

Security Assessment of Pakistan Government Websites and Proposing a Framework for Countering National Websites' Security Threats



MCS

by

Imama Ghazanfar

A thesis submitted to the faculty of Information Security Department, Military College
of Signals, National University of Sciences and Technology, Rawalpindi in partial
fulfillment of the requirements for the degree of MS in Information Security

August 2020

ABSTRACT

With the growing usage of internet in Pakistan, Government of Pakistan is also utilizing the internet for communication and delivery of e-services to the people. Websites being one of the easiest ways of communication over the internet, almost each department of Pakistan government owns a website. Most of these websites collect personal identifiable information of Pakistani citizens in one form or another. A minor attack can pose huge risk to the critical data being handled by these websites. Besides this, a simple defaming attack can cause a serious impact on govt-citizen trust relationship. Therefore, it is important to regularly assess the vulnerabilities in govt. websites in order to timely address and mitigate the threats posed by their exploitation.

In this research, at first the open source web vulnerability scanning tools are tested on DVWA. Based on the test results, two scanners are finalized for testing Pakistan govt. websites. A dataset of vulnerabilities of 60 websites is created and analyzed. At the end a framework is proposed for countering national website security threats. The framework is based on the guidelines of NIST Framework for improving critical Infrastructure Cyber Security, NIST special Publication 800-30 [1], FIPS 199 [2] and NIST Special Publication 800-61 [3].

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by **Ms. Imama Ghazanfar**, Registration No. **00000106045** of **Military College of Signals** has been vetted by undersigned, found complete in all respects as per NUST Statutes/Regulations/MS Policy, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members and local evaluators of the scholar have also been incorporated in the said thesis.

Signature: _____

Name of Supervisor: **Assoc Prof Dr. Haider Abbas**

Date: _____

Signature (HOD): _____

Date: _____

Signature (Dean/Principal): _____

Date: _____

Declaration

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

The testing on the websites was carried out solely for the purpose of research and development and with the permission from the Department of Information Security MCS.

DEDICATION

This thesis is dedicated to my father for giving me unconditional love, for always holding my hand in tough times and for being my safe heaven, to my mother for her prayers and to my husband for his support and cooperation.

ACKNOWLEDGMENTS

All praises to Allah for blessing me with the strength to complete this thesis.

I would like to pay my gratitude to my supervisor Dr. Haider Abbas for his worthy guidance and supervision. I am also thankful to my committee members Dr. Imran Rashid for the valuable suggestions and Asst. Prof. Mian M. Waseem Iqbal for his constant support, guidance and provision of resources throughout this task. Without his support and encouragement, it would have been impossible for me to complete this thesis.

Lastly, I am highly thankful to my parents, sisters, parents in law and my dear husband for the care, love, appreciation and support they have given me throughout this task.

Table of Contents

ABSTRACT	ii
DEDICATION	v
Table of Contents	vii
List of Figures	x
LIST OF TABLES	xi
ACRONYMS	xii
Introduction.....	1
1.1 Problem Statement.....	1
1.2 Objectives.....	2
1.3 Thesis Contribution	2
1.4 Thesis Organization.....	2
Background.....	4
2.1 Introduction to Website.....	4
2.1.1 Static and dynamic websites.	5
2.1.2 Client-side vs Server-side	5
2.1.3 Universal Resource Locator.....	5
2.1.4 Top Level Domains	6
2.1.5 HTTP and HTTPS	7
2.1.6 HTTP status Code.....	7
2.2. Related Work.....	8
2.3 Chapter Summary.....	8
Website Security.....	9
3.1 Introduction.....	9
3.2 Website Vulnerabilities.....	9
3.2.1 OWASP TOP 10.....	9
3.2.2 SANS/CWE top 25.....	12
3.3 CWE, CVE and CAPEC by MITRE Corp.....	12

3.4	National Vulnerability Database (NVD)	13
3.5	The Web Application Security Consortium (WASC)	13
3.6	Chapter Summary	13
	Data Collection Using the Harvester and Penetration testing on DVWA	14
4.1	Data Collection using the Harvester:	14
4.1.1	The Harvester:	14
4.1.2	Selected Websites for Testing and Analysis	15
4.2	Web Vulnerability scanning and Penetration testing	17
4.2.1	Vulnerability Scanner	17
4.2.2	Penetration Testing:	18
4.2.3	Popular Web Vulnerability Scanners and Pen-testing tools.	18
4.3	Testing on DVWA (Damn Vulnerable Web Application)	19
4.3.1	DVWA Installation and configuration.....	20
4.3.2	Comparison of results and selection of tools	22
4.4	Chapter Summary	23
	Vulnerability Assessment of Pakistan	24
	Government websites	24
5.1	OWASP Zap and Arachni.....	24
5.2	Results and Analysis.....	24
5.2.1	Comparative analysis.....	25
5.3	Critical Analysis of 10 Important Websites.....	29
5.4	Chapter Summary.....	31
	Framework for mitigating Threats to Government Websites	32
6.1	Identify.....	32
6.1.1	Identification of category:.....	32
6.1.2	Identification of components.....	34
6.1.3	Identification of Vulnerabilities:	34
6.1.4	Risk Assessment:.....	35
6.1.5	Risks Prioritization	39
6.2	Protect.....	39
6.2.1	Protection from vulnerabilities.....	39

6.2.2 Protection from threats.....	39
6.3 Detect and Analyze.....	40
6.4 Contain.....	40
6.5 Eradicate and Recover	40
6.6 Improve.....	41
6.7 Validation.....	41
6.8 Chapter Summary.....	41
Conclusion and Future Work	42
BIBLIOGRAPHY	43

List of Figures

Figure 2 .1: Parts of URL.....	6
Figure 4.1: theHarvester	14
Figure 4.2: DVWA Configuration.....	20
Figure 4.3: Configuration file for DVWA application	20
Figure 4.4: Database Configuration for DVWA.	21
Figure 4.5: Configuration of apache 2 server.....	21
Figure 4.6: Results of Open Source Pen-Testing Tools	22
Figure 5.1: Number of Websites affected by vulnerabilities in table 5.1	25
Figure 5.2: Results from Arachni	27
Figure 5.3: Results from OWASP ZAP.....	29
Figure 6.1: Framework for Mitigation of threats to National websites.....	32

LIST OF TABLES

Table 2.1: Second and third level domains of ".pk" domain	6
Table 4.1: No. of websites extracted against each domain.....	15
Table 4.2: Websites selected for the research.....	15
Table 4.3: Web vulnerability scanners	19
Table 5.1: Vulnerabilities found in Pak govt. websites	25
Table 5.2: Detailed results from Arachni.....	26
Table 5.3: Detailed results from Arachni.....	27
Table 5.4: Critical Analysis of 10 Most Important Websites	29
Table 6.1: CIA Matrix	37
Table 6.2: CVSS scores, Qualitative assignment.....	37
Table 6.3: Overall likelihood of exploitation of a vulnerability	38
Table 6.4: Risk Evaluation Matrix	38

ACRONYMS

National Institute of Standards and Technology	NIST
Federal Information Processing Standards	FIPS
Uniform Resource Locator	URL
Hyper Text Transfer Protocol	HTTP
Hyper Text Transfer Protocol Secure	HTTPS
Open Web Application Security Project	OWASP
Extensible Markup Language	XML
Common Vulnerability Scoring System	CVSS
Common Weakness Enumeration	CWE
Common Vulnerabilities and Exposures	CVE
Common Attack Pattern Enumeration and Classification	CAPEC
Web Application Security Consortium	WASC
National Vulnerability Database	NVD
Confidentiality, integrity and Availability	CIA
Web Application Firewall	WAF

Introduction

1.1 Problem Statement

Using web to communicate with citizens or delivering e-services to people brings new security threats that can affect confidentiality, integrity and availability of information shared through this channel. A security breach in private sectors causes threats to a specific company and people related to that company only, but for the government sectors, it is more lamentable. In past years, Pakistan has encountered several cyber-attacks in this field. On Pakistan's 70th Independence Day, August 14, 2017, the websites of the Ministry of Defense, Ministry of Water and Power, Ministry of Information, Ministry of Environment Change and Ministry of Food Security, Ministry of inter-provincial coordination, were hacked and defaced [4]. The attack recorded in 2010, resulted in hijacking of 36 government websites [4]. In 2013, a report by Norman Shark revealed a silent and sophisticated attack that was in action from several past years from a neighbor country [5]. The motive of attack was spying and stealing national security related information [6]. In 2015, Indian hackers targeted about 200 Pakistani websites [7]. In 2018, not only govt. ministries were targeted, but also Careem, a public transport service application, was attacked. Important data of 14 million users was stolen from many countries, including Pakistan [8]. The details suggest that information such as email id, customer identity, trip history and contact numbers were compromised. Similarly, occurrence of cyber-attacks on multiple banks have surfaced and such attacks are rising day by day in Pakistan. According to Federal Investigation Agency, almost all Pakistani banks were attacked in 2018, that resulted in monetary and credential losses [9]. Most of these attacks are related to websites and web applications because of the functionalities provided by web services. It is essential to perform security assessment of govt. websites on regular basis in order to find out existing vulnerabilities and prevent hackers from exploiting these vulnerabilities and gain access to national assets.

1.2 Objectives

The main objectives of thesis are: -

- To evaluate the security of critical websites of Pakistan Government.
- Analyze common vulnerabilities that can have potential adverse effects.
- To design a framework for mitigation of threats to government websites .

1.3 Thesis Contribution

The important contributions of this thesis are given below:

- The research plays a vital contribution in current situation of COVID-19 pandemic, as organizations are trying to maximize the communication process and provision of services over the internet in order to encourage people to stay at home.
- Government organizations can utilize this research to analyze the security of their websites.
- Common vulnerabilities and threats that are faced by the websites are presented in this thesis for quick reference and prioritization of protection measures.
- The framework gives integrated strategies for vulnerability assessment, risk assessment, protection and incident response in order to secure websites related to all types of departments / organizations in government.
- With drastic increase in the utilization of online services amid the current situation of pandemic, the proposed framework helps in quick and efficient security management of a website.

1.4 Thesis Organization

The thesis is structured as follows:

- **Chapter 1:** This chapter presents the problem statement, objectives and contributions of this thesis towards the research and development of country.

- **Chapter 2:** This chapter gives a brief introduction to the development, structure and working of websites of websites. Moreover, the related work done in this field is also highlighted.
- **Chapter 3:** A brief discussion about the importance of website security, vulnerabilities present in websites, organizations dealing with web security field and top 10 vulnerabilities of modern times is given in this chapter.
- **Chapter 4:** This chapter demonstrates the collection of websites using theHarvester tool, selection of websites, list of popular opensource and commercial vulnerability scanners and penetration testing on DVWA using OWASP ZAP, Nikto ,Arachni and W3af.
- **Chapter 5:** Here, introduction to the tools utilized for the assessment of websites i-e ZAP and Arachni, creation of a list of common vulnerabilities and their mapping to standard vulnerability listings (OWASP top 10, WASC, CWE, CAPEC) is given. The analysis of vulnerabilities found by the tools with number of websites affected by each vulnerability is also given.
- **Chapter 6:** In this chapter, the Cyber Security Framework for mitigation of threats against government websites is modeled and explained.
- **Chapter 7:** The conclusion and future work is discussed in this chapter.

Background

2.1 Introduction to Website

A website consists of collection of web pages. These web pages contain data in the form of text, images, multimedia files, which are hosted under a single domain name and are publicly accessible. A website can be owned by an individual, organization or government. Website is developed by professional web developers and can serve for different purposes. These days, even if one is not a professional developer, there are several website makers available for example Wix and Wordpress that only require some basic knowledge to design and develop your website. There are various types or categories of websites including educational websites, business websites, government websites, health websites, ecommerce websites etc.

Websites can be owned by an individual person, business organization or government. A website can be accessed by typing its name or URL in search engine. Websites are developed by web developers using different languages, libraries and frameworks. The most basic website which is only for visual purposes can be made through HTML and CSS, where HTML is a markup language based on opening and closing tags like XML. CSS is a style sheet language used for styling the documents written in HTML.

There is also a database necessary for your website in order to manage the storage of data. After development, a website needs to be hosted so that it becomes available over the internet and can be accessed by requesting the web server, hence making a request response cycle between the web server and browsers. Browser makes an HTTP request to the web server which then responds with HTTP response with the requested web pages. There are web hosting service providers that provide necessary technologies for web hosting. Firstly, one needs a domain name which is the identity of the website on www and used to search the website using a search engine e.g. Google and Yahoo. Then web hosting services provide a server space where all the web pages, HTML documents,

images and videos etc. are placed which are sent as a response when user requests the website through domain name

2.1.1 Static and dynamic websites.

Static websites are developed exclusively using HTML and CSS on client side, they are static in a way that they display same content for every user that visits it. In browser, the same layout is displayed for every user and doesn't change based on user's actions. They are truly informational and don't have many options for user interaction.

Dynamic websites are more functional and display different content based on the user and user's actions. In addition to HTML and CSS, scripting languages such as JS, PHP, and ASP etc. are used. Just for instance if a website provides the current time in the content sent to a client, then it needs dynamic structuring.

2.1.2 Client-side vs Server-side

Each website has a front-end/ client side and a back-end / server side. Client side is the program that is runs in the client/user's browser. It can include text, images, user interface as well as actions taken by user, that the web application responds to in the browser. HTML and CSS are interpreted in end user's browser and the client-side scripting language JS also runs in browsers. Server side or backend means everything in a web application that runs on the server. In past, almost all of the business logics were written to run on the server side in dynamic web pages including notifications in order to render the webpage. This delayed the request-response time. These days, majority of the web applications' dynamic functionalities run on client side instead of server side to reduce latency and for this purpose scripting languages such as Java Script for client side and PHP for server side run scripts in the browser to change the content of the user interface based on the user actions.

2.1.3 Universal Resource Locator

Every website has a separate unique URL which is Uniform Resource Locator and serves as the address of the websites on World Wide Web. There are five parts of a URL as shown in Figure 2.1.

Scheme identifies the protocol that is being used such as http or https.

Subdomain: identifies the World Wide Web www.

Second Level Domain: It is the name of your website or the name used to represent your website on the internet.

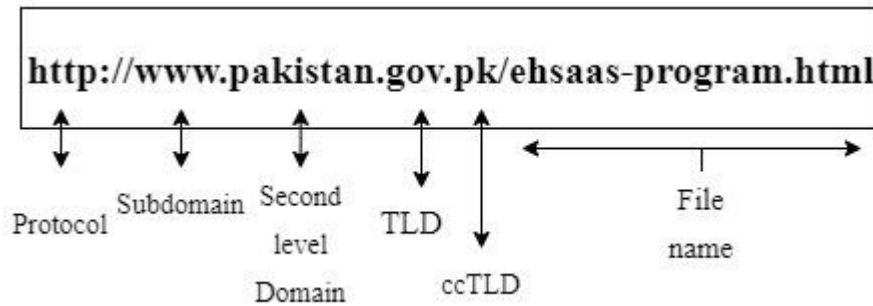


Figure 2.1: Parts of URL

There is Path after slash ‘/’ in URL which specifies the specific directory/file or web page for example **index.html**.

2.1.4 Top Level Domains

It is the extension of entity your organization is part of. The Internet Assigned Numbers Authority officially distinguishes three types of TLDs:

Generic Top-Level Domains, gTLD: These include most generic domains utilized by bodies related to a wider group such as : **.com** (commercial), **.org** (organization), **.net** (networks) , **.edu** (education) , **.gov** (generally for govt. owned websites and **.mil** (US military).

Sponsored Top-Level Domains, sTLD: sponsored by specific agencies. sTLD is restricted to specific groups. For example “**.travel**” domain is associated with websites owned by agencies or organizations related to traveling.

Country Code Top-Level Domains ccTLDs: represent specific countries. For example: **.us** for USA , **.uk** for United Kingdom, **.pk** for Pakistan. Table 2 . 1 lists the Most common and poplar second and third level domain used with “.pk” domain.

Table 2 . 1: Second and third level domains of ".pk" domain

Domain	Applicant
.com.pk	Commercial entities related to Pakistan
.org.pk	All types of organizations in Pakistan can register this domain

.net.pk	Network services registered by PTA
.edu.pk	Educational Institute in Pakistan
.gov.pk	Mainly for federal agencies and ministries of Pakistan but some provincial organizations also use it
.gop.pk	Reserved for departments and ministries of Govt. of Punjab
.gos.pk	Reserved for departments and ministries of Govt. of Sindh
.gob.pk	Reserved for departments and ministries of Govt. of Baluchistan
.gog.pk	Reserved for departments and ministries of Govt. of Gilgit Baltistan
.gok.pk	Reserved for departments and ministries of Govt. of Azad Jammu & Kashmir
.gkp.pk	Reserved for departments and ministries of Govt. of Khyber Pakhtunkhwa

2.1.5 HTTP and HTTPS

HTTP is an application layer protocol. This protocol is responsible for communications between client computers and web servers by exchanging HTTP requests and responses. HTTP with encryption is HTTPS where S is for Secure which uses SSL (Secure Sockets Layer) to encrypt request-response in normal HTTP. Https is way more secure than http.

2.1.6 HTTP status Code

HTTP status codes are an indication that whether the HTTP request that client made is successfully completed or not e.g. HTTP 404 or 404 Not Found is a status code when server is unable to find the requested resource or URL is not recognized.

Other HTTP response status codes include:

- 100-199 Information Response.
- 200-299 Successful Response.
- 300-399 Redirects.
- 400-499 Client Errors.
- 500-599 Server Errors.

2.2. Related Work

Website Security is a huge challenge in modern times. As hackers come up with new ways to exploit the vulnerabilities present in the web structure, any weakness left unaddressed can pose a serious threat to the organization owning the website. The effect is catastrophic on government organizations. Upon thorough review of literature, it became evident that researchers in different countries have reviewed and analyzed the security postures of the websites of important departments and organizations of their country. In [10] Abdullah A. Ali, Mohd Z. Murah conducted the security assessment of 16 critical websites of Lybian Govt using a penetration testing framework utilizing Acunetix and Netsparker. The content analysis was also conducted to gather information about the security policies being implemented on these websites. A similar kind of research conducted by Idris et al. in [11] analyzes the security vulnerabilities present in 10 MDA's websites of Nigerian government y running a Acunetix web vulnerability scanner. The severity associated with these vulnerabilities was analyzed against OWASP top 10. J. Mtsweni [12] used a passive scanning approach to analyze the security of 70 South African Websites among which 40 websites were govt. owned. From OWASP top 10, only 6 vulnerabilities were tested in this study that do not require active scanning approach. The author also assessed the client-side security of these websites by manual inspection. The security strategies were compared with top 10 global websites. In [13] 150 Saudi Arabian websites were tested using W3af and Skipfish scanners. The websites were related to different government, educational and commercial sector organizations. Akgul Y. in [14] investigated the usability, accessibility and vulnerabilities of 51 websites of government of Turkey.

2.3 Chapter Summary

This chapter gives a brief introduction to the website architecture. The working of website on front-end and back-end is explained. The structure, development and designing of static and dynamic websites is also discussed along with the parts of URL and types of domains. Moreover, the work done by the researchers in the field of security assessment of government websites in various countries is highlighted.

Website Security

3.1 Introduction

Though underestimated, website security is of major importance for a country in this digital era. Web developers often focus more on design of their websites rather than secure development of websites. The loopholes left are often the result of lack of awareness and security knowledge among web developers and a lack of understanding among the users of products or services. Often, the developers and users do not find their information to be so important to be misused and this misunderstanding can lead to severe loss. Website is the first impression of an organization. Along with responsive website design, one needs to take care of the security right from the first stage of its development of web applications especially if the website is a platform which, for one purpose or another, involves taking user personal information such as credit card details or personally identifiable information as inputs. A compromise in security can affect relationships among clients and the owners of the organization at large scale.

3.2 Website Vulnerabilities

There are different nonprofit and open source organizations which regularly study and publish data related to the web security for general public. They provide instructions and standards for organizations in order to secure their websites. Besides this, they also publish the lists of top security vulnerabilities on the basis of rigorous research. The lists include:

3.2.1 OWASP TOP 10

One of the all time favorite and beneficial listing, published by OWASP foundation, is OWASP top 10 [15]. For the first time it was released in 2004, with updated versions released in 2004 and 2007. The second version was released in 2010, third one in 2013. The latest version became available in 2017 which is based on the vulnerability and

weaknesses data collected from 40+ firms specialized in web application security. It orders top 10 most common and dangerous vulnerabilities gathered from 100,000 applications. An overview of these vulnerabilities is given below.

A1 Injection

At the top of the list, injection flaws include:

SQL injection, LDAP injection, XML Injection, Null byte injection, OS Command injection, SSL injection, Xquery injection and Xpath injection.

This vulnerability is exploited when an attacker enters a malicious script, command, query or data in the input fields or entries. If interpreted as valid, these scripts results in an outcome desired by the attacker. These attacks have severe technical and business impacts from effecting confidentiality, integrity and availability of data or services to total takeover of target.

A2 Broken Authentication

As evident from the name, this vulnerability occurs because of flaws or misconfigurations in the implementation of procedures required for user authentication or session management. This vulnerability also poses severe risk to the users as well as to the organization.

A3 Sensitive Data Exposure

This vulnerability has become more common in past years. In 2013 release of OWASP top 10, it had 6th position, and now it's the third one [15]. Attackers get access to the sensitive data stored in or transmitted through web applications, if data is not properly handled or encrypted.

A4 XML External Entities

XML stands for eXtensible Markup Language, like HTML, but its functionality differs from HTML. It deals with the storage and transport of data and not how the data is displayed on website as in HTML. In order to interpret data, applications need XML parsers XML entities are used to represent an item of data of an XML document. The XML Document Type Definitions (DTD) contains declarations of XML entities. XML external entities are declared inside DTD but are defined outside DTD. If parsers are poorly configured, they allow the external entities references to internal document.

Attackers can get access to or manipulate the information in internal files using these external entities.

A5 Broken Access Control

Access controls are implemented in order to give privileges to the authenticated users that are only meant to access an information or functionality. Any misconfiguration left in these controls can allow the attackers or malicious users to take advantage by accessing or modifying sensitive information, passwords and functions.

A6 Security Misconfiguration

These vulnerabilities arise if any configuration setting is left unnoticed and default settings are not checked. Security misconfigurations cover a large scope of all configurations vulnerabilities in structures and components related to web applications and their working e.g. servers, frameworks, code, applications, libraries etc.

A7 Cross Site scripting (XSS)

In XSS the attacker injects a malicious JavaScript code in a vulnerable webpage. When any user visits the webpage, the webpage is sent to the user along with this malicious script in HTML body. Thus, the script is executed, and the attacker gets access to the victim's personal information stored in the browser [16].

A8 Insecure Deserialization

This vulnerability is a new addition in latest release of OWASP top 10. Serialization is the process of converting the object (data in a specific form) into a format (e.g. Json or XML) or a byte stream in order to persist it or transmit it over the network. In this way the state of the data object is saved and upon deserialization, which is opposite to serialization, the format is again converted into the same object (actual form). The problem occurs when untrusted data input by an attacker is deserialized. The attacker can abuse the deserialization process and can perform remote code execution attacks. Some other severe attacks such as DOS, injection attacks and privilege escalation attacks also become possible if an attacker becomes successful [17].

A9 Using Components with known vulnerabilities

Vulnerabilities in components used in the design, structure and development of websites which are published in NVD and not patched or updated can lead to catastrophic effects. These vulnerabilities are well known to the attackers. Whether it is a 0-day exploit or a

vulnerability found out by the vendors, the risk associated with the components in your web architecture with these vulnerabilities should always be kept in check.

A10 Insufficient logging and monitoring

Ineffective or no protection mechanisms imposed by organizations can prove to be an open gate for attackers. If an attack goes un-noticed or is not properly monitored, it can persist and can lead to further attacks.

3.2.2 SANS/CWE top 25

SANS institute is an information security research and education organization just like OWASP. This organization also focuses on the training and certifications of information security professionals around the world. SANS/CWE Top 25 are the most dangerous flaws from CWE listed by SANS institute [18]. This list was published in 2019 and therefore contains most recent acknowledged flaws and vulnerabilities related to web.

3.3 CWE, CVE and CAPEC by MITRE Corp.

- **CWE**

CWE is the Common Weaknesses Enumeration, a community made log of software and hardware weaknesses by The MITRE Corporation. Details of causes of each of the weakness, its likelihood of occurrence and preventive measures are also given with each weakness listed in CWE [19].

- **CVE**

The vulnerabilities resulted from these weaknesses or flaws are listed in CVE ,The Common Vulnerabilities and Exposures list. These vulnerabilities are specific to certain software or hardware or its component. Each vulnerability is given a unique CVE ID. For example, CWE-79, XSS resulted in thousands of exploits in applications from different vendors, each of them is registered with unique CVE-ID [20].

- **CAPEC**

The purpose of maintaining CAPEC is to keep an updated list of attack patterns along with their details, which are used to exploit the vulnerabilities. The latest CAPEC release

of 2019 contains more than 500 attack patterns. Details of mitigation CWE ID, originator or linked patterns against each attack pattern are also given [21].

3.4 National Vulnerability Database (NVD)

NVD is a huge worldwide database of vulnerabilities related to security flaws in software and hardware components. This database is maintained by NIST and is represented using SCAP [22]. Each vulnerability registered in this database contains a CVE ID with complete details about the published date, vendors, specifications of component in which vulnerability appeared, detailed technical and business impact and CVSS score.

3.5 The Web Application Security Consortium (WASC)

A nonprofit organization developed and maintained by security practitioners and experts. WASC specifically deals with the classification and identification of threats, attacks and vulnerabilities related with web applications. Besides this, the organization also publishes articles and standards related to web application security [23].

3.6 Chapter Summary

Website security is a major concern these days due to increase in their complex structure and dynamic functionalities. This chapter discusses the list of top vulnerabilities provided and maintained by some international organizations such as OWASP and SANS. Latest list by OWASP foundation was released in 2017 known as OWASP Top 10, a standard for identification of flaws in websites. Moreover SANS/CWE top 25 are most dangerous software flaws released by SANS foundation in 2019. Some organizations maintain a database of reported vulnerabilities such as CWE, CVE and CAPEC by Mitre Corp. and NVD maintained by NIST. This chapter introduces all these organizations along with the listings and database maintained by them.

Data Collection Using the Harvester and Penetration testing on DVWA

4.1 Data Collection using the Harvester:

In order to collect data related to Pakistan government websites, following study and experimentation is carried out.

4.1.1 The Harvester:

This tool collects data from various search engines, key servers and mainly from SHODAN database. The tool was used to gather the websites with **.gov.pk** domain . Below is the command used and results extracted.

-d specifies the domain to be searched.

-b specifies the Data Source from which the domain is to be searched. .

The tool is utilized to find all the websites with domains mentioned in Table 2 . 1, which is demonstrated in Figure 4 . 1.

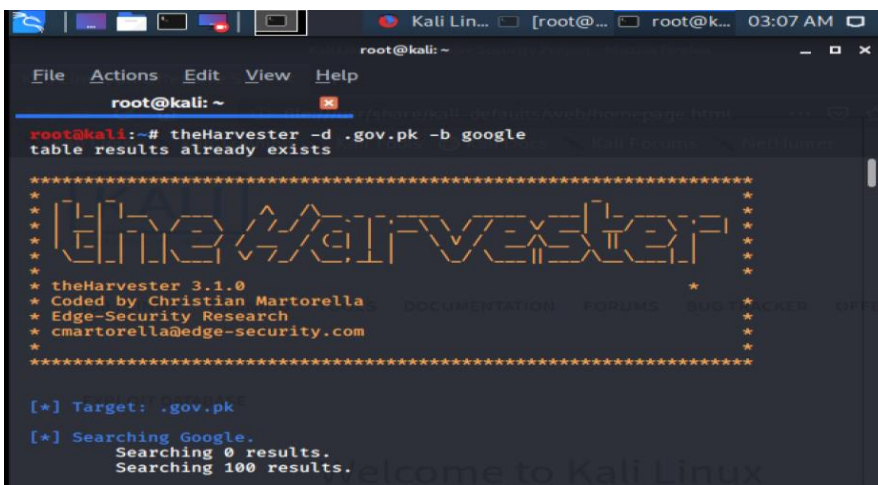


Figure 4 . 1: theHarvester

The tool was able to find total 345 websites related to Pakistan Government and 742 other major domains. Table 4 . 1 shows the number of websites found. (extracted in October 2019) :

Table 4 . 1: No. of websites extracted against each domain.

No.	Domain	No.of Websites
1	Government of Pakistan: gov.pk	147
2	Government of KPK: gkp.pk	45
3	Government of AJ&K: gok.pk	22
4	Government of Punjab: gop.pk	55
5	Government of Sindh: gos.pk	56
6	Government of Baluchistan: gob.pk	20
7	Edu.pk	165
8	Com.pk	204
9	Net.pk	167
10	Org.pk	206

4.1.2. Selected Websites for Testing and Analysis

Table 4 . 2 contains the set of websites selected for the purpose of vulnerability assessment in this research.

Table 4 . 2: Websites selected for the research

Website	URL
1. Prime Minister's Office	https://pmo.gov.pk/
2. Auditor General of Pakistan	http://agp.gov.pk/
3. Accountant General Pakistan Revenues	http://www.agpr.gov.pk/
4. Airports Security Force	http://www.asf.gov.pk/
5. Bureau of Emigration & Overseas Employment	https://beoe.gov.pk/
6. Banking Mohtasib Pakistan	https://bankingmohtasib.gov.pk/
7. Benazir Income Support Program	http://bisp.gov.pk/
8. Cabinet Division Govt of	http://www.cabinet.gov.pk/

Pakistan	
9. Capital Development Authority	http://www.cda.gov.pk/
10. Ministry of Science & Technology, Islamabad	http://www.cipmost.gov.pk/
11. Directorate General Defence Purchase	https://www.dgdp.gov.pk/
12. Drug Regulatory Authority of Pakistan	https://www.dra.gov.pk/
13. Employees Old-Age Benefits Institution	http://www.eobi.gov.pk/
14. Express Mail Track & Trace Sys. Pakistan Post	http://ep.gov.pk/#
15. Expanded Programme on Immunisation	http://www.epi.gov.pk/
16. E-Rozgar Scheme Govt. of Paksitan	https://erozgaar.pitb.gov.pk/
17. Pakistan Estate Office	https://estate-office.gov.pk/
18. Financial Accounting and Budgeting System	https://fabs.gov.pk/
19. Federal Board of Revenue	https://e.fbr.gov.pk/AuthLogin.aspx
20. Pak Air Force	http://paf.gov.pk/#/
21. Pakistan Army	https://pakistanarmy.gov.pk/
22. Pakistan Navy	https://paknavy.gov.pk/
23. Islamabad High Court	http://www.ihc.gov.pk/
24. Ministry of Interior Govt. of Pakistan	https://www.interior.gov.pk/
25. Board of Investment	https://invest.gov.pk/home
26. Ministry of Inter Provincial Coordination	http://www.ipc.gov.pk/
27. Excise and taxation department	http://islamabadexcise.gov.pk/
28. Inter-Services Public Relations	https://www.ispr.gov.pk/
29. Punjab Job Portal	https://www.jobs.punjab.gov.pk/
30. Khyber Pakhtunkhwa Information Technology Board	https://www.kpitb.gov.pk/
31. Khyber Pakhtunkhwa Public Service Commission	https://www.kppsc.gov.pk/
32. Ministry Of Foreign Affairs	http://mofa.gov.pk/
33. National Assembly of Pakistan	http://www.na.gov.pk/en/index.php
34. The National Accountability Bureau	http://nab.gov.pk/
35. National Database & Registration Authority	https://www.nadra.gov.pk/
36. National Disaster Management Authority	http://www.ndma.gov.pk/
37. National Information	https://nitb.gov.pk/

Technology Board	
38. NATIONAL RESPONSE CENTRE FOR CYBER CRIME	http://www.nr3c.gov.pk/
39. National Security Division	http://www.nsd.gov.pk/
40. National School of public policy	http://nspp.gov.pk/
41. The Ministry of Overseas Pakistanis and Human Resource Development	http://www.ophrd.gov.pk/
42. Indus River System Authority (IRSA)	http://pakirsa.gov.pk/
43. Government of Pakistan	http://www.pakistan.gov.pk/
44. Pakistan Post Shop	http://pakpostshop.gov.pk/
45. Provincial Assembly of Pujab	https://www.pap.gov.pk/
46. Press Information Department	http://pid.gov.pk/
47. Pakistan Remittance Initiative	http://www.pri.gov.pk/
48. Radio Pakistan	https://www.radio.gov.pk/
49. Special communication organization	https://sco.gov.pk/
50. Senate of Pakistan	http://www.senate.gov.pk/en/index.php?id=-1&cattitle=Home
51. Sindh Government	https://www.sindh.gov.pk/
52. Sindh Public Service Commission	https://www.spsc.gov.pk/
53. Pakistan Tourism Development Corporation	http://www.tourism.gov.pk/
54. Pakistan Water and Power Development Authority	http://www.wapda.gov.pk/
55. Pakistan Telecommunication Authority	https://www.pta.gov.pk/en
56. Office of Chief Secretary Punjab	http://chiefsecretarypetitioncell.gop.pk/login.aspx
57. Pakistan Railways	https://www.pakrail.gov.pk/
58. Web Based One Customs	https://www.weboc.gov.pk/
59. PM Sehat Sahulat Program	https://www.pmhealthprogram.gov.pk/
60. Provincial Disaster Management Authority (PDMA)	http://pdma.gop.pk/

4.2. Web Vulnerability scanning and Penetration testing

4.2.1 Vulnerability Scanner

A Web application Vulnerability scanner is a software or tool used to assess the loopholes present in a web application that can be exploited by an attacker and damage

the confidentiality, integrity and availability of functionalities and information shared by the web application. These tools are either open source or proprietary. An **open-source software (OSS)** is a copyrighted program that is available freely along with its source code. The developers grant permission in the license to change, modify, study or redistribute the program. Source code is also available to anyone who wants to contribute in the development of the software [24]. Whereas a proprietary program is bought from the developer or distributor on payment. The source code is not available and only members permitted by the owners are allowed to make changes in the software. Some proprietary programs also have a community edition where some features of the program can be utilized without cost and changes can be made in the code of these features [24].

4.2.2 Penetration Testing:

A pen-testing tool, like vulnerability scanner, is used by security practitioners to assess the vulnerabilities present in a software. Pen-testing tools differ from vulnerability scanners in terms of automation. Pen testing tools are run by pen-testers who have knowledge and experience about the working of tool in order to exploit specific vulnerability. In vulnerability scanner tools, most of human interaction requirements are automated in a way that certain tools need just a URL and a click to run.

There are three common strategies used to pen-test a software or program which include black box, white box and grey box penetration testing. In white box testing, the code, framework, design methods, structure and implementation procedures are known to the tester. In black-box testing, the pen-tester does not have any knowledge related to the design, implementation and structure of the software being tested. Whereas in the grey box testing, the tester has some knowledge about the components and functionality of the software being tested. In other words, in white box testing strategy, both black box and white box testing techniques are used.

4.2.3 Popular Web Vulnerability Scanners and Pen-testing tools.

Numerous open source and proprietary web vulnerability scanners are available to use these days. Some of the popular ones are mentioned in Table 4 . 3 with their details.

Table 4 . 3: Web vulnerability scanners

Scanner	Company	Type	Purpose (Detection of)
Netsparker	Netsparker Ltd.	Proprietary	Web application vulnerabilities
Acunetix	Acunetix	Proprietary	Network and web vulnerabilities. Malwares in websites, malicious link and malicious files.
Comodo HackerProof	Comodo Group, Inc.	Proprietary	Website Vulnerabilities
Owasp ZAP	OWASP	Open Source	Web-app vulnerabilities
Arachni	Tasos Laskos	Open Source	Web app vulnerabilities
W3af	W3af	Open Source	Web app Vulnerabilities
Vega	Subgraph	Open Source	Web app vulnerabilities
BurpSuite	PortSwigger Ltd.	Community & Pro	Web application and website scanner
Nikto	Netsparker Ltd.	Open source	Website and Web server vulnerabilities
Wapiti	Nicolas Surribas	Open source	Web application and website scanner

4.3. Testing on DVWA (Damn Vulnerable Web Application)

DVWA (coded in PHP/MySQL) is a web application specially designed for penetration testing purposes so that pen-testers and developers can practice their security skills on this web application. Four different levels of security can be configured on the application, these are: Low, medium, high and impossible. Each level offers different security challenges and has different set of loopholes to be exploited. The application is also used to test the efficiency and accuracy of web application vulnerability scanning tools.

4.3.1 DVWA Installation and configuration

DVWA can be downloaded directly from GIT hub. First of all the directory should be shifted to “/var/www/html” For a web application to run all the files should be present in this directory .In Kali linux, the command used to clone the targeted repository is “git clone” . Figure 4.3 and Figure 4.3 show the download and configuration procedure of DVWA respectively.

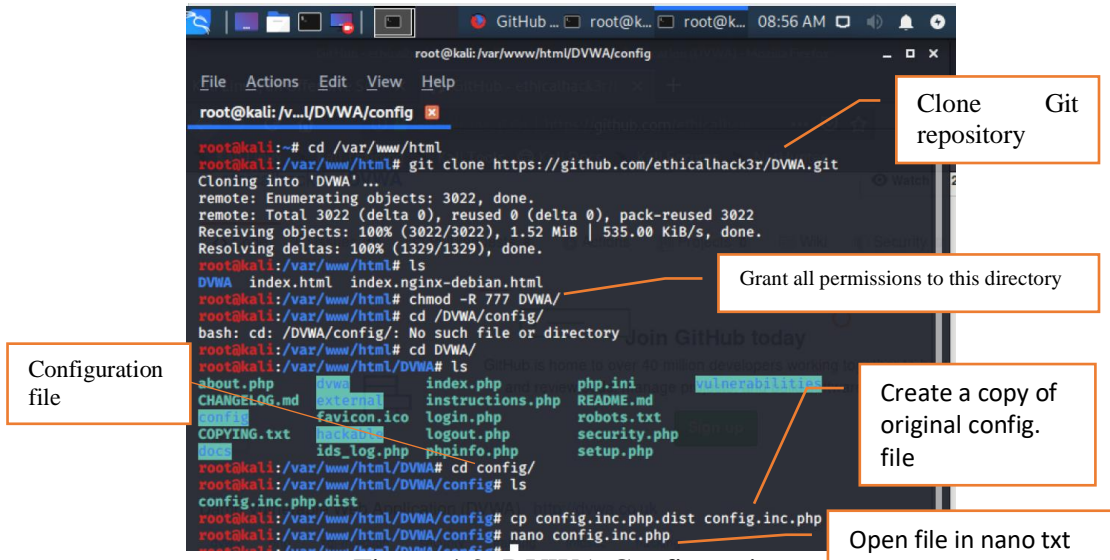


Figure 4.2: DVWA Configuration

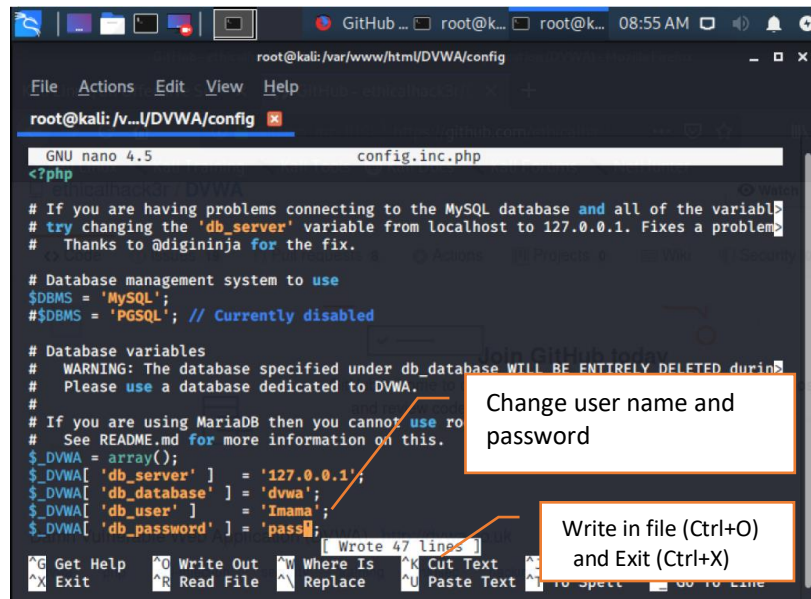
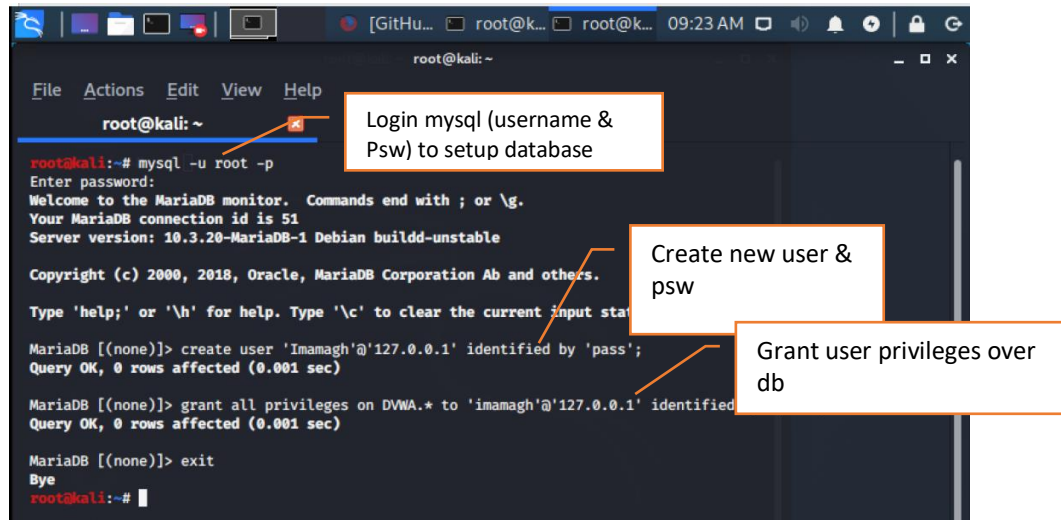


Figure 4.3: Configuration file for DVWA application

Next in order to configure the database, start the database service using command: Service mysql start. Next login the mysql as depicted in Figure 4.4.



The screenshot shows a terminal window with the following commands and output:

```
root@kali:~# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 51
Server version: 10.3.20-MariaDB-1 Debian buildd-unstable

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement

MariaDB [(none)]> create user 'Imamagh'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> grant all privileges on DVWA.* to 'imamagh'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> exit
Bye
root@kali:~#
```

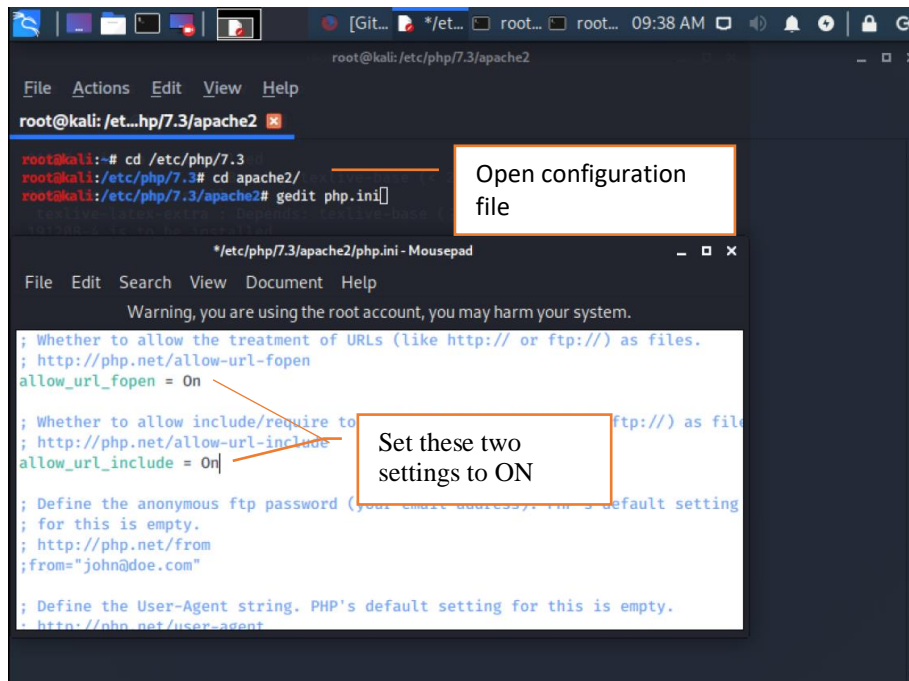
Annotations in the image:

- "Login mysql (username & Psw) to setup database" points to the `mysql -u root -p` command.
- "Create new user & psw" points to the `create user 'Imamagh'@'127.0.0.1' identified by 'pass';` command.
- "Grant user privileges over db" points to the `grant all privileges on DVWA.* to 'imamagh'@'127.0.0.1' identified by 'pass';` command.

Figure 4.4: Database Configuration for DVWA.

The third step is to configure the server. In order to do so use command: Service apache2 start.

Next follow the steps in Figure 4.5.



The screenshot shows a terminal window and a Mousepad window. The terminal window shows the following commands:

```
root@kali:~# cd /etc/php/7.3
root@kali:/etc/php/7.3# cd apache2/
root@kali:/etc/php/7.3/apache2# gedit php.ini
```

The Mousepad window shows the `php.ini` file with the following settings highlighted:

```
allow_url_fopen = On
allow_url_include = On
```

Annotations in the image:

- "Open configuration file" points to the `gedit php.ini` command in the terminal.
- "Set these two settings to ON" points to the `allow_url_fopen = On` and `allow_url_include = On` lines in the Mousepad window.

Figure 4.5: Configuration of apache 2 server.

Next step is to start the apache2 service using command:

```
Service apache2 start.
```

After completing the configuration settings, DVWA can be accessed using browser on 127.0.0.1.

4.3.2 Comparison of results and selection of tools

Four open source tools were tested on DVWA. These are:

OWASP ZAP 2.8.1 (released August, 2019), Arachni 1.5.1 (released March 2017), W3af (V1.6 released April 2015) and Nikto (2.1.6). The security level of DVWA was set to medium. The vulnerabilities are divided into 4 risk levels: High, Medium, Low and Informational. The Figure 4.6 shows the number of detected vulnerabilities by each of these tools.

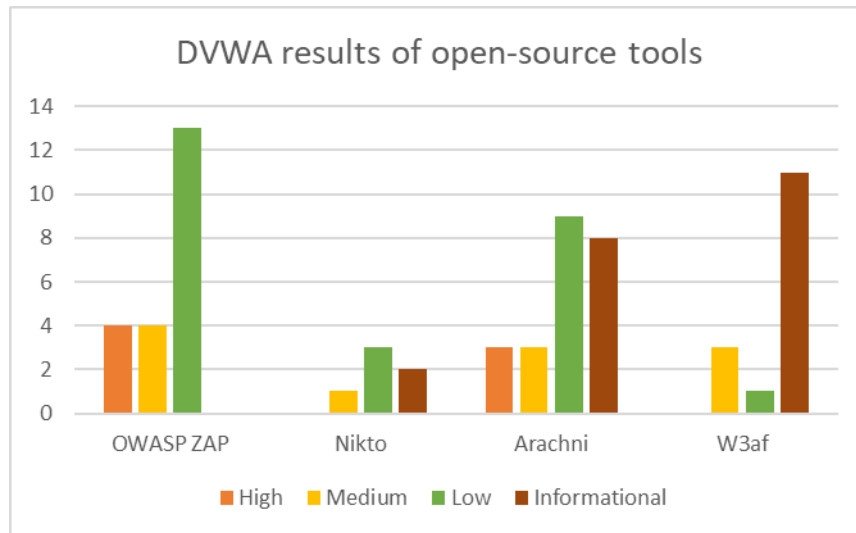


Figure 4.6: Results of Open Source Pen-Testing Tools

The results of scans demonstrated in the Figure 4.6 show that ZAP and Arachni found maximum high-risk vulnerabilities. Whereas the number of medium risk vulnerabilities found by Zap, Arachni and w3af were same. Nikto and w3af could not find any high-risk vulnerability. Zap found maximum low-level vulnerabilities but no informational issues. Informational level issues were maximum in Arachni and w3af scans. Overall, the performance of Arachni and Zap were better than Nikto and w3af. Owasp ZAP and

Arachni were selected for the purpose of website scanning in this research on the basis of tests and literature review [25] [26].

4.4 Chapter Summary

The Harvester is utilized to extract websites related to “.PK” domain. The tool extracted 345 websites related to government sector and 742 other websites. 60 websites were selected for this research. Furthermore, web vulnerability scanners, W3af, OWASP ZAP, Arachni and Nikto were tested on DVWA and the results were compared. OWASP Zap and Arachni were selected in order to carry out the vulnerability assessment of websites because of their better performance as compared to other two tools.

Vulnerability Assessment of Pakistan Government websites

5.1 OWASP Zap and Arachni

ZAP is developed by OWAP foundation for the purpose of web vulnerability scanning. ZAP is a Java based open-source tool that runs both on windows and Linux. It offers a very user-friendly GUI for automated scans. Besides the GUI, the HUD (Heads up display) also offers direct browsing of site through proxy. This way user can manually scan and crawl the site and webpages deeply. Both automatic and manual testing schemes were utilized in this research.

Arachni is a Ruby based open source penetration testing tool developed by Tasos Laskos. It runs on windows, Mac OS and Linux. Its web user interface can be utilized to run scans by multiple users on multiple instances as well as command line interface can be used for quick scans. The web UI was utilized in this research.

5.2 Results and Analysis

The list of common vulnerabilities found in the tested websites is given in Table 5 . 1. Each vulnerability is mapped with the OWASP Top 10 listings from year 2007, 2010, 2013 and 2017. In

Table 5 . 2 and

Table 5.3, the subcategories of each vulnerability found by the Arachni and ZAP respectively, are given along with their CWE ID, CAPEC ID and WASC ID on the basis of thorough literature review. It is important to note that the severity of a vulnerability depends upon its impact. For example, a website is having SQL injection flaws but if the database does not contain any file or data that can be considered PII, then the severity of this vulnerability is not considered high.

Table 5 . 1: Vulnerabilities found in Pak govt. websites

NO	Name	OWASP Top 10
V1	Injection	A1 ,2017
V2	Sensitive Data Exposure	A3, 2017
V3	Broken Access Control	A5,2017
V4	Security Misconfiguration	A6,2017
V5	Cross Site Scripting	A7,2017
V6	Cross Site request forgery	A8, 2013
V7	Insufficient transport layer protection	A10, 2010, A3 2017
V8	Malicious File Inclusion	A3, 2007
V9	Improper Error Handling	A6, 2007
V10	Old, Backup and Unreferenced files	A10, 2007
V11	Cookie related vulnerabilities	

5.2.1 Comparative analysis

Figure 5.1 shows the comparative test results of Zap and Arachni. The number of websites affected by each group of vulnerabilities is demonstrated. Most of the websites contain vulnerabilities related to security misconfigurations.

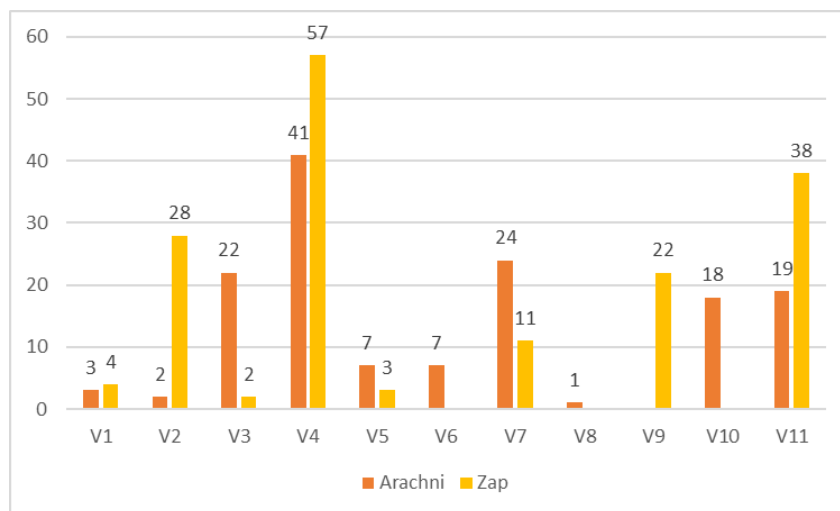


Figure 5.1: Number of Websites affected by vulnerabilities in Table 5.1.

5.2.1.1 Analysis of Results from Arachni

Table 5 . 2 demonstrates the results from Arachni. The vulnerabilities found by the tool, number of websites affected by each vulnerability, mapping of these vulnerabilities to weaknesses and subcategories along with their CWE, CAPEC and WASC IDs are given.

Table 5 . 2: Detailed results from Arachni

Vul. No	Name	Affected websites	Vulnerabilities Mapped	CWE ID	CAPEC ID	Wasc ID
V1	Injection	3	SQL Injection	89	66	19
V2	Sensitive Data Exposure	2	Directory Listing	548	127	16
V3	Broken Access Control	22	Common Directory	200		
			Backup Directory	552		
			Accessible Admin Interface.			
V4	Security Misconfiguration	41	Private IP address disclosure	212/200		
			X Frame Options Header Missing	693	103	
			Insecure "Access-Control-Allow-Origin" Header (CORS)	16		15
V5	XSS	7	XSS in HTML	79		8
			XSS in Script Context	79	19	8
V6	CSRF	7		352	62	9
V7	Insufficient Transport Layer Protection	24	Strict-Transport-Security Header missing			4
			Resources sent over unencrypted channel (despite HTTPS)	311		4
			Unprotected Password Form	523		4
V8	Malicious File	1		98	193	5

	Inclusion					
V10	Old ,Backup & Unreferenced files	18	Backup file	530	87	34
			Common sensitive file	200		
V11	Cookie Related	19	Insecure cookie	614		

Figure 5.2 demonstrates the overall percentage of websites affected by High severity, Medium Severity and Low Severity vulnerabilities on the basis of severity levels mentioned by the Arachni itself.

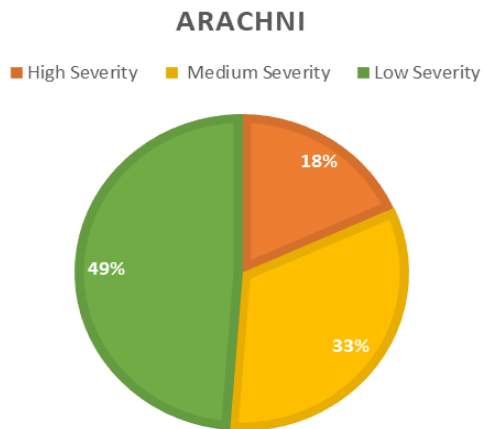


Figure 5.2: Results from Arachni

5.2.1.2 Analysis of results from ZAP

Table 5.3 demonstrates the results from ZAP. The vulnerabilities found by the tool, number of websites affected by each vulnerability, mapping of these vulnerabilities to weaknesses and subcategories along with their CWE, CAPEC and WASC IDs are given.

Table 5.3: Detailed results from Arachni

Vul. No	Name	Affected websites	Vulnerabilities mapped	CWE ID	CAPEC ID	Wasc ID
V1	Injection	4	SQL Injection	89	66	19
			Remote OS Command	78	88	31

			Injection			
V2	Sensitive Data Exposure	28	Directory Listing	548	127	16
			Server Leaks Information via X-Powered-By HTTP response header field	550	118	13
V3	Broken Access Control	2	Path Traversal	22	126	33
V4	Security Misconfiguration	57	Private IP Address Disclosure	200		13
			ViewState without MAC Signature	642		14
			X-frame-Options Header related	16		15
			Cross domain script inclusion	829		15
			XSS protection not enabled	933		14
			Anti-CSRF token missing	352		9
V5	XSS	3		79		8
V7	Insufficient Transport Layer Protection	11	Resources sent over unencrypted channel (despite HTTPS)	311		4
V9	Improper Error Handling	22	Application error disclosure	209		13
			Debug error messages	200		13
V11	Cookie Related	38				

Figure 5.3 demonstrates the overall percentage of websites affected by High severity, Medium Severity and Low Severity vulnerabilities on the basis of severity levels mentioned by the ZAP. Remaining vulnerability testing requires rigorous penetration testing and is recommended to be performed by the tester authorized by the organization.

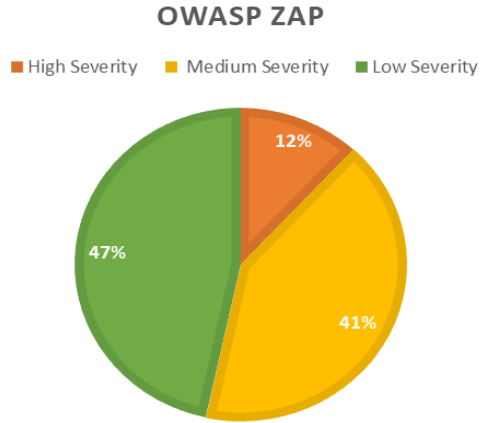


Figure 5.3: Results from OWASP ZAP

5.3. Critical Analysis of 10 Important Websites

From the 60 selected websites, 10 most significant ones were chosen for critical analysis. In this analysis, presence of any security solution such as WAF or IDS/IPS, technologies used, outdated components used and secure/insecure transmission of data was checked. This analysis was carried out using additional tools which include Burp Suite, nmap, WafW00f, Nikto, Sucuri (<https://sucuri.net/>, online tool) and Wappalyzer. The results are shown in Table 5.4.

Table 5.4: Critical Analysis of 10 Most Important Websites

No	Website	Technologies	Vulnerabilities	Severity	HTTP/HTTPS	Firewall/IDS/IPS
1.	Federal Public Service Commission	Apache 2.2.10	Outdated apache server	H	HTTP	No result
		PHP 5.2.14	Outdated PHP	H		
		Drupal 7.59	Unpatched CMS	M		
		jQuery	View-state without MAC	H		
			X-Frame-Options-Header not set	M		
			Absence of Anti-CSRF token	M		
			Access to			

			directories not restricted e.g /CHANGELOG.txt in robot file			
2.	National Database and Registration Authority	WordPress v5.4.2	Multiple X-frame-options headers. (can result in Clickjacking)	M	HTTPS	Cloudflare WAF
		Nginx	Insecure cookie	L		
3.	Sindh Public Service Commission		Admin login accessible	H	HTTP	Mod Security WAF
			Missing X-frame-options Header (result in clickjacking)	H		
			Admin login page accessible.	M		
4.	Punjab Public Service Commission	Microsoft IIS-7.5 server	Outdated server + vulnerabilities in CVE	H	HTTP	A solution is present
			CSRF	H		
			View state without MAC signatures	H		
5.	Join Pakistan Army		X-Frame opt header not set	M		
			Absence of anti-CSRF token	M		
			Sensitive information disclosure. Code reveal	M		
6.	Join Pakistan Airforce		Absence of anti-CSRF token	M	HTTP	WAF present
			Vulnerable to XSS	H		
7.	Excise and Taxation Dept.	MS-IIS 7.5	Outdated server	H	HTTP	Not present
		PHP 7.3.8	Outdated version +600 cve vulnerabilities	H		
			OS command Injection	H		
			XSS protection not enabled	M		
8.	Punjab Job		Vulnerable to	M	HTTPS	Not present

	portal		session hijacking			
			Admin login accessible	M		
			Absence of anti-csrf token	M		
9.	Special communication organization	MS-IIS 8.5			HTTPS	WAF present
		PHP 7.2.7	Outdated PHP			
		ASP.NET	XSS protection not present			
			CSRF token missing			
10.	Khyber Pakhtunkhwa Public Service Commission		CSRF in admin login	H	HTTP	WAF present
			Admin login accessible	M		
			HSTS Missing	L		

5.4. Chapter Summary

Both tools were capable of finding different sets of vulnerabilities in websites because of their varied algorithm and testing approach. These vulnerabilities were studied and compared against standard listings such as Owasp top 10, CWE, CAPEC and WASC. Arachni was able to find high severity vulnerabilities in 18% websites. Owasp results depict that almost 12 % websites were vulnerable to high severity vulnerability. A comparative analysis of found vulnerabilities is done in this chapter and results are demonstrated.

Framework for mitigating Threats to Government Websites

The proposed framework in Figure 6.1 is based on the international standards and guidelines that include NIST Framework for improving critical Infrastructure Cyber Security, NIST special Publication 800-30 (Guide for conducting Risk Assessments) , FIPS 199 (Standards for security categorization of Federal Information and Information systems) [2]. The guidelines for incident detection and handling were taken from NIST special Publication 800-61 [3]. The framework utilizes Qualitative Risk Assessment approach and Vulnerability-oriented Risk Analysis approach [1].

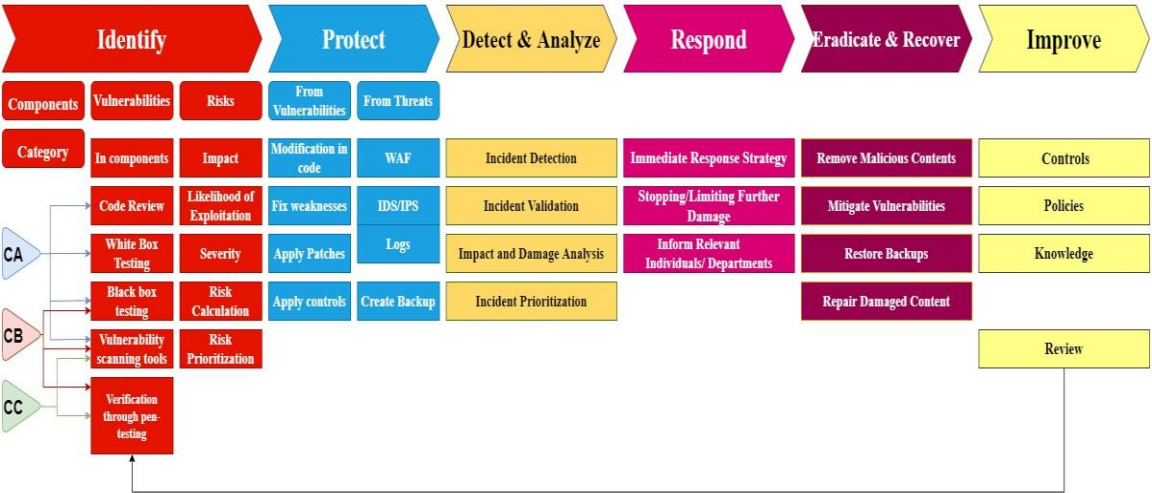


Figure 6.1: Framework for Mitigation of threats to National websites

6.1 Identify

6.1.1 Identification of category:

The websites of government department can be divided into 3 categories on the basis of :

- Criticality of information handled by the websites and impact on the individuals, citizens, organization or on the country in case of compromise of information.
- Availability of services provided through the website.

CAT A (CA): $\{(C + I + A), H\}$ OR (S, H) (6.1)

CAT B (CB): $\{(C . I . A), M\}$ OR $\{(C . I) M + (C . A) M + (I . A) M\}$ OR (S, M) (6.2)

CAT C (CC): $\{(C . I . A), L\}$ OR $\{(C.I)L + (C.A) L + (I.A) L\}$ OR $(S.L)$ (6.3)

H, M & L used to represent High, Medium and Low impact, S: Services. The term (C)H represents that impact of compromise of confidentiality of the information is High.

“+” Represents OR i.e. $\{(C+I+A), H\}$ means compromise in either C OR I OR A will have a High Impact.

“.” Represents AND e.g. $\{(C.I.A), M\}$ means compromise in all C, I and A will result in a medium impact.

According to FIPS 199,

Impact is **HIGH** if the compromise in CIA or S result in

- Severe damage to the organization itself, multiple organizations, individuals related to those organizations or to the citizens of the country.
- Severe damage to finances, reputation, and operations of an organization or multiple organizations.
- Disruption of critical services that can cause a severe impact on a national project.
- Severe psychological trauma or injury to a person.
- An adverse impact on national security and defense.

Impact is **MEDIUM** if the compromise in C I A result in a

- Significant damage to the organization itself, multiple organizations, individuals related to those organizations or to the citizens of the country.
- Damage that result in disruption and availability of services and functionality of the organization but the basic operations go on.
- The caused damage cost significant amount and time for repair

- A damage that has minor effects on the psychological or physical health of a person.

Impact is **LOW** if the compromise in C I A result in a

- Minor damage to the one or multiple organizations, individual or individuals.
- An insignificant damage to organization's functions and services that causes little hindrance in the operation of organization and an insignificant harm to finances.
- A minor or no damage to individual's health.

6.1.2. Identification of components.

The steps include

- Make a table listing all the components used in the design and development of the website. These include all the technologies used for the front end and back end, client-side and server-side development such as the frameworks, libraries, languages, OS, DBMS, servers and protocols along with their version and vendor details.
- After listing components, check if these components are up to date and are supported by the vendors.
- Check for latest updates or any latest versions available against each component.
- Consult CVE database for the existing vulnerabilities in these components.

6.1.3. Identification of Vulnerabilities:

Next step is identification of vulnerabilities. For this purpose, it is recommended to follow the following steps:

If a website is in Category A, that means it is highly critical and important. It is recommended to do code review for checking the bugs and weaknesses in the code, penetration testing that include white box and black box testing against top SANS/CWE 25 most common and critical vulnerabilities. The testing should be carried out using OWASP Penetration Testing Guidelines [27]. It is up to organization to select the scanner according to the resources. Using multiple open source vulnerability scanners can be cost

effective but a rigorous penetration testing will be required with it in order to validate the vulnerabilities found for true positives and false positives.

Make a list of vulnerabilities found by testing, assign numbers to them, list them against OWASP top 10, SANS/CWE Top 25, WASC ID, CWE ID. This will help in assessment of severity, likelihood of exploitation and impact of exploitation.

6.1.4 Risk Assessment:

Once the vulnerabilities are identified, the next step includes identification of Risk associated with each vulnerability. It is recommended that any component identified with known vulnerability or any component that is outdated and lacks support from vendor should be considered HIGH RISK.

The Risk is calculated using equation 6.4.

$$\text{Risk} = \text{Likelihood} * \text{Impact} \tag{6.4}$$

The framework identifies threats and likelihood of exploit against each vulnerability assessed. The reason is that the threats faced by websites of government organizations differ from commercial and private sectors for example a private sector organization is more likely to have a threat from a competitor but govt. organizations can face threats from a foreign country or political party. Private sector companies usually have their own separate cyber security departments, but most govt. organizations have a centralized department for this purpose e.g. NR3C-FIA and NCCS (National center for Cyber Security). Similarly, the private sector organizations usually rely on their own earning. The budget and finances for cyber security tasks is assigned accordingly. In govt. sectors, organizations usually receive funds for this purpose whether it is a collective fund, or a separate budget assigned for this task.

6.1.4.1 Impact of exploitation of vulnerability

The framework recommends calculating the impact of vulnerabilities before calculating likelihood. The impact of exploitation of certain vulnerability decides the likelihood of its

exploitation. The impact on either CIA is High, Medium or Low on the basis of following metrics.

- **High impact** means that exploitation of vulnerability results in adverse catastrophic damage to the organization's assets, operations, individuals, citizens of the country or to the nation. Or it can result in severe or life-threatening effects on physical or mental health of an individual. The damage results in total halt of operations or crucial services of the organization or halt in a crucial project of the country. For example, the impact is high if a vulnerability compromises the confidential report of an investigation agency that can pose threat to the life or reputation of an entity that could result in severe physical or mental health consequences. A compromise of database server results in deletion or modification of documents and results related to thousands of candidates in public service commission examination.

- **Medium impact** means that the exploitation of a vulnerability can result in severe damage to the organization's assets, operations, services, individuals, citizens of country or to the nation as a whole. Or it can result in physical and psychological health consequences to an individual or citizen. The damage does not result in total halt of operations or services. It does not pose threat to the time value and can be repaired timely without delaying major country projects. For example, a vulnerability exploitation results in the disruption of services by an examination center, so that candidates are not able to contact the organization but the general operations of the organizations continue as usual.

- **Low impact** means that the exploitation of vulnerability results in some effect or minor damage to the organization's assets, operations, individuals, citizens of the country or to the nation. Or the exploitation can have some minor impact on the health of individuals. For example a vulnerability results in change in the content appeared on the website. An attacker puts its own banner on the website but all operations and functions of organization continue as usual.

The overall impact can be analyzed using the CIA matrix [28] given in Table 6 . 1.

Table 6 . 1: CIA Matrix

Overall Impact	Confidentiality									
		L			M			H		
Availability	Integrity	L	M	H	L	M	H	L	M	H
	L	L	L	M	L	M	M	M	M	H
	M	L	M	M	M	M	H	M	H	H
	H	M	M	H	M	H	H	H	H	H

6.1.4.2 Overall Likelihood

The overall likelihood of a vulnerability depends upon the likelihood of exploitation and severity of the vulnerability.

Likelihood of exploitation of certain vulnerability highly depends upon the organization for example, a vulnerability that can result in the exposure of confidential data related to war strategies or details about the personnel, has a high likelihood of exploitation in times of war. Here the vulnerability impacts the confidentiality of information.

Table 6 . 2: CVSS scores, Qualitative assignment.

CVSS v2.0		CVSS v3.0	
Severity	Range	Severity	Range
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

A vulnerability that can give access to the database of an examination system in order to finalize the candidates results, has a high likelihood of exploitation before candidates are

finalized for a post. That is a vulnerability that can impact the integrity of information. Similarly, near elections, the political parties are in action. Any vulnerability that can expose the confidential information related to the investigation of a case in National accountability bureau has a high likelihood of exploitation. It is recommended that organization must consider all these factors related to time while calculating the likelihood of exploitation.

Table 6 . 3: Overall likelihood of exploitation of a vulnerability

Overall Likelihood	Severity				
		LOW	Medium	H	C
Likelihood of Exploitation	H	M	H	V.H	V.H
	M	L	M	H	V.H
	L	L	L	M	H

Second main entity is Severity of a vulnerability. The framework utilizes CVSS score in order to measure the severity of a vulnerability. The scores from CVSS are translated in Table 6 . 2. The overall likelihood can be calculated using Table 6 . 3.

Table 6 . 4: Risk Evaluation Matrix

Risk	Impact			
		LOW	Medium	H
Overall Likelihood Of Exploitation	V.H	M	H	C
	H	M	H	V.H
	M	L	M	H
	L	L	L	M

It is recommended that organizations in category A should utilize CVSS V3 and V3.1 in order to assess the severity of a vulnerability according to the components utilized for web application development.

The risk is calculated according to the matrix. In Table 6 . 4.

6.1.5 Risks Prioritization

The next step is risk prioritization. This is necessary in order to apply controls or in order to decide which vulnerabilities need to be fixed first according to the resources. The vulnerabilities with critical associated risk score should be dealt first. Vulnerabilities with High risk should be given second priority and so on.

6.2 Protect

6.2.1 Protection from vulnerabilities

Once the risk associated with each vulnerability is assessed and risks associated with different vulnerabilities are prioritized, a fix is recommended immediately for critical and high-risk vulnerabilities. It is recommended to consult the NVD data base, to check for associated weaknesses causing the vulnerability and CWE, CAPEC, WASC and OWASP guidelines to select appropriate fix.

6.2.2 Protection from threats

Once the vulnerabilities are fixed, it is crucial for the organization to implement the protection measures in order to avoid and detect insider and outsider attacks. These measures include:

WAF IDS & IPS

Web application firewalls are used to protect against application level threats with known attack patterns. WAF are helpful especially in cases where a vulnerability remains unrevealed or undetected through pen-testing or scanning, or takes huge effort and compromise in the services of organization [29]. WAF along with intrusion detection and preventions systems can provide effective protection. Although some WAF claim to give

maximum protection against top web application threats, but these protection measures still have limited scope [30] and cannot compensate with the effectiveness of previous steps of 6.1.2. Prevention is always better.

6.3 Detect and Analyze

It is very important to monitor all the activities related to the web. The detailed knowledge of what is normal helps in detection of any abnormal or different activity. A proper incident response team CSIRT can help in the detection and analysis of the incidents [3]. In case of government sector, this team can be a centralized team for multiple organizations, or a separate team dedicated for security of single organization. The team's general duties include over all monitoring of cybersecurity activities. In case an event happens, the first step is to identify whether it is an incident or not. Next, the impact of the incident, systems affected and damage caused should be analyzed immediately. In case of multiple incidents, the incidents should be prioritized on the basis of their impact [31].

6.4 Contain

Once the incident/incidents have been analyzed and prioritized, an immediate response is required. The response can be for example, making a containment strategy for each incident, spreading information to the relevant entities in appropriate ways, taking immediate backups (that will help in forensics), shutting down the affected servers or systems. Detailed guidelines for specifically handling incidents related to web applications are given in OWASP's project "Top 10 Considerations for Incident Response".

6.5 Eradicate and Recover

Main steps in this part of incident handling include removal of malicious content for example malware, a modified file, a piece of software that was vulnerable and lead to the incident such as an attack specified in OWASP A9. Restore backups, Recover lost files if possible.

6.6 Improve

Finally, after learning the causes and impact of malicious incident, it is highly important to improve the security structure of web application. Review each step from start and if possible, redo penetration testing in order to analyze and mitigate further threats. Improve policies. Implement patches and updates.

6.7 Validation

The framework was validated in Annexure A using a case study of website of Federal Public Service Commission which is a critical website of Pakistan Government. The framework effectively helped in efficient security assessment of the website.

6.8 Chapter Summary

A framework for mitigation of identified threats and vulnerabilities present in the analyzed websites in previous sections, is proposed in this chapter. The framework categorizes government websites in three categories on the basis of criticality of data handled through them. Appropriate steps and guidelines for proper vulnerability assessment and penetration testing are required to be taken according to the category of the website. Further a process for calculation of risk associated with each found vulnerability is given. Procedures required for mitigation of risks and incident handling are given step by step.

Conclusion and Future Work

Government websites play a crucial role in provision of e-services to the citizens. The ease of using internet facility for communication and services comes with a great threat because of vulnerabilities present in the websites. After conducting this research, it became evident that many critical Pakistan government websites are vulnerable because of insufficient testing, monitoring and patch management. This poses a huge risk to the information being handled through these websites. The common vulnerabilities and weaknesses found in the websites were analyzed and IDs from CWE, CAPEC, WASC and OWASP top 10 were provided for detailed analysis and mitigation of threats. It was also observed that websites of govt. departments were different from the websites of non-govt. organizations in terms of data, structure and architecture. Most of these websites have embedded iframes from other websites. For example, on many website, embedded content from PM Ehsas Program and PM Citizen's Portal was given. Some websites gather critical citizen's data (PII), while others are linked to important departments such as Pak Army and ISPR. Therefore, a single vulnerability assessment approach was not suitable for all websites. Hence, a framework was proposed to help improve the website security of Pakistan Government sector. For future directions and research:

- In future, an automated tool can be developed for Pak Govt. websites based on the proposed framework. The tool will carry out comprehensive security assessment of websites according to its category and requirement of the organization.
- The study can help in development and implementation of security standards for Pakistan e-government.
- The study can be combined with risk assessment and mitigation of network threats to Pakistan government websites.
- The study can be conducted using different set of open-source or proprietary vulnerability scanning and penetration testing tools which are not used in this study or another set of websites which are not analyzed in this study.

BIBLIOGRAPHY

- [1] Joint Task Force Transformation Initiative, "Guide for Conducting Risk Assessments", NIST Special Publications 800-30 , National Institute of Standards and Technology, 2012.
- [2] Federal Information Processing Standards Publication, "Standards for Security Categorization of Federal Information and Information Systems", NIST, 2004.
- [3] P. Cichonski, T. Millar, T. Grance and K. Scarfone, "Computer Security Incident Handling Guide", NIST Special Publications 800-61 Rev. 2, National Institute of Standards and Technology, 2012.
- [4] K. Geers, D. Kindlund, N. Moran and R. Rachwald, "WORLD WAR C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks", FireEye.
- [5] R. Syed, A. Khaver and M. Yasin, "Cyber Security: Where Does Pakistan Stand?", Sustainable Development Policy Institute (SDPI), 2019.
- [6] Pakistan Today, "Operation Hangover: India's three-year silent cyber war on Pakistan", May 21, 2013. Accessed on: Jan.2, 2020. [Online]. Available: <https://www.pakistantoday.com.pk/2013/05/21/operation-hangover-indias-three-year-silent-cyber-war-on-pakistan/>
- [7] M. Baezner, "Regional rivalry between India-Pakistan: tit-for-tat in cyberspace", Risk and Resilience Team, Center for Security Studies (CSS), ETH Zürich, 2018.
- [8] R. Jahangir, "Over 14m users' data compromised in Careem cyber attack", DAWN, 2018. [Online]. Available: <https://www.dawn.com/news/1403533>
- [9] S. Qarar, "Almost all Pakistani banks hacked in security breach, says FIA cybercrime head", DAWN, Nov 6, 2018. [Online]. Available: <https://www.dawn.com/news/1443970>
- [10] A. A. Ali and M. Zamri Murah, "Security Assessment of Libyan Government Websites," 2018 Cyber Resilience Conference (CRC), Putrajaya, Malaysia, 2018, pp. 1-4, doi: 10.1109/CR.2018.8626862.
- [11] I. Idris, M. U. Majigi, S. Abdulhamid, M. Olalere, and S. I. Rambo, "Vulnerability assessment of some key Nigeria government websites," International Journal of Digital Information and Wireless Communications, vol. 7, no. 3, pp. 143–153, 2017.

- [12] J. Mtsweni, "Analyzing the security posture of South African websites," 2015 Information Security for South Africa (ISSA), Johannesburg, pp. 1-8, 2015.
- [13] M. S. Al-Sanea and A. A. Al-Daraiseh, "Security evaluation of Saudi Arabia's websites using open source tools," 2015 First International Conference on Anti-Cybercrime (ICACC), Riyadh, 2015, pp. 1-5.
- [14] Akgul, Y. (2016) "Web Site Accessibility, Quality and Vulnerability Assessment: a Survey of Government Web Sites in the Turkish Republic", Journal of Information Systems Engineering & Management, 1:4 (2016), 50.
- [15] "Top 10 Web Application Security Risks, OWASP Top 10", OWASP Foundation. 2017. [Online]. Available: https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/
- [16] S. K. Mahmoud, M. Alfonse, M. I. Roushdy and A. M. Salem, "A comparative analysis of Cross Site Scripting (XSS) detecting and defensive techniques," 2017 Eighth International Conference on Intelligent Computing and Information Systems (ICICIS), Cairo, 2017, pp. 36-42.
- [17] "Insecure Deserialization", OWASP Top 10. [Online]. Available : https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A8-Insecure_Deserialization
- [18] "2019 CWE/SANS Top 25 Most Dangerous Software Errors". SANS Institute/Common Weakness Enumeration. 2019. [Online]. Available: <https://www.sans.org/top25-software-errors>
- [19] CWE, Common Weakness Enumeration , A Community Developed List of Software and Hardware Weakness Types, The MITRE Corporation. Available: <https://cwe.mitre.org/>
- [20] CVE, Common Vulnerabilities and Exposures, The MITRE Corporation.. Available: <https://cve.mitre.org/index.html>
- [21] CAPEC, Common Attack Pattern Enumeration and Classification, A community Resource for Identification and Understanding Attacks, The MITRE Corporation. Available: <https://capec.mitre.org/>
- [22] NVD, National Vulnerability Database , U.S Govt. Repository of Standards Based Vulnerability Management Database, National Institute of Standards And Technology. Available: <https://nvd.nist.gov/>
- [23] The Web Application Security Consortium Threat Classification V2. Available: <http://projects.webappsec.org/w/page/13246978/Threat%20Classification>.

- [24] "What is Open Source" Available: <https://opensource.com/resources/what-open-source> .
- [25] Alsaleh, M., Alomar, N., Alshreef, M., Alarifi, A., & Al-Salman, A.S. "Performance-Based Comparative Assessment of Open Source Web Vulnerability Scanners". Security and Communication Networks, 6158107:1-6158107:14. 2017
- [26] Suteva, N., Zlatkovski, D., & Mileva, A. (2013). Evaluation and Testing of Several Free/Open Source Web Vulnerability Scanners. In: The 10th Conference for Informatics and Information Technology (CIIT 2013), 18-21 Apr 2013
- [27] OWASP Web Application Penetration Testing Guide. Internet: https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf
- [28] Shemlse G. Kassa, "IT Asset Valuation, Risk Assessment and Control Implementation Model", ISACA. Accessed on: Feb 2, 2020. [Online]. Available: IT-Asset valuation, Risk Assessment and Control Implementation Model" ISACA, May 2017.
- [29] M. Dermann et al., "Use of Web Application Firewalls Version 1.0.5", OWASP Foundation, 2008.
- [30] Agarwal, N., & Hussain, S.Z. (2018). A closer look on Intrusion Detection System for web applications. Security and Communication Networks, 2018, 9601357:1-9601357:27.
- [31] P. Kral "Incident Handler's Handbook" , SANS Institute, Information Security Reading Room, 2011. [Online]. Available: <https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>

Validation on a Critical Website

Here the framework is validated on the website of Federal Public Service Commission.
Website url: <http://www.fpsc.gov.pk/>

1. Identification:

i. Identification of Category of the website:

The website is linked to an important project of recruitment for the posts related to Federal Public Services.

- The information communicated/stored by the website contains: CNIC , Education information , Contact information (Phone number, email id , residential and permanent addresses) of citizens which appear against a vacancy and are being selected for the jobs. The compromise of PII of officers of an important department can pose a risk to their security and can be used by terrorist groups and criminals.
- The impact of compromise in the confidentiality, integrity and availability of information or disruption of service is assessed as.
- Impact of compromise in confidentiality: **HIGH**
- Impact of compromise in integrity: **MEDIUM**
The change in the education information of a candidate or candidates can result in rejection.
- Impact on availability: **MEDIUM**

The compromise of services and operations of the website does not have severe, catastrophic adverse impact on the functions of the organization. Therefore:

Impact on compromise of Service: **MEDIUM**

The website is categorized in **Category A** according to framework.

ii. Identification of components:

The website uses following technologies:

Table A1: List of technologies

No	Technology	Version	Latest supported version & release	Supported	Vulnerabilities
1.	Apache 2	2.2.10	2.4x	No	32
2.	PHP	5.2.14	7.4.6	No	77
3.	Drupal	7.59	7.71/9.0.0	No	5
4.	JQuery	1.10.--	3.5	--	--
5.	HTTP				Not Secure

iii. Identification of Vulnerabilities.

The rigorous penetration testing was not used. OWASP ZAP , Burp and Nikto were utilized to assess the vulnerabilities present in the website. Table A2 shows the vulnerabilities were found through penetration testing.

Table A2: List of vulnerabilities & weaknesses

No.	Vulnerability	Index	OWASP Top 10	CWE ID	WASC ID	SANS/CWE top 25
1.	Path Traversal	Y1	A5(2017)	22	33	10
2.	Outdated Apache Server	Y2	A9(2017)	937		
3.	Outdated PHP version	Y3	A9(2017)	937		
4.	Unpatched Drupal	Y4	A9(2017)	937		
5.	X-Frame-Options Header not set	Y5	A6(2017)	693	15	
6.	Anti CSRF Token Missing	Y6	A6(2017)	16,352	15	
7.	Insecure Communication	Y7	A10 (2010)	311		

iv. Identify Risk associated with each Vulnerability

A. Path Traversal.

Impact of Exploitation

By exploiting this vulnerability, the attacker gets access to a restricted path or directory. As a result, the restricted files such as the important configuration files, program files or other data files e.g a file containing PII of users, can be exposed to the attacker [1 CWE]

Impact on confidentiality: **HIGH**

- Exposure of configuration information.
- Exposure of technology used by website that can aid in launching further attacks.
- Exposure of confidential files e.g files containing PII of candidates.

Impact on Integrity: **HIGH**

- Change a configuration setting
- Bypass a security mechanism, if the accessed file is used to implement a security mechanism.
- Creation of a new file in the directory.

Impact on Availability : **LOW**.

- Modification, manipulation and deletion of critical configuration files can disrupt the working of website.
- Modification or deletion of a file containing security mechanism can lock user accounts.

Overall Impact by utilizing CIA matrix in table 6.1: **HIGH**

Overall likelihood:

CVSS Calculator was used to identify the severity of the exploitation.

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:L, Score=7.7, HIGH

Referring to the table 6.2 , the severity is **HIGH**. For likelihood of exploitation, CWE database is considered. The likelihood of exploitation of this vulnerability is **HIGH**.

Overall likelihood using table 6.3 is: **VERY HIGH**. The associated risk with this vulnerability is calculated using table 6.4 **Risk : CRITICAL**

B. Outdated Components and Components with known vulnerabilities.

The components with known vulnerabilities should be considered **CRITICAL** or **HIGH** Risk according to the severity of the vulnerabilities listed in CVE database .

Risk Associated with Apache 2.2.10

APACHE 2.2.10 is an outdated version and has 32 reported vulnerabilities in CVE database. 23 of which are of medium severity, 5 high severity and 1 critical. Therefore, the associated risk is considered **CRITICAL**.

Risk Associated with PHP 5.2.14

PHP 5.2.14 is completely outdated version with 77 reported vulnerabilities in CVE database. 37 of which are of MEDIUM severity ,9 HIGH severity and 2 CRITICAL. Therefore the associated risk is considered **HIGH**.

Risk associated with Drupal 7.59

This version of drupal has a patch release of 7.71 . Drupal 7.59 has 5 reported vulnerabilities in CVE database . 2 are MEDIUM severity and 1 with HIGH severity. The associated risk is considered **HIGH**.

C. X-Frame Options Header not set.

Impact of Exploitation

Impact on Confidentiality: **MEDIUM**. Impact on Integrity: **LOW**, Impact on Availability: **LOW**

Overall impact : **LOW**

Overall likelihood

Following metrics are used to calculate the score.

CVSS 3.1: AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N , Score =5.8 , MEDIUM [1]

Likelihood of exploitation of this vulnerability is also considered as Medium (because the vulnerability is a security misconfiguration and is not listed as a vulnerability in CWE metrics) .

the overall Likelihood of exploitation of this vulnerability using table 6.3 is Medium.

The associated risk with this vulnerability is calculated using table 6.4.

(The vector string is taken from:

[https://www.acunetix.com/vulnerabilities/web/clickjacking-x-frame-options-header-missing/.](https://www.acunetix.com/vulnerabilities/web/clickjacking-x-frame-options-header-missing/))

Risk : LOW

D. Absence of Anti-CSRF Token

The Anti CSRF token helps in preventing CSRF attacks. In case of exploit, the impact highly depends upon the functions and privileges of the victim. Lets suppose the victim in this case is a candidate.

Impact of Exploitation

Impact on confidentiality: **MEDIUM**. The victim's PII can be revealed to the attacker.
Impact on Integrity: **LOW**, change in the CNIC is not possible in the form because the form only validates authentic CNIC. Change in other details does not impact the victim significantly.

Impact on Availability: **LOW**. Overall impact: **LOW**

Overall likelihood

Severity: The attack vector to measure CVSS score :

CVSS V3.1AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N , Score =4.8, MEDIUM

(The vector string is taken from <https://www.acunetix.com/vulnerabilities/web/html-form-without-csrf-protection/>) . Whereas, the likelihood of exploitation: **MEDIUM**. (CWE database consulted). Therefore, the overall Likelihood of exploitation using table 6.3 is: **MEDIUM**.

Associated Risk using table 6.4: **MEDIUM**

E. Insecure Communication

The site does not use encryption channel for secure communication. Even the pages that take the user PII such as the page for online application is not secure. In case of any exploit

Impact of Exploitation

Impact on confidentiality: **HIGH**. Impact on Integrity: **LOW**. Impact on availability: **MEDIUM**

Overall impact using table 6.1: **MEDIUM**

Overall likelihood

Overall Likelihood of exploitation :**HIGH** Whereas multiple vulnerabilities and attacks are associated with not having HTTPS so the likelihood of exploitation is considered **HIGH** for critical websites (Online: [https:// web.dev/why-https-matters/](https://web.dev/why-https-matters/)).

Using table 6.4 Associated risk is **Risk: HIGH**

v. Risk Prioritization

No.	Vulnerability	Vul. Index	Risk
1.	Path Traversal	Y1	Critical
2.	Outdated Apache Server	Y2	Critical

3.	Outdated PHP version	Y3	V.High
4.	Unpatched Drupal	Y4	High
5.	Insufficient Transport Layer Protection	Y7	High
6.	Anti CSRF Token Missing	Y6	Medium
7.	X-Frame-Options Header not set	Y5	Low

1. Protection

i. Protection from Vulnerabilities.

A. Path Traversal protection mechanisms

CAPEC Path Traversal Mitigation. (Available: <https://capec.mitre.org/data/definitions/126.html>)

B. Outdated Components.

OWASP top 10 2017.

C. X-frame Options Header not set.

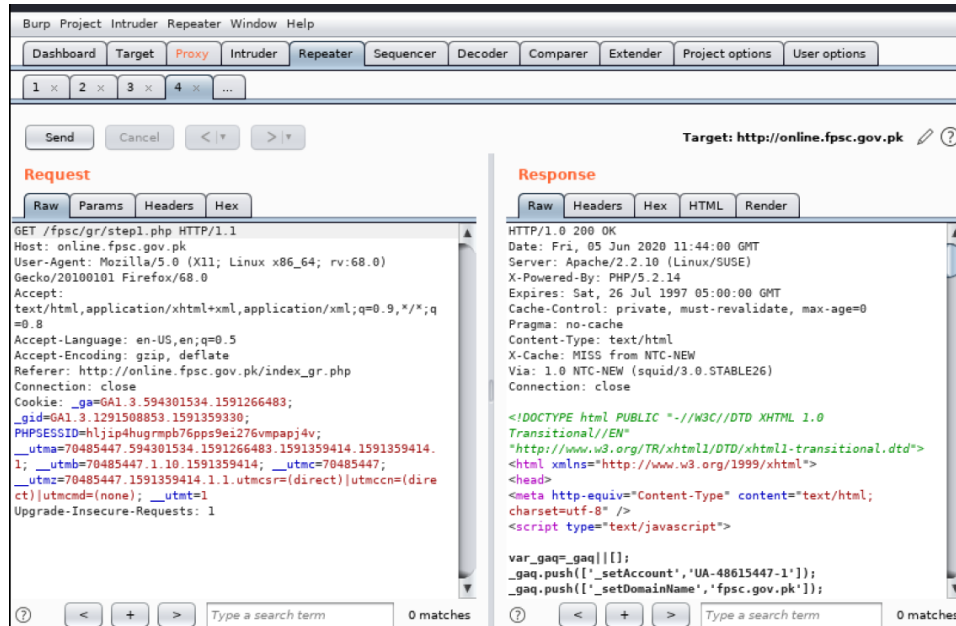
Netsparker : Remediation Missing X-Frame-Options Header (Available: <https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/misconfigured-x-frame-options-header/>).

D. Anti CSRF Token Missing.

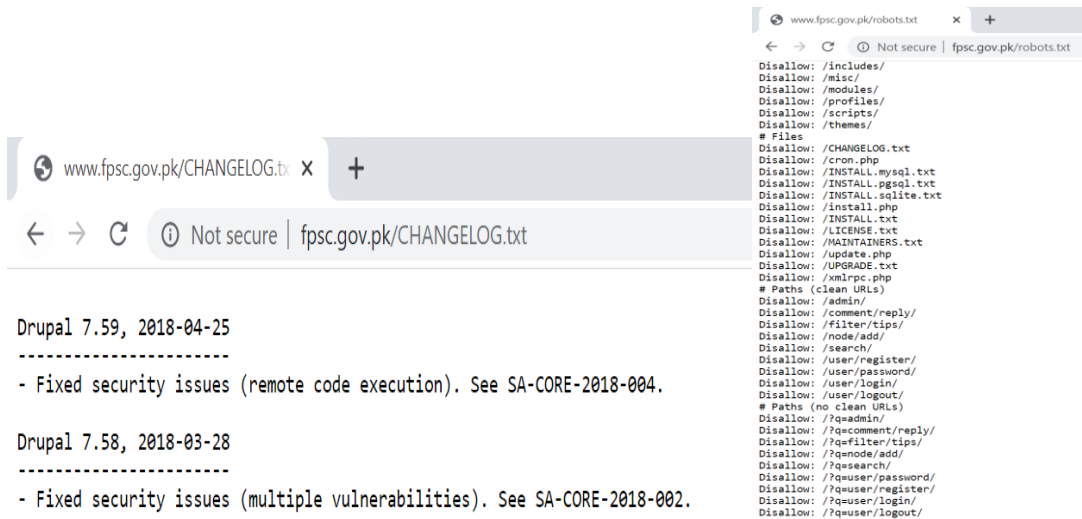
Refer to the guidelines by Netsparker (Available: <https://www.netsparker.com/blog/web-security/protecting-website-using-anti-csrf-token/>) and Portswigger (Available: <https://portswigger.net/web-security/csrf/tokens>) in order to configure Anti-CSRF tokens.

E. Insufficient Transport Layer Security:

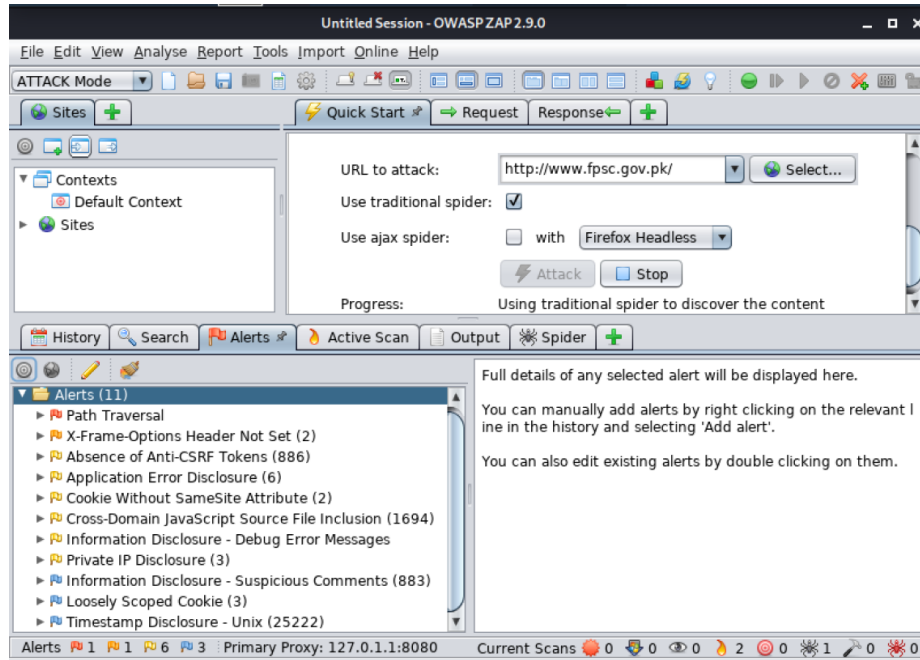
Reference: Secure your site with HTTPS, Google Webmaster support (Available : <https://support.google.com/webmasters/answer/6073543?hl=en>)



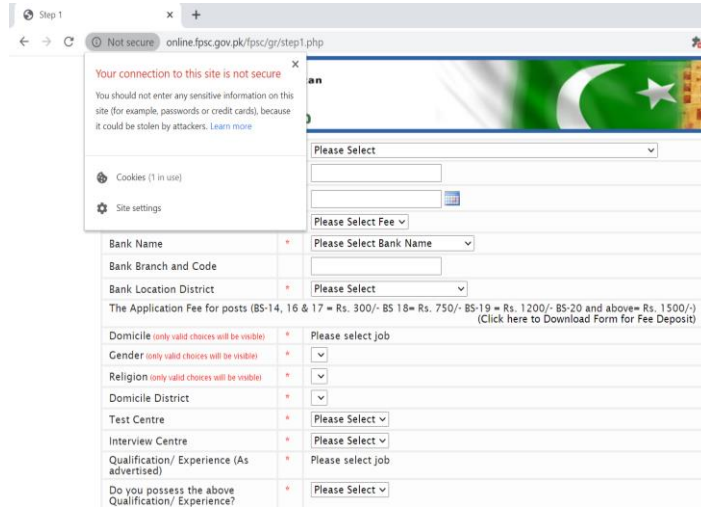
Burp Proxy utilized to analyze the technologies used by the website



The CHANGELOG.txt shows Drupal version (left) and the Robots.txt file on the website (Right)



OWASP ZAP report



Connection is not secure

