

WEB SERVER VULNERABILITY TESTING AND RISK ANALYSIS

BY

MD. SHAHADAT HOSSAIN

ID: 152-19-1763

MD. GOLAP HOSEN.

ID: 152-19-1788

MANABENDRA ROY

ID: 152-19-1804

This Report Presented in Partial Fulfillment of the Requirements of the
Degree of Bachelor of Science in Electronics and Telecommunication
Engineering

Supervised By

Professor Dr. A.K.M. Fazlul Haque

Associate Dean and Professor

Department of ETE

Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA-1207, BANGLADESH

JUNE 2019

APPROVAL


This Project titled “**Web Server Vulnerability Testing and Risk Analysis**” submitted By Md. Shahadat Hossain, Md. Golap Hosen. and Manabendra Roy to the Department of Electronics and Telecommunication Engineering (ETE), Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Electronics and Telecommunication Engineering and approved as to its style and contents. The presentation was held on June, 2019.

BOARD OF EXAMINERS



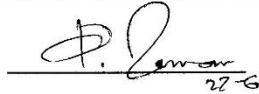
Md. Taslim Arefin
Associate Professor and Head
Department of ETE
Faculty of Engineering
Daffodil International University

Chairman



Professor Dr. A.K.M. Fazlul Haque
Associate Dean and Professor
Department of ETE
Faculty of Engineering
Daffodil International University

Internal Examiner



Dr. Eng. M. Quamruzzaman
Professor
Department of ETE
Faculty of Engineering
Daffodil International University

Internal Examiner



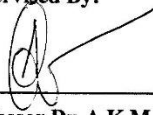
Dr. Saeed Mahmud Ullah
Associate Professor
Department of EEE
University of Dhaka

External Examiner

DECLARATION

We hereby declare that this project is our own work and effort under the supervision of **Professor Dr. A.K.M. Fazlul Haque, Associate Dean and Professor, Department of Electronics and Telecommunication Engineering, Daffodil International University, Dhaka.** It has not been submitted anywhere for any award. Where other sources of information have been used, they have been acknowledged.

Supervised By:



Professor Dr. A.K.M. Fazlul Haque,
Associate Dean and Professor,
Department of ETE
Daffodil International University

Submitted By:

Md. Shahadat Hossain
Md. Shahadat Hossain
ID: 152-19-1763
Department of ETE
Daffodil International University

Golap

Md. Golap Hosen.
ID: 152-19-1788
Department of ETE
Daffodil International University

Manabendra

Manabendra Roy
ID: 152-19-1804
Department of ETE
Daffodil International University

ACKNOWLEDGMENTS

First of all, we would like to convey our gratitude to the Almighty, for giving us the right direction while attempting the task.

The real spirit of achieving a goal is through the way of excellence and austere discipline. We would have never succeeded in completing our task without the cooperation, encouragement and help provided to us by various personalities.

This work would not have been possible without the support and guidance of **Professor Dr. A.K.M. Fazlul Haque, Associate Dean and Professor**, Department of Electronics and Telecommunication Engineering, Daffodil International University, Dhaka, under whose supervision we chose this topic and developed the project. Deep Knowledge and keen interest of our supervisor in the field of Web Server Security which influenced us to carry out of this project.

We would like to express our heartiest gratitude to **Md. Taslim Arefin, Associate Professor and Head**, Department of Electronics and Telecommunication Engineering, for his kind help to finish our thesis and also to other faculty members, the staffs of the ETE Department of Daffodil International University.

We must acknowledge with due respect the constant support and patience of our family members for completing this project.

Md. Shahadat Hossain,

Md. Golap Hosen.

and

Manabendra Roy

ABSTRACT

In the recent view the tendency of using internet based communication increase rapidly with respect to this the cybercriminal also. In order to protect and identify the kind of threats there need to build a strong infrastructure. Vulnerability testing is a very evidential and easily operative way of monitoring the regular base web leakage of the web applications security. The aim of the project is to serve the web developers to understand their web leakage and easily find out the livability. This project is only based on the software. The responsible of the project is to compare the fault of different web server given solution and suggested the way of web security.

TABLE OF CONTENTS

CONTENTS	PAGE
APPROVAL	i
DECLARATION	ii
ACKNOWLEDGEMENTS	iii
ABSTRACT	iv
TABLE OF CONTENTS	v - x
LIST OF FIGURES	x-xi
LIST OF TABLE	xi
CHAPTER 1: INTRODUCTION	1-4
1.1 Overview	1
1.2 Motivation of the Work	3
1.3 About the Report	4
CHAPTER 2: BACKGROUND THEORY	5-22
2.1 History of Recent Attacks	5
2.2 Types of Vulnerability	6
2.2.1 Buffer Overflows	6
2.2.2 Non-validated Input	7
2.2.3 Race Conditions	8
2.2.4 Access Control Positions	8
2.2.5 Secure storage and Encryption	9
2.2.6 Social Engineering	9
2.3 Types of Viruses	9

2.3.1 Virus	9
2.3.2 Worm	10
2.3.3 Trojan Horses	10
2.3.4 Malware	10
2.3.5 Adware	10
2.3.6 Spyware	11
2.3.7 Ransomware	11
2.3.8 Shortcut Virus	11
2.3.9 RootKit	11
2.3.10 Mail Virus	11
2.3.11 Browser Hijacker	12
2.3.12 Bots	12
2.3.13 Malware Detection	12
2.4 Webserver Vulnerability	13
2.4.1 SQL Injection	13
2.4.2 Cross Site Scripting	14
2.4.3 Broken Authentication and Session Management	14
2.4.4 Cross Site Request Forgery	15
2.4.5 Insecure Cryptographic Storage	16
2.5 Types of Webserver Attackers	16
2.5.1 Amateurs	16
2.5.2 Hackers	17
2.5.3 Organized Hackers	17
2.5.4 White Hat Hackers	17
2.5.5 Gray Hat Hackers	17

2.5.6 Black Hat Hackers	18
2.6 Webservers Attacks	19
2.6.1 DoS Attack	19
2.6.2 Misconfiguration Attacks	19
2.6.3 Phishing Attack	19
2.6.4 Password Attacks	20
2.7 Vulnerability Identification	20
2.7.1 OpenVAS	20
2.7.2 Nexpose Community	21
2.7.3 Nikto	21
2.7.4 Wireshark	21
2.7.5 Nessus Professional	22
CHAPTER 3: WORKING PROCEDURE	23-29
3.1 Vulnerability Scanning With Nexpose	24
3.2 Nexpose Terminology	24
3.3 Some Feature of Nexpose Community	25
3.3.1 Real Risk of Score	25
3.3.2 Safety Adaptive	25
3.3.3 Policy Evaluation	26
3.3.4 Reporting of the Remedy	26
3.3.5 Metasploit Integration	26
3.4 Procedures	27
CHAPTER 4: PERFORMANCE MEASUREMENT OF WEB SERVER	30-42
4.1 Daffodil International University Webserver Vulnerability	30

4.2 SomReP Organization Vulnerability	34
4.3 Xitech BD Vulnerability	38
4.4 Campus TV Vulnerability	41
CHAPTER 5: RESULT AND ANALYSIS	43-59
5.1 Risk Score Calculation	43
5.2 Daffodil International University	43
5.3 SomReP Organization Risk	44
5.4 Xitech BD Risk	45
5.5 Common Ports	45
5.6 Web server port related Services	46
5.6.1 HTTP	46
5.6.1.1 Problem Identify and Approximate Solution	46
5.6.2 HTTPS	47
5.6.3 IMAP	47
5.6.4 IMAPS	47
5.6.5 POPS	47
5.6.6 SMTP	48
5.6.6.1 Problem Identify and Approximate Solution	48
5.6.7 SSH	48
5.6.7.1 Reuse of Personal Host Keys	48
5.6.7.2 Approximate Solution	49
5.6.8 DNS	49
5.6.8.1 Port 53 against Attack and Approximate Solution	49
5.6.9 FTP	50
5.6.9.1 Port 20 and 21 against Attack and Approximate	

Solution	50
5.7 Approximate Suggestions	51
5.7.1 Joomla!	51
5.7.2 Apache	51
5.7.3 ISC Bind	52
5.7.4 SMTP server VRFY Vulnerability (smtp-general-vrfy)	52
5.7.5 HTTP OPTIONS Method enabled (http-options-method-enabled)	52
5.7.6 TCP timestamp response (generic-tcp-timestamp)	53
5.7.7 X.509 Certificate Subject CN Does Not Match the Entity Name (certificates-common-name-mismatch)	53
5.7.8 FTP credentials transmitted unencrypted (ftp-plaintext-auth)	54
5.7.9 IMAP credentials transmitted unencrypted (imap-plaintext-auth)	54
5.7.10 POP credentials transmitted unencrypted (pop-plaintext-auth)	55
5.7.11 SMTP credentials transmitted unencrypted (smtp-plaintext- auth)	55
5.7.12 TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32) (ssl-cve-2016-2183-sweet32)	56
5.7.13 TLS/SSL Server Supports RC4 Cipher Algorithms (CVE-2013- 2566) (rc4-cve-2013-2566)	56
5.7.14 TLS/SSL Server is enabling the BEAST attack (ssl-cve-2011- 3389-beast)	57
5.7.15 TLS/SSL Server Supports the Use of Static Key Ciphers (ssl-static-key-ciphers)	57
5.7.16 TLS/SSL Server Is Using Commonly Used Prime Numbers (tls- dh-primes)	58
5.7.17 ICMP timestamp response (generic-icmp-timestamp)	58

5.7.18 TLS/SSL Server Supports 3DES Cipher Suite (ssl-3des-ciphers)	58
5.7.19 Nmap	59
CHAPTER 6: CONCLUSION	60
REFERENCES	61-62

LIST OF FIGURES

FIGURES	PAGE
Figure 1.1: Our Data	1
Figure 2.1: Example of Buffer Overflow	7
Figure 2.2: Non-validated Input	7
Figure 2.3: Race Condition	8
Figure 2.4: Cyber Attackers	18
Figure 3.1: Nexpose Home Page	27
Figure 3.2: Creating a Site	28
Figure 3.3: The Assets	28
Figure 3.4: The Templates	29
Figure 3.5: Save and Scan	29
Figure 4.1: Summery of Vulnerabilities	31
Figure 4.2: Common Vulnerability Categories	33
Figure 4.3: Common Services	33
Figure 4.4: Vulnerabilities by Service	34
Figure 4.5: Summery of Vulnerabilities	35
Figure 4.6: Common Vulnerability Categories	36

Figure 4.7: Common Services	37
Figure 4.8: Vulnerabilities by Service	37
Figure 4.9: Summery of Vulnerabilities	38
Figure 4.10: Common Vulnerability Categories	40
Figure 4.11: Common Services	40
Figure 4.12: Vulnerabilities by Service	41
Figure 4.13: Summery of Vulnerabilities	42
Figure 5.1: Highest Risk Vulnerabilities	44
Figure 5.2: Highest Risk Vulnerabilities	44
Figure 5.3: Highest Risk Vulnerabilities	45

LIST OF TABLE

TABLE	PAGE
Table-1: Summery of Vulnerabilities by Severity	30
Table-2: Summery of Vulnerability Category	32
Table-3: Summery of Vulnerabilities by Severity	34
Table-4: Summery of Vulnerability Category	35
Table-5: Summery of Vulnerabilities by Severity	38
Table-6: Summery of Vulnerability Category	39
Table-7: Summery of Vulnerabilities by Severity	41

CHAPTER 1

INTRODUCTION

1.1 Overview

Now we are in the 4th industrial revelation. The mentality of the generation based on the IoT, Big data and machine learning. As an out bounding technology, IoT has qualify the purchase, technology and communication [1] in the smart data management. As IoT reaching a large applications with respect to the real time networks applications for example eHealth, smart cities etc. so these features attracted the city planners and health professionals. All the information's and various businesses related activities are based on the database. Those information's are stored as a data that's are distributed to our daily activities such as medical records, employment, online information, education records, financial records etc. The distribution of the data can show in the bellow figure.



Figure 1.1: Our data

As the significant increase of web popularity and the web application tools use day by day the security concern plays a vital role. As a result the privacy and the security [2] manifestation in

the web server are vulnerable both in the business and the users end. So the Web server data base security concern is the main issues today's. The aim of the security system is to find out the untraced vulnerabilities which can be exploited. The vulnerabilities can be inaugurated by the functionality of the system that is not generally involved with the security equipment of the system. Because of the increasing of Web server the challenges of the internet security face difficulty, particularly in the confidentiality [3] in the data terms. The risk arises in security branches from different technologies which are used in the current applications which may have extremely denying statement on the users. The term web server security means that it's a process to protect the information assets and which can be accessed from the web server. It is important for any organization that has a physical or virtual Web server connected via Internet. Any leakage of a web server is a great harmful for any organization. As security is the most complex topic it is important for modern world to concern about web security. For being the purpose webserver requires a layered defense and is especially important for organizations with customer-facing websites. Server security comes to being confidentiality, integrity, availability of appropriate information and authentication. The three terms confidentiality, integrity and availability plays a vital role to make the webserver more secure. The role of the term confidentiality is to ensure include data encryption, username ID and password, two factor authentication and minimizing exposure of sensitive information. Availability maintaining the equipment performing hardware repairs, keeping operating systems and software up to date, and creating ensure of the network and data to the authorized users. Firewalls, guard against downtime such as security equipment is used due to the denial of service attacks. To make the web server secure those three terms must be followed. The term vulnerability means web-based attack and fault in the web port. There are lots of vulnerabilities in the webserver such of then the most common vulnerabilities are SQL injections, Cross-site-scripting (XSS), Broken Authentication and Session Management, Insecure Direct Object References, Security misconfiguration, Cross-site Request Forgery (CSRF), Buffer Overflow and so all. At the analyzing period in the databases the common vulnerabilities [3] are found as the name of Cross-site scripting (XSS) and SQL injection which is emphasize the lacking of resistance in code injection. For Examples, in world-wide millions of customers loss their credit card information. This problems can be happened because of the harsh of programming code in the web sever the attacker try for such lack of programming code. In this situation for testing the web vulnerabilities a scanner of trusting vulnerability is needed for automated detection of vulnerabilities. For identifying the vulnerabilities [3] there two ways can be followed one is false positive and another false negative though the human confirmation and exploration are

also asserted. The target of the work is to develop the exactitude and clearness of the vulnerabilities by removing the both false positive and false negative. Lots of techniques and tools are implementing for analyzing to discover the vulnerabilities in the web server for removing and exploit vulnerabilities from the web server. The attacker use different types of technique and try to vulnerable the webpages. For identifying the injection attacks and vulnerabilities in the Data-Base Management System Iberia Medeiros, Miguel Beatriz, Nuno Neves and Miguel Correia proposed [5] to use the realm of binary application and inserted the programming libraries systems. Their works is that only at the runtime in the database management system the block injection will attacks they named the process is Self-Protecting Database from Attacks in this process the developed of the work is that the injections are stored and the plugins method deals with specific attacks before inserted the data in the data management systems. In the work of Jose Fonseca, Marco Vieira and Henrique Madeira showed the comparison between the scanning [4] tools of SQL injection and cross site scripting attacks (XSS). They recommended in their works to prevent the occurrence to follow the greatest programming pattern, monitoring and reviews the code regularly, to use the vulnerabilities detectors. For developing the less vulnerability Wenliang Du and Aditya P. Mathur approach a software system for testing the possible security flaws. Their presentation of the work is based on the famous technique of fault injection. In their scheme they used to classify 142 security flaws in the vulnerability management system. The classification announced that 91% of security flaws in the database management are captured by EAI model.

1.2 Motivation of the Work

Web security is an action to ensure the web data is not exploited by the cyber hackers. This is the system to prevent any loss of web data from any unwanted occurrences. Because of some leakages in the web server sometimes the attacker down the website and stolen the valuable information. There are lots of way to find out those leakages but vulnerability testing is the way and also economical. Firstly the target is to find out top listed attacks in the web applications. To prevent those attacks there we propose a solution. The method evaluates automatically the benchmark vulnerability of the webpages using scanners and finds the fault injection of techniques by software. The pragmatic vulnerabilities [6] are guided by the formation of a channel which is related with the test patterns and the logical vulnerabilities are directed through proper patterns.

The main performance of this work are as following:

- The argumentation of the conventional testing access to create vulnerabilities cases in the web server.

1.3 About the report

This report is assemble in 6 chapters. Chapter 1 provides the overview of the project. The background theory are discussed in chapter 2. It describe the various type of attacks in present time. And what are the types of attacks on the web server. Also discussed webserver vulnerability. Chapter 3 concentrates on working procedure of vulnerability test. Chapter 4 depicts the performance measurements of webserver. It gives clear ideas of procedure of identify the vulnerability from the webserver. And it also measurement the common vulnerability and percentage of vulnerability on the webserver. In Chapter 5, the results and analysis are given. Finally the chapter 6 concludes the outcome of the project.

CHAPTER 2

BACKGROUND THEORY

In recent years, we have seen an inordinate variety of cybersecurity meltdowns. And that they weren't simply your common place company breaches.

2.1 History of Recent Attacks

Shadow Brokers

It's known as mysterious hacking group which first appear in August 2016. In 2016, it offered a sample of accused purloined National Security Agency knowledge and tried to auction a much bigger hoarded wealth, according with exposes for day and Black Friday. The identification of it continues to be unfamiliar, however the group's exposes have recovered argument regarding the risk of mistreatment glitches in industrial product for knowledge-assembling.

WannaCry

It unfold all of the universe, many thousands of goals, as well as open benefit and enormous firms. Its contact partly due to each in every of the exposed Shadow Brokers Windows vulnerabilities, Eternal Blue. Microsoft had discharged the MS17-010 patch for the glitch, however several establishments hadn't practical and it were thus liable to its taint [7].

Cloudbleed

The web substructure organization Cloudflare proclaimed that a weakness in its stage caused disorderly escape of probably sensitive customer knowledge. Thus the exposes were sporadic and solely concerned little particles of information, the role player of unlimited pool of knowledge [7].

VPN filter

Officers caution a few Russian hacking group which has wedged over five hundred thousand routers globally. However it may operate internet activities on the routers. These abilities are often used for numerous functions. VPN filter infected variable routers such as D-link, ASUS, Huawei and TP link. However researchers are still distinctive the complete scope and vary of this attack [8].

2.2 Types of Vulnerability

- Buffer overflows
- Non-validated input
- Race condition
- Access-control problem

2.2.1 Buffer overflows

A buffer overflow happens when an application makes an attempt to write down information before the tip of buffer. It will reason for request to crash, will settle information, it may offer an attack for more advantage step-up to settle the process that the appliance on going. Software package security indicate it as a serious supply of vulnerabilities. Most application memory is hold on in one among 2 places [9]:

- Stack — For taking a specific perform, method or alternative equivalent construct we need an area storage data for one decision in a component application.
- Heap — It remains out as the information keep in it for the reason going on the application.

Buffer (8 Bytes)								Overflow	
U	S	E	R	N	A	M	E	1	2
0	1	2	3	4	5	6	7	8	9

Figure 2.1: Example of Buffer Overflow

2.2.2 Non-validated input

As a general rule, you ought to look all input obtained by your program to create certain that the data is cheap. A simple program making an attempt to browse a file would try to portion a buffer of a misconfigured method, resulting in the potential for a heap overflow attack. For this cause, we need to look our put in data choicely.

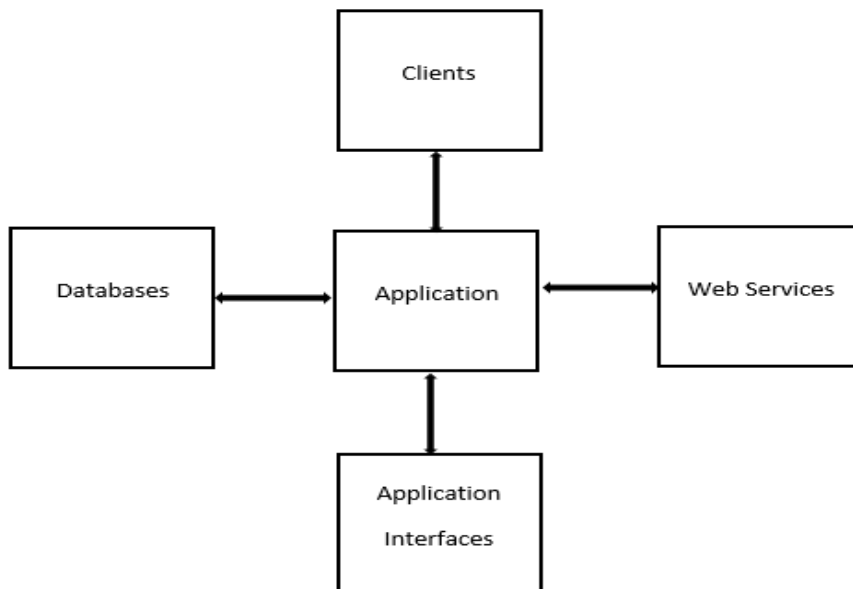


Figure 2.2: Non-validated input

It received any input from an unauthorized supplier as a main target for an attack. Samples of input from an unauthorized supply involve [9]:

- Text input fields.
- Commands tried and true an address accustomed start the program.
- Over a network any data browse from an unfaithful server.
- Over a network any unfaithful data browse from a trustworthy server.

2.2.3 Race condition

It will reason for a change in behavior which exists modifications to a lot of events. This is often a bug for the correct functioning of the program if the proper order of execution is needed. Within the process of software operations attackers will typically cash in from a little time of gaps, then they exploit it [9].

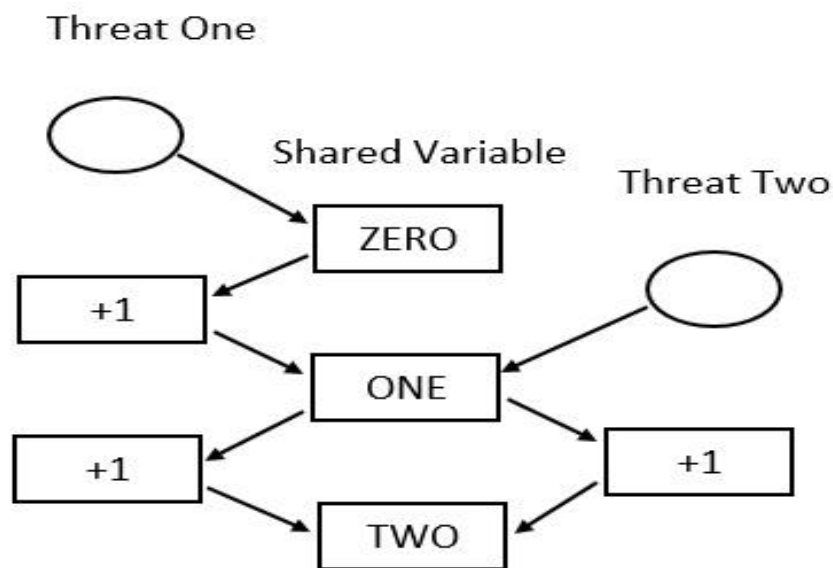


Figure 2.3: Race Condition

2.2.4 Access control problem

This is the method of dominant which is accommodated to do and try. For keeping the serves in barred area the range is kept from dominant physical access to a computer. The individual application are compulsory by the access management device of a server [9].

2.2.5 Secure storage and encryption

The following terms are related for the secure storage and encryption of security choices [9]:

- Encrypted disk flexibility pictures.
- Email Encryption.
- SSL/TLS based secure system.
- Encoding.
- Feature of digital block information.

2.2.6 Social engineering

Attackers more and more delivering malicious code for breakdown the passwords, card numbers, and alternative personal data doing trick on users for trapping. Deceptive a user into leave secrets on a PC to offender is thought as Social Engineering [9].

2.3 Types of Viruses

2.3.1 Virus

Tiny items of software package that combine themselves to original programs [10].

- i. It is usually and additional term for mistakenly habit to check with alternative forms of viruses that don't have the procreative capability.
- ii. A real Virus will unfold from each PC to different.
- iii. Viruses will raises their probabilities of distillation on to substitute PC by corrupting files on a network classification method that's way in by another computer.

2.3.2 Worm

A self-reflecting program [10]

- i. The most important distinction among a scourge and it doesn't link itself to alternative subsisting program as viruses do.
- ii. As this form of taint moves itself, it will have demolishing impression.

2.3.3 Trojan horse

Hackers achieved far entry of a target system [10].

- i. The hacker will access the target system remotely and execute varied operation.
- ii. Trojan will find necessary login lawlessly details of users on-line.

2.3.4 Malware

It is software based malicious program [10].

- i. It a range of malicious program may be an extended term.

2.3.5 Adware

It announce software supported package [10]

- i. Mechanically it delivers advertisements on any software package.
- ii. "Free" versions abound with adware on some unprotected software packages and applications.

2.3.6 Spyware

The spy within your computer [10]

- i. In secretly, when this program placed in someone's computer regarding the user and relay it to alternative interested parties, it will gather data.
- ii. Results of a software virus package can get in a replacement program.

2.3.7 Ransom ware

Holds a computer system or the information it includes safeguard against its user by calling for a ransom for its renewal [10]

- i. It is thought-about a scareware because it forces customers to pay a premium or ransom by frightening or dismaying them.

2.3.8 Shortcut virus

Creates all-place route documents throughout the computer ends up using room.

2.3.9 RootKit

Energized by booting up the system [10]

- i. Trouble finding as a consequence of being energized before the package of the system has fully appeared.

2.3.10 Mail Virus

Virus develops through an email [10].

- i. Such an outbreak is concealed in an email and once the receiver opens the mail the outcome is also seen.

2.3.11 Browser Hijacker

Changes the home page and default search provider of the internet browser to a special one while not authorizing the user [10].

- i. In particular it infects bound browser activities by redirecting the user to certain locations mechanically.

2.3.12 Bots

Subtle crimeware varieties [10].

- i. They're like Trojans and worms.
- ii. They perform a big kind of machine-controlled duties on behalf of their proprietor the world health organization is usually laid securely across the internet somewhere.

2.3.13 Malware Detection

Here are a number of things you'll use to detect whether or not malware has tormented the computation system:

- i. Exaggerated use of computerized machinery.
- ii. Slow speeds of the program desktop or apps.
- iii. Freeze or bally frequently.

Mechanically sent emails / letters and not user data [10].

2.4 Webservice Vulnerabilities

The most common vulnerabilities are

- SQL Injection
- Cross Site Scripting
- Broken Authentication and Session Management
- Cross Site Request Forgery
- Insecure Cryptographic Storage

2.4.1 SQL Injection

Description

It occurs once the customer input is delivered to an attacker as part of the issue and the translator tricks fortuitous instructions into capital punishment and provides exposure to unlawful data.

Implication [11]

- Inject harmful elements into susceptible areas by attackers.
- Intelligence in data can be altered.
- Leading activities on the information may be dead.

Vulnerable Objects [11]

- Together with the information universal resource locators operate.

2.4.2 Cross Site Scripting

Description

It's also called XSS formally. XSS vulnerabilities enable attackers to interject harmful material from trusted network servers into network pages. The harmful supply pattern software runs on the same floor as other content on the web and demonstrates reliable authority's false presence [15].

Implication [11]

- If this vulnerability is created an attacker will inject codes into the database rob essential content and run illegitimate applications.

Vulnerable Objects [11]

- Fields of input
- Locators of universal resources.

2.4.3 Broken Authentication and Session Management

Description

One of the prospective sites for real estate alternatives is to follow strategic methods that have been backed by thorough assessment and knowledge of problems rather than some prevalent military science and sometimes reactive ways [16]. If the cookies are not nullified the system may have the delicate data. An attacker utilizes the same scheme once the same susceptible website is browsed the sufferer's former meeting is opened.

Implication [11]

- Taking cookies or surveys using xss the activities may be completely hijacked victimization.

Vulnerable Objects [11]

- Universal resource locator session ids will guide in a session solidity harassment.
- Timeouts left of the meeting are not correctly undertaken.
- An occasional favorite customer may recycle the session.

2.4.4 Cross Site Request Forgery

Description

It might have been a strong insistence which originated from either the cross site. CSRF attack is an attack that happens once in a phishing site message or system which creates a user's browser to conduct an unnecessary activity on a reliable page that the client is actually real.

Implication [11]

- Using this vulnerability as an attacker will modify client profile details change standing etc.

Vulnerable Objects [11]

- Business dealings page.

2.4.5 Insecure Cryptographic Storage

Description

It may be a prevalent vulnerability that remains once there is no firm hold on to the delicate data. Client identities account information health data master card information etc. are returned on a website under delicate data. This information will also be held in the information about the appliance. Once this information is held incorrectly by secret writing or parsing of no victimization it will be responsible to the attackers.

Implication [11]

- Victimization of this vulnerability will outcome in an attacker modifying such infirm understanding to fraud or alternative crimes.

Vulnerable objects [11]

- Data on the application.

2.5 Types of Webserver Attackers

Attackers are people or teams arranged by the agency of the United Nations to exploit vulnerability for private use. Attackers have an interest in everything from credit cards to product styles and price.

2.5.1 Amateurs

These people are commonly referred to as script kiddies. They are typically very talented attackers generally victimizing current instructions on sand lance attacks found on the internet. Some are merely inquisitive while others attempt to clarify and injure their skills.

2.5.2 Hackers

The attackers cluster compelled the lock networks to enter. These assailants are classified as white gray or black caps based on the intention of breaking and entering. Weaknesses were compelled by the white hat attackers to make the locking networks more secure. on the contrary black hat aggressors profit from any felonious private monetary or political gains vulnerability. Somewhere between white and black hat aggressors there are gray hat aggressors.

2.5.3 Organized Hackers

In general cyber criminals are teams of qualified criminals aimed at leadership authority and wealth. The criminals are highly sophisticated and organized and could even give distinct criminals legal breaches as a service. These assailants are usually highly educated and funded and their attacks are aimed at particular objectives that your nation needs.

2.5.4 White hat hacker

These are the moral hackers United Nations agency which continuously use programming abilities ethics and legal features white hackers can undertake network entry to resolve their pc security systems information by victimizing networks and systems. Developers are rumored to address security vulnerabilities before they are susceptible.

2.5.5 Gray hat hackers

These are people who anticipate iniquities by UN agencies and who can do evil things but not for personal gains or harm. One instance would be someone who establishes a network by the United Nations but does not then publicly disclose the vulnerability.

Once your network has been established a gray hacker may reveal a vulnerability to the concerned organization. This allows the company to change the situation.

2.5.6 Black hat hackers

These are ethical criminals UN agency for personal purposes or for malicious purposes such as offensive networks which violate computer security and network security.

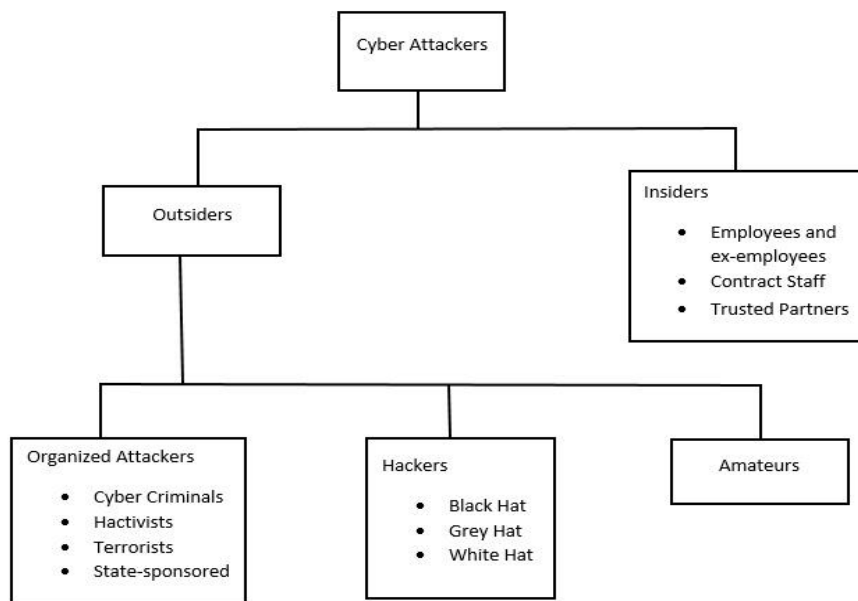


Figure 2.4: Cyber Attackers

Internal Security Threats

Attacks may be caused by an enterprise at intervals or by a company as shown in figure 2.4. An enclosed user will by opportunity or deliberately as an employee or contract partner acquire an understanding of confidentiality.

- Enable assaults externally via the business computer system by linking the infected USB technique.

External Security Threats

External threats from amateurs or excellent attackers will harness web vulnerabilities or to use social engineering to attain entry.

2.6 Webservice Attacks

Web Server Attacks types are given below.

2.6.1 DOS attack

During such assaults malicious buyers automatically send a wide range of insurances to the target net server. While the http-get calls are formatted and sent via conventional login [14]. An attacker could cause a dos attack by causing various serving insurance packets fatal the coupling capability of the net server or he could attempt to exploit a computer error within the application inflicting a dos attack [12].

2.6.2 Misconfiguration attacks

When redundant service is activated or default setup files are being implemented error information should not have been intended to an attacker will solve the net server by countless attacks such as Arcanum cracking injection of error-based SQL injection command etc. [12].

2.6.3 Phishing Attack

An attacker may send the victim to revised web sites by emailing him herself to an invisible link but he she will be redirected to the revised internet site by thieving his her information. Several alternative attacks are made on web implementation which could

lead to an assault by an internet server: interference-type parameter cookie interference unapproved inputs SQL injection buffer overflow attacks [12].

2.6.4 Password Attacks [12]

- Guessing/Default passwords
- Brute Forcing
- Wordbook Attacks.

2.7 Vulnerability Identification

Most useful vulnerability scanner

- OpenVAS
- Nexpose Community
- Nikto
- Wireshark
- Nessus Professional

2.7.1 OpenVAS

That's an average person vulnerability scan tool [13].

- Works seem to be accessible and typically registered there under wildebeest state and local government domain covers multiple processing techniques.
- Custom spot associated security problems on servers as well as separate connected devices could be an all in one vulnerability assessment tool.

2.7.2 Nexpose Community

Rapid7 uses it as an open source instrument to scan the vulnerabilities and execute countless web checks [13].

- It's used to control the vulnerability revealer over time and also to educate itself with fresh problems in modern understanding.
- Some vulnerability scanners generally identify high-or medium-or low-scale threats.
- A metasploit framework is often mobilized.

2.7.3 Nikto

It can be a tremendously loved and open source net scanner used to evaluate the likely issues and vulnerabilities [13].

- Additionally it is customary to approve the server version as to whether or not it is out-of-date and in addition to check for any particular disadvantage that senses the functioning of the server.
- Numerous protocols such as communication protocol https HTTPS etc. are scanned using this tool to scan various server ports.

2.7.4 Wireshark

It is that network protocol tool that is prominent and widely used in the world [13].

- It is used across a variety of channels such as academic institutions public organizations companies and so on to appear in microscopic equality in the networks.
- It has the ability to inspect several protocols thoroughly with extra extra protocols all the time.

2.7.5 Nessus Professional

The vulnerability scanner created by sensitive information security is generic as well as stained [13].

- This tool has been introduced and has been used by large clients worldwide for vulnerability evaluation installation problems etc.
- It can be used to avoid systems from either the high penetration generated by hackers by evaluating vulnerabilities as soon as possible.

CHAPTER 3

WORKING PROCEDURE

Vulnerabilities appear daily. We would like constant intelligence to get them, find them, order them for your business, and make sure your exposure has been reduced. Nexpose, Rapid7's on premise choice for vulnerability management code, monitors exposures in period of time and adapts to new threats with contemporary information, making certain you'll perpetually act at the instant of impact.

Get a real-time view of risk

1. Notice new devices and vulnerabilities as presently as they enter your network with adaptation security.
2. Integrate with virtualization and cloud infrastructure answer like VMWare and AWS/Azure to know changes to your network.
3. Hook into Rapid7's web wide scanning analysis initiative, Project echo sounder, to know your external exposure quicker than the attackers.

Know where to focus

1. Produce quality teams with 50+ filters that mechanically update when each scan to stay up with dynamic networks.
2. Tag necessary assets as important to filter them to the highest of your remedy reports.
3. Grasp that vulnerabilities are often actively exploited – and which to mend initial – via Metasploit integration.

Set IT up for Success

1. Redress reports embrace the highest twenty five actions which will cut back the foremost risk, similarly as clear directions on precisely what to try and do.

2. Produce trending reports for management to indicate ROI and progress of your security program.
3. Scan systems for policy misconfigurations to make sure your security controls are operating properly.

3.1 Vulnerability Scanning with Nexpose

Vulnerability scanning an evaluation is the technique that identifies and evaluates the vulnerabilities within the same internet environment. A vulnerability a quality that an attacker exploits may be a feature of performing unlawful access to secret data injecting encrypted data or generating a resource assault rejection. It is vital to spot and repair security vulnerabilities that can reveal a value to an assault in order to protect safety violations. Use Nexpose to check a vulnerability network. Nexpose describes the effective facilities accessible servers and apps functioning of each device and tries to detect vulnerabilities which will occur supported by metaphorical systems and apps characteristics. Nexpose reveals the leads to a scan record which will assist you assign vulnerabilities that support the threat issue and monitor most efficient response to be implemented. Nexpose incorporates to metasploit specialists who provide a vulnerability analysis and confirmation instrument which helps remove false results simply check vulnerabilities and investigate corrective action. There's a number of forms you'll just be using Nexpose's metasploit expert. Metasploit specialist offers a link which facilitates you to use a Nexpose controller to check a vulnerability straight from inside the net panel as well as to mechanically transfer the survey outcomes in to a task. To execute vulnerability detection and verification you would be able to operate searches from Nexpose and enter a test records into metasploit specialist. You chose on its best approach for you.

3.2 Nexpose Terminology

Some conditions take problem for those working in metasploit in Nexpose. Here are a few Nexpose concepts you will have to get acquainted with:

- Quality — a service provider bunch.
- Website — a practical resource cluster featuring a specific scanning motor. A website runs over an extended amount of your time and provides you with trend-setting historical data and is comparable to a metasploit experiment.
- Scan example — A model that describes the amount of inspection used among Nexpose to check its vulnerability.

3.3 Some features of Nexpose community

1. Real Risk of Score
2. Safety Adaptive
3. Policy Evaluation
4. Reporting of the Remedy
5. Metasploit Integration

3.3.1 Real Risk of Score

The standard rating of 1-10 CVSS leads to hundreds of vulnerabilities critical. The real risk of score from vulnerability scanner offers a lot of unfair insight. bringing into account its period of vulnerability also as government exploits malicious software packages our scale of 1-1000 highlights the vulnerabilities which can be used in associated degree attacks which will serve you as really important issues. Once used with our robust tagging scheme you can even mechanically rank the systems that are most important to your company.

3.3.2 Safety Adaptive

Reactive monitoring from occasional information pours is filled with false alarms and off understanding. With Nexpose adaptation safety the instant they enter your system you will mechanically notice and evaluate fresh equipment and new vulnerabilities.

Paired with strong links to VMWare and AWS and inclusion with scientific analysis on navigational instruments Nexpose offers real virtual observation of your vibrant workplace.

3.3.3 Policy Evaluation

Hardening your devices is only as essential as identifying and fixing vulnerabilities. To assist you benchmark your devices against popular norms such as cis and NIST Nexpose offers embedded policy scanning. Intuitive remediation reports give you instructions on the actions you might choose to create the greatest impact on compliance in tiny phases.

3.3.4 Reporting of the Remedy

Help IT make you easier. With reports of Nexpose correction show it the twenty-five actions they will take immediately to reduce the main risk. Your knowledge may simply be sliced and diced to convey the accurate data they need to induce their work done to the right folks while not walking through 10 000 page reports or manual spreadsheets.

3.3.5 Metasploit Integration

In the case of an real attack the objective of any safety item is to shore up your defenses— what greater thanks to looking at them than by simulating one with metasploit specialist you will validate an automatic closed-loop system technique of victimizing your vulnerability scanner outcomes making sure you prioritize the most important assets mechanically first: those that are best to break.

3.4 Procedures

First we're entering the browser and shifting to the localhost Nexpose and showing us the home page of Nexpose.

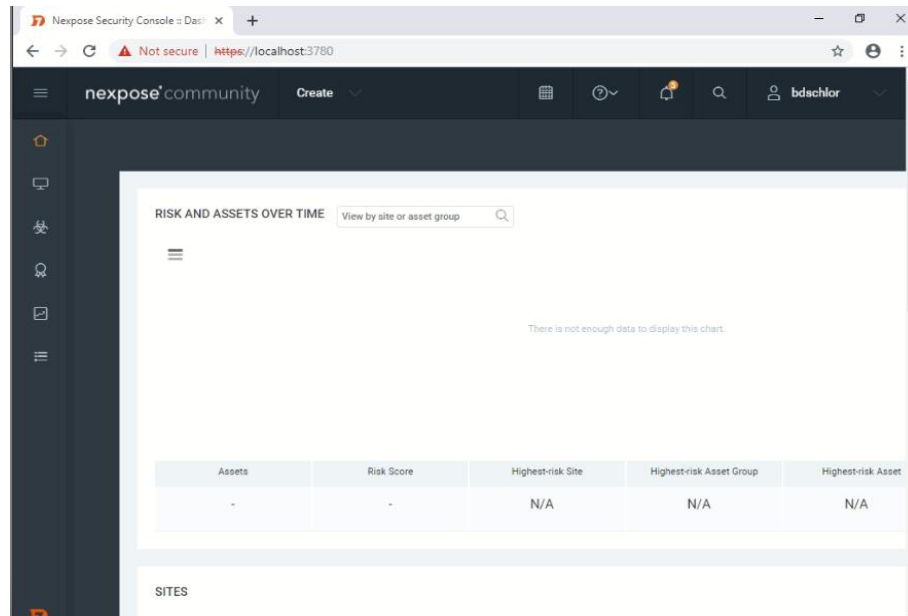


Figure 3.1: Nexpose Home Page

There was still a variety of “Create site” on the home page clicked on it and so it gave configurations for “Site configuration”. We gave a name “Site”. Set the “High” importance and add some site interpretation.

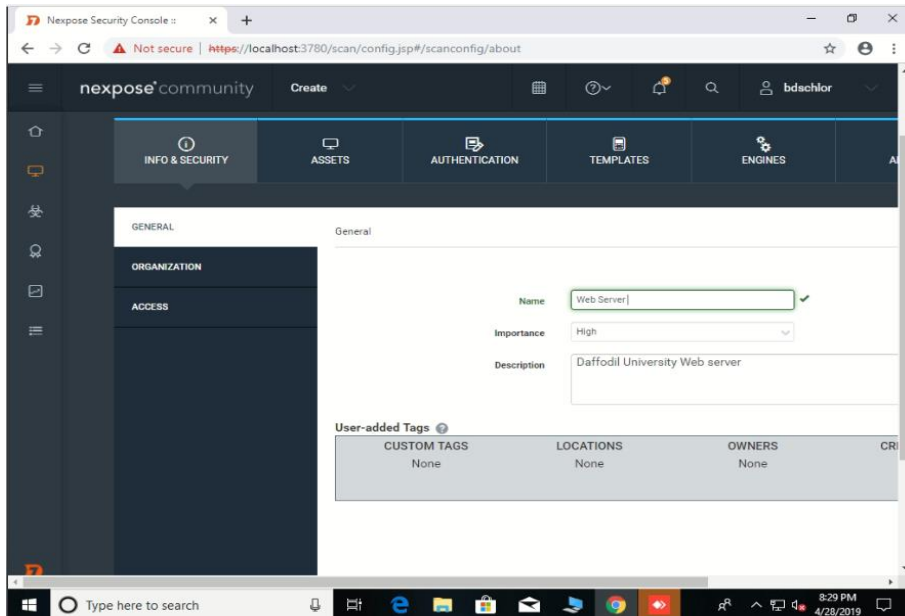


Figure 3.2: Creating a Site

The “Assets” settings page has two parts as shown in the figure below: “Included assets” and “Excluded assets”. We supply two destination IP addresses in the included assets section. If you have a chosen IP number instead of using the import list feature you can insert the document. To exclude assets from processing excluded assets is being used. If you choose to check the entire IP variety that exclude a few of the IPs from of the test place those IPs in protected assets.

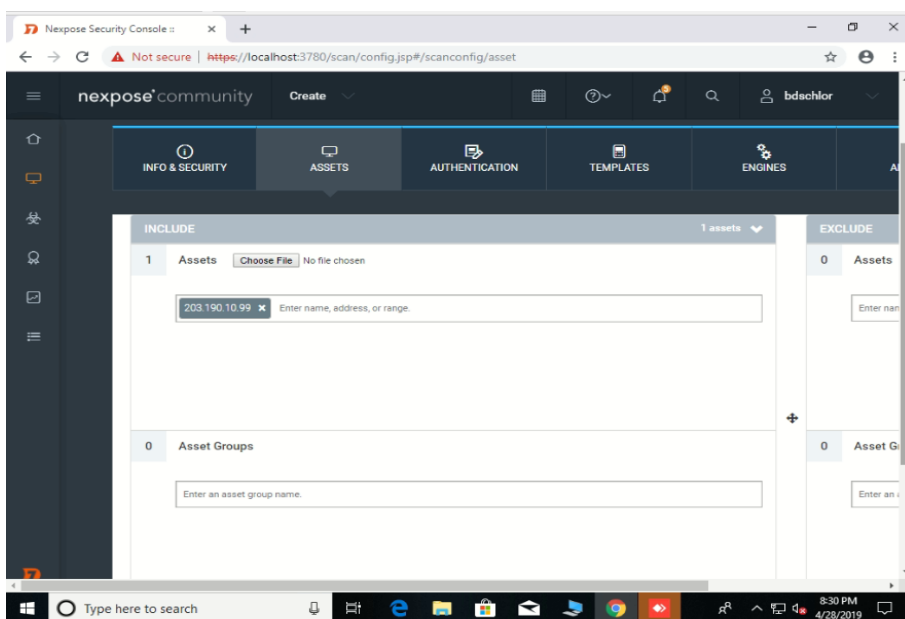


Figure 3.3: The Assets

The next configuration is for "Templates," pick a template, and that for our test we using the "Full audit" template.

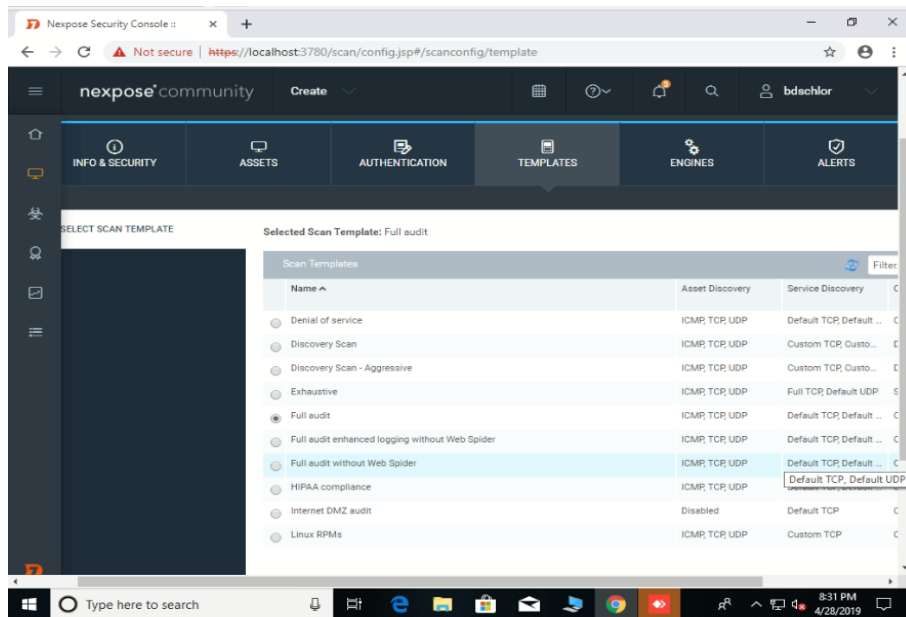


Figure 3.4: The Templates

An option to "Save and Scan" was reflected. Clicked on it and made the configurations and gave a site document. As shown in the following figure:

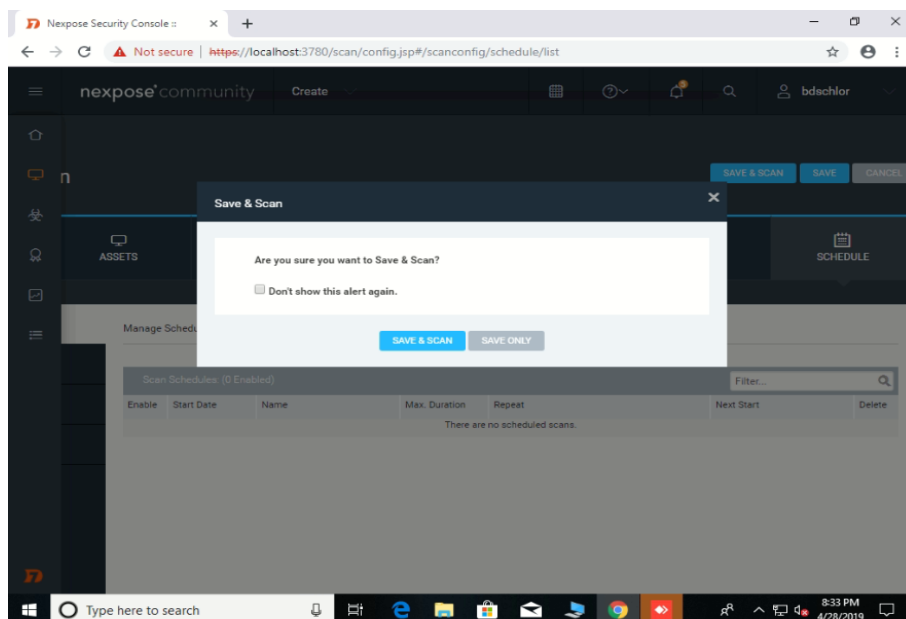


Figure 3.5: Save and Scan

CHAPTER 4

PERFORMANCE MEASUREMENT OF WEB SERVER

Web application security vulnerabilities like cross-site scripting, SQL injection, and Cross-site request forgeries are recognized problems with thousands of vulnerabilities indicated each year. These vulnerabilities allow attackers to perform envious actions that range from occurrence unauthorized account access to attachment sensitive data like credit card numbers. Because of the risks of web application vulnerability redress has been mobilized into the willingness process of major commercial and governmental standards. Web application scanners that find out vulnerabilities and generate compliance reports. Since the last few years, the web vulnerability scanner market has become a very active commercial space. The Nexpose scanner runs as a network service approached by browser via an IP port. It generate http requests as test vectors and analyze the http reply sent by the web server for vulnerabilities.

4.1 Daffodil International University Web Server Vulnerability

Vulnerabilities by Severity table given below

Table-1: Summary of Vulnerabilities by severity

SL. No.	Category of Vulnerabilities	Number of Vulnerabilities
01	Critical	01
02	Severe	10
03	Moderate	02

During this scan, 13 vulnerabilities were identified. One of these vulnerabilities were critical. Immediate attention is needed to address critical vulnerabilities. They are comparatively simple to exploit for attackers and can give them complete control of the impacted systems. There were 10 severe vulnerabilities. Significant vulnerabilities are often more difficult to exploit and may not provide equal access to impacted systems. There were 02 found moderate vulnerabilities. These often provide attackers with data

that can help them to mount subsequent assaults on your network. These should be corrected timely as well, but they are not as important as the other vulnerabilities.

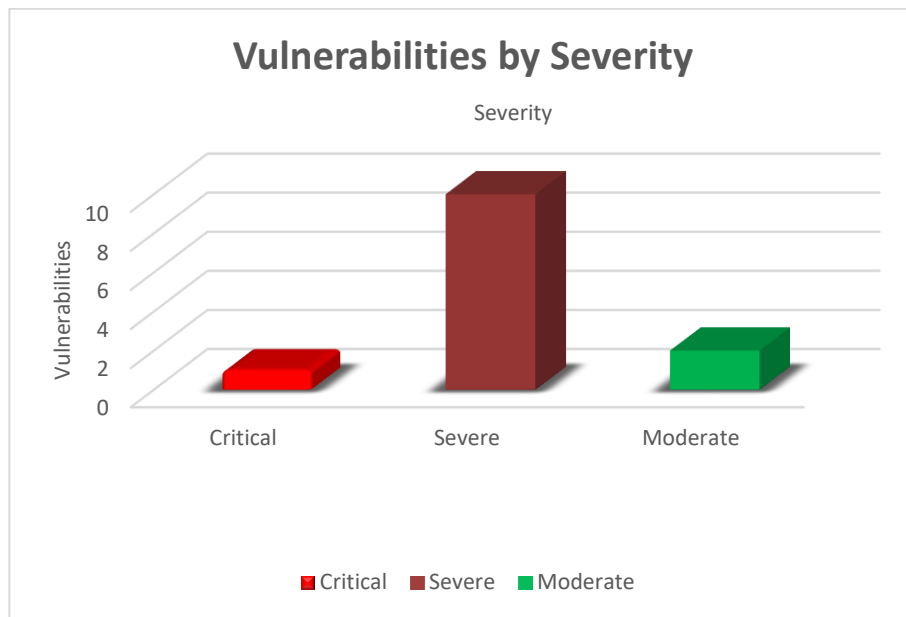


Figure 4.1: Summary of Vulnerabilities

The most common vulnerability of this webserver are Joomla!, Mail, CSRF, HTTP, IMAP, Network, POP, Remote execution, SMPT, Web. We converted the total vulnerability into 100%.

Formula of Performance Measurement

$$\text{Percentage of vulnerability} = \frac{\text{Number of vulnerability}}{\text{Total number of vulnerability}} \times 100\%$$

Example:

For Joomla!

Here,

Number of Vulnerability = 8

Total Number of Vulnerability = 18

$$\text{Percentage of vulnerability} = \frac{8}{18} \times 100\% = 44.444\%$$

The percentage of vulnerability category given below

Table-2: Summary of Vulnerability Category

SL. No.	Name of vulnerability	Number of vulnerability (Approximate)	Percentage of vulnerability = $\frac{\text{Number of vulnerability}}{\text{Total number of vulnerability}} \times 100\%$
01	Joomla!	08	44.444%
02	Mail	02	11.111%
03	CSRF	01	5.556%
04	HTTP	01	5.556%
05	IMAP	01	5.556%
06	Network	01	5.556%
07	POP	01	5.556%
08	Remote execution	01	5.556%
09	SMTP	01	5.556%
10	Web	01	5.556%
		Total = 18	Total = 100%

There were 1 occurrences of the joomla-20180801-core-hardening-the-inputfilter-for-phar-stubs, imap-plaintext-auth, joomla-20181002core-inadequate-default-access-level-for-com-joomlaupdate, joomla-20181004-core-acl-violation-in-com-users-for-the-adminverification, joomla-20181005-core-csrf-hardening-in-com-installer, pop-plaintext-auth, joomla-20180803-core-acl-violation-in-customfields, smtp-general-vrfy, joomla-20180802-core-stored-xss-vulnerability-in-the-frontend-profile and joomla-20181001-core-hardeningcom-contact-contact-form vulnerabilities, forming them the most common vulnerabilities. There were 8 vulnerability instances in the Joomla! Category, forming it the most common vulnerability category.

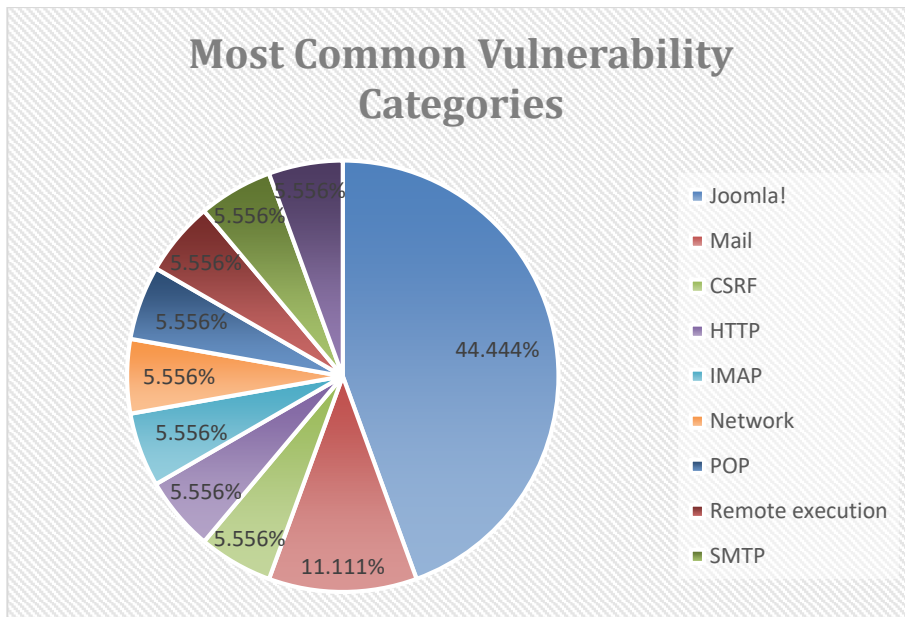


Figure 4.2: Common Vulnerability Categories

One operating system was identified during this scan. There were 7 services discovered to be running during this scan.

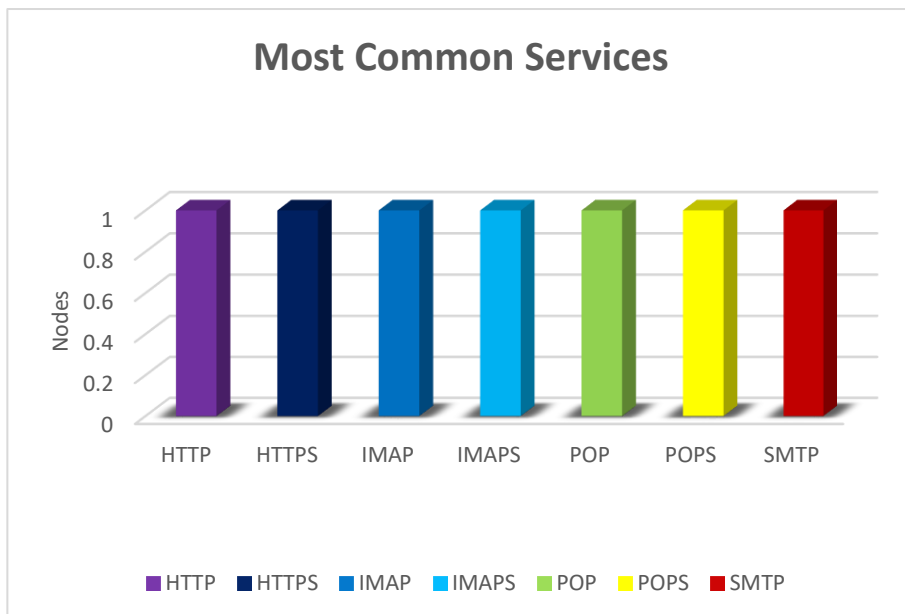


Figure 4.3: Common Services

The HTTP, HTTPS, IMAP, IMAPS, POP, POPS and SMTP services were discovered on 1 systems, forming them the most common services.

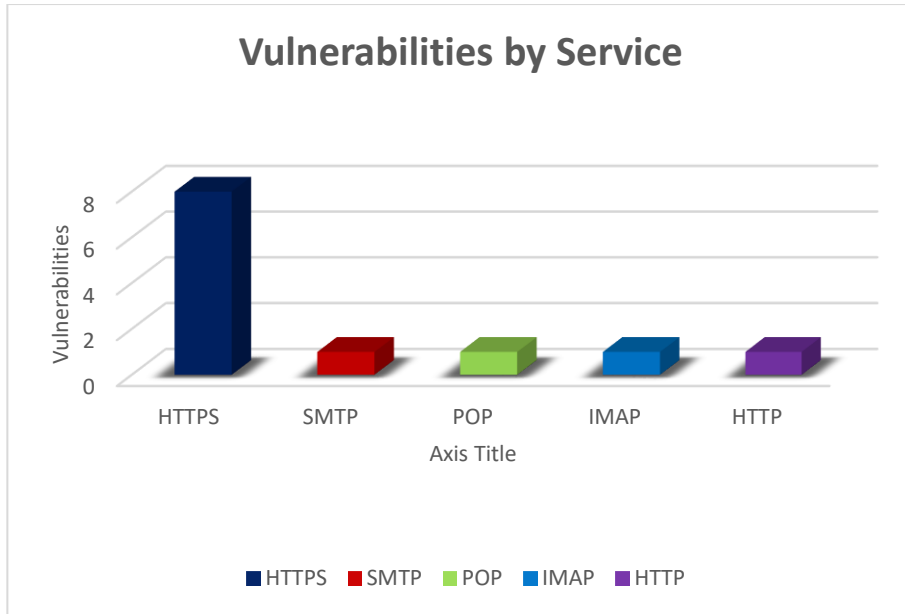


Figure 4.4: Vulnerabilities by Service

The HTTPS service was discovered to have the most vulnerabilities during this scan with 8 vulnerabilities.

4.2 SomReP Organization Vulnerability

Vulnerabilities by Severity table given below

Table-3: Summary of Vulnerabilities by severity

SL. No.	Category of Vulnerabilities	Number of Vulnerabilities
01	Critical	03
02	Severe	28
03	Moderate	04

During this scan, 35 vulnerabilities were identified. Three of these vulnerabilities were critical. Immediate attention is needed to address critical vulnerabilities. They are comparatively simple to exploit for attackers and can give them complete control of the impacted systems. There were 28 severe vulnerabilities. Significant vulnerabilities are often more difficult to exploit and may not provide equal access to impacted systems. There were 4 found moderate vulnerabilities. These often provide attackers with data

that can help them to mount subsequent assaults on your network. These should be corrected timely as well, but they are not as important as the other vulnerabilities.

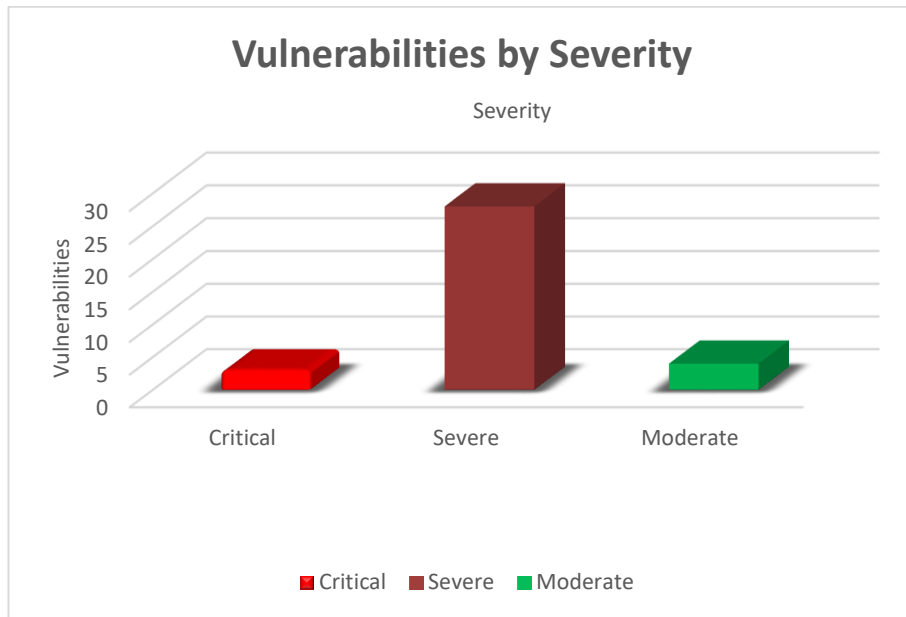


Figure 4.5: Summary of Vulnerabilities

The most common vulnerability of this webserver are Apache, Apache HTTP server, Web, Denial of service, IAVM, Network, LDAP, Privilege Escalation, Remote execution, Rapid7 critical. We converted the total vulnerability into 100%.

The percentage of vulnerability category given below

Table-4: Summary of Vulnerability Category

SL. No.	Name of vulnerability	Number of vulnerability (Approximate)	Percentage of vulnerability = $\frac{\text{Number of vulnerability}}{\text{Total number of vulnerability}} \times 100\%$
01	Apache	56	26.923%
02	Apache HTTP server	56	26.923%
03	Web	56	26.923%
04	Denial of service	16	7.692%
05	IAVM	10	4.808%
06	Network	07	3.365%
07	LDAP	02	0.962%

08	Privilege Escalation	02	0.962%
09	Remote execution	02	0.962%
10	Rapid7 critical	01	0.481%
		Total = 208	Total = 100%

There were 2 occurrences of the apache-httpd-cve-2017-3167, apache-httpd-cve-2017-3169, apache-httpd-cve-2017-7679, apachehttpd-cve-2017-15715, apache-httpd-cve-2018-1312, apache-httpd-cve-2017-9788, apache-httpd-cve-2016-0736, apache-httpd-cve-2016-2161, apache-httpd-cve-2016-4979 and apache-httpd-cve-2016-5387 vulnerabilities, forming them the most common vulnerabilities. There were 56 vulnerability instances in the Apache, Apache HTTP Server and Web categories, forming them the most common vulnerability categories.

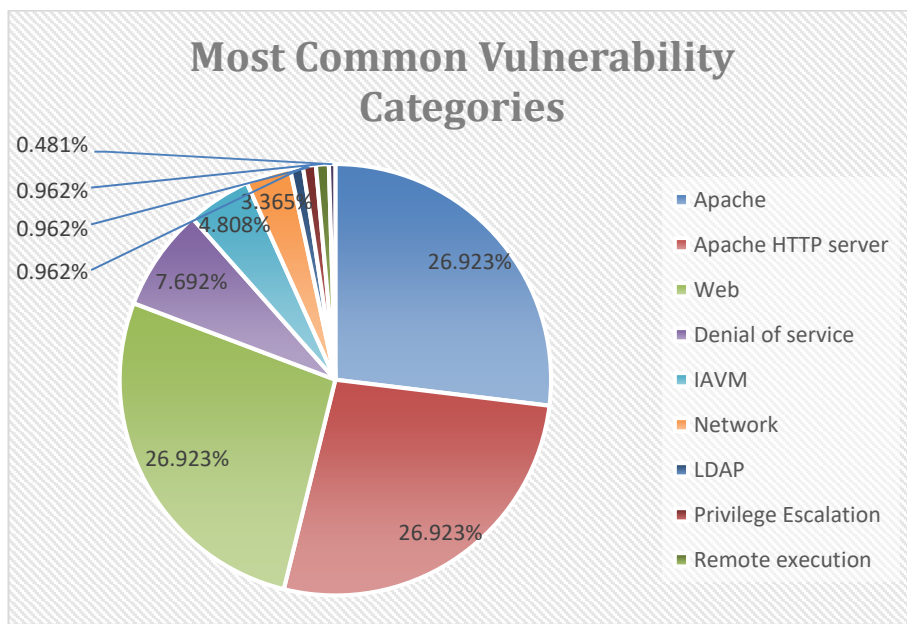


Figure 4.6: Common Vulnerability Categories

One operating system was identified during this scan. There were 3 services discovered to be running during this scan.

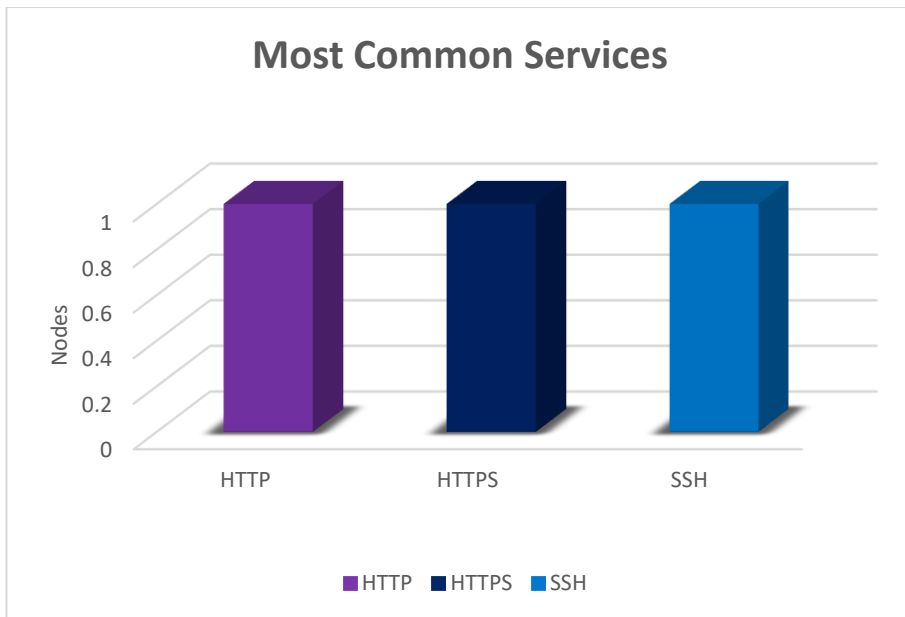


Figure 4.7: Common Services

The HTTP, HTTPS and SSH services were discovered on 1 systems, forming them the most common services.

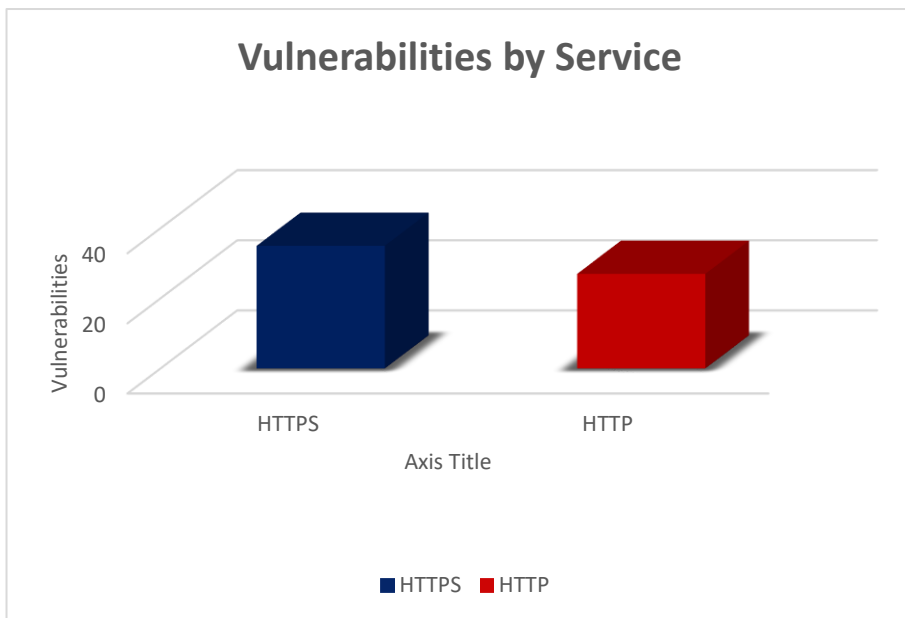


Figure 4.8: Vulnerabilities by Service

The HTTPS service was discovered to have the most vulnerabilities during this scan with 35 vulnerabilities.

4.3 Xitech BD Vulnerability

Vulnerabilities by Severity table given below

Table-5: Summery of Vulnerabilities by severity

SL. No.	Category of Vulnerabilities	Number of Vulnerabilities
01	Critical	13
02	Severe	30
03	Moderate	09

During this scan, 52 vulnerabilities were identified. Thirteen of these vulnerabilities were critical. Immediate attention is needed to address critical vulnerabilities. They are comparatively simple to exploit for attackers and can give them complete control of the impacted systems. There were 30 severe vulnerabilities. Significant vulnerabilities are often more difficult to exploit and may not provide equal access to impacted systems. There were 9 found moderate vulnerabilities. These often provide attackers with data that can help them to mount subsequent assaults on your network. These should be corrected timely as well, but they are not as important as the other vulnerabilities.

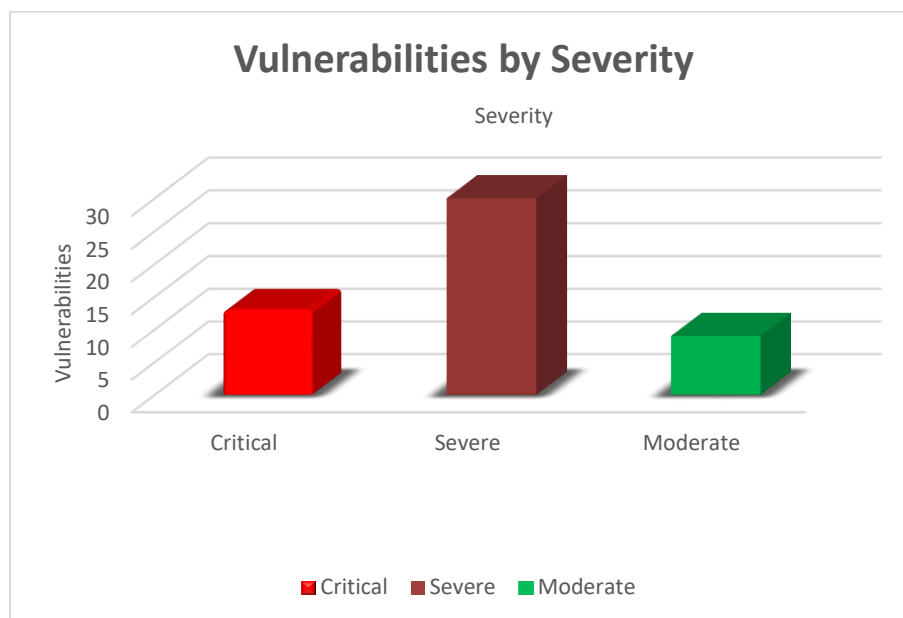


Figure 4.9: Summery of Vulnerabilities

The most common vulnerability of this webserver are DNS, ISC, ISC BIND, Denial of service, Network, IAVM, HTTP, Web, Mail, SMTP. We converted the total vulnerability into 100%.

The percentage of vulnerability category given below

Table-6: Summary of Vulnerability Category

SL. No.	Name of vulnerability	Number of vulnerability (Approximate)	Percentage of vulnerability = $\frac{\text{Number of vulnerability}}{\text{Total number of vulnerability}} \times 100\%$
01	DNS	65	20.44%
02	ISC	65	20.44%
03	ISC BIND	65	20.44%
04	Denial of service	49	15.409%
05	Network	35	11.006%
06	IAVM	14	4.403%
07	HTTP	08	2.516%
08	Web	08	2.516%
09	Mail	05	1.572%
10	SMTP	04	1.258%
		Total = 318	Total = 100%

It was 8 occurrences of the certificate-common-name-mismatch and tls1_1-enabled vulnerabilities, forming them the most common vulnerabilities. There were 65 vulnerability instances in the DNS, ISC and ISC BIND categories, forming them the most common vulnerability categories.

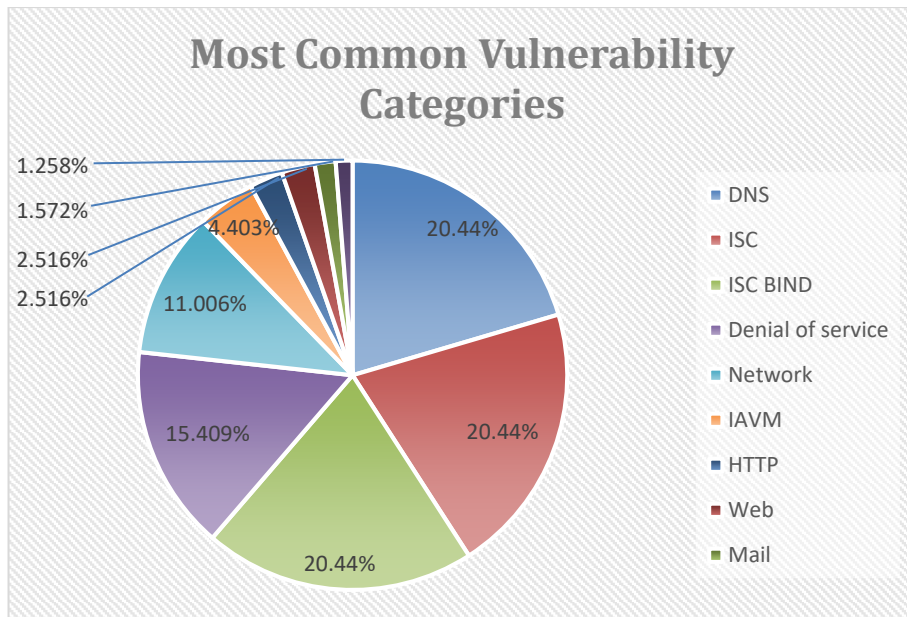


Figure 4.10: Common Vulnerability Categories

During this scan, one operating system was recognized. 11 services were found to run during this scan.

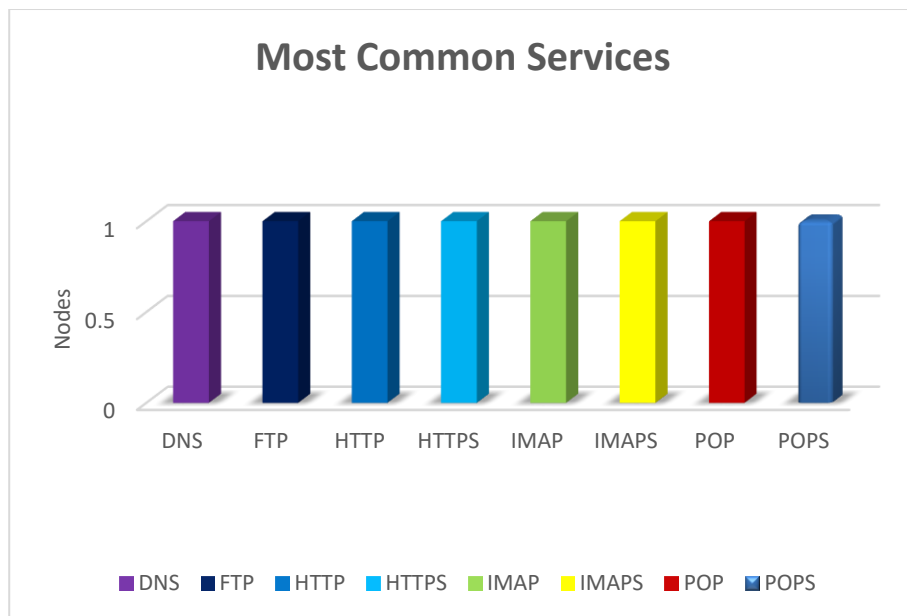


Figure 4.11: Common Services

The DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, POP and POPS services were discovered on 1 systems, forming them the most common services.

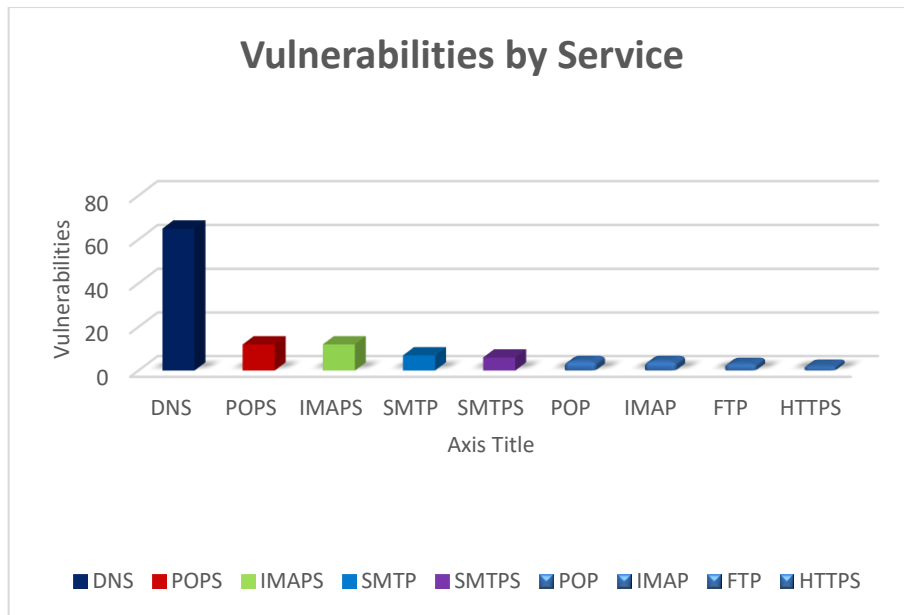


Figure 4.12: Vulnerabilities by Service

The DNS service was discovered to have the most vulnerabilities during this scan with 65 vulnerabilities.

4.4 Campus TV Vulnerability

Vulnerabilities by Severity table given below

Table-7: Summary of Vulnerabilities by severity

SL. No.	Category of Vulnerabilities	Number of Vulnerabilities
01	Critical	00
02	Severe	00
03	Moderate	01

During this scan, one vulnerability was detected. No critical vulnerabilities have been identified. Critical vulnerabilities require instant attention. They are comparatively simple for attackers to exploit and can provide the impacted systems with complete energy.

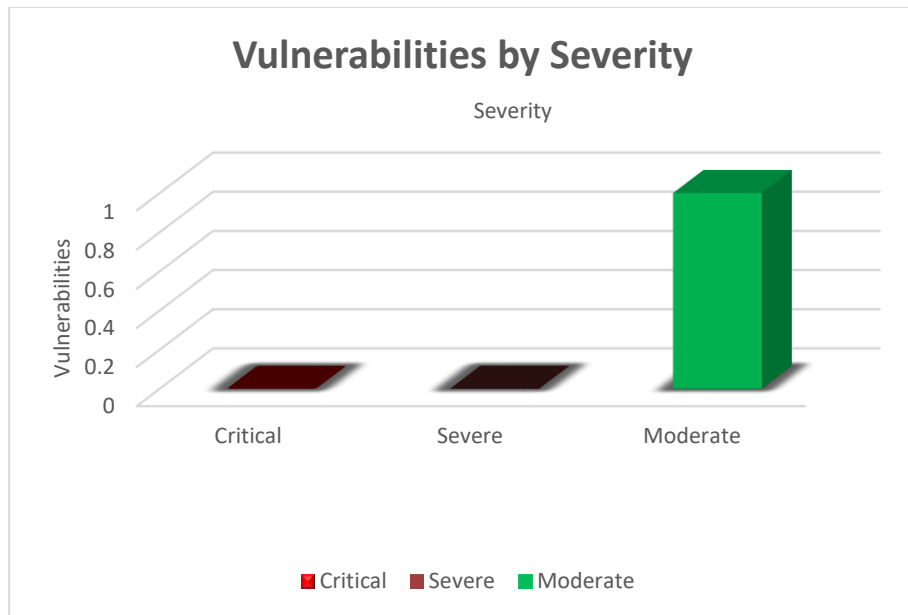


Figure 4.13: Summary of Vulnerability

There have been no serious vulnerabilities. Significant vulnerabilities are mostly more difficult to exploit and may not provide the same access to affected systems. There was one discovered moderate vulnerability. These mostly provide attackers with information that may help them mount subsequent attacks on your network. These vulnerabilities should also be fixed in a timely manner, but are not as instantaneous as the others.

CHAPTER 5

RESULTS AND ANALYSIS

5.1 Risk Score Calculation

We used to calculate risk score for web server is given below [17]

$$\text{Risk} = \frac{\text{time*proximity based impact}}{\text{exploit difficulty}}$$
$$\text{Risk} = \frac{\sqrt{t}*(AV+C+I+A)!}{(AC+Au)^2}$$

Where,

t (Time-based likelihood) = the number of days as vulnerability publicly disclosed.

AV (access vector) = locally access webserver from outside the network.

C (confidentially impact) = disclosure to unauthorized system.

I (integrity impact) = unauthorized data modification.

A (availability impact) = loss of access to data.

AC (access complexity) = it based on how much skill is needed to perform the exploit.

Au (authentication) = it based on authentication requirements.

5.2 Daffodil International University Risk

The imap-plaintext-auth and pop-plaintext-auth vulnerabilities pose the greatest risk to the institution and it risk score of 866. Risk scores are calculated by based on the types and numbers of vulnerabilities on affected port.

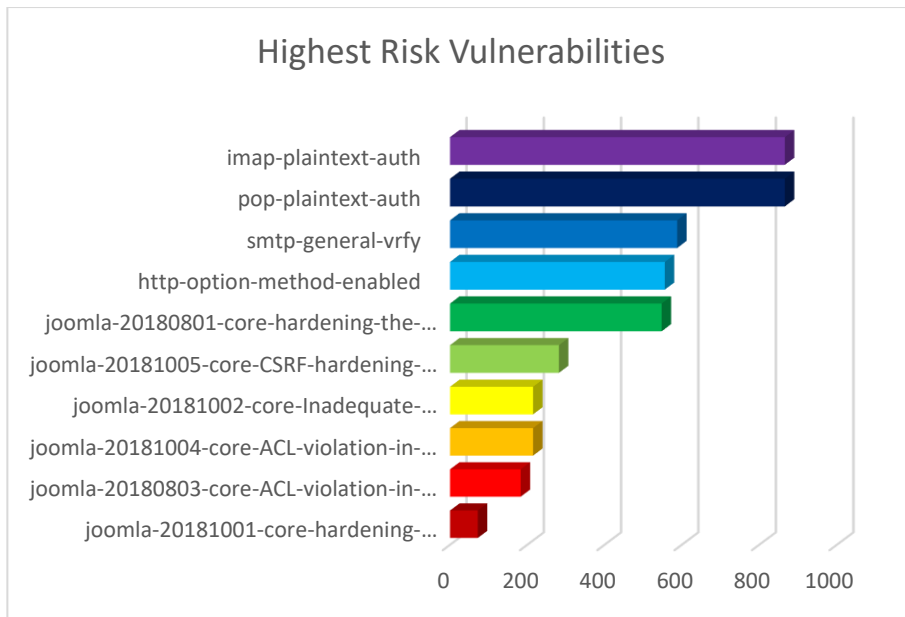


Figure 5.1: Highest Risk Vulnerabilities

5.3 SomReP Organization Risk

The apache-httpd-cve-2017-7679, apache-httpd-cve-2017-3167 and apache-httpd-cve-2017-3169 vulnerabilities pose the greatest risk to the institution and it risk score of 1,195. Risk scores are calculated by based on the types and numbers of vulnerabilities on affected port.

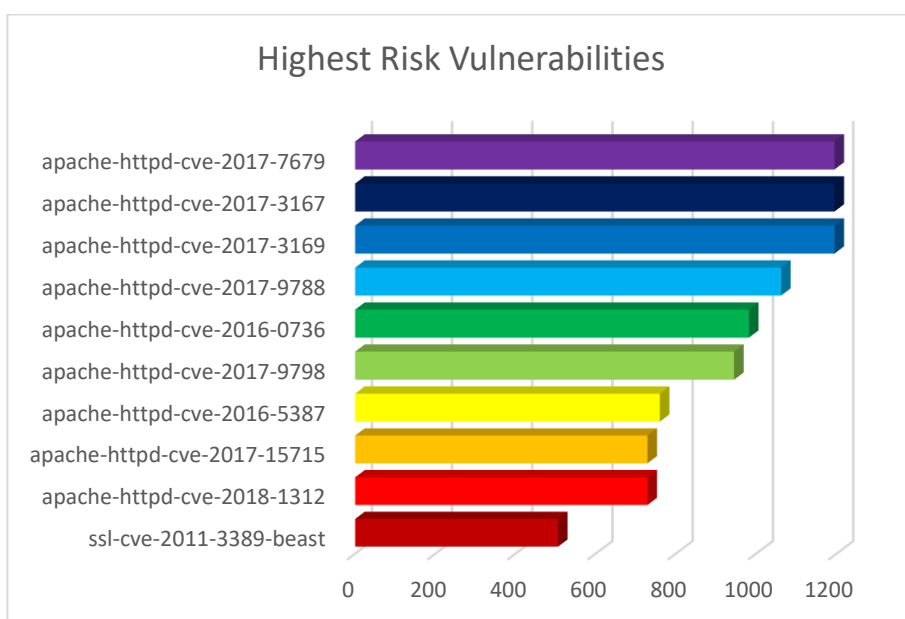


Figure 5.2: Highest Risk Vulnerabilities

5.4 Xitech BD Risk

The certificate-common-name-mismatch vulnerability pose the greatest risk to the institution and it risk score of 6,379. Risk scores are calculated by based on the types and numbers of vulnerabilities on affected port.

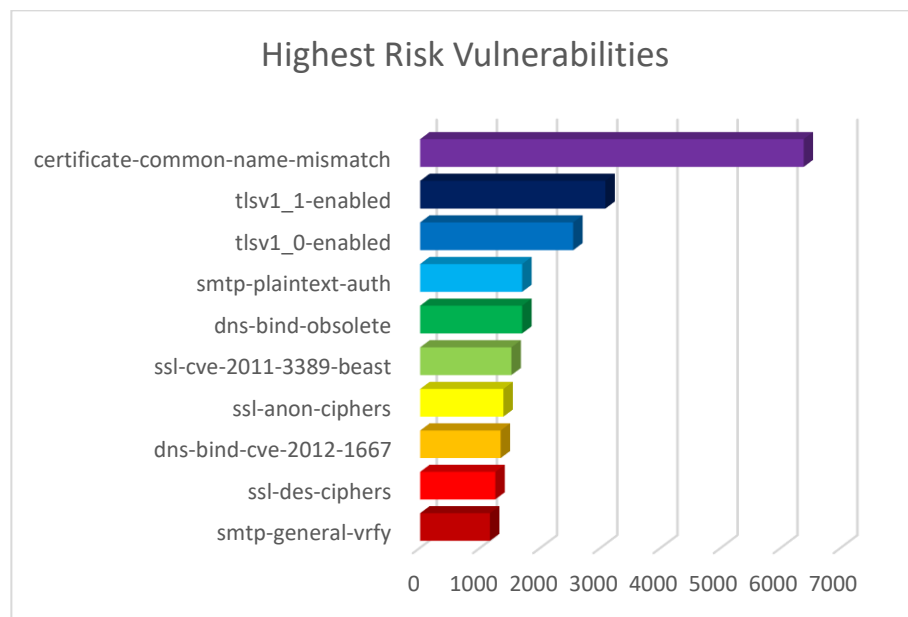


Figure 5.3: Highest Risk Vulnerabilities

5.5 Common Ports

A port is a termination of communication. Physical and wireless connections are entered at ports of hardware devices. Ports are gives multiple services and multiple communication sessions at the network address. The client-server were designed, a multiple service is established, and in order to that the multiple synchronic communication sessions is established for the identical service. Almost every port generally used TCP and UDP protocols.

The most common port numbers are

- 20: File Transfer Protocol (FTP) Data Transfer
- 21: File Transfer Protocol (FTP) Command Control

- 22: Secure Shell (SSH) Secure Login
- 23: Telnet remote login service, unencrypted text messages
- 25: Simple Mail Transfer Protocol (SMTP) E-mail routing
- 53: Domain Name System (DNS) service
- 68: DHCP (Dynamic Host Control Protocol)
- 80: Hypertext Transfer Protocol (HTTP) used in the World Wide Web
- 110: Post Office Protocol (POP3)
- 115: SFTP (Secure File Transfer Protocol)
- 119: Network News Transfer Protocol (NNTP)
- 123: Network Time Protocol (NTP)
- 143: Internet Message Access Protocol (IMAP) Management of digital mail
- 161: Simple Network Management Protocol (SNMP)
- 194: Internet Relay Chat (IRC)
- 220: IMAP3 (Internet Message Access Protocol 3)
- 443: HTTP Secure (HTTPS) HTTP over TLS/SSL

5.6 Web server port related services

5.6.1 HTTP

HTTP, the Hyper Text Transfer Protocol, is used to connect the client device and web server. Every multimedia files such as text, sound, images and video are generally used with HTTP.

5.6.1.1 Problem Identify and Approximate Solution

Many HTTP servers use BASIC as their primary mechanism for user authentication. This is a very simple plan that uses base 64 to encode the clear text user ID and password. If a malicious user monitoring HTTP traffic, user IDs and passwords can be

stolen by using decoding method from data. To secure the authentication procedure, use HTTPS to transmit the authentication data.

5.6.2 HTTPS

HTTPS, the Hyper Text Transfer Protocol over TLS/SSL. When TLS/SSL connection is established, must be standard HTTP protocol is applied. Every multimedia files such as text, sound, images and video are generally used with HTTP.

5.6.3 IMAP

IMAP, the Interactive Mail Access Protocol or Internet Message Access Protocol, is used to way in and manipulate electronic mail (email). IMAP servers can contain several folders, such as mailboxes, containing messages (e-mails) for users.

5.6.4 IMAPS

IMAPS, the Internet Message Access Protocol over TLS/SSL, is used encrypted (TLS/SSL) electronic mail (email) transfer. When TLS/SSL connection is established, must be standard IMAP protocol is applied. IMAP servers can contain several folders, known as mailboxes, containing messages (e-mails) for users.

5.6.5 POPS

The Post Office Protocol is used to repair email from a mail server. POPS simply adds SSL support to POP3.

5.6.6 SMTP

SMTP, the Simple Mail Transfer Protocol, is used in sending and receiving email. Clients typically submit outgoing e-mail to their SMTP server.

5.6.6.1 Problem Identify and Approximate Solution

Must be enable STARTTLS on the main program. All Unencrypted connection will be rejected. Normally SMTP used port 465 for outgoing mail but after enable STARTTLS they used port 587 for outgoing mail.

The most common security issue with SMTP servers is says open relay. Any servers which accept and relay mail from anywhere. When SMPT allows open relay, an unauthorized user or third parties (spammers) to use your mail server to send their spam to unwanted recipients. Promiscuous relay checks are performed on all over SMTP servers.

5.6.7 SSH

SSH, or Secure Shell, is also called Telnet protocol. Primarily it adds encryption and data integrity to Telnet, but can also produce superior authentication mechanisms such as public key authentication.

5.6.7.1 Reuse of personal Host keys

Shocking because it might sound however there are IP Addresses have the identical public host keys. These are preconfigured within the microcode of the many devices, specified each device of a given model shares the similar key try unless the user changes it.

5.6.7.2 Approximate Solution

- Use the newest software algorithms
- Don't share personal host keys

5.6.8 DNS

DNS, the naming service provide by Domain name system on the Internet. DNS is used to alter any names, such as www.rapid7.com to their corresponding IP address for network browsing.

5.6.8.1 Port 53 against Attack

Domain Hijacking

Generally domain hijacking is caused by lots of things associated with exploiting a vulnerability within the name registrar's system, however may be achieved at the DNS level at a time attackers head of your DNS records.

Distributed Reflection Denial of service

The final word goal of any DDoS is to overburden your network with an outsized variety of packets or a large number of bandwidth-consuming requests, to either overload your network capability or to exhaust your hardware resources.

DNS Tunneling

This is a sort of cyber-attack familiar to materialize encoded knowledge from alternative applications within DNS responses and queries.

In order to perform DNS tunneling, attackers must gain access to a compromised system, further as access to an inside DNS server, a site name and DNS authoritative server.

5.6.9 FTP

FTP, the File Transfer Protocol, is used to transfer files between systems. On the Internet, it is used to download files from a web site using a browser. FTP uses two connections, one for control connections applied to authenticate. The other connection is applied to transfer data.

5.6.9.1 Port 20 and 21 against Attack and Approximate Solution

FTP Bounce Attack

Once there's a logy network affiliation, individuals usually resort to employing a proxy FTP that makes the consumer instructs the info transmission directly between 2 FTP servers. A hacker will favor of this sort of file transfer and gain access knowledge transmitted over the network.

Packet Capture (or Sniffing)

The data transfer via FTP is in clear text, any sensitive data like usernames, passwords will be only scan network packet capture techniques like packet sniffing.

Spoof Attack

When a limited network address access to FTP servers, a cyber-criminal will use an external computer and can easily find out the host address of a computer on the network, and transfer files without permission.

Approximate Solution

Managed File Transfer Remedies the Vulnerabilities in FTP

Managed file transfer (MFT) is the most suitable choice for file transfer compared to all other file sharing ways like mistreatment FTP, HTTP, TFTP, peer-to-peer file sharing and cloud drives. The MFT server software system provides secure internal, external and ad-hoc file transfers for each pull-based and push-based file transfers. In IPv4 or IPv6 network MFT transfer secure file via FTP, FTTPS, HTTP, and HTTPS. It monitor real time transfer file and notified them

5.7 Approximate Suggestions

5.7.1 Joomla!

Description

Some issue was discovered in Joomla! Inadequate checks regarding disabled fields can lead to a certain violation.

Vulnerability Solution

Check and update the Joomla! Version regularly.

5.7.2 Apache

Description

The affected asset is vulnerable to the vulnerability ONLY if it is running one of the Apache modules. Review the web server configuration for validation.

Vulnerability Solution

Check and update the Apache version regularly.

5.7.3 ISC Bind

Description

ISC BIND versions allow remote attackers to cause a denial of service (assertion failure and named daemon exit) via a query for a long resource record.

Vulnerability Solution

Check and update the ISC Bind version regularly.

5.7.4 SMTP server VRFY Vulnerability (smtp-general-vrfy)

Description

The SMTP "VRFY" command allows you to verify whether a system can hand over mail to a particular user. The "VRFY" command can be used by attackers to prepare the valid usernames on the target system.

Vulnerability Solution

Disable the EXPN and VRFY commands on your SMTP server.

5.7.5 HTTP OPTIONS Method enabled (http-options-method-enabled)

Description

Web servers that respond to the OPTIONS HTTP method reveal what other methods are supported by the web server, allowing attackers to narrow and intensify their efforts.

Vulnerability Solution

- Disable HTTP OPTIONS method
- Disable HTTP OPTIONS method on your web server. Refer to your web server's instruction manual on how to do this.

5.7.6 TCP timestamp response (generic-tcp-timestamp)

Description

TCP timestamp used remotely control the host. The TCP timestamp reaction can be used to approximate the remote host's uptime, as it potentially support in further attacks. In addition, some operating systems can be finger printed based TCP timestamps.

Vulnerability Solution

Disable TCP timestamp responses.

5.7.7 X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch)

Description

The X.509, subject common name (CN) field in certificate does not match the name of the entity appearing the certificate. The standard certificate validation process, the subject CN field of a certificate to match the original name of the presenting certificate. For example, in a certificate submitted by "https://www.example.com/", the CN should be "www.example.com".

In order to detect and prevent active eavesdropping attacks, the validity of a certificate must be verified, an attacker could man-in-the-middle attack and reach full control of the data system. It importance that the subject's CN must be match the name of the entity (hostname).

Vulnerability Solution

The X.509 subject's common name (CN) should be fixed the name of the entity introducing the certificate. This procedure of certificate usually signed by a Certification Authority (CA) trusted by both the client and server.

5.7.8 FTP credentials transmitted unencrypted (ftp-plaintext-auth)

Description

The server supports authentication methods in which credentials are sent in plaintext regarding unencrypted channels. If an attacker were to make up traffic between a client and this server, the credentials would be exposed.

Vulnerability Solution

Disable plaintext authentication methods and enable encryption for the FTP service. Refer to the software's documentation for particular instructions.

5.7.9 IMAP credentials transmitted unencrypted (imap-plaintext-auth)

Description

When a server supports authentication methods that credentials are sent in plaintext regarding unencrypted channels. If an attacker were to make up traffic between a client and this server, the credentials would be exposed.

Vulnerability Solution

Disable plaintext authentication methods for the IMAP service.

5.7.10 POP credentials transmitted unencrypted (pop-plaintext-auth)

Description

The server assistance authentication methods where credentials are sent in plaintext over unencrypted channels. If an attacker were to make up traffic between a client and this server, the credentials would be exposed.

Vulnerability Solution

Disable plaintext authentication methods for the POP service.

5.7.11 SMTP credentials transmitted unencrypted (smtp-plaintext-auth)

Description

The server supports authentication methods where credentials are sent in plaintext regarding unencrypted channels. If an attacker were to make up traffic between a client and this server, the credentials would be exposed.

Vulnerability Solution

Disable plaintext authentication methods for the SMTP service.

5.7.12 TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32) (ssl-cve-2016-2183-sweet32)

Description

Legacy block ciphers use 64-bit block size. As an attacker used in CBC technique and to find out the vulnerability easily. All versions of the SSL/TLS protocols use 3DES that condition the symmetric encryption cipher are affected. The current block cipher use 128-bit blocks. For example, AES. The birthday bound corresponds to 256 exabytes. When block cipher used 64-bit blocks, the birthday use only 32 GB, however it can easily reach vulnerable. Once an impact between two cipher blocks happens it is possible to use the impact to extract the plain text data.

Vulnerability Solution

Configure the server to disable support for 3DES suite.

5.7.13 TLS/SSL Server Supports RC4 Cipher Algorithms (CVE-2013-2566) (rc4-cve-2013-2566)

Description

Recent cryptanalysis results exploit biases in the RC4 key stream to recover frequently encrypted plaintexts. As a result, RC4 cannot provide sufficient security for SSL/TLS sessions. It has a single-byte bias, as a remote attacker can easily plaintext-recovery attacks via statistical analysis.

Vulnerability Solution

Configure the server to disable support for RC4 ciphers.

5.7.14 TLS/SSL Server is enabling the BEAST attack (ssl-cve-2011-3389-beast)

Description

The SSL protocol preferred in certain configurations of Microsoft Windows such the browser like Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera and other products negotiating SSL connections encrypts data by using CBC mode.

The attacker such man-in-the-middle attackers to gain plaintext HTTP headers via a block wise chosen boundary attack (BCBA) on an HTTPS session. It supported the affected protocols and ciphers, the server is enabling the clients in to being exploited.

Vulnerability Solution

There is no server-side cannot protect against the BEAST attack. Only one option, disable the influenced protocols (SSLv3 and TLS 1.0) and safe configuration is to help Authenticated Encryption with Associated Data (AEAD), e.g. AES-GCM, AES-CCM in TLS 1.2.

5.7.15 TLS/SSL Server Supports the Use of Static Key Ciphers (ssl-static-key-ciphers)

Description

The server was configured to support ciphers, it also known as static key ciphers. These ciphers cannot support "Ahead Secrecy". The new version of HTTP/2, this ciphers has been blacklisted.

Vulnerability Solution

Configure the server and disable static key cipher suites.

5.7.16 TLS/SSL Server Is Using Commonly Used Prime Numbers (tls-dh-primes)

Description

The server was used common prime number during the Diffie-Hellman key exchange. This makes the secure session vulnerable to a pre-count attack. An attacker can expend a significant amount of time to generate a lookup table for a particular prime number. This lookup table can then be favored to obtain the shared secret for the handshake and decrypt the session.

Vulnerability Solution

Configure the server to favor a randomly generated Diffie-Hellman group. It's recommend that you generate a 2048-bit group.

5.7.17 ICMP timestamp response (generic-icmp-timestamp)

Description

Remote host response to requests for ICMP timestamps. The ICMP timestamp response includes the date and time of the distant host. Using weak time-based random number generators in other facilities, this data could theoretically be preferred against some schemes.

Vulnerability Solution

Disable ICMP timestamp responses

5.7.18 TLS/SSL Server Supports 3DES Cipher Suite (ssl-3des-ciphers)

Description

Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) include cipher suites based on the 3DES (Triple Data Encryption Standard) algorithm. 3DES can provides an efficient security of 112 bits, it is considered close to end of life by some agencies. BSI Germany (from 2015) and ANSSI France (from 2014), some recommendation, 128 bit recommended symmetric size must be necessary after 2020. While NIST (from 2012) still considers 3DES being appropriate to favor until the end of 2030.

Vulnerability Solution

Configure the server to disable support for 3DES suite.

5.7.19 Nmap

Description

Nmap (Network Mapper) is a free and open source safety scanner that is supported by structuring the map of the computer network to identify hosts and services on a network. Primarily supported in network stock, safety auditing, promoting service administration agenda. Port scanning can be seen as a precursor to a network assault and should therefore not be performed without authorization on government Internet servers or on a business network.

Vulnerability Solution

For this condition “deny icmp any any” favor this command for a webserver.

CHAPTER 6

CONCLUSION

Vulnerability testing plays an important role to detect of any threats from the cyber criminals. Because of the simply way of implementation the web users can easily discover their leakage in their web server by using vulnerability testing. By using it the leakage of vulnerability in the web server will easily find out and reduced it. In this assessment, there show and identified the recent threats in the web server here also highlighted the awareness of cyber threats operation and prove how it effect the web users. In this project, there were given a proper suggestions to the author of the web server who want to get a web security in an economical way and it also proposed to improve the quality of vulnerability scanners. The over view of the work suggested that the mechanism can identify and stop the attacks and comparison the better performing among the all other tools.

REFERENCES

- [1] Abebe Abeshu Diro, Naveen Chilamkurti “Distributed Attack Detection Scheme using Deep Learning Approach for Internet of Things”.
- [2] TIAN Wei, YANG Ju-Feng, XU Jing, SI Guan-Nan,” Attack model based Penetration test for SQL injection vulnerability” 2012 IEEE 36th International Conferences on computer and software and applications Workshops.
- [3] M. Utting and B. Legiard Practical Model-Based Testing - A tools Approach, Morgan and Kaufman Eds. San Francisco,CA, USA Elsevier Science,2006.
- [4] Jose Fonseca, Marco Vieira, Henrique Maderia ,” Testing and comparing web vulnerabilities scanning tools for SQL injections and XSS attacks, 13th IEEE international symposium on Pacific Rim Dependable Computing.”
- [5] Iberia Medeiros, Miguel Beatriz, Nuno Neves and Miguel Correia, ”Detecting injection attacks and vulnerabilities inside the DBMS ”.
- [6] Giuseppe Antonio Di Lucca, Anna Rita Fasolino, Francesco Faralli, Ugo De Carlini , “Testing Web Applications”.
- [7] The Biggest Cybersecurity Disasters of 2017 So Far (n.d) [Online]. Available: <https://www.wired.com/story/2017-biggest-hacks-so-far/> [Accessed: 09-May-2019].
- [8] The Worst Cybersecurity Breaches of 2018 So Far (n.d) [Online]. Available: <https://www.wired.com/story/2018-worst-hacks-so-far/> [Accessed: 09-May-2019].

- [9] Types of Security Vulnerabilities (n.d) [Online]. Available: <https://developer.apple.com/library/archive/documentation/Security/Conceptual/SecureCodingGuide/Articles/TypesSecVuln.html> [Accessed: 17-April-2019].
- [10] Types of Infections (n.d) [Online]. Available: <https://www.geeksforgeeks.org/worms-viruses-and-beyond/> [Accessed: 07-May-2019].
- [11] Most Common Web Security Vulnerabilities (n.d) [Online]. Available: <https://www.guru99.com/web-security-vulnerabilities.html> [Accessed: 24-April-2019].
- [12] Web Server Types of Attacks (n.d) [Online]. Available: <https://www.greycampus.com/opencampus/ethical-hacking/web-server-and-its-types-of-attacks> [Accessed: 19-March-2019].
- [13] Most Powerful Vulnerability Assessment Scanning Tools (n.d) [Online]. Available: <https://www.softwaretestinghelp.com/vulnerability-assessment-tools/> [Accessed: 07-May-2019].
- [14] Takeshi Yatagai, Takamasa Isohara, and Iwao Sasase, “Detection of HTTP-GET flood Attack Based on Analysis of Page Access Behavior”.
- [15] Bhupendra Singh Thakur, Sapna Chaudhary, “Content Sniffing Attack Detection in Client and Server Side: A Survey”.
- [16] Daniel Huluka, Oliver Popov, “Root cause analysis of session management and broken authentication vulnerabilities”.
- [17] Formula of Risk Score (n.d) [Online]. Available: https://help.rapid7.com/nexpose/en-us/Files/Risk_scoring_FAQ.html [Accessed: 07-April-2019].