that sensitive information does not leak out and users receive meaningful error messages.

To avoid hijacking sessions and other session-related attacks, secure session management ensures that session tokens are generated, sent, and invalidated securely.

To store passwords safely and avoid vulnerabilities linked to passwords, one should use strong cryptographic hashing methods and salting procedures.

```
# Example of securely storing passwords using bcrypt library in Python
import bcrypt
def hash_password(password):
```

```
    # Generate salt and hash password
    salt = bcrypt.gensalt()
    hashed_password = bcrypt.hashpw(password.encode('utf-8'), salt)
    return hashed_password
# Usage example
password = "securepassword"
hashed_password = hash_password(password)
print(hashed_password)  # Output: Hashed password
```

Safe Communication: Preventing surveillance and data interception by encrypting all component-to-component communication using secure protocols (such as HTTPS).

4.5.2 Code Review

To ensure the Lead The board Framework (LMS) is secure and solid, code audit is fundamental. Code shortcomings and average weaknesses can be found with the utilization of robotized code investigation apparatuses, albeit these techniques could miss more unpretentious weaknesses or rationale issues. Thus, to reinforce the LMS's security, it is imperative to enhance computerized methods with human code survey.

Significant pieces of exploring the LMS code are:

Reviewing for Subtle Vulnerabilities:

To find bugs or security openings that mechanized devices could miss, it is important to do a manual code survey. Robert Beam (2020). Secure Coding CRC Press. Guaranteeing strength and protection from various assault vectors includes completely inspecting input approval frameworks, information handling processes, and muddled business rationale.

Assessing Adherence to OWASP Top 10:

The reason for the code audit is to guarantee that the LMS sufficiently fixes the main 10 weaknesses distinguished by OWASP. To lessen the effect of these

weaknesses, analysts ought to zero in on regions including input approval, confirmation techniques, information encryption, access controls, and mistake dealing with. Site Security Attack Gathering. (n.d.). It was recovered from the accompanying URL: https://owasp.org/www-project-top-ten/.

Evaluating Secure Coding Practices:

Ensure the code sticks to get coding norms by checking it during the code survey. Client input approval, yield encoding for XSS assault anticipation, secret word stockpiling serious areas of strength for using procedures, secure correspondence conventions, and least honor standards for access control are all important for this.

Identifying Logic Flaws and Business Logic Errors:

Not exclusively should security weaknesses be the essential focal point of code audit, however, blames and imperfections in the LMS's business rationale ought to likewise be effectively searched out. Its motivation is to guarantee that the program does nothing startling or take advantage of safety holes by making sure that it handles edge cases accurately and complies with the characterized business rules.

Providing Constructive Feedback:

By working together, reviewers can improve the codebase's quality and security by giving developers helpful criticism, drawing attention to security flaws, proposing solutions, and disseminating best practices for creating code that is both secure and easy to maintain.

4.6 Web Application Security Checklist

To begin the process of protecting an LMS web application, use this checklist. New dangers appear all the time, and technology changes rapidly, so it's crucial to examine and update security measures often.

Web Application Security Checklist.xls

Table 6: OWASP Application Security Verification Standard v4.0 (Source: ministryofsecurity.co)

The provided checklist outlines various architectural requirements and verification steps for ensuring the security of a web application. Here is a summary of the key sections covered in the checklist:

The OWASP Application Security Verification Standard (ASVS) is a framework designed to verify the security of web applications. Version 4.0 includes three security levels (Level 1, Level 2, and Level 3) with a total of 89 controls. Here's a brief overview of each control category:

Architecture, Design, and Threat Modeling Controls: This includes controls related to secure application architecture, design reviews, and threat modeling.

Authentication Controls: Covers controls for user registration, login, password management, multi-factor authentication, session management, and more.

Session Management Controls: Focuses on managing user sessions securely, including session tokens, cookies, and session expiration.

Access Control Controls: Involves controls for enforcing proper access control mechanisms, authorization checks, and privilege escalation prevention.

Cryptographic Controls: Includes controls for encryption, key management, secure random number generation, and cryptographic algorithm usage.

Input Validation and Output Encoding Controls: Covers controls for validating input data, sanitizing output, preventing injection attacks, and handling error messages securely.

Error Handling and Logging Controls: Focuses on proper error handling, logging sensitive information securely, and monitoring application logs for security events.

Data Protection Controls: Involves controls for data encryption, data masking, secure data storage, data leakage prevention, and secure data transmission.

Communication Security Controls: Covers controls for securing network communications, using TLS/SSL, enforcing secure communication protocols, and preventing man-in-the-middle attacks.

API Security Controls: Includes controls for securing APIs, authentication and authorization for API endpoints, input validation, rate limiting, and API documentation security.

Security Configuration Controls: Focuses on securely configuring application components, third-party libraries, frameworks, and security-related settings.

Software Development Lifecycle (SDLC) Integration Controls: Involves controls for integrating security practices into the software development lifecycle, including secure coding standards, code reviews, and security testing.

Malicious Code and Attack Prevention Controls: Covers controls for preventing common web application attacks such as XSS, CSRF, SQL injection, command injection, path traversal, and more.

Business Logic Controls: Includes controls for securing business logic, transaction authorization, business process validation, and preventing business logic flaws.

File and Resource Management Controls: Focuses on securely managing files and resources, including file uploads, downloads, access controls, and file system security.

Mobile Security Controls: Involves controls specific to mobile application security, such as secure data storage, secure communication, mobile platform security, and mobile device management.

Web Services Security Controls: Covers controls for securing web services, API gateways, XML/JSON security, SOAP/REST security, and web services authentication.

These controls are further categorized into three levels (Level 1 being the least stringent and Level 3 being the most stringent) to accommodate different security requirements based on the application's sensitivity and risk level. Implementing these controls helps improve the overall security posture of web applications and reduces the risk of common security threats.

Overall, this checklist provides a comprehensive set of guidelines and verifications to ensure that a web application is developed, deployed, and maintained with robust security measures in place.

5 Advantages of design Security Strategy for Web Application (Lead Management System)

Information security is critical in the present computerized world, especially for web applications like Lead The board Framework (LMS) that handle delicate data. Guaranteeing the security of a Lead The board Framework is critical for associations to maintain certainty, conform to guidelines, and run effectively. This framework is fundamental for coordinating, following, and supporting new leads. To safeguard information, ensure consistence, and reinforce organization tasks, this article investigates the advantages of making and executing serious areas of strength for an arrangement explicitly for a Lead The executives Framework.

Data Protection

Safeguarding delicate data ought to be the main goal while fostering a security plan for a Lead The executives Framework. There should be a framework set up to forestall the misfortune, abuse, or change of delicate information, for example, client data, correspondence records, and lead data. A solid security engineering should consolidate encryption techniques, access controls, and safe validation methods. Organizations might safeguard their information resources against unapproved access and keep them hidden by following these means.

Prevention of Data Breaches

Associations face a significant gamble of monetary misfortunes, reputational hurt, and legitimate outcomes because of information breaks. Safeguarding the Lead The board Framework from potential dangers and shortcomings is the objective of an intensive security methodology. Weakness checking, entrance testing, and security evaluations ought to be performed consistently to find and fix security openings in the framework. Organizations might safeguard their image and the trust of their clients by going to proactive lengths to cure security shortcomings, which diminishes the probability of information breaks.

Maintaining System Availability

For proceeded with business activities, it is essential to guarantee that the Lead The board Framework is accessible. Conveyed Disavowal of Administration (DDoS) and other cyberattacks can overpower a framework to the place where it becomes unusable. To make the framework more impervious to dispersed disavowal of administration attacks, it is prescribed to carry out measures like burden adjusting, server overt repetitiveness, and DDoS assurance. Organizations might lessen the probability of personal time and assurance ceaseless admittance to imperative lead the executives highlight by keeping their frameworks accessible.

User Trust and Confidence

Client trust and certainty, cultivated by a solid Lead The executives Framework, are significant for connecting with and holding clients. Right when clients believe in a phase's wellbeing endeavours, they are more ready to give that stage permission to their own information. Associations could sway clients' trust and foster devoted clients by focusing on wellbeing endeavours that protect their own information.

Compliance Requirements

One of the principal bits of running a Lead The chiefs Structure is guaranteeing you're as per each significant rule and security guidelines. Serious data security and insurance standards are constrained by rules like the General Data Confirmation Rule (GDPR), the California Client Assurance Act (CCPA), and explicit industry rules. To adjust to these necessities and avoid fines or other legal repercussions, basic to encourage a security method notices their guidelines. Consistence with regulatory necessities displays a vow to moral key strategies and gives accomplices trust in how the association handles their data.

Protection Against Cyber Threats

To defend Lead The chiefs Structures against computerized attacks, proactive advances are required in light of the continuously changing risk scene. Data security and structure genuineness are widely take a chance by typical attack vectors like SQL implantation, cross-site setting up (XSS), and phishing tries. Safeguarding the structure from these dangers is possible with the usage of wellbeing controls like interference revelation systems, web application firewalls, and security event response plans. Associations could shield their lead the chiefs establishment from cyberattacks by being prepared and taking hindrance measures.

Business Continuity

Interference of business assignments, money related incidents, and reputational harm can result from security events. To diminish the blow of security breaks and keep errands moving ahead true to form when conditions become troublesome, business movement orchestrating is a certain necessity. Associations can keep lead the load up processes moving along true to form and diminish the likelihood of individual time by laying significant solid areas for out measures and support strategies. In addition to the fact that this defend organizations resources, however it likewise empowers partners to return quickly and be geared up for any eventuality.

6 Conclusion

Conclusion based on PDCA (Plan-Do-Check-Act):

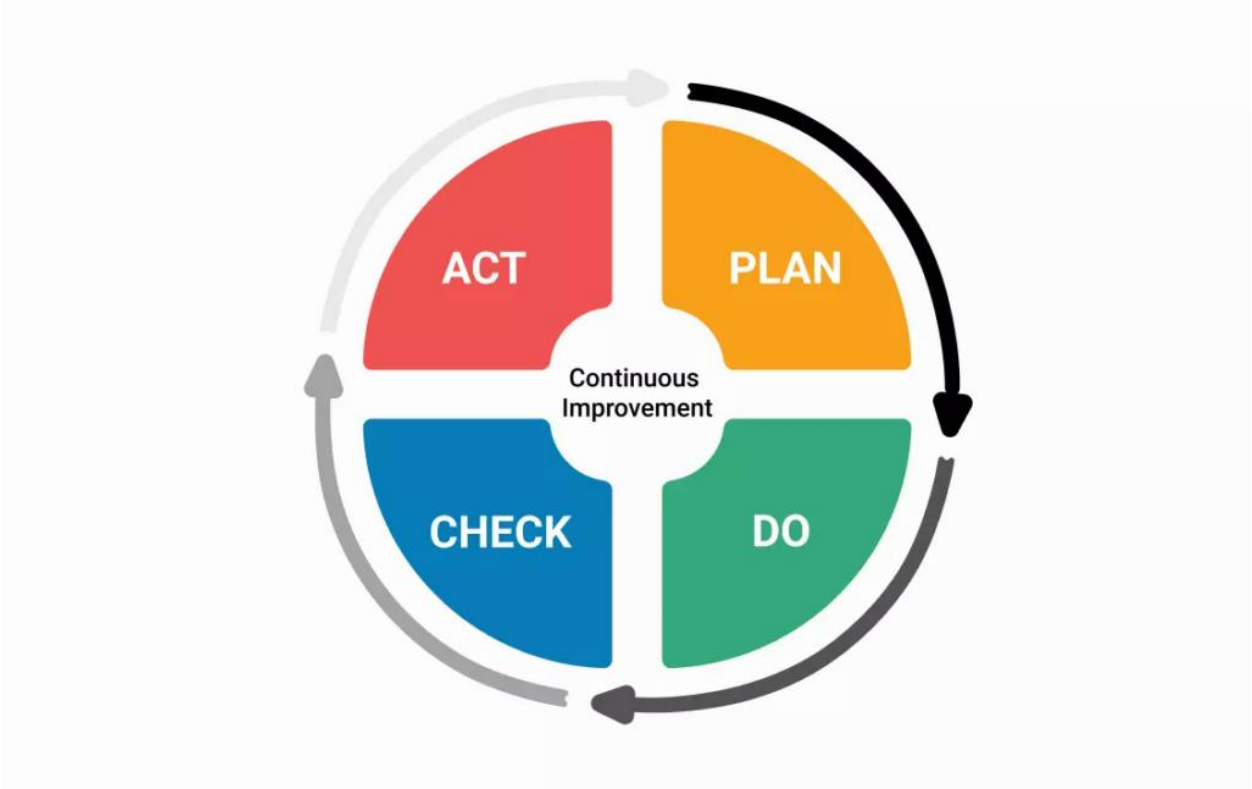


Figure 21: PDCA(Plan-Do-Check-Act) Cycle (Source: Deming Cycle, author: Mohamed Gabr)

Plan: The initial step in securing the Lead Management System (LMS) involves planning a comprehensive security strategy. This includes identifying potential vulnerabilities, implementing encryption protocols, establishing access controls, conducting regular security audits, and ensuring compliance with relevant data protection regulations.

Do: Once the security plan is in place, it must be executed effectively. This involves implementing data encryption measures, setting up access controls based on roles, conducting security training for employees, developing an incident response plan, and ensuring compliance with data protection laws such as HIPAA and GDPR.

Check: Regular monitoring and evaluation are crucial to ensure the effectiveness of the security measures. This involves conducting vulnerability assessments, security audits, and penetration testing to identify any weaknesses or gaps in the system's security posture.

Act: Based on the findings from the checking phase, appropriate actions must be taken to address any identified issues or areas for improvement. This may include updating encryption protocols, refining access controls, enhancing employee training programs, revising incident response plans, and ensuring ongoing compliance with data protection regulations. Details are mentioned below.

At long last, a urgent piece of maintaining a cutting edge business is fostering a security plan for the picked web application, for this situation the Lead The executives Framework (LMS) that spotlights on computerized lead procurement. We have investigated the Lead The board Framework's internal functions and shown that it is so pivotal to current computerized showcasing efforts all through this discussion. The LMS fills in as a comprehensive answer for upgrade and smooth out the lead obtaining experience, from rapidly assembling prompts supporting them through customized commitment methods and eventually transforming them into steadfast clients.

With every one of the extraordinary highlights of the Lead The executives Framework, it is significant to have solid safety efforts set up. Names, email addresses, telephone numbers, and conceivably even monetary subtleties are among the numerous touchy bits of customer information took care of by the framework. This makes it an obvious objective for miscreants who need to exploit security openings for their own benefit, whether that is monetarily or regarding their standing. To decrease weaknesses and guarantee the accessibility, mystery, and uprightness of delicate information put away Leading the pack The board Framework, it is critical to have an exhaustive security plan that is tweaked to the framework.

A thorough engineering and code investigation of the web application is important for the recommended security methodology's meticulous methodology. The framework's weaknesses can be purposefully found and characterized utilizing industry-standard systems like the OWASP Top 10. If we have any desire to be truly careful as we continued looking areas of strength for, we want to take a gander at something other than the OWASP Top 10

weaknesses. Like that, we can get a superior image of the framework's general weakness.

Significant pieces of the suggested security plan are:

Information Encryption: To ensure the protection and security of delicate client data, it is vital for utilize hearty encryption calculations for information while it is on the way and when it is very still. Information encryption decreases the probability of information breaks by delivering caught data muddled even on account of unlawful access.

Constraints on Access: To shield classified lead information from inquisitive eyes, strong validation and access controls are required. To ensure clients just have the freedoms they need to go about their responsibilities, job based admittance ought to be set up. Unapproved access and information breaks can be successfully decreased by putting severe access controls in the framework.

To find and fix conceivable Lead The executives Framework weaknesses, it is vital for direct security reviews and weakness evaluations consistently. Framework flexibility and security notwithstanding always showing signs of change digital dangers can be accomplished by proactive weakness distinguishing proof and remediation.

Staff Instruction: It is basic to teach laborers on the meaning of safety best practices and how to safeguard delicate information. To decrease the probability of insider dangers and inadvertent information exposure, developing a security-mindful culture inside the organization is vital. Human blunder is as yet a main source of safety breaks.

Powerful administration and relief of the impacts of safety episodes requires the turn of events and constant testing of an occurrence reaction procedure. To lessen free time and information openness, associations ought to have occurrence reaction designs that are plainly expressed and fit to be carried out on account of a security break.

It is basic to conform to information insurance and security regulations like HIPAA and the Overall Information Assurance Guideline (GDPR). Clients

are turning out to be increasingly more stressed over the security and protection of their information, thusly lessening legitimate dangers and it is fundamental for construct trust through consistence. The association shows its commitment to moral information dealing with techniques and gives partners trust in its information security act by keeping legal guidelines.

A mind-boggling endeavour requires a comprehensive methodology that is tweaked to the Lead The executives Framework's singular necessities to plan a security plan for the framework. Organizations might safeguard their clients' very own data, keep their partners' trust, and diminish the probability of safety breaks by laying areas of strength for our strategies and empowering a security-cognizant culture all through the organization. Safeguarding touchy information inside the Lead The executives Framework and guaranteeing the association's drawn-out progress and maintainability in an undeniably computerized and interconnected world are both made conceivable by putting resources into a powerful security methodology.

7 References

- "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard and Marcus Pinto.

- The Web Application Hacker's Handbook Finding and Exploiting Security Flaws, ISBN: 781118026472, 1118026470

- Web services and grid security vulnerabilities and threats analysis and model, doi:10.1109/GRID.2005.1542751

- Derailer: Interactive Security Analysis for Web Applications, doi:10.1145/2642937.2643012

- Evaluating Performance of Web Application Security Through a Fuzzy Based Hybrid Multi-Criteria Decision-Making Approach: Design Tactics Perspective

- https://blog.omnetworks.com.np/owasp-top-10-understanding-the-most-critical-application-security-risks/

- https://www.forescout.com/blog/how-to-comply-with-the-5-functions-of-the-nist-cybersecurity-framework/

- https://www.linkedin.com/pulse/nist-cybersecurity-framework-shanneece-alberts/

- B. Bordbar and K. Anastasakis. Mda and analysis of web applications. Trends in Enterprise Application Architecture, pages 44--55, 2006.

- https://medium.com/@cybersecurityCo/web-application-security-testing-audit-services-application-security-check-list-e74e4d0fcc93

- Web Services and Grid Security Vulnerabilities and Threats Analysis and Model (Yuri Demchenko, Leon Gommans, Cees de Laat, Bas Oudenaarde)

- https://www.sprintzeal.com/blog/cybersecurity-controls

- Advanced Internet Research Group, University of Amsterdam Kruislaan 403, NL-1098 SJ Amsterdam, The Netherlands

- Web Application Security Consortium: Threat Classification, Version: 1.00, 2004. Available at http://www.webappsec.org/projects/threat/
- https://www.softwaresuggest.com/blog/lead-management-process/

- Soltani, H., & Tashakkori, A. (2020). The role of security measures in enhancing customer trust in e-commerce: A systematic review and meta-analysis.

- A Guide to Securing XML and Web Services. - ZapThink, LLC - January 1, 2004 - http://whitepapers.itsj.com/detail/RES/1073404572_221.html

- Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology
- Author open overlay PanelJai Narayan Goel, B.M. Mehtre.
- The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Second Edition Published by John Wiley & Sons, Inc.
- https://medium.com/redcatstudio/user-centered-design-method-28e3aafc8c8a
- https://ministryofsecurity.co/product/web-application-security-checklist/
- https://www.linkedin.com/pulse/pdca-cycle-deming-mohamed-gabr-wu9sf

.

8 List of figures and tables

8.1 List of figures

8.2 List of Tables

8.3 List of Case Studies