PENETRATION TESTING FRAMEWORK TO FIND SECURITY FLAWS IN A WEB APPLICATION

A PROJECT REPORT

Submitted by

SOWMYA MANIVEL(18BCS053)

TAARINI V (18BCS089)

VISNU SANKER SS (18BCS112)

In partial fulfillment for the award of the degree

of

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

KUMARAGURU COLLEGE OF TECHNOLOGY

COIMBATORE-641 049

(An Autonomous Institution Affiliated to Anna University, Chennai)

December 2021

KUMARAGURU COLLEGE OF TECHNOLOGY

COIMBATORE 641 049

(An Autonomous Institution affiliated to Anna University, Chennai)

BONAFIDE CERTIFICATE

Certified that this project report **"PENETRATION TESTING FRAMEWORK TO FIND SECURITY FLAWS IN A WEB APPLICATION"** is the bonafide work of "**SOWMYA MANIVEL (18BCS053), TAARINI V (18BCS089), VISNU SANKER SS (18BCS112)"** who carried out the project work under my supervision.

SIGNATURE

Dr. Devaki. P, Ph.D.,

HEAD OF THE DEPARTMENT

Department of Computer Science and Engineering,

Kumaraguru College of Technology

Coimbatore – 641 049.

SIGNATURE

Mr. R. KIRUBAKARAN, M.E.,

SUPERVISOR

Department of Computer Science and Engineering,

Kumaraguru College of Technology

Coimbatore – 641 049.

The candidates with university register number **18BCS053,18BCS089,18BCS112** were examined in the Project Viva-Voce examination held on ……

Internal Examiner

External Examiner

DECLARATION

We affirm that the project work titled **"PENETRATION TESTING FRAMEWORK TO FIND SECURITY FLAWS IN A WEB APPLICATION"** is being submitted in partial fulfillment for the award of B.E Computer Science and Engineering is the original work carried out by us. It has not formed the part of any other project work submitted for the award of any degree or diploma, either in this or any other University.

SOWMYA MANIVEL (18BCS053) **TAARINI V (18BCS089)**

VISNU SANKER SS (18BCS112)

I certify that the declaration made above by the candidates is true.

Mr. Kirubakaran.R,

Assistant Professor,

Department of Computer Science and Engineering,

Kumaraguru College of Technology,

Coimbatore – 641 049.

ACKNOWLEDGEMENT

We express our profound gratitude to the management of Kumaraguru College of Technology for providing us with the required infrastructure that enabled us to successfully complete the project.

We extend our gratitude to our Principal, **Dr. D. Saravanan,** for providing us with the necessary facilities to pursue the project.

We would like to acknowledge **Dr. P. Devaki,** Professor, and Head of, Department of Computer Science and Engineering, for her support and encouragement throughout this project.

We thank our project coordinator **Dr.L. Latha,** Professor, Department of Computer Science and Engineering and guide **Mr.R. Kirubakaran**, Assistant Professor, Department of Computer Science and Engineering, for their constant and continuous effort, guidance, and valuable time.

Our sincere and hearty thanks to staff members of the Department of Computer Science and Engineering of Kumaraguru College of Technology for their good wishes, timely help, and support rendered to us during our project. We are greatly indebted to our family, relatives, and friends, without whom life would have not been shaped to this level.

- SOWMYA MANIVEL
TAARINI V
VISNU SANKER SS

ABSTRACT

Penetration testing is an attempt to get into a system using techniques and tools similar to those used by genuine hackers. The ultimate purpose of penetration testing is to expose as many current vulnerabilities as possible, then devise realistic solutions to address the issues, hence improving overall system security. Penetration testing for web applications involves simulating authorised exploits both within and externally in order to get access to sensitive data. End-users can utilize web penetration to determine the likelihood of a hacker gaining access to their data through the internet, the security of their email servers, and the security of their web hosting site and server. The technique is nothing more than a set of security industry best practices for doing testing. There are some well-known methodologies and standards for testing, however because each web application requires distinct sorts of tests, testers might design their own methodology by referencing the standards accessible on the market. This project will discuss about what is penetration testing, steps involved in it, types of pentesting, existing systems. This project acts as a huge advantage in providing secure web applications by verifying the ability of a system to protect its networks, applications, endpoints, and users against both internal or external threats.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

People generally tend to underestimate the new technology hazards that firms are exposed to as they digitise their company operations and processes. Hackers exploiting a weakness in an IT infrastructure is one of the most serious threats. Once a hacker gains access to the internal network, the chance of them taking complete control of the entire IT infrastructure increases dramatically. Penetration testing is a security exercise where a security expert attempts to find and exploit vulnerabilities in a computer system or a website. It is an authorized simulated attack performed on a network or a website to evaluate its security. The purpose of this simulated attack is to identify any weak spots in a system's defenses which attackers could take advantage of. A web application penetration test is a sort of ethical hacking exercise that evaluates web application architecture, design, and configuration. Cyber security threats that potentially lead to unauthorised access and/or data disclosure are identified through assessments. The number and types of web applications to be tested, the number of static and dynamic pages, the number of input fields, and whether the test will be authenticated or unauthenticated (where login credentials are unknown/known) are all examples of information needed to help scope a web application security test. Penetration testing for web applications necessitates not only familiarity with the most up-to-date web application security testing technologies, but also a thorough understanding of how to make the most of them. Ethical hackers use a variety of specialised tools to assess the security of web apps. Our project is split into four modules namely Reconnaissance Tools, Vulnerability Assessment Tools, Exploitation tools, Post Exploitation Tools. Active reconnaissance tools are meant to engage directly with devices on the target network to obtain data that would otherwise be unavailable. Vulnerability assessment tools are meant to automatically examine an application for new and existing threats. Vulnerabilities are ineffective if they cannot be exploited or cause harm to the application. In order to understand the effects of a vulnerability, it has to be exploited, which often means taking down a hacker's or spammer's website.

CHAPTER 2

OBJECTIVE AND SCOPE

A penetration tester's primary goal is to find security flaws in a network, system, or piece of software. Once that is established, the vulnerabilities can be mitigated or deleted before hostile parties find and exploit them. Few of the focus areas are the types of risks an institution is concerned with, specific compliance requirements, level of data protection, inherent risks, cyber security objectives. The course of action is to develop a command line interface framework to perform all the phases of penetration testing. The tool allows users to actively scan a website, look for possible potential security threats and exploit them as well. The framework enables to simulate a safe cyber attack to identify any weak spots in a website inorder to mitigate them. Penetration Testing is very important in this modern phenomena since in the information systems arena, security is one of the major issues.

CHAPTER 3

LITERATURE SURVEY

3.1 VULNERABILITY ASSESSMENT AND PENETRATION TESTING : A PORTABLE SOLUTION IMPLEMENTATION

The paper was published in the year 2020 at an International conference on CICN. It is authored by Rajiv Pandey, Vuthukuru Jyothindar, Umesh K Chopra. This paper discusses penetration testing that was carried under a controlled environment**.**

This paper presents effective methods for doing penetration testing in a controlled environment. Using evaluation tools such as the built-in pen-testing tool, the Raspberry Pi 3b+ (portable mini-computer) was utilized to investigate and assess network penetrability and uncover network flaws. The focus of this paper is on the value and application of smart devices in penetration testing and vulnerability assessment.

When a credit card-sized computer competes toetoe with covenantal means of VAPT like computers and more frequently used laptops, using a single board to do VAPT can be fantastic. Future work based on this research will involve attaching a single-board computer to a drone to expand range and accessibility to new heights. Because single board computers are inexpensive and simple to learn, a new generation of ethical testers will advance in leaps and bounds. This study will aid in the development of new and creative portable gadgets to improve and boost cyber security.

3.2 TOWARDS A MODEL-BASED SECURITY TESTING APPROACH OF CLOUD COMPUTING ENVIRONMENT

The paper was published in the year 2017. The authors of the paper are Philipp Zech, Michael Felderer and Ruth Breu. It discusses penetration testing on cloud systems. Assuring the security of a Cloud computing environment is a continuous process that must be carried out throughout the cloud's existence. This is due to the fact that clouds are constantly evolving in terms of freshly deployed apps and services. Based on this premise, a unique model-based, change-driven approach to testing the security of a cloud computing system across all tiers using risk analysis in this work is presented

Our strategy uses public service interfaces as a significant intrusion point since they are a large source of newly introduced vulnerabilities, which could lead to serious security incidents.

The technology allows users to create test suites that are platform and language neutral. In terms of customising or transferring the contents of the Vulnerability Knowledge Database, it is both extensible and generic. It approaches the concept of security testing from a negative standpoint; in other words, it does not guarantee a system's validity at any moment but aggressively strives to demonstrate its flaws, which are frequently overlooked.

3.3 WEB APPLICATION SAFETY BY PENETRATION TESTING

The paper was published in the year 2018. The authors of the paper are Ashikali Hasan and Divyakant Meva. The paper gives a brief overview of the various methods and tools that can be used to perform VAPT. It is a very compressive technique. Researchers have provided many research and methods to assist the VAPT process. Literature has been surveyed and examined for an overview of the VAPT process, identifying some shortcomings. Several tools that can aid with the VAPT process to find SQLI, XSS, LFI, and RFI vulnerabilities are available. It has been concluded that VAPT is an important method that aids in the detection of security flaws. Many repositories provide information about the tools, methods, and mechanisms that can be used to assist VAPT.

3.4. A COMPARATIVE OVERVIEW ON PENETRATION TESTING

The impact of penetration testing and the methodology utilised are briefly discussed in this paper. The article also provides an outline of the impact of IPv6 on remote server and web application penetration testing. Penetration testing is a common and well-known way of determining and assessing the security of a network or information. A penetration tester should follow a specific topology in order to correctly detect the threats that a hacker poses to an organization's network or information assets, as well as to reduce an organization's IT security expenses by ensuring a greater return on security efforts.

3.5 ANALYSIS AND IMPACT OF VULNERABILITY ASSESSMENT & PENETRATION TESTING

The rapid advancement of machinery, whether mobile or computer systems, has resulted in more advanced and efficient Windows, Web, and mobile applications, but it has also increased system complexity, which leads to weaknesses that attackers exploit. The utilisation of web applications and web hacking activities has exploded in recent decades. In today's world, businesses and institutions face a challenging scenario when it comes to protecting their systems and data from growing vulnerabilities, which is why it's better to detect and identify these flaws ahead of time, before an attacker can use them. As a result, vulnerability assessment and penetration testing methodologies assist it in determining if the measures in place for securing the system are working effectively or not and, if not, how to close those security breaches. This paper will examine and analyse the life cycle of the VAPT process and VAPT tools for identifying system vulnerabilities. The significance of updating security procedures at various organisational levels in order to give protection from various cyber-attacks has also been emphasized.

3.6 A SURVEY ON VULNERABILITY ASSESSMENT AND PENETRATION TESTING FOR SECURE COMMUNICATION

As technology advances, the development of systems and software becomes increasingly complicated. As a result, the security of software and web applications is jeopardised. The use of internet applications and security hacking operations have been on the rise in the previous two decades. Organizations face the most difficult task in securing their online applications against the fast expanding cyber threats since they cannot risk the security of their sensitive data. Techniques such as vulnerability assessment and penetration testing may aid organisations in identifying security flaws. If the organisation is unaware of the weakness, it may become an asset for the attacker.

Vulnerability Assessment and Penetration Testing assist a business in identifying security flaws and determining whether or not their security measures are operating in accordance with stated policies. It is vital to build security patches to cover the tracks and mitigate dangers.

This article covers a survey of existing vulnerabilities, their determination, the technique used to determine them, and the tools used to determine them in order to protect companies from cyber threats.

CHAPTER 4

EXISTING SYSTEMS

4.1 Penetration Testing Tools:

4.1.1 Metasploit:

Metasploit is the most used penetration testing automation framework in the world. Metasploit helps professional teams verify and manage security assessments, improves awareness, and arms and empowers defenders to stay a step ahead in the game.

It is useful for checking security and pinpointing flaws, setting up a defense. An Open source software, this tool will allow a network administrator to break in and identify fatal weak points. Beginner hackers use this tool to build their skills. The tool provides a way to replicate websites for social engineers.

4.1.2 Nessus:

Nessus has been used as a security penetration testing tool for twenty years. 27,000 companies utilize the application worldwide. The software is one of the most powerful testing tools on the market with over 45,000 CEs and 100,000 plugins. Ideally suited for scanning IP addresses, websites and completing sensitive data searches. This can be used to locate ‘weak spots’ in systems.

The tool is straightforward to use and offers accurate scanning and at the click of a button, providing an overview of the network’s vulnerabilities. The pen test application scans for open ports, weak passwords, and misconfiguration errors.

4.1.3 Burp Suite:

There are two different versions of the Burp Suite for developers. The free version provides the necessary and essential tools needed for scanning activities. Or, one can opt for the second version if advanced penetration testing is needed. This tool is ideal for checking web-based applications. There are tools to map the track surface and analyze requests between a browser and destination servers. The framework uses Web Penetration Testing on the Java platform and is an industry-standard tool used by the majority of information security professionals.

4.2 Possible drawbacks of Existing Systems:

A misconfigured automated pentest that is not done properly can crash servers, expose sensitive data, corrupt crucial production data, or cause a host of other adverse effects associated with mimicking a criminal hack. The vulnerability scanner is not totally accurate in some situations and some results must be checked to verify the vulnerability. Even though these are large frameworks they are not 100% accurate.

CHAPTER 5

PROPOSED SYSTEM

5.1 Penetration Testing Strategy:

Based on the amount of information available to the tester, there are three penetration-testing strategies: black box, white box and gray box. In black box penetration testing, the testers have no knowledge about the test target. They have to figure out the loopholes of the system on their own from scratch. This is similar to the blind test strategy in, which simulates the actions and procedures of a real attacker who has no information concerning the test target.

On the contrary, in white box penetration testing, the testers are provided with all the necessary information about the test target. This strategy is referred to as targeted testing where the testing team and the organization work together to do the test, with all the information provided to the tester prior to test.

Partial disclosure of information about the test target leads to gray box penetration testing. Testers need to gather further information before conducting the test. Based on the specific objectives to be achieved, there are two penetration testing strategies which include external and internal testing.

5.2 Phases of Penetration Testing:

Through penetration testing, one can proactively identify the most exploitable security weaknesses before someone else does. However, there's a lot more to it than the actual act of infiltration. Penetration testing is a thorough, well thought out project that consists of several phases.

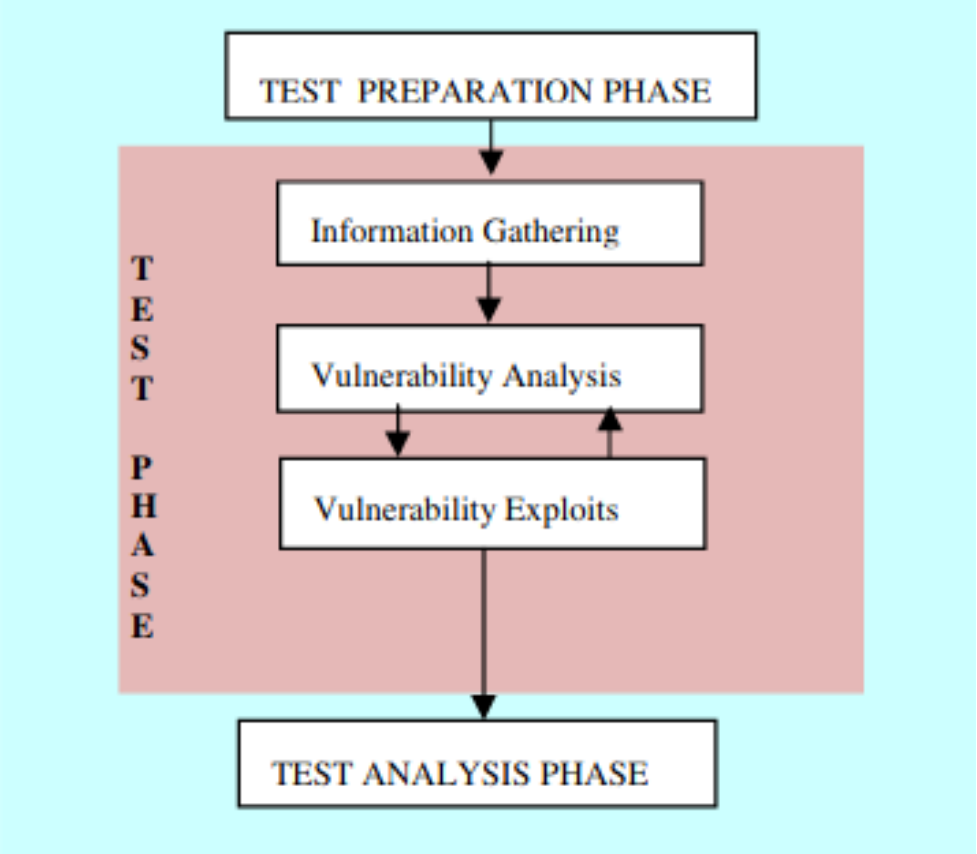

Fig 5.1 - Pentesting Phases

5.2.1 Information Gathering:

Information Gathering is the first and foundation step in the success of penetration testing. With more useful information about a target, the more chances there are to find vulnerabilities in the target and find more serious problems in the target by exploiting them. Involves defining the scope and goals of a test, including the systems to be addressed and the testing methods to be used.

5.2.2 Vulnerability Assessment:

A vulnerability assessment is conducted in order to gain initial knowledge and identify any potential security weaknesses that could allow an outside attacker to gain access to the environment or technology being tested. A vulnerability assessment is never a replacement for a penetration test, though. Understands how the target application will respond to various intrusion attempts. It is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.

5.2.3 Exploitation:

This is where the action happens! After interpreting the results from the vulnerability assessment, penetration testers will use manual techniques, human intuition, and their backgrounds to validate, attack, and exploit those vulnerabilities. Advantage of a system vulnerability or security flaw is taken and then try to manipulate, crash or steal information from it.

5.2.4 Post Exploitation:

As the term suggests, post exploitation basically means the phases of operation once a victim's system has been compromised by the attacker. The value of the compromised system is determined by the value of the actual data stored in it and how an attacker may make use of it for malicious purposes. The concept of post exploitation has risen from this fact only as to how the victim's compromised system's information can be used. This phase actually deals with collecting sensitive information, documenting it, and having an idea of the configuration settings, network interfaces, and other communication channels. These may be used to maintain persistent access to the system as per the attacker's needs.

5.2.5 Final Analysis & Review:

In this phase the results of the penetration test are then compiled into a report detailing. Details like Specific vulnerabilities that were exploited, Sensitive data that was accessed, The amount of time the pen tester was able to remain in the system undetected are collected and noted for reporting. This information is analyzed by security personnel to help configure the network's security settings and other application security solutions to patch vulnerabilities and protect against future attacks.

5.3 Types of Penetration Testing:

5.3.1 Network Penetration Testing:

Most of the systems and computers are connected to a network. If a device is connected to the internet, that means the device is connected to the network because the internet is a really big network. A network penetration test is the process of identifying security vulnerabilities in applications and systems by intentionally using various malicious techniques to evaluate the network's security, or lack of, responses. These are performed by organizations to evaluate the susceptibility of information systems to network attacks.

5.3.2 Web/Mobile Application Penetration Testing:

Web application penetration testing is the process of using penetration testing techniques on a web/mobile application to detect its vulnerabilities. It is similar to a penetration test and aims to break into the application using any penetration attacks or threats. The tests involve implementing any of the known malicious penetration attacks on the application. The main area of focus is only on web/mobile applications.

5.3.3 Wireless Penetration Testing:

Wireless penetration tests are typically performed on the client's site as the pen tester needs to be in range of the wireless signal to access it. Similar to all other pentesting methods and techniques but the gateway of exploiting into the system is via wireless medium such as routers, modem, etc.

5.3.4 Social Engineering:

Social engineering can be defined as the art of exploiting the human in order to gain access to a network, system, or valuable information. Social engineering comes in many different forms: it can be performed via email, over the phone, or even in person. The different varieties of social engineering used by scammers can make training employees effectively a difficult task. These are some of the common hacking methods in our day to day life.

CHAPTER 6

SYSTEM REQUIREMENTS

To Successfully get down with the project, there are certain hardware and software requirements to adapt with. The following describes it all:

6.1 Hardware Requirements:

Any PC or Laptop with RAM > 512MB.

6.2 Software Requirements:

- Python
- Bash
- Linux Environment (Kali Linux - Preferred)

CHAPTER 7

LIST OF MODULES

7.1 Reconnaissance :

Tools for gathering all basic information about the system are included in the module. Details such as web technology used, dns records, reverse-ip lookup can be retrieved.

7.2 Vulnerability Assessment:

After reconnaissance a proper scanning for possible vulnerabilities are looked into the system. Some popular and common vulnerabilities include SQL injection, Cross-Site-Scripting, Code Execution, File inclusion, Cross-Site Request Forgery, etc.

7.3 Exploitation:

The security flaws found in the previous step have been taken advantage of to exploit into the system. Exploitation techniques include shell scripting, reverse shell uploading, creating backdoors, opening sessions into the target machine, etc.

7.4 Analysing the results:

The analysis of all the above data will provide suggestive methods to patch the security flaws. It gives an idea of the existing security level of the application.

CHAPTER 8

IMPLEMENTATION

8.1 Snapshots:

8.1.1 Information Gathering - Web Crawler :

```
kali@kali:~/Desktop$ python3 crawler.py
Please Enter the website which you want to scrapp : https://www.kct.ac.in
[!] External link: https://kctbs.ac.in/
[!] External link: javascript://void(0);
[!] External link: https://blog.kct.ac.in/
[!] External link: https://careers.kct.ac.in/
[!] External link: https://www.youtube.com/channel/UCQ71Y6dp5f-HZaKB4ZQZDlg
[!] External link: https://www.facebook.com/KCT.edu/
[!] External link: https://www.instagram.com/kct_84/
[!] External link: https://www.linkedin.com/school/kct/
[!] External link: https://admissions.kct.ac.in/
[!] External link: https://kct.ac.in/announcement/
[!] External link: https://www.youtube.com/watch
[!] External link: https://propvr.tech/embed.html
[!] External link: https://www.aicte-india.org/sites/default/files/list-suggested-books-indian-authors-publishers.p
df
[!] External link: https://kct.directverify.in/student/index.html
[!] External link: http://smartapps.kct.ac.in/
[!] External link: http://grievances.kct.ac.in/
[!] External link: https://twitter.com/KCTOfficial
[!] External link: https://admissions.kct.ac.in/ug/
[!] External link: https://admissions.kct.ac.in/uglateral/
[!] External link: https://admissions.kct.ac.in/pg/
[+] Total External links: 20
```

Fig. 8.1 - Web Crawler

8.1.2 Information Gathering - Reverse IP Lookup

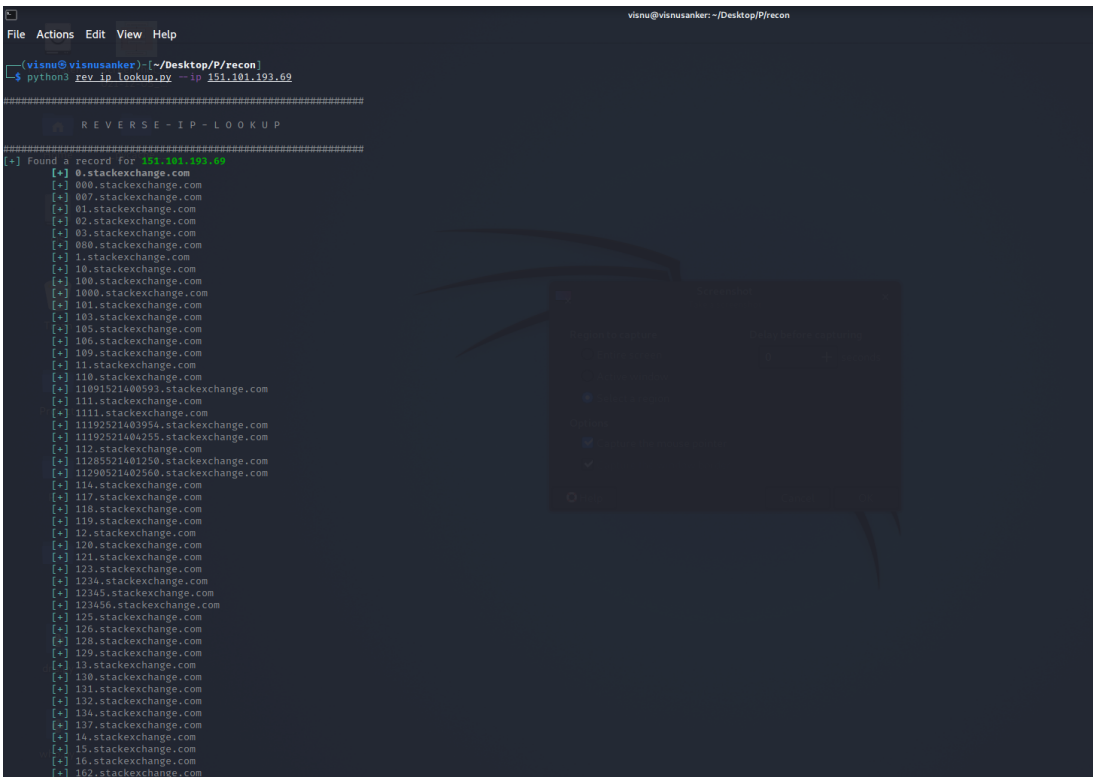

Fig. 8.2 – Reverse IP Lookup

8.1.3 Vulnerability Assessment - SQL Injection

Fig. 8.3 - Sql Injection

8.1.4 Vulnerability Assessment - Cross Site Scripting

Fig. 8.4 - XSS

CHAPTER 9

CONCLUSION

Penetration testing is a comprehensive method to identify the vulnerabilities in a system. It can be an efficient and cost-effective strategy to protect the organization's systems against attacks. If done properly, it helps the organization identify the internal practices that give rise to vulnerabilities and other sources of vulnerabilities. The identified sources enable the organization to remove the vulnerabilities, properly direct the system's security efforts, pressure vendors to improve their products, improve its internal business security practices and prove to customers, shareholders and regulatory agencies that it is making a good faith effort to properly protect critical business data. The final report needs to have enough detail and substance to allow those doing remediation to simulate and follow the attack pattern and respective findings.

REFERENCE

[1] R. Pandey, V. Jyothindar and U. K. Chopra, "Vulnerability Assessment and Penetration Testing: A portable solution Implementation," 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN), 2020, pp. 398-402, doi: 10.1109/CICN49253.2020.9242640.

[2] P. Zech, M. Felderer and R. Breu, "Towards a Model Based Security Testing Approach of Cloud Computing Environments," 2012 IEEE Sixth International Conference on Software Security and Reliability Companion, 2012, pp. 47-56, doi: 10.1109/SERE-C.2012.11.

[3] Hasan, Ashikali and Meva, Divyakant, Web Application Safety by Penetration Testing (2018). International Journal of Advanced Studies of Scientific Research, Volume 3, Issue 9, 2018.

[4] Reza, S & Hasan, Wahidul & Reza, S M & Chakraborty, Sajib. (2015). A Comparative Overview on Penetration Testing.

[5] Y. Khera, D. Kumar, Sujay and N. Garg, "Analysis and Impact of Vulnerability Assessment and Penetration Testing," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), 2019, pp. 525-530, doi: 10.1109/COMITCon.2019.8862224.

[6] K. Patel, "A Survey on Vulnerability Assessment & Penetration Testing for Secure Communication," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 320-325, doi: 10.1109/ICOEI.2019.8862767.

[7] Budzak D. Information security – The people issue. Business Information Review. 2016;33(2):85-89. doi:10.1177/0266382116650792

[8] S. Sandhya, S. Purkayastha, E. Joshua and A. Deep, "Assessment of website security by penetration testing using Wireshark," 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), 2017, pp. 1-4, doi: 10.1109/ICACCS.2017.8014711.

[9] Jai Narayan Goel, B.M. Mehtre, Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology, Procedia Computer Science, Volume 57, 2018.

[10] Michael Williams. “A Risk Assessment on Raspberry PI using NIST Standards”, 2018.

[11] Github link of the project - https://github.com/visnu05/Penetration-testing-framework-to-find-the-security-flaws-in-a-web-application