Web Application Bug Hunting

Project Synopsis

<Version 1.0>

<Guideline: Change the Version No. inside document in Header also>

Major Project (ICI651)

Degree

BACHELOR OF COMPUTER APPLICATION(CTIS)

PROJECT GUIDE:

Mr. Praful Saxena

Senior Faculty (i-Nurture TMU)

SUBMITTED BY:

Abdul Ahad (TCA2056002)
Kafeel Ahmad (TCA2056013)
Rishi (TCA2056018)

February,2023

FACULTY OF ENGINEERING & COMPUTING SCIENCES

TEERTHANKER MAHAVEER UNIVERSITY, MORADABAD

Table of Contents

1 Project Title

Web Application Bug Hunting

2 Domain

Cyber Security

3 Problem Statement

Web application penetration testing, also known as "pen testing," is the process of testing a web application to identify potential vulnerabilities and security issues. The goal of pen testing is to identify any weaknesses or vulnerabilities that could be exploited by attackers to gain unauthorized access, steal sensitive data, or disrupt the normal operation of the web application.

There are several reasons why web app pen testing is important:

1. **To identify vulnerabilities**: Web applications can have a wide range of vulnerabilities, such as SQL injection, cross-site scripting (XSS), and file inclusion vulnerabilities, among others. Pen testing helps identify such vulnerabilities so that they can be addressed before attackers exploit them.
2. **To prevent data breaches**: Web applications can store sensitive data, such as customer information, credit card details, and other personal information. Pen testing helps identify security weaknesses that could lead to data breaches and helps prevent such breaches.
3. **To meet compliance requirements**: Organizations in certain industries, such as healthcare and finance, have compliance requirements that mandate regular security testing. Pen testing helps organizations meet these requirements and avoid penalties for non-compliance.
4. **To improve security posture**: Pen testing provides valuable insights into an organization's security posture and helps identify areas for improvement. This can help organizations proactively address security weaknesses and reduce the risk of a security breach.

In summary, web app pen testing is essential for organizations that want to ensure the security of their web applications and protect against potential threats.

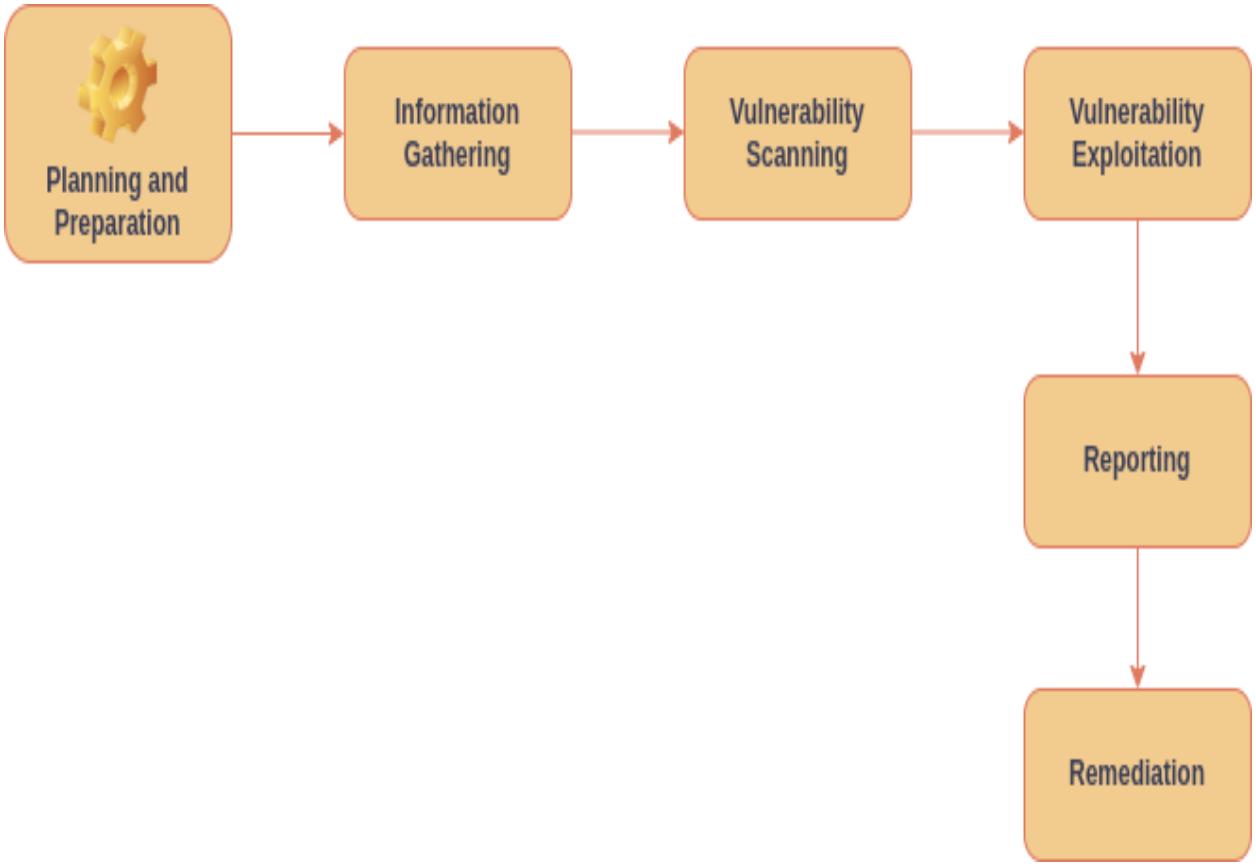
4 Project Description

Web application penetration testing, commonly referred to as "pen testing," is a security testing process that involves assessing the security of a web application by identifying and exploiting vulnerabilities that could be used by attackers to gain unauthorized access, steal data, or disrupt the regular operation of the application. Web application penetration testing, also known as web app pen testing, is the process of identifying vulnerabilities in a web application by attempting to exploit its weaknesses. This is typically done by using various tools and techniques to simulate attacks that a malicious hacker might use, with the goal of identifying and remedying any security flaws before they can be exploited by real attackers. The ultimate aim is to improve the web application's security posture and protect against potential security breaches. Basically, WAPT (Web Applications and Penetration Testing) is finding web app-based vulnerabilities on Websites. In this project, we will find vulnerabilities and exploit them and we also give remediation of those vulnerabilities.

The pen testing process involves the following steps:

1. **Planning and reconnaissance**: In this initial phase, the pen tester gathers information about the web application, such as its functionality, architecture, and technologies used.
2. **Vulnerability scanning**: The pen tester uses automated tools to scan the application for known vulnerabilities, such as SQL injection, cross-site scripting (XSS), and file inclusion vulnerabilities.
3. **Manual testing**: The pen tester manually probes the application to identify and exploit vulnerabilities that cannot be detected by automated tools. This can involve attempting to bypass authentication mechanisms, injecting malicious code into the application, or manipulating input fields to access unauthorized data.
4. **Reporting**: The pen tester prepares a report that summarizes the findings of the pen testing process, including identified vulnerabilities, their severity, and recommendations for addressing them.

Overall, the goal of web app pen testing is to identify security weaknesses in the application so that they can be addressed before attackers exploit them. By conducting regular pen testing, organizations can ensure that their web applications remain secure and protected against potential threats.



4.1 Scope of the Work

The scope of work for a web application penetration testing (pen testing) engagement depends on several factors, including the size and complexity of the application, the business goals, and the level of risk associated with the application. we will find vulnerabilities and exploit them and we also give remediation to those vulnerabilities.

4.2 Project Modules

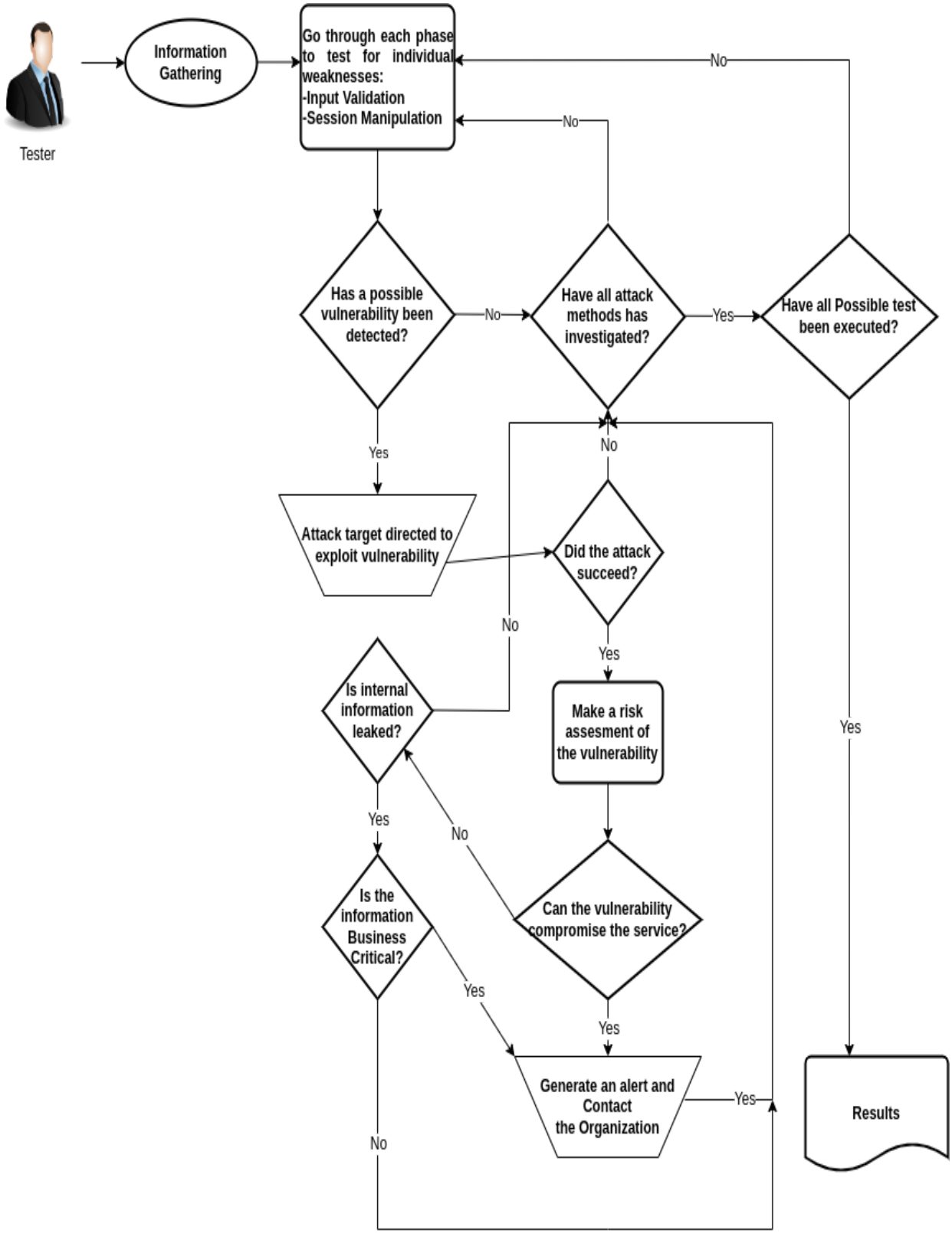
There are two modules:

1. **Vulnerability finding**: In this module, We will find the vulnerability following a particular project.
2. **Reporting:** In this module, we make a document report of what vulnerability we find in the first module.

5 Implementation Methodology

- DFD (Data Flow Diagram)

- Flow Chart


Tester
Information Gathering
Go through each phase to test for individual weaknesses:
-Input Validation
-Session Manipulation
No
No
Has a possible vulnerability been detected?
No
Have all attack methods has investigated?
Yes
Have all Possible test been executed?
Yes
No
Yes
Attack target directed to exploit vulnerability
Did the attack succeed?
No
Yes
Is internal information leaked?
Make a risk assesment of the vulnerability
Yes
No
Yes
Is the information Business Critical?
Can the vulnerability compromise the service?
Yes
Yes
Generate an alert and Contact the Organization
Yes
No
Results

6 Technologies to be used

6.1 Software Platform

a) **Front-end:** Burp Suite

6.2 Hardware Platform

RAM: 8GB

SSD: 256GB

OS: Parrot Security, Kali Linux, Windows, etc.

Browser: Firefox

6.3 Tools

- **Burp-Suite Community Edition:** Burp Suite Community Edition is a popular web application security testing tool developed by PortSwigger Web Security. It is a free and open-source version of the more advanced Burp Suite Professional, but still offers a wide range of features that make it a valuable tool for performing web application security testing.
- **OWASP Zap:** OWASP Zap (short for Zed Attack Proxy) is a free and open-source web application security testing tool developed by the Open Web Application Security Project (OWASP). Its main purpose is to identify vulnerabilities and security issues in web applications by performing automated security scans and manual testing.
- **Nikto:** Nikto is a free and open-source web server scanner that helps identify security vulnerabilities in web servers and applications. It is designed to be used by security professionals and penetration testers to scan web servers and generate a report of any security issues found. Nikto is capable of detecting various types of vulnerabilities, such as outdated versions of software, insecure configurations, and known security vulnerabilities in web server software and applications. It can also be used to scan web servers for default files and directories, unsecured CGI scripts, and other potentially sensitive information

7 Advantages of this Project

1. Identify Security Vulnerabilities
2. Improve Security Posture
3. Meet Compliance Requirements
4. Save Money and Reputation
5. Enhance User Trust
6. Continuous Improvement

8 Future Scope and further enhancement of the Project

We will find out the valuable Vulnerabilities in the other large-scale web applications.

9 Team Details

Project Name & ID	Course Name	Student ID	Student Name	Role	Signature
Web Application Bug Bounty	BCA (Cloud Technology and Information Security)	TCA2056002	Abdul Ahad	Bug Hunter	
		TCA2056013	Kafeel Ahmad	Bug Hunter	
		TCA2056018	Rishi	Reporting	

10 Conclusion

Web application penetration testing is a critical process for identifying vulnerabilities and weaknesses in web applications. By simulating attacks against the application, pen testers can identify potential weaknesses and provide recommendations for improving the application's security posture. A thorough web app pen testing engagement typically involves a range of modules, such as information gathering, vulnerability scanning, authentication and authorization testing, input validation testing, session management testing, business logic testing, and reporting. These modules help to ensure that a comprehensive and systematic assessment of the web application is conducted. The ultimate goal of web app pen testing is to identify vulnerabilities and recommend mitigation strategies to enhance the security of the web application. Pen testers should work closely with the development team and other stakeholders to ensure that identified vulnerabilities are addressed in a timely and effective manner. In conclusion, web app pen testing is an important process for ensuring the security of web applications in today's digital landscape. By identifying and addressing vulnerabilities, organizations can help to mitigate the risk of cyber-attacks and protect sensitive data and resources.

11 References

- *https://www.ecsbiztech.com/web-vulnerability-assessment-penetration-testing-vapt/#:~:text=Web%20Application%20VAPT%20is%20essentially,in%20web%20applications%20and%20APIs.*
- *https://xiarch.com/services/web-application-penetration-testing/*
- *https://ieeexplore.ieee.org/abstract/document/8463920*
- *https://link.springer.com/article/10.1007/s11416-014-0231-x*
- *https://ieeexplore.ieee.org/abstract/document/5593250*