CYBERGUARD PRO

A thesis submitted by

Ghulam Yaseen (GL) (20SW077)

Supervisor

Prof. Dr Qasim Arain

In the Partial Fulfillment of the Requirements for the Degree of
Bachelor of Engineering in Software Engineering

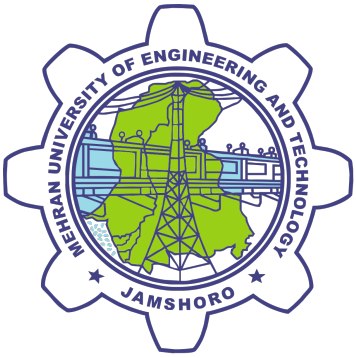
DEPARTMENT OF SOFTWARE ENGINEERING
MEHRAN UNIVERSITY OF ENGINEERING &
TECHNOLOGY, JAMSHORO

November, 2024

DEDICATION

This thesis is wholeheartedly and proudly dedicated to the people we can take inspiration from including our beloved parents, respected faculty of Mehran University of Engineering and Technology, and mentors who assisted us in the midst of challenges while completing this thesis.

DEPARTMENT OF SOFTWARE ENGINEERING



CERTIFICATE OF APPROVAL

This is to certify that the Project / Thesis report on the **Cyber-Guard Pro** is submitted in partial fulfillment of the requirements for a Bachelor's degree in Software Engineering by the following students:

Ghulam Yaseen (GL) (20SW077)

Project/Thesis Supervisor	Chairman
Prof. Dr Qasim Arain	Prof. Dr Qasim Arain

Dated: _____

ACKNOWLEDGEMENT

We extend our heartfelt gratitude to everyone who contributed to the success of this project. First and foremost, we are deeply thankful to Allah Almighty for His guidance and blessings throughout this journey. We express our profound appreciation to Prof. Dr. Qasim Arain, our mentor, for his invaluable support and guidance. Our sincere thanks also go to the staff, faculty, and students at Mehran University of Engineering and Technology, Jamshoro, for their assistance and contributions, which have been instrumental in the completion of this project and our graduate program.

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

In a world of ever changing dynamics in cyberthreats, every website looks for security and safety. Website's functioning and interaction with their clients have been altered significantly. This change has also brought with itself enormous challenges in cybersecurity such as SQL injection, cross-site scripting (XSS) data breach, flaws in the wordpress and other areas. Websites providing services to people have been extremely vulnerable to these attacks. For the purpose of countering this threat, this thesis introduces Cyberguard pro, a full proof security edifice. The tool ensures complete security for websites of all nature, across the spectrum with eight cutting edge products. These products include, Sensitive file detector, Sub-domain Scanner, Port Scanner, Wordpress Scanner, XSS Scanner, Wordpress Backup Grabber, SQL injection Scanner and Wordpress Username enumerator to identify and fix problems of all sorts. CyberGuard Pro possesses multilayered structure to combat exploitatives from all directions, no matter how lethal and severe the attack may be. The thesis presents the making and implementation of Cyberguard to protect data and overall website from ever-changing cyber attacks.

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW OF CYBERGUARD PRO

CyberGuard Pro has been designed to naturalize cyber threat of every kind. The entire structure contains numerous cutting-edge tools to immediately recognize the attack and then to mitigate it. The tool prevents the illicit penetration and attempts to steal sensitive data which further can be used for other illegal activities. The arena of cybercrimes is becoming complex to even understand, let alone getting rid of it. The CyberGuard protects and defends the confidentiality of the clients and owners of websites simultaneously. Its devised to maintain the integrity and confidence of people in digital world. The world is fast moving towards the adaptation of digital services. Online services are easy to access and are also extremely convenient to carry out the business. These services entail the interaction and communication between the customers and providers. Some of the most important sectors and most vulnerable, at the same time, to these attacks are banks, businesses, healthcare services, educational platforms, and e-commerce. Each of these sectors carry personal and secretive information about the people utilizing these services,

which even the owners of those industries are forbidden to access. Banking in particular are subject to cyber attacks quite frequently for their financial information and assets. Therefore, Cyberguard is the remedy to be pursued to combat the real time threat of these gargantuan incursions. The entire tool is devised with Port Scanning, XSS payload Testing, Password brute Force, and many more sub-tools, to fight the illegal activity occurring in website.

1.2 PROBLEM STATEMENT

With advent of digitization, all the sectors of services have shifted to online platforms. This shift has invited cyber threats of multiple nature. Some of the attacks include, Data breaches, cross-site scripting (XSS), SQL injection and many more. The threats contain loss of finances, data and information of the company, as well as, clients who come to seek service. The real of cyber threats are not static but rather dynamic. The attacks are not always linear and straight. The nature of the attack varies, at times being highly complex and multi faceted. To face such kind of grave threats, existing tools fall short of the requirements. They neither identify the nature of the problem nor resolve it. Therefore, despite their presence, successful cyber breaches are carried out, resulting in massive losses In the

midst of such on-going threats, a requirement of a tool is imperative. A tool which designed to fight wide variety of cyber breaches at all times possible. Furthermore, the tool must possess strong ability to identify the threat and then to reduce it immediately. A complex structure that is equally powerful, if not more, as the attack it faces, is paramount and necessary at all cost.

These are indeed alarming and the only solution to this is a strong solution that provides advanced security tools to be incorporated into one platform that offers an automatic defense mechanism, intelligence, and real-time threat detection. There is thus a pressing need for an advanced and integrated form of protection as provided by CyberGuard Pro, which offers a comprehensive and robust means of guarding Web applications against the ever burgeoning catalog of current threats.

1.3 FEATURES OF CYBERGUARD PRO

There are eight mapping capabilities integrated in CyberGuard Pro to ensure the security of dynamic Web sites. Through eradicating different weaknesses, every tool provides comprehensive protection against most cyber risks. These tools are as follows regarding what you can do with them.

1.3.1 WordPress Username Enumerator

This utility can be used in identifying people's usernames on WordPress sites that are open to the public domain. If you can identify these usernames, you can stop cracking attacks, which usually target login passwords.

1.3.2 Sensitive File Detector

As with file deletion, this application let you search for exposed sensitive files that may give hackers valuable information about your website such as backup settings or logs. Since these files are protected, a possibility of suffering data breaches is minimal.

1.3.3 Sub-domain Scanner

This tool identify all the subdomains associated with a particular website. Identifying these subdomains makes sure that no part of your connected ecosystem goes unnoticed, let alone unsecured or poorly overseen.

1.3.4 Port Scanner

In this program, the attendant chooses to view the Service and the open Ports so that Services that can be accessed can be known. One

way in which you are shielded against attacks is by avoiding likely avenues through which a hacker could penetrate your CPU.

1.3.5 WordPress Scanner

The WordPress scanner looks for vulnerabilities particular to WordPress websites, like out-of-date plugins, unsafe themes, or improper setups. It guarantees that your WordPress installation is current and safe.

1.3.6 XSS Scanner

reviews input fields of a form and other active website components for cross-site scripting flaws. By dealing with the mentioned vulnerabilities, rogue scripts cannot corrupt user data or your website.

1.3.7 WordPress Backup Grabber

This program searches for openly available WordPress backup files, which may contain personal data, such as login details. In doing so, it will be possible to ensure that hackers cannot use these files to get to your website.

1.3.8 SQLI Scanner

This utility identifies characteristics of Website that are vulnerable to SQL injection attacks. These issues can be solved and this way you can stop unwanted access and manipulation of your database.

1.4 PROPOSED SOLUTION

CyberGuard has been launched to thwart off all the aforementioned dangers of cyber crimes. The tool has the most comprehensive products, aiming to prevent any sort of breach of data or penetration. The tool possess the equal armors, complexity and efficiency as the complexity and effectiveness of those trying to break in the system. The software fights threats such as, SQL injection, Cross-site scripting (XSS), open and weak files, and flaws in wordpress or on other platforms. In total, the tool carries 8 products to understand, address and kick out the illegal incursion in the first instant. The system ensures maintenance of sporadic weaknesses that may possibly exist in the website, which in return is exploited by the hackers. CyberGuards best feature is that it the complex method of making websites secure from complex attacks. Recognizing unnecessary plugins, poor setups, publicly exposed usernames is one of the jobs it accomplishes. For instance, Sensitive File Detector and Wordpress

Backup Grabber are responsible for making date secure from the hackers which is unintentionally left open and exposed. The SQL Scanner and XSS scanner have been equipped to eradicate the most widespread and dangerous weak spots in a given online system. The port scanner meanwhile looks at server configuration to spot exploitable areas in a website. Then comes the sub-domain scanner which enlarges the security parameters and the area to contain cyber threats in sub domains.

It has been structured keeping in mind the desires, aspiration, accessibility and needs of the user. It boosts the confidence of the user in the digital world and thus it enhances and expands the electronic world. CyberGuards interactive interface and real time tracking ensures easy way of moving along, tracing, run scans, and setups. Furthermore, the utilization of reports shall further help the user to secure accounts and dealings. The CyberGuard has extremely simplified the process of safety in all the spheres of sectors. The entire purpose of this endeavor has been to formulate user-friendly tool that can safeguard all the information in the webiste. With most efficient tools available in the system, CyberGuard makes sure that everything in the website is safe and secure for long period of time.

1.5 AIMS AND OBJECTIVES

Aims: CyberGuard Pro's primary objective is to provide a comprehensive, proactive, and easy cybersecurity architecture for the protection of dynamic websites from a range of today's online threats. CyberGuard Pro identifies vulnerabilities in real time, stops exploitation, and ensures security, integrity, and functioning of online applications across industries by integrating many cutting-edge security solutions into one platform.

Objectives:

- Accurately identify vulnerabilities such as SQL injection and cross-site scripting.
- Enhance WordPress security by using specific tools that strengthen login security.
- Protect infrastructure by revealing exposed files and hidden subdomains.
- Facilitate ease of detection with automated scanning and real-time reporting.
- Usability through an interactive and user-friendly interface.
- Build a multi-layered protection system to be completely guarded.

1.6 ASSUMPTIONS

1. Websites targeted adhere to standard web protocols like HTTP/HTTPS.
2. Users have proper authorization for testing systems.
3. Focus on dynamic sites that are vulnerable to SQL injection and XSS attacks. solutions developed should be specific to WordPress for the target websites.
4. Unpatched or otherwise insecure target systems could be vulnerable.

1.7 DEPENDENCIES

Software libraries, system requirements, and many more dependencies are required in order to enable and run CyberGuard Pro properly. By ensuring the correct functionality of the framework, these dependencies provide accurate and effective vulnerability detection.

1. **Python Environment:** For running its scripts, CyberGuard Pro requires a Python interpreter (3.x). It is highly recommended to use Python 3.x for better support and compatibility.
2. **Required Libraries:** A few Python libraries are needed for the framework to operate, including:
    - **Socket:** For network-related operations, including subdomain discovery and port scanning.

- **urllib or urllib.request:** For dealing with URLs and sending HTTP/HTTPS requests.
- **BeautifulSoup (from bs4):**Used to parse and analyze HTML responses during scans.
- **System and Outputs:** Handles system-level functions like console cleanup and user input management.

3. **Internet Connectivity:**CyberGuard Pro requires a steady internet connection to visit target websites, submit queries, and receive analysis-ready responses.
4. **Target System Accessibility:** The framework presupposes that the target systems function and are responsive to HTTP/HTTPS queries. Systems that are down or otherwise inaccessible cannot be assessed.
5. **User Privileges:** Users will be required to have the rights necessary to execute the script, install dependencies, and legally scan target computers. All activities are assumed to be performed with proper authority.
6. **Operating System Compatibility:** CyberGuard Pro is designed to work on Windows, Linux, and macOS. It assumes the availability of necessary system tools, like a terminal or command prompt.

7. **OS Module:** By providing a means of interacting with the operating system, the `os` module enables file management and environment interaction. For instance, it is used to manage directories, verify the existence of specific files, or run system commands.
8. **Sys Module:** The `sys` module provides access to variables and functions that interact with the operating system and Python runtime environment. It can manage command-line arguments, handle system paths, and terminate the application gracefully.
9. **Datetime Module:** The `datetime` module formats and manipulates dates and times. It is useful for logging the scan process, recording timestamps, and generating scan histories.
10. **DNS Resolver:** The `dns.resolver` module from the `dnspython` package is used for DNS lookups. It ensures proper domain resolution and facilitates DNS-based vulnerability assessments.
11. **Requests:** The `requests` library simplifies sending HTTP requests to servers and managing their responses, which is essential for testing endpoints and scanning vulnerabilities.
12. **BeautifulSoup:** Provided by the `bs4` library, it is used for parsing and analyzing HTML or XML documents. It is particularly useful for extracting data and analyzing WordPress websites.
13. **Colorama:** The `colorama` library enhances the readability of ter-

minal outputs by providing colored text for errors, warnings, or successes.

14. **Subprocess Module:** This module is used to execute external commands or programs from within the script. It facilitates integration with third-party tools and utilities.

1.8 THESIS ORGANIZATION

- **Chapter 1: Introduction**

  The matter under discussion in this chapter is the introduction, background, features, and problem statement of thos thesis.

- **Chapter 2: Literature Review**

  This chapter outlines the literature review of the project, discussing research done and alternative solutions in other languages or frameworks.

- **Chapter 3: Design and Methodology**

  This chapter outlines the methodology and design of the project, explaining the overall structure and processes.

- **Chapter 4: Tools and Technologies**

  This chapter lists and describes the tools and technologies used in the project.

- **Chapter 5: Implementation**

This chapter provides an in-depth discussion of how the project was implemented using the identified tools and techniques.

- **Chapter 6: Conclusion and Future Work**

  This chapter sums up the findings of the project and possible improvements and extensions for future work.

CHAPTER 2

LITERATURE REVIEW

CyberGuard Pro is a high-tech software designed to protect computer networks and websites from various types of threats. Some of its features include:SFD – an abbreviation for Sensitive File Detector, which scans for exposed sensitive files that would otherwise be a threat to security. WUE – short for the WordPress Username Enumerator; counts usernames to assist in an identification of potential targets for brute force attacks. The Sub-domain Scanner discriminates potentially exploitable sub-domains which can easily be missed out. The Port Scanner assist in identifying some open ports that are potentially exploitable by hackers further. Also, the WordPress Backup Grabber ensures that backups containing sensitive information can be accessed online. It can discover places that can be exploited by an attacker during a cross-site scripting attack. In addition, it shows if old plugins and themes exist. Lastly, the SQL Injection Scanner discovers and addresses potential threats for SQL injections. To summarize, CyberGuard Pro is an all-rounded solution to cybersecurity because it gives organizations the tools needed to protect themselves against potential dangers and weaknesses.

2.1 RELATED WORK

Most cybersecurity related technologies deal with certain specified threats, such as the following:

- **Burp Suite:** It is used to identify vulnerabilities in websites
- **WPScan:** It specializes in the scanning of WordPress sites security..
- **Nmap:** It scans for ports to discover possible security vulnerabilities.

Such tools would then reveal such basic problems like open ports, unpatched software, and security poor practices. Yet CyberGuard Pro goes one step ahead because it bundles up all those functions in a single application. The service is one of multiple security evaluations performed on the same website with its own assessment of such simple problems such as XSS and SQL injections along with issues particular to WordPress sites including bad usernames and poor backups.

While other tools like OWASP ZAP and Nikto do the job of identifying vulnerabilities in websites, CyberGuard Pro differs with other functionalities that most people miss. For example:

- **WordPress Backup Grabber:** It will find publicly accessible backups that are often overlooked by other tools but might hold

sensitive information.

- **Sensitive File Detector:** Detects files such as database backup files and configuration files that are sensitive to public exposure since their exposure could lead to significant security risks.

Many programs focus on a particular vulnerability, such as SQL injection or XSS. But they often require a different software for each task. CyberGuard Pro simplifies the process by providing one platform that addresses multiple security domains. It not only analyzes web pages but also backup files and subdomains, ensuring every aspect of a website is secure.

Besides enhanced security for WordPress, CyberGuard Pro offers greater security capabilities over tools like Wordfence and Sucuri. While both of these tools protect the website from malware and different types of attacks, CyberGuard Pro checks specifically for outdated plugins and themes, commonly targeted by hackers. Due to this, it identifies vulnerabilities in a broader range that the previously discussed tools do.

2.2 CONCLUSION

CyberGuard Pro integrates different technologies into one platform, allowing an enhanced and user-friendly cyber security solution. This

way of approach will make the detection and solving of a wide range of vulnerabilities easy and more efficient in safeguarding websites and online-based platforms.

CHAPTER 3

DESIGN AND METHODOLOGY

3.1 METHODOLOGY

CyberGuard Pro interface of the offered Python-based web application was structured according to passed practices to provide productivity and user-friendly result. Here is the given following methodology of implementation of features:

3.1.1 CyberGuard Pro Security Model (CGPSM)

CyberGuard Pro Security Model works in the process of combining several features into a well-ordered framework. This approach ensures seven of its eight technologies work in unison to identify and tackle security vulnerabilities. The methodology works as follows: First, there are the integrated scanner tools where the analyst scans either the website or the server. It starts with lists usernames on sites such as WordPress using queries to find possible weak points that attackers can exploit. At the same time, it performs a search for files likely to contain valuable data within the target system in order to look for configuration files, backup, or database output files. Lastly, a complete domain enumeration is performed to determine the layout of the domain and the existence of other neglected or weak

subdomains. The Port Scanner is used to find intensively utilized services with improperly configured ports which may be attacked.The model also utilizes a WordPress scanner to detect out of date plugins, themes, and core files. The Vulnerability assessment tools like the XSS and SQL Injection scanners look at input based attacks whereby they send a designed payload and analyse the response for signs of exploitation of vulnerability. In turn, based on such unification, it guarantees the accuracy of the detected vulnerabilities and their performance, allowing bearing several threats at once during one stage of execution.

3.2 PHASES OF THE CYBERGUARD PRO MODEL

Phase 1: Reconnaissance

In reconnaissance phase, the Hacker's priority is to find all the information they can about the target they are focusing on. This includes networks, protocols such as IP addresses, domain names and any public data from sites and social media. Here, passive and active methods are applied to discover objects of the technology, including DNS records, subdomains, and server types. The purpose of gather all this information is to outline target profile and determine the ways to penetrate during the next steps.

Phase 2: Scanning

During the scanning phase, tools will be used to continue to identify the active services in the target and the ports that are open. This involves the identification of System surface area for scan such as Network layer scan and application layer scan for example http, ftp, ssh or smtp services. Network mapping, vulnerabil-ity assessment, and enumeration for banners are the common methods that identify types of software as well as their versions and settings, which can be potential threats. This particular phase creates possibilities that are exploitable during the other phases targeting.

Phase 3: Vulnerability Exploitation

In this phase, identified vulnerabilities are used to extend privileges means to get more access than is authorized. The possibilities include buffer overflow, SQL injection or denying service using unpatched software bugs. This phase tries to capitalize on the weaknesses that have been identified by the scanning process so as to penetrate into the systems.

Phase 4: WordPress Username Enumerator

This phase is meant to gather the current list of WordPress usernames using login or API endpoints that are genuine. Some username schemes can be checked automatically, and common user IDs patterns can be enumerated in order to carry out more credential-oriented attacks such as brute force, and guessing attacks.

Phase 5: Sensitive File Detector

In this phase we are mainly concerned with finding out files or directories which contains data such as configuration files, database files and their credentials. Tools are employed to search for some known misconfiguration targets, such as backup files or ".env" files that might contain valuable information for an attacker.

Phase 6: WordPress Scanner

The WordPress Scanner reveals system weaknesses within the target's WordPress system, such as plug-ins, themes, and the core that are out of date or have known vulnerabilities. Smart system recognize vulnerable patterns, i.e., plugin exploits or insecure configurations that enable the attacker to gain privileges and execute code of their choice.

Phase 7: XSS Scanner

The XSS Scanner aims for cross-site scripting vulnerabilities by experimenting with input fields and forms as well as URL parameters for inefficient sanitation. This phase outlines the possibility of introducing evil JavaScript, a code which is capable of purloining session cookies, credentials or night marching through the account of the victim.

Phase 8: WordPress Backup Grabber

This phase is a process of searching and downloading files, which are backups from WordPress sites. These backup files frequently contain data that is sensitive or contain user names and passwords, or old programmes that dumpers can mine for potential weaknesses in the defense perimeters.

Phase 9: Reporting

During the reporting phase all findings that were found out, vulnerability exploited, attempts made to do so and any information that might be sensitive are recorded. The findings of the report are more specific with respect to the identified security vulnerabilities supplemented by the viable suggestions for change.

Phase 10: Exit

During the reporting phase all findings that were found out, vulnerability exploited, attempts made to do so and any information that might be sensitive are recorded. The findings of the report are more specific with respect to the identified security vulnerabilities supplemented by the viable suggestions for change.

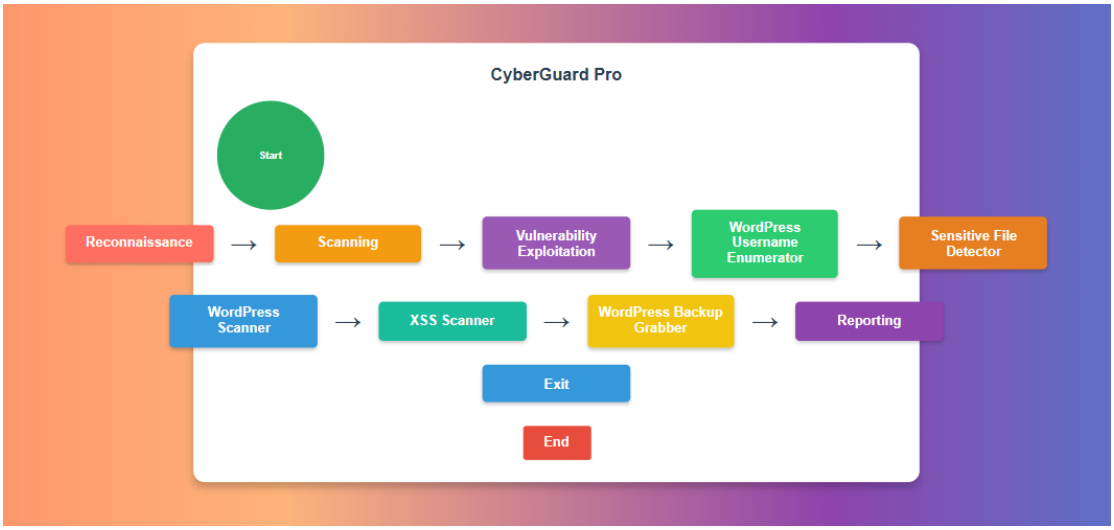


Figure 3.1: Workflow Diagram

3.2.1 When to Use the CyberGuard Pro Security Model?

The CyberGuard Pro Security Model is the best model if strong cybersecurity measures are highly required. Here are some instances where such a model should be applied:

- **Before deployment:** Ensure the website is secured against vulnerabilities such as exposed open ports, sensitive file exposure, or

subdomain flaws.

- **Regular assessment:** Scan a website or server to detect new vulnerabilities and ensure all plugins, themes, and software are safe and updated.
- **Incident analysis:**Identify how an attacker gained access, detect sensitive files made public, and correct configuration errors to prevent future breaches.
- **Penetration testing:** Test a website or application for vulnerabilities such as SQL injection or XSS. Ensure flaws are fixed before exploitation.
- **System updates:** Be sure no new vulnerabilities arise from updating with new plugins or structural changes.
- **Compliance efforts:** Help find and protect sensitive information and ensure proper configurations in place for cybersecurity standards or regulatory requirements.

3.3 BENEFITS

- **Complete Vulnerability Detection:** It addresses different types of vulnerabilities, such as injection errors, misconfigurations, and weak credentials.
- **Efficiency:** Reduces the time and effort needed for a comprehensive

security evaluation by combining several tools into a single model.

- **Proactive Threat Identification:** Threat Identification: It identifies potential security threats before the attackers can exploit them.
- **Improved Data Security:** Protects against exposure and unauthorized access to sensitive information.
- **Scalability:**Adapts to platforms and systems of different sizes, ensuring safe administration for both small and large infrastructures.
- **Frequent Maintenance:** Assists with regular updates and checks, protecting the system from emerging threats.
- **Customizable:** Can be tailored to address certain vulnerabilities or needs.
- **Cost-effective:** Packs several security measures in one, saving time and avoiding the need for various solutions.
- **Better Compliance:** Supports the fulfillment of industry and regulatory security standards.

3.4 CHALLENGES

- **Complex Configuration:**Merging several tools into a single framework does require technical know-how as well as proper configuration.
- **Resource-intensive:**If all eight tools are deployed together, it is

going to be very CPU-intensive and time-consuming.

- **False Positives:** Some tools might report trivial issues; therefore, improper investigations take place and delays result.
- **Maintenance Overhead:** Tools and models require frequent updates to eliminate emerging vulnerabilities and remain functional.
- **Limited Scope:** Generally, it is more inclined towards web applications, hence may not be used in other security issues such as insider threats or advanced persistent attacks.
- **Scalability Issues:** Huge complex infrastructures require significant customizations to work effectively.
- **Dependency on User Expertise:** Using the model effectively requires knowledge of cybersecurity principles and tool output.
- **Dynamic Threat Landscape:** Cyber threats are constantly changing, meaning that updates are constantly required to detect new attack vectors.
- **Tool Interoperability:** nteroperability of all eight tools can be difficult, especially in diverse environments.
- **Cost of Upgrades:** If the tools are not open-source, maintaining the tools may come at an extra cost.

3.5 WHY USE THE CYBERGUARD PRO SECURITY MODEL?

The CyberGuard Pro Security Model was developed in response to the necessity for a strong, comprehensive security framework for systems and web applications. It brings together eight key tools into one unified program for identifying and mitigating incidences of open ports, outdated plugins, misconfigured sub-domains, exposed sensitive files, and injection flaws such as SQL and XSS.The approach reduces the need for many single tools, saving time and cost while making it available on a user-friendly interface for all technical levels. It can cater to a small or even a large infrastructure and is, thus, a great boon for organizations of every category. Apart from vulnerability detection, CyberGuard Pro also provides actionable insights for risk mitigation, thus taking a wholesome view of cybersecurity. Regular and efficient evaluations by a model enhance compliance with industry standards and regulations, enabling organizations to take proactive steps to strengthen their security posture.

3.6 DIAGRAMMATIC MODELS

In this section, we illustrate our system using various diagrams. We provide and analyze the system's flowchart in conjunction with a use case diagram. The system has the diagrams and flowcharts to ensure

that everything is analyzed

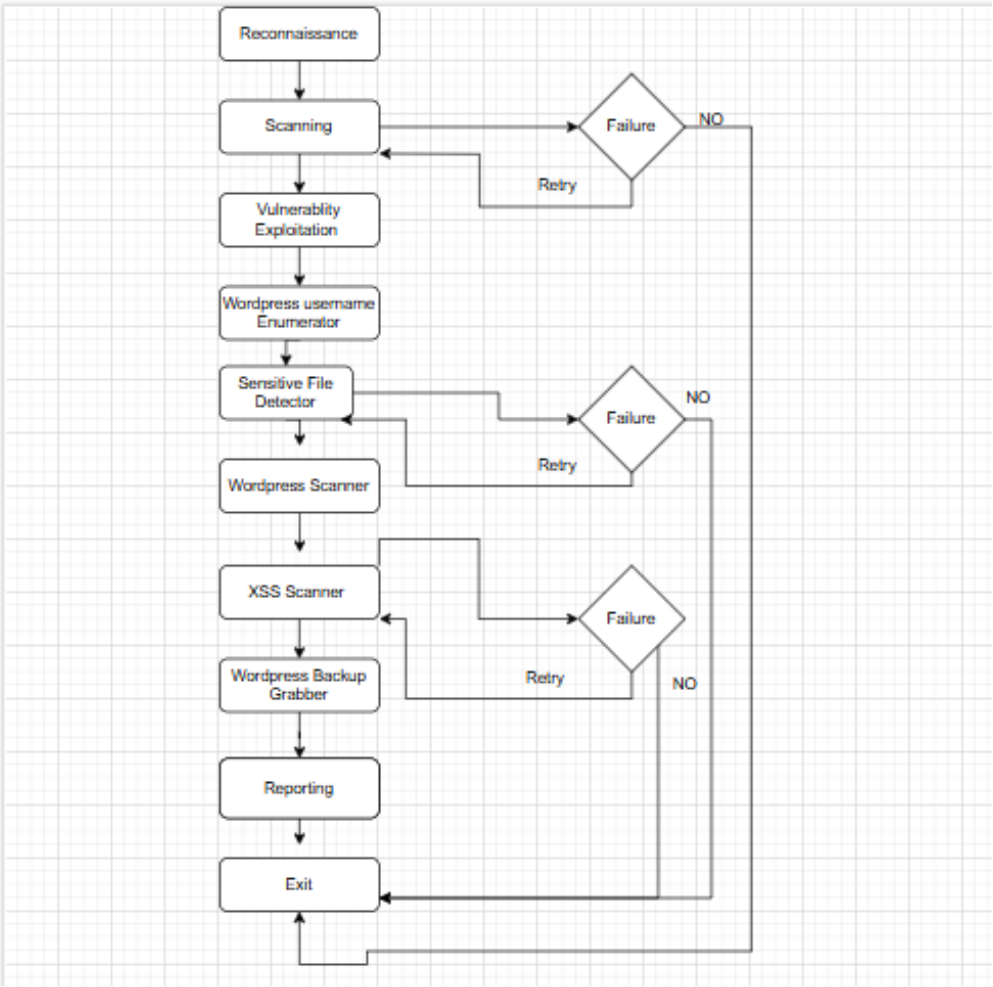


Figure 3.2: System Flowchart of CyberGuard Pro

A CyberGuard Pro workflow begins with reconnaissance or any information on the target system gathered over subdomains, WHOIS, DNS records, geolocation, and some OSINT. This would create an excellent foundation for the further testing. This is followed by Activities in Scanning, which would reveal open ports and active services identified by the banners to portal possible entry points to

them. The next step would then be Explotation efforts of exploiting such identified vulnerabilities like SQL Injection, XSS, or directory traversal. These vulnerabilities are then adjudged and surveyed for their exploitability. The decision then lies in retrying or bypassing or abandoning the exercise if exploitation is said to be futile.

A WordPress Username Enumerator, dedicated module to the tool, detects active usernames, the Sensitive File Detector scans for backup files as well as other highly required resources that might give away potential sensitive information. Both modules allow retrying or skipping because of failure. The WordPress Scanner investigates vulnerabilities in the plugins and themes. The other is the XSS Scanner that checks for Cross-Site Scripting vulnerabilities by sending payloads and looking for weaknesses in the sanitization mechanism. Decision points are included into every module to handle failures in the most effective way possible.

In the end, the WordPress Backup Grabbers will download backup files stored for deeper inspections, and the Reporting module will look at gathering everything into a single report. If report generation fails, the error is logged and the process ended. Each and every step of the process includes decision points so that if things do not go smoothly, the process can either retry, skip, or log the error. The

last step in the workflow is a successfully created final report or clean egress in case of severe errors. It guarantees that this method is really structured.

3.7 USE CASE OF THE CYBERGUARD PRO

CyberGuard Pro is an all-in-one complete cyber solution that comes with penetration testing and vulnerability assessments. It functions through well-defined roles where the user regards pentester who uses the tool to accomplish multitasks including reconnaissance, scanning, exploitation, and so on. The target system is the entity being analyzed, such as domains or even IP addresses assessed through modules covering pot scanning, vulnerability identifications, and exploitation methods.

To augment its capabilities, CyberGuard Pro connects with external services such as:

- **WHOIS:** For domain registration information.
- **DNS Resolver:** For DNS record queries.
- **Shodan API:** For detecting public exposure.
- **Geolocation APIs:** To gather location-based intelligence.
- **Reverse IP Lookup Services:** For comprehensive intelligence gathering.

Additionally, external tools like `sslscan`, `nmap`, `smbclient`, and `onesixtyone` enhance its functionality by providing strong support for SSL/TLS analysis, port scanning, and protocol enumeration.

3.7.1 System Operation

The system operates through a modular process:

1. **Reconnaissance:** Initial data collection about the target through subdomain enumeration, WHOIS information, and DNS queries.
2. **Scanning:** Detection of open ports and active services using sophisticated tools like `nmap`.
3. **Exploitation:** Simulated attacks to identify vulnerabilities such as SQL injection, XSS, and directory traversal.
4. **Specialized WordPress Modules:** Dedicated to uncovering issues related to plugins, themes, and sensitive files.
5. **Reporting:** Consolidation of findings into a structured document for record-keeping and future reference.

Temporary data is retained throughout the operations to facilitate a smooth workflow, and the final report is saved as a text file for future reference.

3.7.2 Modular Architecture

The modular architecture of CyberGuard Pro promotes efficiency and flexibility, establishing it as a vital resource for penetration testers aiming for thorough security assessments. Its design seamlessly integrates with contemporary external tools and APIs, enhancing its functionality and utility for diverse cybersecurity scenarios.

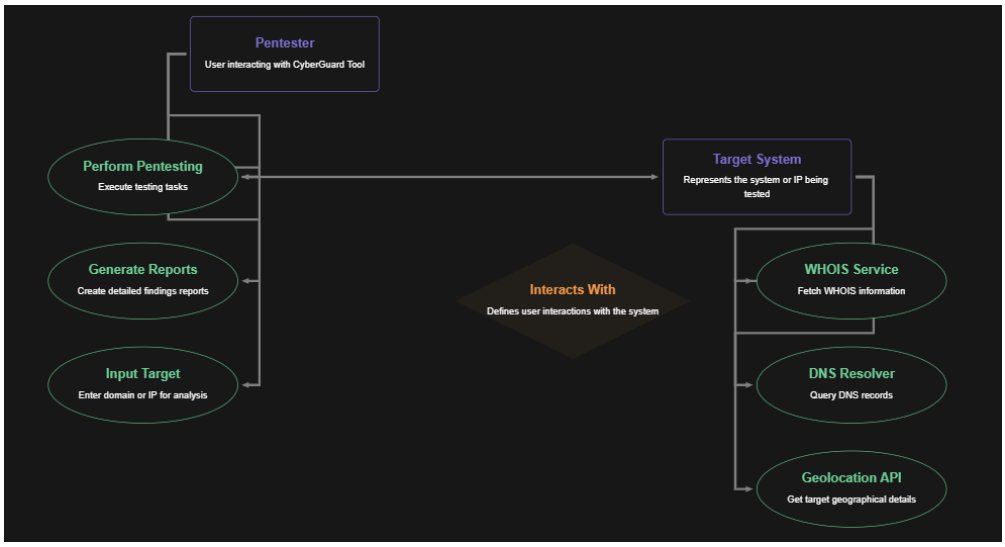


Figure 3.3: System Flowchart of CyberGuard Pro

3.8 FUNCTIONAL REQUIREMENTS

There are some necessary functionalities that the CyberGuard Pro should possess in order to be able to secure web applications. The application is designed to crawl through sites, especially WordPress websites, and enables searching for usernames using URL pattern recognition techniques to identify accounts that might be targeted

by an attacker. Other features are identifying private items that might be publicly available, like configuration files and database backups, which can seriously compromise security. It needs to search for each and every subdomain belonging to it so as to locate hidden or forgotten subdomains, which might be gateways for cybercriminals. CyberGuard Pro must nevertheless have a port scanner that will detect vulnerable services and open ports on the server that can be abused when left unattended. The system should include a WordPress vulnerability scanner which seeks out obsolete themes, plugins, and core files-the places whereby security loopholes are most likely to be available for hackers. Another salient feature is the XSS (Cross-Site Scripting) scanner which tests for those possibilities on the web pages where attackers can directly inject their malicious scripts and create havoc through data theft or other attacks. CyberGuard Pro must also incorporate a SQL injection scanner to evaluate entry fields and parameters that might possibly permit hackers to change databases or retrieve private information. The last element that the program has to bear is the WordPress Backup Grabber, which searches the website for freely available backups that might contain crucial data such as keys, passwords, and configuration information. When all these are put together, CyberGuard Pro offers

total security by identifying and alerting users to several vulnerabilities that may be used to safeguard their web applications.

3.9 NON-FUNCTIONAL REQUIREMENTS

Specific non-functional requirements define operational and quality standards that must be satisfied by CyberGuard Pro for proper working and fulfilling user expectations. Those specifications focus on certain factors that contribute to the overall success of the system. These include performance, usability, security, and reliability features. Some of the non-functional requirements critical for CyberGuard Pro are as follows:

3.9.1 Responsiveness

The firm has designated projects really capable of being responsive given the capability of CyberGuard Pro to operate effectively on a variety of displays and devices. The UI remains functional and user-friendly, regardless of whether it is on a desktop, tablet, or mobile device. They adapt automatically to different screen sizes, ensuring a seamless experience on all platforms. The applicability of CyberGuard Pro means that customers would never have to worry about layout problems or low usability while performing security

scans, viewing results, and managing tasks. The speed of the system in processing requests and yielding the results also contributes to responsiveness.

3.9.2 Usability

CyberGuard Pro's usability is geared towards making the system sufficiently simple and easy to understand and utilize by the user, regardless of the user's experience level. The tools and accompanying clear instructions enable any user to navigate the eight phases without obstacles. With real-time feedback in conjunction with detailed reports to identify weaknesses and recommend workable answers, users can easily solve threats. Clear error handling ensures smooth operation while customization options allow scans to be tailored to specific requirements. CyberGuard Pro is ease-of-use, flexible, and clear, so website and application security becomes a straightforward and simple process for every individual.

3.9.3 Modifiability

This is modifiability as per CyberGuard Pro: it guarantees the flexibility of the whole system and responsiveness to the changes in security demands and emerging technologies. Cybersecurity is an arena where threats and vulnerabilities are quite dynamic; thus, this

property became essential. CyberGuard Pro achieves modifiability through a modular design. Each tool functions as an independent phase that still integrates seamlessly into the broader system. For example, updating or changing the Username Enumerator or the Subdomain Scanner will not affect the other functions of the CyberGuard Pro. This modularity thus makes maintenance simpler and also allows installation of new tools, for instance, advanced AI threat detection modules, without a complete redesign. CyberGuard Pro's modifiability ensures the flexibility of the system and responsiveness to the changing requirements of security, as much as to technological breakthroughs. In fact, such property would be essential in an ever-changing field of cybersecurity, where threats and vulnerability are all dynamic. Modifiability can even be improved through clear and reusable coding resources. The consideration to keep things simple in understanding and modification accompanied standards, such as clean coding, organized documentation, and clear function definitions. For instance, if newer scanning protocols or compliance standards emerge, one can put it on the current model without sweat for the perfect absorption.

CHAPTER 4

TOOLS AND TECHNOLOGIES

4.1 FRONT-END TECHNOLOGY

Kali Linux, Nano Editor, Python are the main frontend system tools that used for implementation of the CyberGuard Pro project. Combined with each other, these factors provide the environment to execute the backend code, interact with the users, and denote and operate the graphical user interface of the system.

4.1.1 Python

CyberGuard Pro project basing on which works on CyberGuard is created with the help of programming language, Python. This makes it popular as it is easy, comprehensive for automation and preferably suitable for systems programming. Pyton controls whole procedure of the logic connected to the vulnerability tests, reporting and scans in CyberGuard Pro. It allows the system to scan servers, navigate web pages, converse with other tools, and perform other tasks that are essential to evaluate security of networks or Web sites.

- Python manages network scanning, vulnerability analysis, and sensitive data exploration.

- Python is also used for logging and reporting, which allows users to view the results of each vulnerability check or scan. The results are recorded and printed in an easily legible style.
- Python can execute custom scripts or other tools as needed to expand its capability, such as examining DNS setups.

4.1.2 Nano Editor (Text Editor)

Nano is a Linux text editor that lets you make changes to files straight from the command line. Because of its ease of use and portability, developers and system administrators frequently use it when they need to quickly edit code, build scripts, or make changes to configuration files.

You can utilize Nano in your CyberGuard Pro project to:

- Modify any project-related configuration files or your Python scripts.
- Modify your system's behavior (e.g., by adding new features or altering the settings).
- Test the system and make changes quickly from the terminal without a graphical user interface.

4.1.3 Kali Linux

Kali Linux is a specialized operating system (OS) built on the Linux platform that is intended for penetration testers and security ex-

perts. It includes a set of tools designed especially for system testing, assessment, and security. CyberGuard Pro employs it due to its numerous built-in tools for network testing, vulnerability detection, and exploitation.

Kali Linux is crucial for your CyberGuard Pro project for the following main reasons:

- Kali Linux comes with a number of built-in tools for network security scanning, web application testing, and penetration testing.The tool has the ability to identify the vulnerabilities and take that advantage, which are consistent with the overall project aims.
- Without affecting adversely to your system of website, Kali Linux exhibits a secure environment for your website
- Kali Linux is a command-line operating system, with the terminal with the ability to use it for wide range of activities, for example, executing payloads. Therefore, CyberGuard Pro is perfect tool for carrying out commands and finding out vulnerabilities via scripting.

4.2 BACK-END TECHNOLOGIES

Backend technologies and tools play a vital role in the CyberGuard Pro project. Below are the key tools and their purposes:

4.2.1 Subdomain Enumeration - Sublist3r, Amass

Subdomain mapping is the first step in reconnaissance process where the researcher discovers the new subdomains related to a target domain use the Sublist3r and Amass. Several subdomain structures are out there, some of which if vulnerable or misconfigured are very vulnerable. The discovery of these subdomains brings out attack prospects unnoticed in domain scans, traditional domain scans can miss.

4.2.2 OSINT via Shodan - Shodan

Shodan is a search-engine designed to search for devices connected to the Web, like servers, routers, webcams, and other IT equipment. It works by scanning devices that are directly connected to the internet and specifically runs a powerful OSINT that commonly finds potential security risks such as unshielded database, outdated services, and/or insecure IoT gadgets.

4.2.3 Reverse IP Lookup - YouGetSignal, IPinfo.io

Some search tools it includes are YouGetSignal and IPinfo.io since the latter will provide all domains associated with a particular IP address. Exploiting this leads to broadening of the attack canvas

since the webmaster of the targeted site may also host other websites or applications within the same server, and they might have similar vulnerabilities or arrangements.

4.2.4 Port Scan - Nmap

One of the most crucial techniques of assessing open ports and the services supporting a target computer is the Port scan. Nmap stands out for this purpose and is important for penetration testing since can quickly identify which is the state of the ports and the services that are running. Port scanning assists in identifying these open ports such as the SSH,HTTP or FTP which can be assaulted.

4.2.5 Banner Grabbing - Netcat, Telnet

Banner grabbing involves establishing a connection with a service, running on the host on an open port in order to obtain a banner; usually containing information concerning the software and the version running within the target computer. Application like Netcat or Telnet are usually employed for this kind of approach. The collected banners information indicates that the old versions or vulnerabilities of services such as web servers, mail servers, and databases are more likely to be revealed.

4.2.6 Nmap Full Port Scan - Nmap

Some of the options that Nmap supports are very basic for port scanning whereas other are much more advanced to help do a full-port scan. It gives an amplification of all the vulnerable services and applications with the use of 65,535 TCP/UDP ports on the target host. This scan is essential because it allows identifying what is potentially vulnerable in a given system since the earlier mentioned types of vulnerabilities are often masked.

4.2.7 Web Vulnerability Scanning - Nikto

Nikto is an instruments that is used for performing web server and applications vulnerability scans. Some of the problem areas include; SQL injection, Cross-Site Scripting (XSS), outdated software, unsafe methods, and weak configurations. Nikto helps to discover important vulnerabilities on web servers and can do this before criminals use it for their purposes.

4.2.8 SNMP Enumeration - Snmpwalk, OneSixtyOne

A lot of devices connected to a network are managed through SNMP (Simple Network Management Protocol /. Software available such as Snmpwalk and OneSixtyOne help in the enumeration process of

SNMP data to give information about the network connected devices such as servers, routers, and printers. SNMP enumeration reveals the system's users, passwords, and other network configuration details, so it is an attacker's favorite point of entry.

4.2.9 SQL Injection - SQLmap, Havij

A long-time favorite for attackers, SQL Injection, or SQLi, enables the former to insert SQL commands into input fields of an application and the backend database runs them. Automated Metasploit Framework such as SQLmap and Havij can efficiently discover the presence of SQL injection flaws and also exploits in an improved way resulting to remote code execution, leakage of data and also complete control of whole database.

4.2.10 File Inclusion - Burp Suite, OWASP ZAP

File inclusion vulnerabilities are typically ones in which an application allows an attacker to read files from the server directory and possibly display the contents on the Web site. The aforementioned tools, such as Burp Suite and OWASP ZAP, identify such vulnerabilities with the help of URL parameters manipulation . File inclusion vulnerability, if exploited can lead to different levels of erecting system privileges, running programs as well as accessing internal data.

4.2.11 Command Injection - Commix

Command injection vulnerabilities are vulnerabilities whereby an attacker can input and execute commands on the server host of the web application. There are tools known as Commix (Command Injection Exploiter), which will automate the entire process of discovering and settling such weaknesses. When a hacker performs command injection, he then can launch more attacks, acquire important information about the organization, or even bring full control over the server.

CHAPTER 5

IMPLEMENTATION

5.1 RECONNAISSANCE

The reconnaissance phase of CyberGuard Pro gathered critical information about the target, which is vital for comprehending its infrastructure and pinpointing possible vulnerabilities. The tool conducted a search for subdomains (e.g., mail.parisupdate.com), which may reveal admin panels, testing environments, or neglected systems. These areas typically have lower security and expand the attack surface. The attempt to fetch WHOIS data was unsuccessful. Typically, this data provides insights into domain ownership and contact information, which can be leveraged for phishing or to identify associated domains. The tool successfully retrieved the A Record, disclosing the server's IP address (213.186.33.2). This information enables attackers to circumvent defenses such as WAFs or CDNs and directly probe the server for open ports or active services. The server operates on Apache with PHP 7.4. These headers indicate backend technologies that may possess known vulnerabilities. If PHP 7.4 is not updated, it could be susceptible to exploits such as remote code execution. Additional information regarding caching and

compression suggests possible misconfigurations. The SSL certificate was issued by Let's Encrypt. Improperly configured certificates or weak protocols can leave the server vulnerable to attacks like Man-in-the-Middle (MITM). In conclusion, this phase equips attackers with insights into the target's systems, highlights weaknesses such as outdated software or exposed services, and facilitates the planning of further exploitation.

```
def reconnaissance(target):
    print(INFO + "Starting Reconnaissance...")

    try:
        findings = []

        # 1. Subdomain Enumeration
        print(INFO + "Enumerating Subdomains...")
        subdomains = ['www', 'mail', 'ftp', 'test', 'dev', 'api', 'shop', 'blog', 'staging', 'support']
        for sub in subdomains:
            subdomain = f"{sub}.{target}"
            try:
                socket.gethostbyname(subdomain)
                findings.append(subdomain)
            except socket.gaierror:
                pass

        # 2. WHOIS Information
        print(INFO + "Fetching WHOIS Information...")
        try:
            import whois
            whois_data = whois.whois(target)
            findings.append(f"WHOIS: {whois_data}")
        except ImportError:
            findings.append("WHOIS: Install 'whois' library for more details.")
        except Exception:
            findings.append("WHOIS: Failed to fetch details.")

        # 3. DNS Records
        print(INFO + "Fetching DNS Records...")
```


Figure 5.1: Code of Reconnaissance

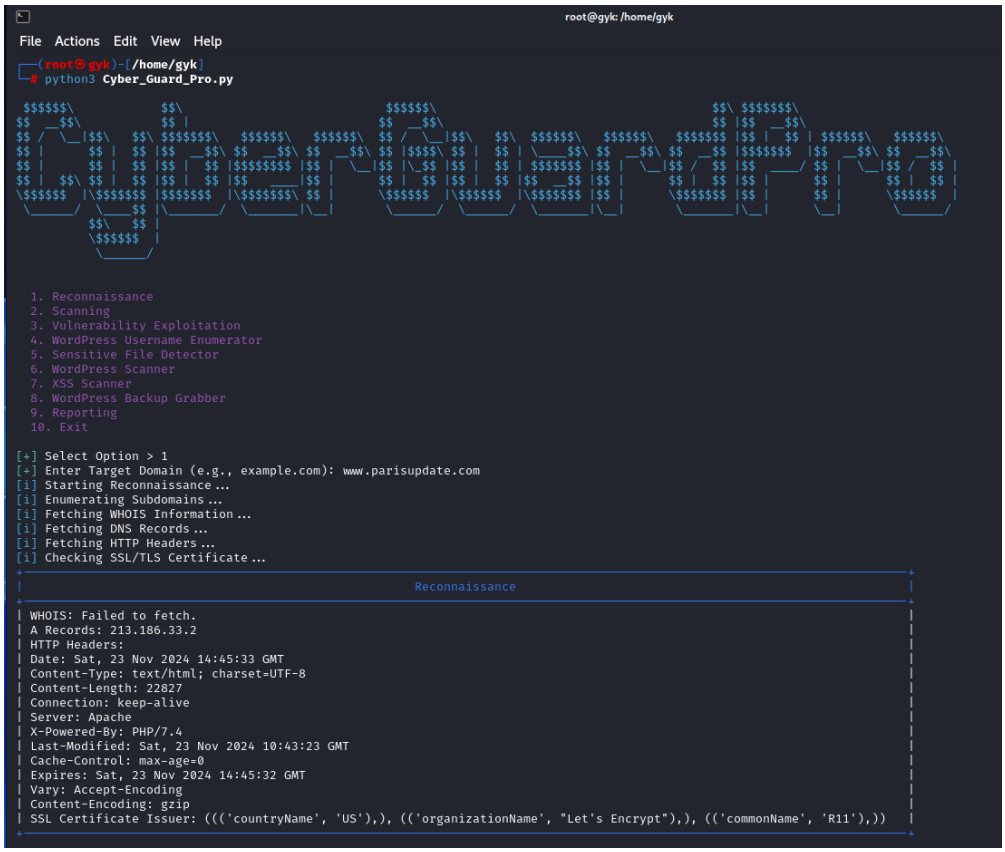


Figure 5.2: Output of Reconnaissance

5.2 SCANNING

The Scanning module of CyberGuard Pro evaluates open ports and the associated services. The results are interpreted as follows: Open Ports: 80, 443 - Port 80: This port facilitates HTTP traffic, indicating that the target server is hosting a website accessible through the standard HTTP protocol. - Port 443: This port is designated for HTTPS traffic, signifying that the server enables secure, encrypted communication.

HTTP/S on Ports 80 and 443: 200 - OK The status code 200 indicates that both HTTP and HTTPS services are functioning properly and responding as expected. This confirmation allows for subsequent tests, such as vulnerability assessments or specific web application feature scans, to be conducted. The absence of FTP service is noted, which is beneficial from a security standpoint, as FTP is often viewed as a less secure protocol due to its lack of encryption.

```python
def scanning(target):
    print(INFO + "Starting Scanning...")

    try:
        findings = []

        # 1. Basic Port Scan
        print(INFO + "Running Basic Port Scan...")
        open_ports = []
        for port in range(1, 1025):  # Test common ports
            with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
                s.settimeout(0.5)
                if s.connect_ex((target, port)) == 0:
                    open_ports.append(port)

        findings.append(f"Open Ports: {', '.join(map(str, open_ports))}")

        # 2. Banner Grabbing
        print(INFO + "Grabbing Banners from Open Ports...")
        for port in open_ports:
            try:
                with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
                    s.settimeout(1)
                    s.connect((target, port))
                    s.sendall(b"Hello\r\n")
                    banner = s.recv(1024).decode('utf-8').strip()
                    findings.append(f"Port {port}: {banner}")
            except:
                findings.append(f"Port {port}: No banner.")
```


Figure 5.3: Code of Scanning

```
root@gyk: /home/gyk
File  Actions  Edit  View  Help

┌──(root㉿gyk)-[/home/gyk]
└─# python3 Cyber_Guard_Pro.py

  1. Reconnaissance
  2. Scanning
  3. Vulnerability Exploitation
  4. WordPress Username Enumerator
  5. Sensitive File Detector
  6. WordPress Scanner
  7. XSS Scanner
  8. WordPress Backup Grabber
  9. Reporting
  10. Exit

[+] Select Option > 2
[+] Enter Target Domain or IP: parisupdate.com
+-------------------------------+
|        Scanning Results       |
+-------------------------------+
| Open Ports: 80, 443           |
| HTTP/S on Port 80: 200 - OK   |
| HTTP/S on Port 443: 200 - OK  |
| FTP Not Detected.             |
+-------------------------------+
[+] Findings for Scanning saved to report.
```

Figure 5.4: Output of Scanning

5.3 VULNERABILITY EXPLOITATION

Currently, the Vulnerability Exploitation module has detected several severe vulnerability types in the target site, which threatens the server's safety. The identified Command Injection vulnerabilities, more specifically, show that an attacker can run any command on the server by exploiting a vulnerable parameter "cmd". This vulnerability lets the attackers to execute command like "ls", "whoami" and "uname -a" that may provide information about configuration of the system and allows the attacker to get authorized access to the server. It is such vulnerabilities that let a person interact with the server OS thus getting full control Such vulnerabilities also include directory traversal which have been noticed to help the attackers modify the path to files and directories which are usually not accessible to everyone. This could lead to means that certain documents, such as the configuration files, passwords or system settings could be accessed individually.

```python
def scanning(target):
    print(INFO + "Starting Scanning...")

    try:
        findings = []

        # 1. Basic Port Scan
        print(INFO + "Running Basic Port Scan...")
        open_ports = []
        for port in range(1, 1025):  # Test common ports
            with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
                s.settimeout(0.5)
                if s.connect_ex((target, port)) == 0:
                    open_ports.append(port)

        findings.append(f"Open Ports: {', '.join(map(str, open_ports))}")

        # 2. Banner Grabbing
        print(INFO + "Grabbing Banners from Open Ports...")
        for port in open_ports:
            try:
                with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
                    s.settimeout(1)
                    s.connect((target, port))
                    s.sendall(b"Hello\r\n")
                    banner = s.recv(1024).decode('utf-8').strip()
                    findings.append(f"Port {port}: {banner}")
            except:
                findings.append(f"Port {port}: No banner.")
```


Figure 5.5: Code of Vulnerability

```
root@gyk: /home/gyk
File  Actions  Edit  View  Help

┌──(root㉿gyk)-[/home/gyk]
└─# python3 Cyber_Guard_Pro.py

  1. Reconnaissance
  2. Scanning
  3. Vulnerability Exploitation
  4. WordPress Username Enumerator
  5. Sensitive File Detector
  6. WordPress Scanner
  7. XSS Scanner
  8. WordPress Backup Grabber
  9. Reporting
  10. Exit

[+] Select Option > 3
[+] Enter Target Domain or IP: www.parisupdate.com
[i] Starting Vulnerability Exploitation...
+-------------------------------------------------------------------+
|                  Vulnerability Exploitation Results               |
+-------------------------------------------------------------------+
| Command Injection Detected: http://www.parisupdate.com/?cmd=; ls  |
| Command Injection Detected: http://www.parisupdate.com/?cmd=&& whoami |
| Command Injection Detected: http://www.parisupdate.com/?cmd=| uname -a |
| Directory Traversal Detected: http://www.parisupdate.com/../../../ |
| Directory Traversal Detected: http://www.parisupdate.com/../../../../../ |
+-------------------------------------------------------------------+
```

Figure 5.6: Output of Vulnerability

5.4 SENSITIVE FILE DETECTOR

The Sensitive File Detector module has detected the existence of such files on the target server which confirm a lot of security breaches. Of these is the wp-config.php file which is used in operation of WordPresss site. It hold key information such as database logins, encryption keys, and others such configuration data. If utilized it means that an attacker could potentially take full control over the entire database or all the website files – thus making I a high-value target for attackers also the tool highlighted that the .htaccess file which contains web server settings has restricted access to it. As much as it has been recommended to put restrictions such that only the admin has the access to this file in order to avoid anyone with ability to tamper with it, then any small mishap or inadvertent disclosure, can prove disastrous. For example, an attacker might use the file to display vital server information or change important configuration settings, which would poses serious threat to the security of web server.

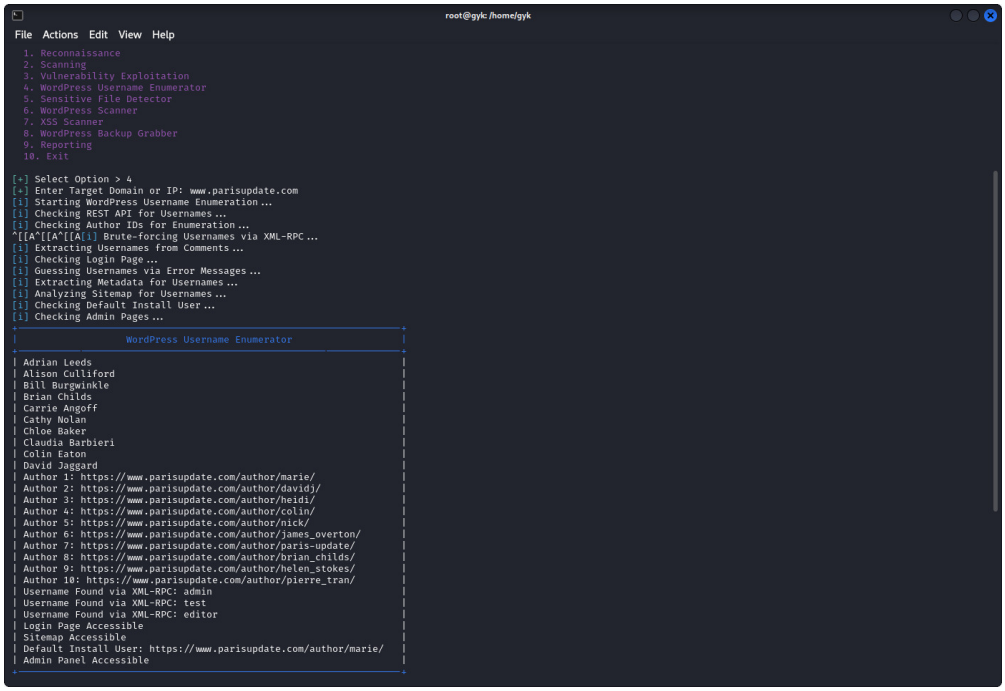


Figure 5.7: Output of Sensitive File Detector

5.5 WORDPRESS SCANNER

WordPress Scanner module has shown 5 critical level vulnerabilities that is lethal to the point that you cannot ignore it in the indicated site address. Making certain of this, the research established that the site is actively running on WordPress 6.7.1. This version should be compared with other known vulnerability lists to find which of the plugins or themes are outdated, and have an exploitable code somewhere;Many threats can be found in the enabled directory listing in the wp-content/uploads directory. The configuration makes it easy for the attackers to have a view of all the files within this directory which they may include configuration files, or more dangerously, scripts which may be executed on the server, putting the whole site at risk.Likewise, the debug mode on the site currently poses danger of passing on info including: server configuration, error logs and file paths among others.

If such details are disclosed to the attackers, other weaknesses and misconfigurations may be leveraged additionally.The last important issue lies in the disclosed REST API that poses as a great threat. Without authentications or restrictive rates mechanisms, attackers could easily penetrate secured accounts and gain full access to the user data or totally mess up mechanisms served by the API opening

new doors to possible leaks.

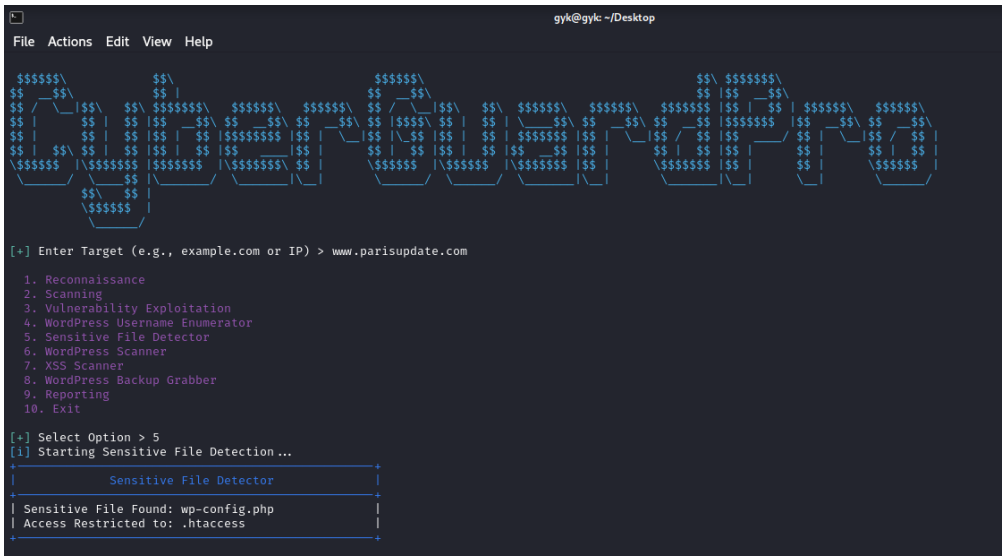


Figure 5.8: Output of Wordpress Scanner

5.6 XSS SCANNER

The XSS Scanner module found a major problem on the target website concerning an open redirect problem that has XSS interconnection. This vulnerability arises from the fact that the URL (http:The third URL (javascript: alert(1)) allows the next parameter to accept unvalidated user input. This means that the attackers can create the URLs of exactly what a string of JavaScript code to load and this code is executed when one clicks the link. Therefore, any user who, for instance, clicks on the link, interacts with the Web page without realizing it, will execute the scripts enabled by attackers to perform actions on the user's behalf compromising his or her data. This vulnerability can be used in many destructive forms For example: Of all the attacks, one of the most frequent ones seen is when the attackers target user information. It can be constructed so that the user will be enticed to click a link, which will cause the engineered JavaScript to obtain session cookies or other authentication tokens, personal information, or anything an attacker would consider valuable. This information is then used to deceive the user and go on to initiate an unauthorized session and stealing the user's information or credit card details etc. An example of this type of vulnerability is in phishing exercises where scammers may take advantage of the of-

ten missed or insecure, weak passwords. Phishing links can redirect people to forged login screens which look like the genuine pages, and therefore users will input their data in the wrong Web site. But once the attacker gains these credentials, then all the abilities belong to the user.

Figure 5.9: Output of XSS Scanner

5.7 WORDPRESS BACKUP

The WordPress Backup Grabber module identified multiple backup files on the target website, including backup.zip, db backup.sql, and wordpress backup.tar.gz. These files are likely to contain essential data such as the website's source code, database credentials, user information, and configuration settings. If an attacker were to access these files, they could replicate the website on their own system, examine its architecture, and look for vulnerabilities without raising any alarms on the live site.

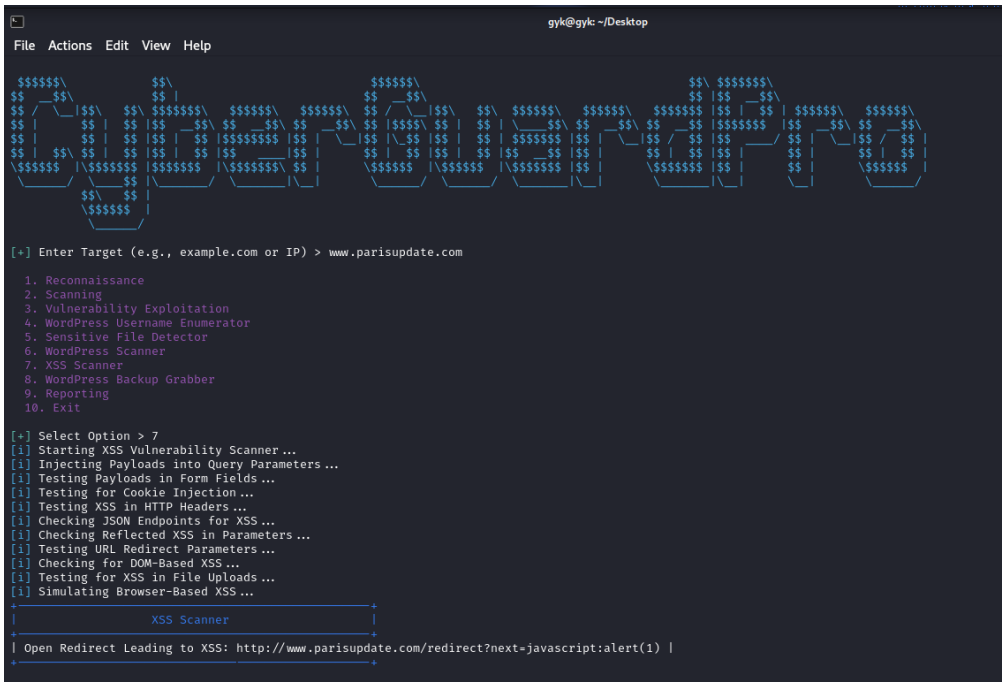


Figure 5.10: Output of WordPress Backup

5.8 REPORTING MODULE

The report named under the filename as "pentestreport2024-11-2321-58-21.txt,", has engendered a complete report regarding the functioning and testing of the products of the tool from all previous testings. It serves as an essential resource for understanding the security challenges present on the target website and can guide administrators in determining necessary remediation measures.

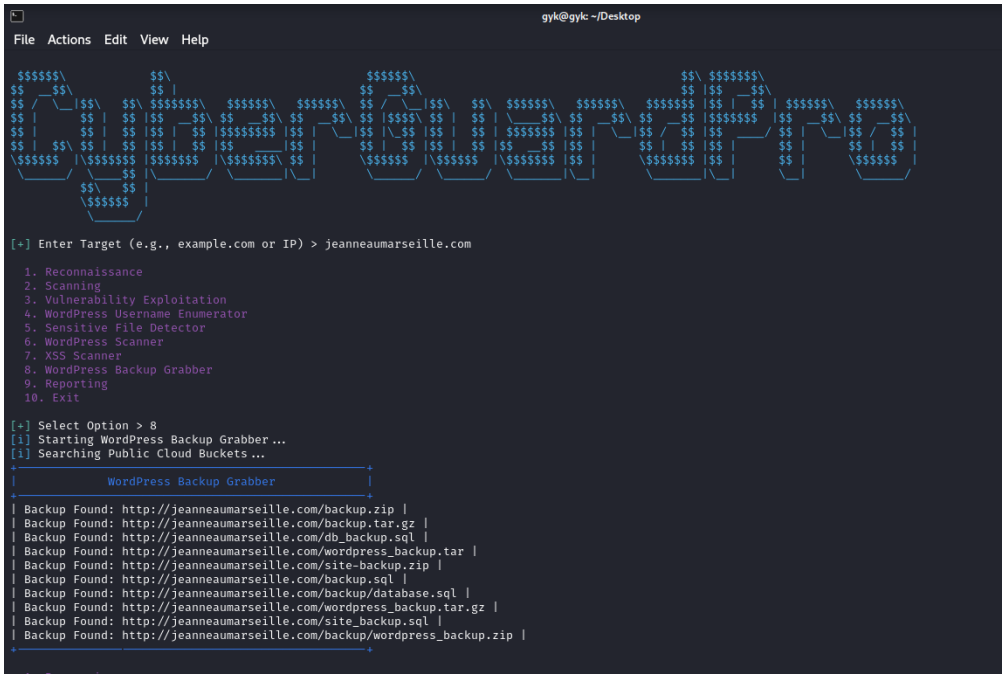


Figure 5.11: Output of Reporting module

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 CONCLUSION

CyberGuard Pro is the set of modules for penetration analysis of various aspects of network security. Such are reconnaissance, scanning, vulnerability exploitation, and detailed reporting, always striving to check one vulnerability critical. Its features useful in automating various processes include subdomain enumeration, port scanning as well as vulnerability testing, which poses minimal dependency on a human interface. Of course, this frees up security experts and encourages them to move from just symptomatically identifying vulnerabilities to actually devising appropriate measures for handling them. As a modular solution, CyberGuard Pro works with multiple targets, ranging from conventional web environment shared hosting targets and WordPress targets to specific customer applications, so it can be used to assess a variety of structures and technologies.

6.2 FUTURE WORK

In the upcoming development phase, we plan to implement a graphical user interface (GUI) for CyberGuard Pro, enhancing its user-

friendliness and visual appeal. This will feature interactive dashboards showcasing real-time scanning results, charts, and logs. Users will have the ability to navigate through various modules effortlessly, access summaries quickly, and engage with the tool without depending exclusively on command-line commands.

• **Multi-Threaded and Parallel Scanning**: The tool will develop the use of multi-threading to enhance its operation since it will perform several operations concurrently. For instance, subdomain enumeration, Port scanning, DNS records will now be performed in parallel; this will dramatically reduce the amount of time needed to perform an exhaustive scan. This capability will indeed prove greatly helpful in extensive assessments or when there are many underlying layers to an organization's structures. .

• **Integration with External APIs**: To make data more qualitative, additional external services like Shodan, Censys, and VirusTotal will be integrated. Such APIs will also provide the following target-specific data in real-time: past vulnerabilities, IP reputation, and exposure to threats around the world. Automating these integration will not only save time for CyberGuard Pro but will also give a greater view for reconnaissance attempts. .

• **Advanced Exploitation Modules** Features of the Cyber-

Guard Pro will include tools for detecting and taking advantage of complex risk factors including buffer overrun, privilege escalation, and Zero-Day exploitation. These improvements will go far beyond increasing the tool's capabilities, allowing it to model more complex attacks and add more value for penetration testers and the security teams. .

•**Real-Time Collaboration** A multiuser functionality will also be added in order to support the co-authoring of penetration tests in real-time. This feature will enable people in a team to convey and exchange information, results, and work-in-progress; thus, this is perfectly appropriate for security processes which are usually team-oriented. .

REFERENCES

[1] F. Vaskovich, *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning.* Nmap Project, 2009.

[2] OWASP, *Nikto Web Scanner Project Documentation*, 2023.

[3] D. Miessler, *The Shodan Guide: A Complete Overview of the Internet's Search Engine for Connected Devices.* Independent Publishing, 2018.

[4] OWASP Foundation, *OWASP ZAP: Comprehensive Guide to Zed Attack Proxy*, 2023.

[5] BinaryEdge, *BinaryEdge: Internet Exposure and Asset Monitoring Platform*, 2023.

[6] PortSwigger, *Burp Suite Professional Documentation*, 2023.

[7] D. M. Dagon, "Shodan and its role in internet-wide scanning for vulnerabilities," *Cybersecurity Insights*, 2019.

[8] OWASP, *Nikto Web Scanner: Automated Security Auditing Tool*, 2023.

[9] Censys, *Censys: Internet-Wide Scanning and Security Data*, 2022.

[10] D. Lodge, *Nikto Web Scanner: An Open-Source Web Server Scanner*, 2020.

[11] Acunetix, *Acunetix: Automated Web Application Security Testing*, 2022.

[12] Tenable, *Nessus Vulnerability Scanner: Network and Web Vulnerability Management*, 2020.

[13] C. Ionescu, *Wapiti: A Web Application Vulnerability Scanner*, 2021.

[14] J. Kettle, *The Burp Suite Cookbook: Web Application Security Testing*. Packt Publishing, 2020.

[15] T. Rashid, *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press, 2018.

[16] S. P., *Practical Web Application Security: A Hands-On Approach*. O'Reilly Media, 2021.

[17] SANS Institute, *Web Application Security Testing with Burp Suite*, 2022.

[18] E. Sparling, *The Art of Web Application Penetration Testing*. Cybersecurity Press, 2021.