SQL INJECTION AND VULNERABILITY DETECTOR

PAIWAND ABDULLA HAMAD

UNIVERSITI TEKNOLOGI MALAYSIA

UNIVERSITI TEKNOLOGI MALAYSIA

DECLARATION OF THESIS / UNDERGRADUATE PROJECT REPORT AND COPYRIGHT

Author's full name : Paiwand Abdulla Hamad

Date of Birth : 01/01/2001

Title : SQL INJECTION AND VULNERABILITY DETECTOR

Academic Session :

I declare that this thesis is classified as:

□ **CONFIDENTIAL** (Contains confidential information under the Official Secret Act 1972)*

□ **RESTRICTED** (Contains restricted information as specified by the organization where research was done)*

☑ **OPEN ACCESS** I agree that my thesis to be published as online open access (full text)

1. I acknowledged that Universiti Teknologi Malaysia reserves the right as follows:
2. The thesis is the property of Universiti Teknologi Malaysia
3. The Library of Universiti Teknologi Malaysia has the right to make copies for the purpose of research only.
4. The Library has the right to make copies of the thesis for academic exchange.

Certified by:

SIGNATURE OF STUDENT	**SIGNATURE OF SUPERVISOR**
QU182SCSR005	DR. Mustafa Ibrahim Khaleel
MATRIX NUMBER	**NAME OF SUPERVISOR**
Date: 13 FEB 2022	Date: 13 FEB 2022

NOTES : If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization with period and reasons for confidentiality or restriction

May 2023

QIU Library

Sir,

CLASSIFICATION OF THESIS AS OPEN
SQL INJECTION AND VULNERABILITY DETECTOR
PAIWAND ABDULLA HAMAD

Please be informed that the above-mentioned thesis entitled “SQL INJECTION AND VULNERABILITY DETECTOR” be classified as OPEN ACCESS.

Thank you.

Sincerely yours.

MUSTAFA IBRAHIM KHALEEL, As Sulaymaniyah Iraq, +964 772 852 6539

“I hereby declare that we have read this thesis and in my
opinion this thesis is suffcient in term of scope and quality for the
award of the degree of BSc of Computer Science (Network & Security)”

Signature	:	______________________________
Name of Supervisor	:	Dr. Mustafa Ibrahim Khaleel
Date	:	14 FEBRUARY 2022

SQL INJECTION AND VULNERABILITY DETECTOR

PAIWAND ABDULLA HAMAD

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Bachelor of Computer Science (Network & Security)

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

FEB 2022

DECLARATION

I declare that this thesis entitled *"SQL INJECTION AND VULNERABILITY DETECTOR"* is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature	:	....
Name	:	PAIWAND ABDULLA HAMAD
Date	:	13 FEBRUARY 2022

DEDICATION

This theory is committed to my dad, who trained me that the most ideal sort of information to have been what is realized for the good of its own. It is additionally devoted to my mom, who instructed me that even the biggest errand can be achieved assuming it is done slowly and carefully.

ACKNOWLEDGEMENT

In setting up this theory, I was in touch with many individuals, specialists, academicians, and experts. They have contributed towards my arrangement and contemplations. Specifically, I wish to communicate my true appreciation to my principal postulation boss, Professor Dr. Mustafa Ibrahim Khaleel, for consolation, direction, pundits and companionship. I'm likewise extremely grateful to my co-boss Professor Dr. Bander and Associate Professor for their direction, advices and inspiration. Without their proceeded with help and interest, this proposal would not have been equivalent to introduced here.

My kindred understudy ought to likewise be perceived for their help. My genuine appreciation additionally reaches out to every one of my partners and other people who have given help at different events. Their perspectives and tips are helpful for sure. Sadly, it is unimaginable to expect to list every one of them in this restricted space. I'm appreciative to all my relative.

ABSTRACT

The sneak peaks scanners and surprisingly robotized scanners have harms on the site yet this venture with the ground-breaking thoughts will diminish the disservices of infiltration testing other than that any associations and surprisingly ordinary individuals can examine their sites by own self in more straightforward manner free of charge and no expected to pay to be gotten, safeguard a consciousness of the weaknesses in a climate and answer rapidly to direct potential risks is through normal weakness finders. WF is a cycle to recognize and quantify the security weaknesses in an association's current circumstance. A total weakness evaluation program conveys associations with the data, mindfulness, and hazard preparing is fundamental to comprehend dangers to their current circumstance and react appropriately. This undertaking will generally concentration to weaknesses and discloses how hazardous they're to the local area and associations, likewise relying upon my experience I will explains and gives the major and well known weaknesses like SQL infusion then, at that point, manages the cost of the answers for fix them by consolidating and placing them into an advanced site subsequently I will share a portion of my python codes that individuals could utilize them to check their site and observed the escape clauses naturally utilizing my code other than that I've wanted to practice an alternate segment for infiltration testing for certain great offers that individuals and associations could pay and claim me to Pen-testing their site and give the answers for shutting the weakness and to quit being assaulted and takes advantage of by others, and to safeguard a site or a server it's important to know where you purchase a space or affiliates and webhosting in addition to the content you're utilizing to code your site in the event that it's a moment one, it's so essential to have a survey to sneak peaks exploits and provisos in that content to try not to rehash a similar misstep in any case assuming you're coding it from zero to end still you ought to have an audit and not letting a similar weakness to occur and allow an opportunity to programmers to take advantage of it.

ABSTRAK

Pengimbas puncak menyelinap dan pengimbas robot yang mengejutkan mempunyai kemudaratan di tapak namun usaha ini dengan pemikiran terobosan ini akan mengurangkan keburukan ujian penyusupan selain daripada mana-mana persatuan dan individu biasa yang mengejutkan boleh memeriksa tapak mereka sendiri dengan cara yang lebih mudah tanpa tanpa caj dan tidak dijangka membayar untuk diperolehi, melindungi kesedaran tentang kelemahan dalam iklim dan menjawab dengan cepat untuk mengarahkan potensi risiko adalah melalui pencari kelemahan biasa. WF ialah kitaran untuk mengenali dan mengukur kelemahan keselamatan dalam keadaan semasa persatuan. Program penilaian kelemahan menyeluruh menyampaikan perkaitan dengan data, kesedaran, dan penyediaan bahaya adalah asas untuk memahami bahaya kepada keadaan semasa mereka dan bertindak balas dengan sewajarnya. Usaha ini secara amnya akan menumpukan kepada kelemahan dan mendedahkan betapa berbahayanya ia kepada kawasan dan persatuan tempatan, begitu juga bergantung kepada pengalaman saya, saya akan menerangkan dan memberikan kelemahan utama dan terkenal seperti penyerapan SQL kemudian, pada ketika itu, menguruskan kos jawapan untuk membetulkannya dengan menyatukan dan meletakkannya ke dalam tapak lanjutan kemudiannya saya akan berkongsi sebahagian daripada kod python saya yang individu boleh menggunakannya untuk menyemak tapak mereka dan memerhatikan klausa melarikan diri secara semula jadi menggunakan kod saya selain daripada yang saya mahu amalkan segmen alternatif untuk ujian penyusupan untuk tawaran hebat tertentu yang boleh dibayar oleh individu dan persatuan dan menuntut saya untuk menguji Pen tapak mereka dan memberi jawapan untuk menutup kelemahan dan berhenti diserang dan mengambil kesempatan daripada orang lain, dan untuk melindungi tapak atau pelayan adalah penting untuk mengetahui tempat anda membeli ruang atau ahli gabungan dan pengehosan web sebagai tambahan kepada kandungan yang anda gunakan untuk mengekod tapak anda sekiranya ia adalah seketika, adalah sangat penting untuk mengadakan tinjauan untuk mengeksploitasi kemuncak dan syarat dalam kandungan itu untuk cuba untuk tidak mengulangi kesilapan yang sama dalam apa jua keadaan dengan mengandaikan anda mengekodnya dari sifar hingga akhir masih anda harus menjalani audit dan tidak membiarkan kelemahan yang sama berlaku dan memberi peluang kepada pengaturcara untuk mengambil kesempatan daripadanya.

Table of Contents

TITLE: PAGE

DECLARATION II

DEDICATION III

ACKNOWLEDGEMENT IV

ABSTRACT V

ABSTRAK VI

LIST OF TABLES IX

LIST OF FIGURES X

CHAPTER 1 INTRODUCTION 1

1.1. OVERVIEW 1

1.2. PROBLEM BACKGROUND 2

1.3. PROJECT AIM 3

1.4. OBJECTIVES 3

1.5. SCOPES 4

1.6. IMPORTANCE OF THE PROJECT 4

1.7. ORGANIZATION OF THE REPORT 5

CHAPTER 2 LITERATURE REVIEW 7

2.1. INTRODUCTION 7

2.2. INTER-ORGANIZATION CASE STUDY 7

2.2.1. VULNERABILITY ASSESSMENT 8

2.3. CURRENT SYSTEM ANALYSIS 9

2.3.1. FEATURES 10

2.3.2. BENEFITS OF VULNERABILITY SCANNING TOOLS (+VE): 11

2.3.3. DISADVANTAGES OF THOSE VULNERABILITY SCANNING TOOLS: 11

2.4. COMPARE BETWEEN EXISTING SYSTEMS 12

2.4.1. REFERENCES AND WEAKNESS WITH ACHIEVEMENTS 14

2.5. LITERATURE REVIEW ON TECHNOLOGY USED 16

2.5.1. NETWORK-BASED SCANNERS 16

2.5.2. HOST CONSTRUCTED SCANNERS 16

2.5.3. WIRELESS SCANNERS 17

2.5.4. APPLICATION SCANNERS 17

2.5.5. DATABASE SCANNERS 17

2.6. CHAPTER SUMMARY 17

CHAPTER 3 SYSTEM DEVELOPMENT **18**

3.1. INTRODUCTION 18

3.1.1. METHODOLOGY EXPLANATION 18

3.2. METHODOLOGY CHOICE AND JUSTIFICATION 19

3.2.1. WHY RAD METHODOLOGY PREFERRED 19

3.3. PHASES WITHIN THE CHOSEN METHODOLOGY 20

3.3.1. DESCRIBES ACTIVITIES AND PROCESS IN EACH PHASE 20
3.3.2. DESIGN MODELING 21
3.3.3. DESIGN TOOLS 22
3.3.4. GANTT CHART FOR PSM 1 AND PSM 2 23

3.4. TECHNOLOGY & TOOLS USED 23

3.5. SYSTEM REQUIREMENT ANALYSIS 24

3.6. CHAPTER SUMMARY 25

CHAPTER 4 REQUIREMENTS ANALYSIS AND DESIGN **26**

4.1. INTRODUCTION 26

4.2. REQUIREMENTS ANALYSIS 27

4.2.1. OOP (UML) 27
4.2.2. SOFTWARE DEVELOPMENT LIFE CYCLE 28

4.3. DESIGN 28

4.3.1. OOP CLASS DIAGRAM 29
4.3.2. USE CASE DIAGRAM 30

4.4. INTERFACE DESIGN 31

4.5. CHAPTER SUMMARY 33

CHAPTER 5 IMPLEMENTATION, TESTING, RESULTS, AND DISCUSSION **35**

5.1. INTRODUCTION 35

5.2. CODING OF SYSTEM MAIN FUNCTIONS 35

5.3. INTERFACES OF SYSTEM MAIN FUNCTIONS 39

5.4. TESTING THE SYSTEM 42

5.4.1. WHITE BOX TESTING 42
5.4.2. USER ACCEPTANCE TESTING 44

5.5. CHAPTER SUMMARY 45

CHAPTER 6 CONCLUSION **46**

6.1. INTRODUCTION 46

6.1.1. OBJECTIVES 46

6.2. ACHIEVEMENTS 47

6.3. SUGGESTED PLANS FOR PROJECT 49

REFERENCES **50**

LIST OF TABLES

TABLE NO. **TITLE** **PAGE**

TABLE 2-1 REFERENCES AND WEAKNESS WITH ACHIEVEMENTS..................................... 14

TABLE 3-1 REQUIREMENTS FOR ACCESSING THE WEBSITE... 24

TABLE 3-2 REQUIREMENTS TO RUN AND ACCESS THE CODES FOR SCANNING............. 24

TABLE 5-1 WHITE BOX TESTING... 44

TABLE 5-2 USER ACCEPTANCE TABLE 45

LIST OF FIGURES

FIGURE NO. **TITLE** **PAGE**

FIGURE 1-1 GANTT CHART 6
FIGURE 3-1 RAD EXPLANATION (NIX-UNITED 2021). 19
FIGURE 3-2 DRAW.IO LOGO, JOE RANNE (PORTAGE BAY 2021). 22
FIGURE 3-3 LUCID CHART LOGO (LUCID CHART 2019). 22
FIGURE 3-4 GANTT CHART (PSM 1 AND PSM2) 23
FIGURE 4-1 UML DIAGRAM 27
FIGURE 4-2 SDLC 28
FIGURE 4-3 CLASS DIAGRAM 29
FIGURE 4-4 USE CASE DIAGRAM 30
FIGURE 4-5 CONTACT PAGE 31
FIGURE 4-6 HACKER MOST-RATED PAGE 31
FIGURE 4-7 ONLINE CHAT & OFFERING PAGE 32
FIGURE 4-8 LAST THREE VULNERABILITY & SOLUTIONS PAGE 32
FIGURE 4-9 DOWNLOAD PYTHON CODES PAGE 33
FIGURE 4-10 MAIN AND VULNERABILITY PAGE 33
FIGURE 5-1 CSS FILES 36
FIGURE 5-2 PHP FILES 1 36
FIGURE 5-3 PHP FILES 2 37
FIGURE 5-4 PHP FILES 3 37
FIGURE 5-5 PHP FILES 4 37
FIGURE 5-6 PHP FILES 5 37
FIGURE 5-7 PHP FILES 6 38
FIGURE 5-8 JS FILES 38
FIGURE 5-9 MYSQL FILES 39
FIGURE 5-10 GUEST ACCESS 39
FIGURE 5-11 GUEST ACCESS 40
FIGURE 5-12 LOGIN & SIGNUP 40
FIGURE 5-13 PEN TESTER ACCESS AFTER LOG INNING. 41
FIGURE 5-14 CUSTOMER ACCESS AFTER LOG INNING. 42
FIGURE 5-15 WHITE BOX TESTING 43
FIGURE 5-16 AVERAGE GOOD RATE FEEDBACK %93 44
FIGURE 6-1 OBJECTIVES 47
FIGURE 6-2 ACHIEVEMENTS 48

Chapter 1

Introduction

1.1. Overview

A vulnerability assessment is a methodical evaluation of safety weaknesses in a data system. It measures whether the system or website is vulnerable to any recognized vulnerabilities, assigns the degree of cruelty to these vulnerabilities, and comments on remedies or reasons when needed. The penetration exam is a full review of a datum flaws in the system's security It determines if the system is vulnerable to any known vulnerabilities, assigns severity ratings to those vulnerabilities, and, if and when necessary, provides treatment or mitigation. The goal of this phase is to make a complete list of vulnerabilities in a submission. Security experts use automated tools to scan applications, servers, and other programs, or perform physical tests and evaluations on them to determine their safety and health. Vulnerability files, vendor vulnerability announcements, strength Specialists also employ management systems and threat intelligence feeds to discover security issues.

Threats that can be prevented via vulnerability assessment include the following:

1. SQL injection, cross-site scripting, and other cipher injection attacks
2. Privileges are being increased as a result of defective verification techniques.
3. Insecure evasions — software having insecure settings, such as a guessable administrator password.

An automatic vulnerability scanner will classify input parameters and will try to inject detailed patterns to recognize vulnerabilities on the mark website. This is complete over the scanner's vulnerability forms. Usually, these checks are advanced to be non-invasive, but there might be the circumstance that some checks need to be aggressive due to the nature of confident vulnerabilities.

1.2. Problem background

The previews scanners and even automated scanners have damages on the website but this project with the new ideas will decrease the disadvantages of penetration testing besides that any organizations and even normal people can scan their websites by own self in easier way for free and no needed to pay to be secured, preserve an awareness of the vulnerabilities in an environment and answer quickly to moderate potential dangers is through regular vulnerability detectors (VD). VD is a process to identify and measure the security vulnerabilities in an organization's environment. A complete vulnerability assessment program delivers organizations with the information, awareness, and risk training is essential to understand threats to their environment and respond accordingly.

This project will mostly focus to vulnerabilities and explains how dangerous they're to the community and organizations, also depending on my experience I will clarifies and provides the major and famous vulnerabilities like SQL injection then affords the solutions to fix them by combining and putting them into a modern website afterward I'm going to share some of my python codes that people could use them to scan their website and found the loopholes automatically using my code besides that I've planned to specialize a different section for penetration testing with some good offers that people and organizations could pay and own me to Pen-testing their website and give the solutions for closing the vulnerability and to stop being attacked and exploits by others, and to protect a website or a server it's necessary to know where you buy a domain or resellers and webhosting plus the script you're using to code your website if it's an instant one then it's so important to have a review to previews exploits and loopholes in that script to avoid repeating the same mistake otherwise if you're coding it from zero to end still you should have a review and not letting the same vulnerability to happen and give a chance to hackers to exploit it. To get a better solution it'll be better to prevent using WordPress and the other instant websites because there is still a chance to have a vulnerability in the future especially by having those much plugins to install, So, to have a better solution there will be not the same mistakes that have done before for example there will be no use of instant open-source sites like WordPress, Joomla, OpenCart, Presta-shop etc. because there is a lot of exploits every year and the patch takes so longer time than having your own script also fixing it by itself. And in this project, the secured webhosting websites and resellers will be recommended to have less chance of affection by bulk exploits because there are many hosting sites that may let the hacker to jump from the affected site to another site that does not have any bugs.

1.3. Project aim

The main goal of this project is to give a clarification about common mentioned vulnerabilities which covers the most common ones like SQL Injection, XSS, RCE and the newest one Loc4j then make a good vision to understand them in full detail as a good source that people can depend on it also to have a web-scanner which can detect them then having an automated scanner so there will be several python programs to detect the vulnerabilities also an online scanner which no needed to use any applications.

1.4. Objectives

The objectives of execution a Vulnerability detector is to make an overview of the security threats to a network or a web application and then use that overview as a guide to resolution those threats which is:

- Performing fixed assessments and regularly resolving all security risks offers a baseline security for the network.
- Managers and users can feel self-assured that potential attackers will be powerless to exploit vulnerabilities on their system.
- A vulnerability appraisal is a rigorous examination of an information system's security flaws.

- It determines if the system is vulnerable to any known flaws, assigns severity ratings to those flaws, and offers remediation or change as appropriate.

1.5. Scopes

The scope of the Vulnerability detectors and automated scanners is to detect the errors and bugs by services and comprises all IT resources that are linked to the organization's system and websites. This project will follow counted scopes:

i. Vulnerability Assessment delivers a vision into an organization's existing state of security, and the efficiency of its countermeasures.
ii. Depending most important the aim is going to be SQL injection techniques such as (In-band SQLi (Classic), Inferential SQLi (Blind), and Out-of-band SQLi) are available, and the other ones as well like log4j vulnerability which is so common now by logging into the library you pretend that you're the admin and can access many data.
iii. also, there will be also a clarification about previews exploits for example RCE. From the combination of previews related projects there will be the most powerful automated scanner to the mentioned vulnerabilities with higher efficiency, brave, correction, avoidance.
iv. And using this project it decreases probability of damages while scanning.

1.6. Importance of the Project

The vulnerability evaluation method helps to reduce the likelihood that an attacker will be able to break a business's IT systems — elastic a better knowledge of resources, their weaknesses, and the overall risk to an organization.

- The main reason to decide making a project like this is to help people understand the vulnerabilities and how they work.
- This system will protect organization's include small business and even famous ones to being attacked from Blackhat hackers.
- User can understand everything that causes vulnerability from his/her website for free
- Users can also have free scanners from online website and software too that could check his/her websites by themself for free.
- Responsibility of less damages while checking will be focused on to protect the system while examination.

1.7. Organization of the Report

In this chapter the most important points have declared to explains what is the project about and how it can be beneficial to the community also in chapter one the difference was clarified between related projects then by finishing the Gantt chart the project could be easier because from now on the project will be done through following the process within the Gantt chart. With chapter 2 and chapter 3 the project goes deeper to answer all the questions and points before starting into practical part from chapter 4 and above.

Project Gantt Chart:

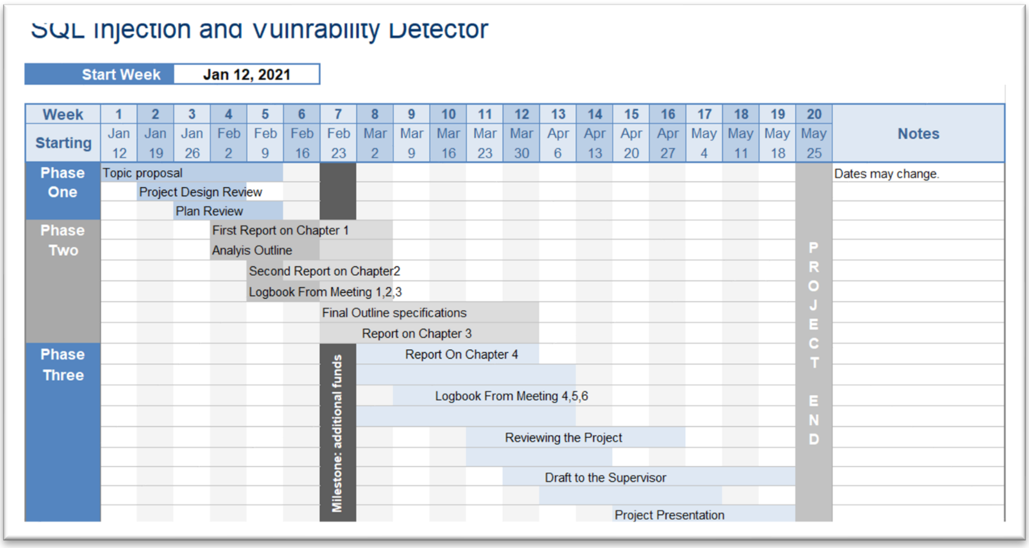


Figure 1-1 Gantt Chart

Chapter 2

Literature Review

2.1. Introduction

Aim of this prose review is to propose a set of principles for defining and measuring vulnerability in current systems for the purposes of targeting and program design. The suggested standards are based on a review of known and unpublished vulnerability assessment methodologies.

The review starts with a description of how vulnerabilities is described and measured in specified ways, sociology, and archeology. Next, depending on a database search of studies on social vulnerability at the community level, an assessment of the research methods used in the published literature is performed. The evaluation comes to the conclusion with a recommended description of system vulnerability and a model for future assessments.

2.2. Inter-organization Case Study

The capabilities of the majority of vulnerability management software are comparable, including asset identification and detection, vulnerability scanning, and vulnerability explanations. Through linkages to information about patches, scripts, and other remediation methods, report generation from templates or custom settings, a central terminal (usually Web-based), and support for a variety of systems are all possible. In contrast, market-leading vulnerability management technologies conduct many of these activities more extensively and exhaustively, including certain capabilities for automated remediation, and give dashboards and data that enable security managers manage systems more effectively, from this research (W.J. and Chen, Y.C., 2010, August).

2.2.1. Vulnerability Assessment

When assessing Vulnerability management entails putting in place suppliers and their products, as well as determining if each device can: (User Requirements)

- Run automated scans and provide alerts.
- Scanners and agents should be controlled from a central location.
- In console displays and gossips, clearly distinguish vulnerability severity levels.
- Long-term path vulnerabilities, such as those considered low- or moderate-risk.
- Scan the network perimeter as well as the inside network — most Web-based scanners simply scan the perimeter.
- Create unique reports, such as those that are subject to auditing or compliance requirements.
- For deeper scanning, use authentication — administrator credentials — to acquire information such as security formations for systems and apps that would otherwise be inaccessible with a conventional scan.
- If desired, automatically modify security panels to reinforce them.

Signing up for a demo that runs in a circumstance is a relatively informal approach to put a vulnerability management software through its paces and compare it to others. All of the top-rated vendors provide product samples, which should aid in the evaluation process.

2.3. Current System Analysis

1. **Netsparker** is an extremely precise mechanized scanner that finds SQL Injection and Cross-Site Scripting weaknesses in web-based applications and web APIs. Netsparker approves found weaknesses in a special strategy to guarantee they are veritable and not misleading up-sides. As a result, when an output is done, you will not need to go through hours physically affirming the weaknesses that were recognized. It's accessible as a Windows programming as well as an internet-based assistance, from this paper (Junjin, M., 2009, April).
2. **Acunetix**: is an internet-based weakness scanner that recognizes and reports on north of 4500 web application weaknesses, including all SQL Injection and XSS varieties. The Acunetix crawler can review confounded, approved applications since it upholds HTML5, JavaScript, and single-page applications. Progressed Vulnerability Management capacities are prepared straightforwardly into the core of the scanner, focusing on gambles with in light of information in a solitary, combined view and incorporating the scanner's outcomes into different apparatuses and stages (Alwan, Z.S. what's more Younis, M.F., 2017).
3. **Intruder**: is a proactive weakness scanner that dissects you when new defects are found. It additionally includes north of 10,000 security checks from an earlier time, including WannaCry, Heartbleed, and SQL Injection (Shinde, P.S. also Ardhapurkar, S.B., 2016). Slack and Jira mixes ready advancement groups when new issues should be fixed, and AWS reconciliation permits you to synchronize your IP addresses for examining. The Intruder is well known among new businesses and little associations since it works on weakness the executives for little gatherings.
4. **SolarWinds**: With its Network Configuration Manager, it offers Network Vulnerability Detection. Its organization computerization abilities will permit it to rapidly redesign network gadgets' firmware. It offers capacities for network setup observing, the executives, and assurance. The apparatus will make network consistence more straightforward and more compelling. Network Configuration Manager conveys alarms when the setup changes. It

does a persistent review to figure out which setups are making the gadget be resistant (Petukhov, A. furthermore Kozlov, D., 2008). It will empower you to make setup reinforcements to help with the observing of arrangement changes. The program can offer data on the setup changes that have been made, as well as the login ID used to roll out such improvements. It will support a speedier recuperation in case of a catastrophe. The arrangement costs $3085 to carry out. It gives a 30-day free preliminary that incorporates full usefulness.

5. **AppTrana**: Indus Face WAS is an automated web application vulnerability scanner that identifies and reports vulnerabilities according to the OWASP top ten (Antunes, N. also Vieira, M., 2013). The company is headquartered in Bengaluru, with offices in Vadodara, Mumbai, Delhi, and San Francisco; its services are used by over 1100 customers in over 25 countries.

2.3.1. Features

- Scan single-page apps with a new era crawler.
- Additional Manual
- Pausing and Resuming In the same dashboard, do penetration testing and produce a report.
- A request for a proof of concept to demonstrate the existence of a reported vulnerability and eliminate false positives.
- Interfacing with the Indus Face WAF is optional for speedy virtual patching with no false positives.
- Crawl coverage may be automatically increased based on real-time data from WAF systems (in case WAF is subscribed and used)
- Assistance is available. To discuss remediation methods and points of contact, we are available 24 hours a day, seven days a week.
- No credit card necessary for a free trial that includes a full single scan.

2.3.2. Benefits of vulnerability scanning tools (+VE):

- **Quick results**
  The main benefit of using an automated scanning technology is that it produces results rapidly. That way, you'll always be able to see an image of your security.
- **Repeatable**
  It's simple to repeat an automated vulnerability scan. You may choose to conduct a scan daily, weekly, or monthly and receive notifications about changes and vulnerabilities found.
- **User-friendly**
  The majority of vulnerability detection products feature a simple user interface and are thus simple to use. As a result, system administrators and anyone who use them face a low barrier to entry. It should be noted, However, the tool's output provides a lot of specialized information. This suggests that a security professional will be needed to examine the results and take suitable action.
- **Continual monitoring**
  When a high number of deployments are done, a vulnerability scanning tool can also be employed for continuous monitoring. Furthermore, it gives system administrators with continuous visibility into the state of the infrastructure.

2.3.3. Disadvantages of those vulnerability scanning tools (-VE):

- A vulnerability scanning device will not find closely all vulnerabilities
  You cannot be certain that your systems are not vulnerable since vulnerability screening techniques also overlook problems. This is one of the most major drawbacks of scanning techniques, since hackers may still be able to exploit vulnerabilities. Two possible reasons exist:
  - The vulnerability is too sophisticated to be uncovered by an automated tool since the attack is not straightforward to automate.
  - The scanner is unaware of the vulnerability, for example because it was only recently discovered.

- Constant updates require

  Make sure the tool is updated on a regular basis to ensure that the most recent vulnerabilities are found.
- False positives

  If you have a vast IT infrastructure with several servers and services, it may be difficult to appreciate the implications of the scanning tool's results and vulnerabilities. As a consequence, there will be an abundance of false positives. Recognizing them is difficult if you are not a security expert, which makes data analysis tedious. In addition, if false positives are not removed, the tool will not learn and will continue to provide misleading findings.
- Implications of vulnerability unclear

  When a vulnerability is discovered, determining what it means for corporate operations can be tough. How will it affect diverse departments, people, and processes? An automated application will not notify you of this, and a system administrator is generally more concerned with the technical components of the vulnerability.

2.4.Compare between existing systems

Acunetix vs. Netsparker

Acunetix and Netsparker are Invictus web application security tools. Prior to 2018, Acunetix's vulnerability scanner and Netsparker's web application security solution was created and distributed by distinct cybersecurity organizations. After the 2018 merger, the items kept their original engines and technology under the Invictus brand. However, the teams behind both products now work together to share their expertise and develop leading-edge functionality. As a result, both products grow much faster together than they used to grow separately and both benefit from the knowledge and experience of twice as many experts as any other web application security scanner on the market (Kumar, P. and Pateriya, R.K., 2012).

Acunetix and Netsparker – similarities

- Vulnerability scanning engines from Acunetix and Netsparker are both cutting-edge. The Netsparker Enterprise employs the Netsparker web application security engine, which was created specifically for business purposes. Acunetix Premium is a vulnerability scanning solution designed specifically for small and medium-sized businesses.
- Both security solutions address a wide spectrum of web application security flaws, with no substantial variations in the area of key flaws addressed. Both are capable of identifying out-of-band vulnerabilities as well as web server configuration issues.
- Both vulnerability scanning packages have cutting-edge vulnerability management and assessment features. Both employ a range of external resources to assist you in integrating with your current environment, no matter how simple or complex it is. Both allow substantial automation and provide RESTful APIs with full functionality. Both can scan APIs and web services in addition to web apps.
- Several technologies that were previously only accessible in one tool are now available in both. The innovative AcuSensor IAST engine, for example, served as the foundation for the creation of the Netsparker Shark IAST engine. The Acunetix proof of exploit technology was inspired by the unique Netsparker Proof-based Scanning.

Acunetix and Netsparker – differences

- Acunetix Premium focuses on covering more bases because it was created for businesses that aren't yet enterprises. As a result, Acunetix provides various unique technologies and functions that would otherwise necessitate the acquisition of additional software. This includes support for antivirus software (Microsoft Defender and ClamAV), as well as an innovative open-source network scanner (OpenVAS). Acunetix Premium is available as a SaaS product as well as on-premises for Windows users.

- Acunetix has a significantly more forgiving learning curve. Acunetix's user interface is widely regarded as one of the easiest in the business, and Invicti is always working to improve it. This enables security teams, as well as IT administrators and other IT workers, to get the most out of the product without having to devote a significant amount of time and effort to its configuration and knowledge. In most circumstances, you can begin an Acunetix scan in under 5 minutes and receive quick actionable scan findings to repair your source code and avoid data breaches.
- Although Acunetix offers several integration features (Jira, Jenkins, and a few web application firewalls), its business solutions are not as comprehensive as Invicti's. Netsparker Corporate, on the other hand, is intended for business installations that generally include additional security solutions. As a consequence, it focuses less on speed and simplicity of use and more on adaptability to various environments. Netsparker offers a multitude of other out-of-the-box connectors. Its Proof-based Scanning method is intended to assist organizations in expanding by detecting which vulnerabilities are genuine and which may be false positives. The primary emphasis of Netsparker is on large-scale, targeted cleaning.

2.4.1. References AND Weakness with Achievements

Table 2-1 References AND Weakness with Achievements

References	Weakness	Achievements
Tsaur, W.J. and Chen, Y.C., 2010, August. Exploring the weaknesses of Rootkit detectors using a novel window concealed driver-based Rootkit. Second IEEE International Conference on Social Computing held in 2010 (pp. 842-848). IEEE.	By first showing the faults in its anomaly-detection system and then explaining how an attacker may exploit those holes using usual techniques, the existence of such attacks can be concealed from the detector's viewpoint. Stide was selected because of its Internet accessibility for other scholars. Its transparency not only permits independent verification and replication of the work presented here, but also builds upon and adds to a vast corpus of previously	Even though it offers the benefits of speed and freely accessible datasets, its accuracy and recall must be improved. Anomaly detection and vulnerable pattern learning both seek to improve detection by using syntactic and semantic information in the code. The legal programming pattern is discovered through detecting anomalies in mature software projects. Similarity or relationship between candidates and learned rules is used to identify vulnerabilities.

	published work using the stide detection method.	
Junjin, M., 2009, April. A method for detecting SQL injection vulnerabilities. Sixth International Conference on Information Technology: New Generations took place in 2009. (pp. 1411-1414). IEEE.	It is not always simple to interpret the results of a vulnerability scan. For instance, the application may mistakenly designate as a vulnerability anything that only seems suspicious. Consequently, identifying the true nature of your security posture will take far longer if you lack the capabilities to evaluate the data. Similarly, if you cannot eliminate false positives, the software will continue to provide inaccurate results.	Vulnerability scans are not perfect. As with antivirus software, they depend on a database of known vulnerabilities and are only as effective as the most current update. Performing scans using obsolete or substandard technology, on the other hand, raises the probability of overlooking vulnerabilities and creates a false sense of security. Even with the most modern technology, the scanner will almost certainly overlook certain problems. This might be owing to the vulnerability being newly discovered, or it could be because the vulnerability is too complex to be exploited – and hence detected – by an automated system.
Kumar, P. and Pateriya, R.K., 2012, July. A study of strategies for detecting and preventing SQL injection attacks. Third International Conference on Computing, Communication, and Networking Technologies (ICCCNT'12) took place in 2012. (pp. 1-5). IEEE.	Utilizing a predetermined database of all known vulnerabilities, vulnerability scanning simply utilizes software that searches for any security flaws in a network's security system. The scanner then puts the system through its paces by delivering remote security threats to assess whether or not it can survive severe security threats. At the conclusion of the vulnerability scanning, a report is generated, enabling network administrators to identify and rectify any security system flaws.	Scanners often do hundreds or thousands of tests per second, which is far faster than manual testing. Modern cloud-based architectures enable services to scale up or down their resources to scan small or large environments in similar time frames.
2017: Alwan, Z.S., and Younis, M.F. A overview on the detection and prevention of SQL injection attacks. International Journal of Computer Science and Mobile Computing, volume 6, number eight, pages 5 to 17.	It might be difficult to quantify the effect of a detected vulnerability on your company's operations. This is not something that an automated software would teach you, but a system administrator would be more concerned with the technical component of the vulnerability.	Scanning may be conducted routinely, on-demand, or in response to trigger events such as the publication of a new software project version or the installation of a new server. This enables the upkeep of a current view of the vulnerability landscape.
Shinde, P.S., and S.B. Ardhapurkar, February 2016. Analysis of cyber security through vulnerability assessment and penetration testing. The 2016 World	The contents of an IP packet are read by an IDS, but the network address may still be spoofed. When an attacker employs a false e-mail address, the threat	Numerous vulnerability scanning products provide custom tests to certify compliance with industry standards or an organization's own control baseline.

Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave) was devoted to examining these developments (pp. 1-5). IEEE.	becomes more difficult to detect and assess.	
Petukhov, A. and Kozlov, D., 2008. Using dynamic analysis and penetration testing to detect security flaws in online applications. 1–120 pages. Computing Systems Lab, Department of Computer Science, Moscow State University.	Due to the fact that NIDSs inspect protocols as they are gathered, they are susceptible to the same protocol-based attacks as network hosts. Incorrect data and difficulties with the protocol analyzer might cause an NIDS to crash.	Vulnerability scanning is substantially more cost-effective than manual testing due to the benefits of speed and automation.

2.5. Literature review on technology used

2.5.1. Network-based scanners

On wired or wireless networks, network-based vulnerability scanners identify potential network security assaults and susceptible devices. By identifying unfamiliar or unlawful devices and systems, network-based scanners may assist identify unknown network boundary points, such as illegitimate remote access servers or links to unprotected business partner networks.

2.5.2. Host constructed scanners

Using host-based vulnerability scanners, vulnerabilities in servers, workstations, and other network hosts are detected and identified. These scanners also allow access to the configuration settings and patch history of the examined systems. In addition, host-based vulnerability assessment tools may reveal the potential harm that insiders and outsiders might do to a system if they are given or denied access.

2.5.3. Wireless scanners

The purpose of wireless vulnerability scanners is to discover rogue access points and verify that a company's network is properly configured.

2.5.4. Application scanners

Using application vulnerability scanners, websites are examined for known software vulnerabilities and erroneous configurations in network or online applications.

2.5.5. Database scanners

Scanners for database vulnerabilities assess a database's weak points in order to protect it against malicious attacks.

2.6. Chapter Summary

In this chapter the focus is mostly on current similar systems and explaining the advantages and disadvantages of them also making comparison between the most used ones, besides there is clarification about which technology are used for vulnerability scanners with introduction, therefore. The project will continue and the next one will be chapter three. So, from now on the project will depends on the functionality of developing the system until reaching the practical one which is chapter four and five.

Chapter 3

System Development

3.1. Introduction

In this section the aim is going to be an overview about the methodology of this project and explaining each part of it step by step, so in the beginning there will be only an overview about the methodology type then a small part to express it although next step would be the phases and describing the activities on each process also giving UML diagram and other design modelling, After that, a quick summary of the technology and techniques utilized to construct the complete system from zero to hero will be presented. In addition, the system requirements that may be required to utilize the system from the devices will be outlined, followed by a chapter summary for this section and the others.

3.1.1. Methodology Explanation

A software development methodology is a set of methods or a technique for creating software. Again, this term is fairly broad, but it encompasses things such is the phases of design and development. It's not iterative methods of thinking about things like waterfalls. It takes the shape of clearly defined stages the majority of the time. Its objective is to outline how the life cycle of software should be executed. Additionally, it is a kind of communication that may be controlled. Then, you create a set of norms among a group of individuals that states, "This is how you're all going to communicate information in specific ways, whether it's via documentation, debate, or paper drawings."

3.2. Methodology Choice and Justification

The selected approach for this project is RAD (Rapid Application Development), but first, let's define RAD. Prototyping and iterative development with little (or no) preparation are key to the (RAD) methodology. In general, the RAD approach of software development emphasizes development and prototyping at the expense of planning. The RAD method, Unlike the waterfall paradigm, which emphasizes rigorous definition and preparation, agile development is built on continuously evolving requirements, with more and more lessons learned as the project progresses.

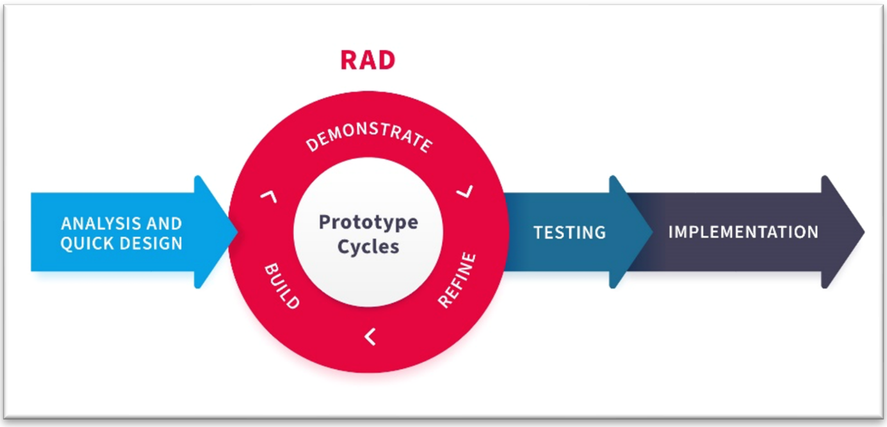


Figure 3-1 RAD Explanation (Nix-United 2021).

3.2.1. Why RAD Methodology Preferred

RAD Prototyping is emphasized as a viable alternative to design requirements. This shows that RAD outperforms non-GUI systems in cases when the user interface is more significant. The agile approach is used with the spiral model in the RAD paradigm.

The following are some of the points in the rapid application development methodology:

1. Information flow: across dissimilar business operations is detected over business modeling.
2. Data modeling: The information collected across the business model is used to define the firm's information objects.
3. Process modeling: In order to meet particular precise business objectives, information objects pronounced in data modeling are transformed to create the business information movement. There are clarifications of the processes for adding, deleting, and altering data items.
4. Application development: The real system has been built, and the coding has been completed with the help of automation tools. This produces the desired outcome from the general idea, methodology, and supporting data. This manufacturer is used as an example due to the fact that it is still in its infancy.
5. Challenging and revenue: The RAD approach decreases entire testing cycle period by testing samples individualistically through each cycle.

3.3. Phases within the chosen methodology

3.3.1. Describes activities and process in each phase

- Analysis And Quick Design

  So, it's the collection and analysis of data, the detection of defects, and the dismantling of a system into its component pieces.
- Prototype Cycle

  Prototype model is among the software development life cycle models that produces a prototype with the bare minimum of requirements. This prototype is then tested and altered in response to client feedback until a final prototype with the required functionality is produced.
- Testing

System testing refers to the examination of a whole software application. This kind of testing is known as black-box testing since it does not need knowledge of the code's underlying design and is conducted by the testing team.

- Implementation

  After system and user acceptance testing, the test system is deployed and made operational in the production environment at this step. Activities in this phase involve implementation activities such as end-user notification, training data entry or conversion, and system monitoring.

3.3.2. Design modeling

- Class Diagram

  The class diagram illustrates a static representation of a program. It illustrates the many types of items present in the system, as well as the interactions between them. A class is composed of its objects, but it may inherit from other classes as well. Class diagrams are used to describe, explain, and document several system components, as well as to generate executable software code.
- Use case Diagram

  A use case diagram is a visual depiction of a system and its users. It is often represented as a graphical depiction of the interactions between different system components. Use case diagrams describe the events that occur in a system and their flow, but do not specify how these events are implemented.
- UML Diagram

  The Unified Modeling Language (UML) is a visual representation language for large software system architecture, design, and implementation. It is difficult to maintain track of the linkages and hierarchies inside a software system when there are thousands of lines of code in an application during development. Using UML diagrams, the software system is separated into components and subcomponents.

3.3.3. Design tools

- **Draw .IO**

  Draw.io by Seibert Media is a proprietary application for creating diagrams and charts. You have the option of adopting the software's default layout or designing your own. You may create a one-of-a-kind diagram or chart using the tens of thousands of graphic components and many form options. Using the drag-and-drop tool, it is easy to create a visually appealing diagram or chart.

Figure 3-2 Draw.io Logo, Joe Ranne (Portage Bay 2021).

- **Lucid Chart**

  Lucidchart is a simple web-based diagramming tool that allows users to collaborate on flowcharts, Venn diagrams, mind maps, and mockups for websites and mobile apps in real time. Lucidchart is linked to Google Apps. Without leaving the editor, collaborators may post comments, upload photographs, import videos, and perform a range of other things.

Figure 3-3 Lucid Chart Logo (Lucid Chart 2019).

3.3.4. Gantt Chart for PSM 1 AND PSM 2

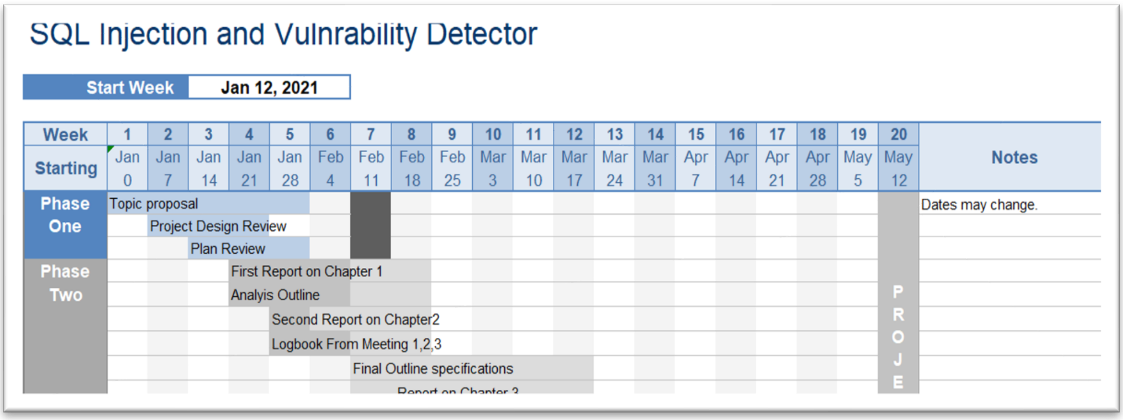


Figure 3-4 GANTT CHART (PSM 1 AND PSM2)

3.4. Describe briefly the technology or tools used to develop the system.

- **WordPress with PHP, HTML, CSS**

  For designing website and share the information about vulnerabilities although latest exploits and solutions for them besides the program codes that available to check and scan vulnerabilities with monthly updates, also user can request for a special request or hiring a job for vulnerability experts…

- **Python**

  Python will be used to code the programs to scan for vulnerabilities. The user can access the program by installing Python and then using it through command prompt or by double-clicking on the Python code. However, as stated previously, to download the code or have updates, the client must access the website.

- **Sublime Text**

  Sublime is a text editor that used for coding it’s so user-friendly and easy to use, so for coding the program and any modification sublime is recommended to use and everything from the code will be separated with different colors to find out things easier

3.5. System Requirement Analysis

The key objective of system constraint analysis is to tackle the hardware and software needs necessary to implement the system. Choosing appropriate hardware and software is essential to ensure the ultimate outcome meets user needs and specifications.

Table 3-1 Requirements for accessing the website

	Windows requirements	**Mac requirements**	**Linux requirements**
Operating system	Windows 7 or advanced	macOS Sierra 10.12 or later	64-bit Ubuntu 14.04+, Debian 8+, openSUSE 13.3+, or Fedora Linux 24+
Processor	Intel Pentium 4 or advanced	Intel	Intel Pentium 4 or later
Memory	1 GB minimum, 2 GB suggested		
Screen resolution	1280x1024 or greater		
Application window size	1024x680 or greater		
Internet connection	Compulsory		

Table 3-2 Requirements to run and access the codes for scanning

	Windows requirements	**Mac requirements**	**Linux requirements**
Operating system	Windows 8 or advanced	macOS Sierra 10.12 or advanced	64-bit Ubuntu 14.04+, Debian 8+, openSUSE 13.3+, or Fedora Linux 24+
Processor	Intel Pentium 4 or advanced	Intel	Intel Pentium 4 or later
Memory	2 GB minimum, 4 GB suggested		
Internet connection	Required		

3.6.Chapter Summary

By reaching this point, several goals and accomplishments have been accomplished, including selecting a methodology for the project and explaining each part of the methodology by providing a clear justification for each of them. Additionally, different types of diagrams that may be required for this project have been described, along with a number of design tools, and by the end of this chapter, all the used programs have been listed, along with an explanation of syslog.

Chapter 4

Requirements Analysis and Design

4.1. Introduction

In this chapter the aim is going to be an overview about the design and structures of this project and explaining each part of it step by step, so in the beginning there will be only an overview about the requirement analysis and the first thing that project starting with is the use cases and activity diagram then development life cycle will be shown, besides the design is another important step which is the class diagram of entire project although depending on the requirement is should be database design but for this project it's not necessary because it's not necessary for this project and it doesn't contains huge databases. From the end it will be also interface design which sometimes called as prototype, so it's going to be the front-end design without functionality but in the future the project can take benefit from it because the design will depend on it.

4.2. Requirements Analysis

4.2.1. OOP (UML)

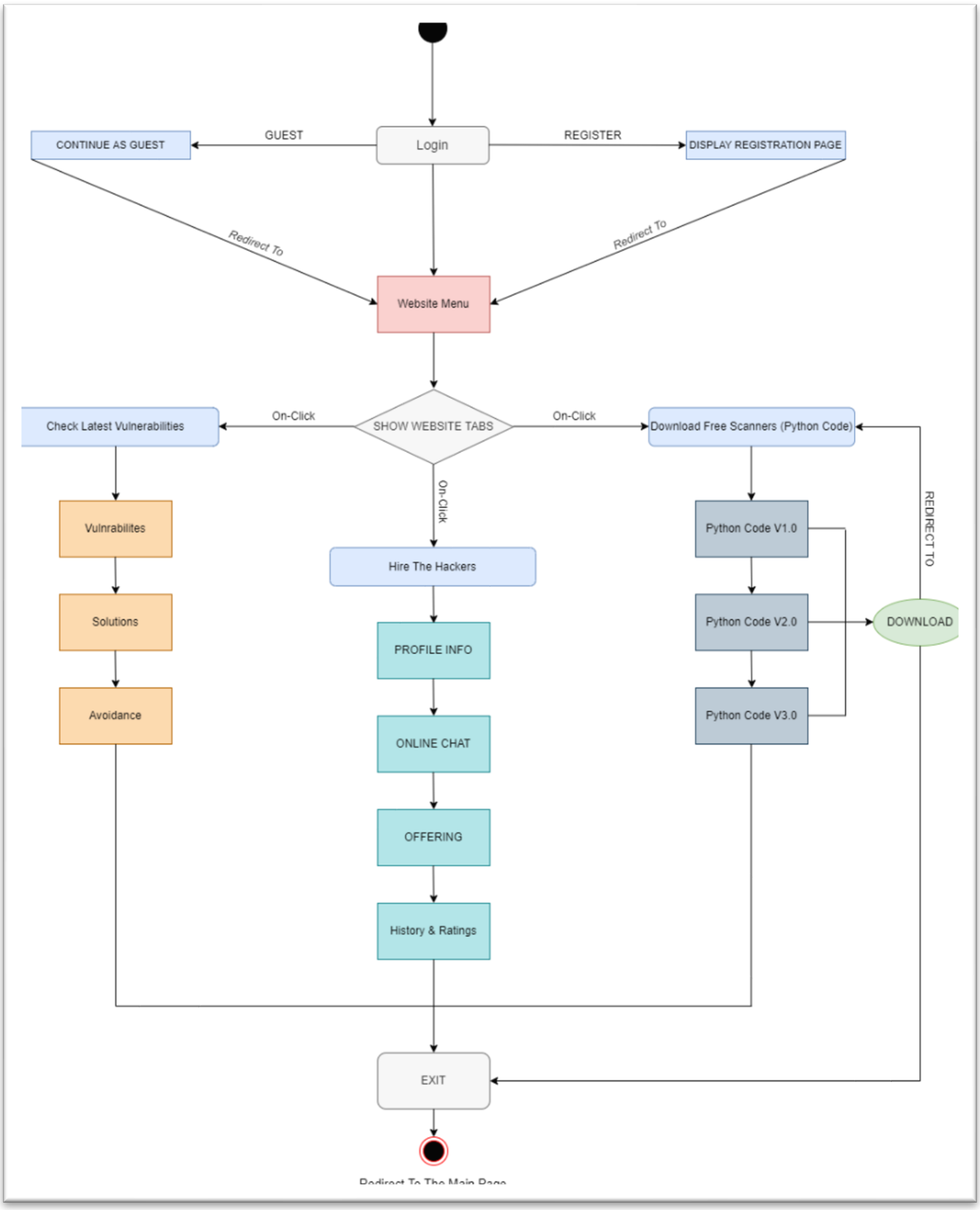


Figure 4-1 UML Diagram

4.2.2. Software Development Life Cycle

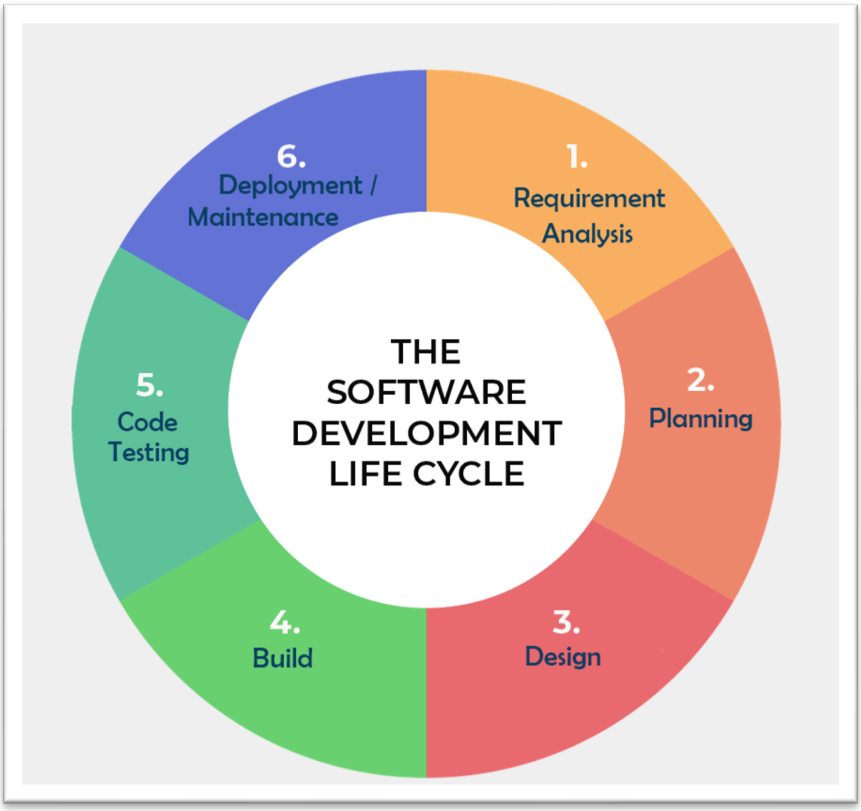


Figure 4-2 SDLC

4.3. Design

This section will focus on the UML class diagram and system architecture diagram. UML class diagram showcases how the data that belong to a different part of the system are connected and have relations to each other. However, the architecture diagram showcases how hardware and software are connected and works in real-time. Figure 4.11 shows the UML Diagram and 4.12 showcases the Architectural Design.

4.3.1. OOP Class Diagram

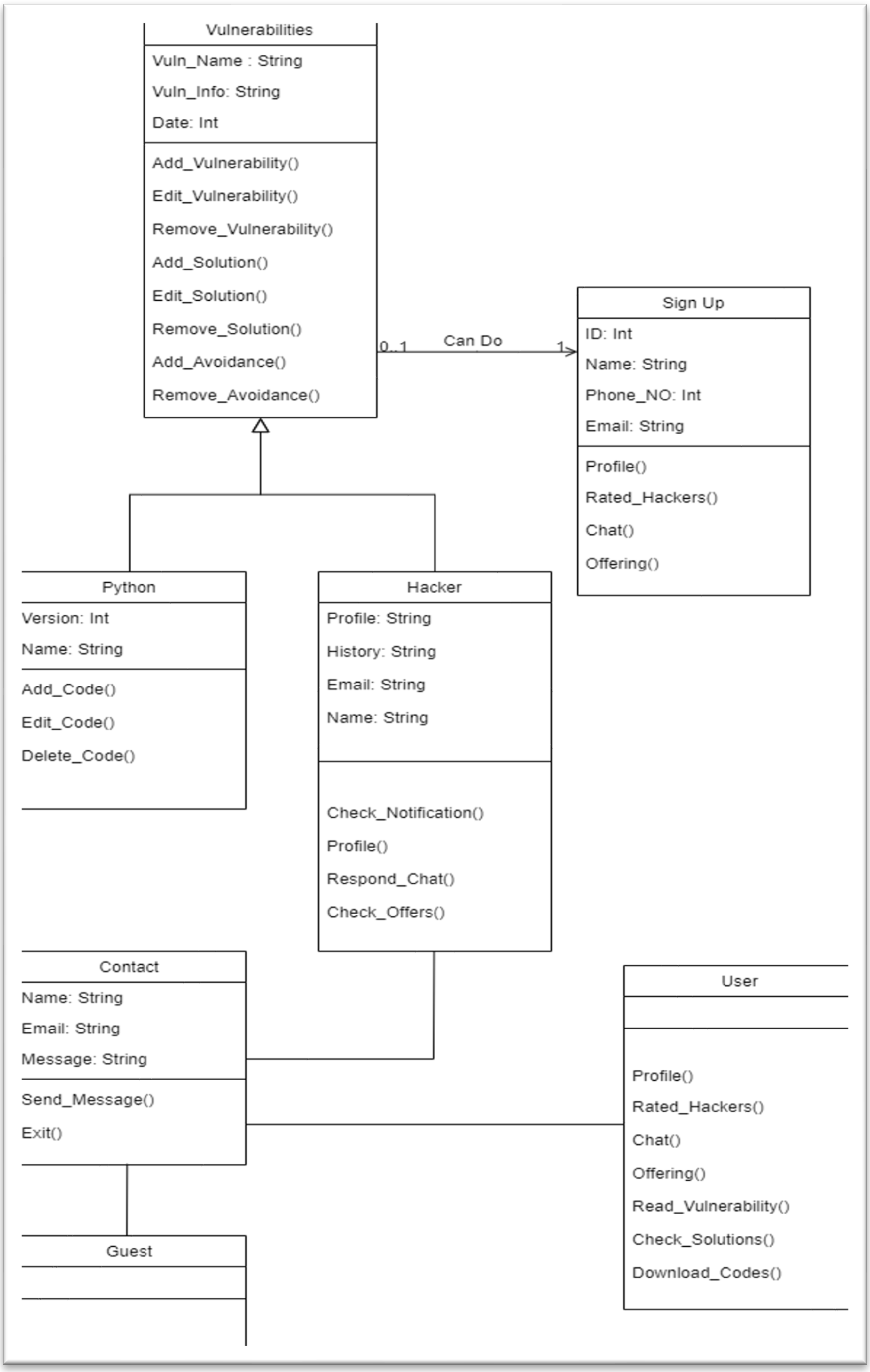


Figure 4-3 Class Diagram

4.3.2. Use Case Diagram

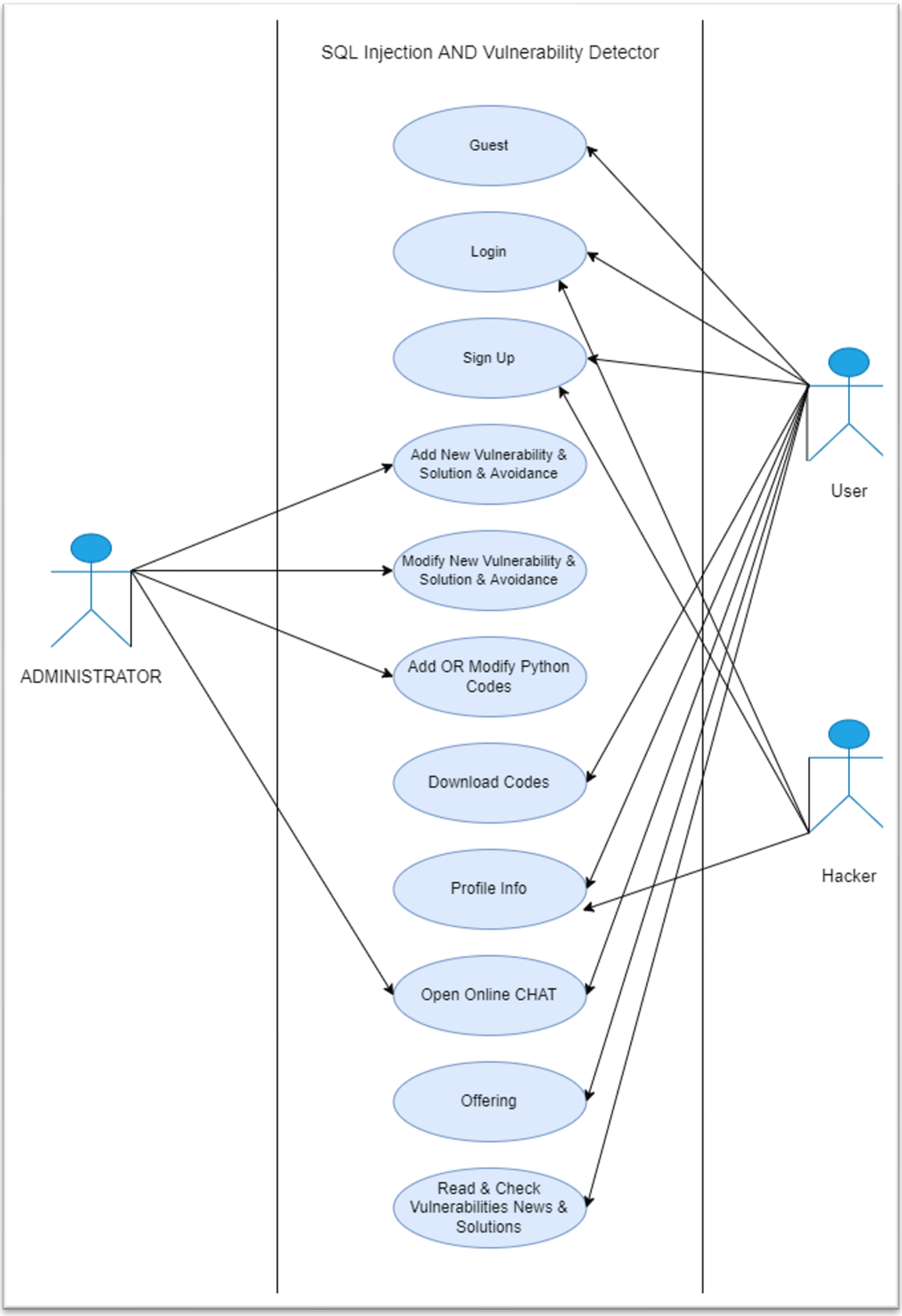
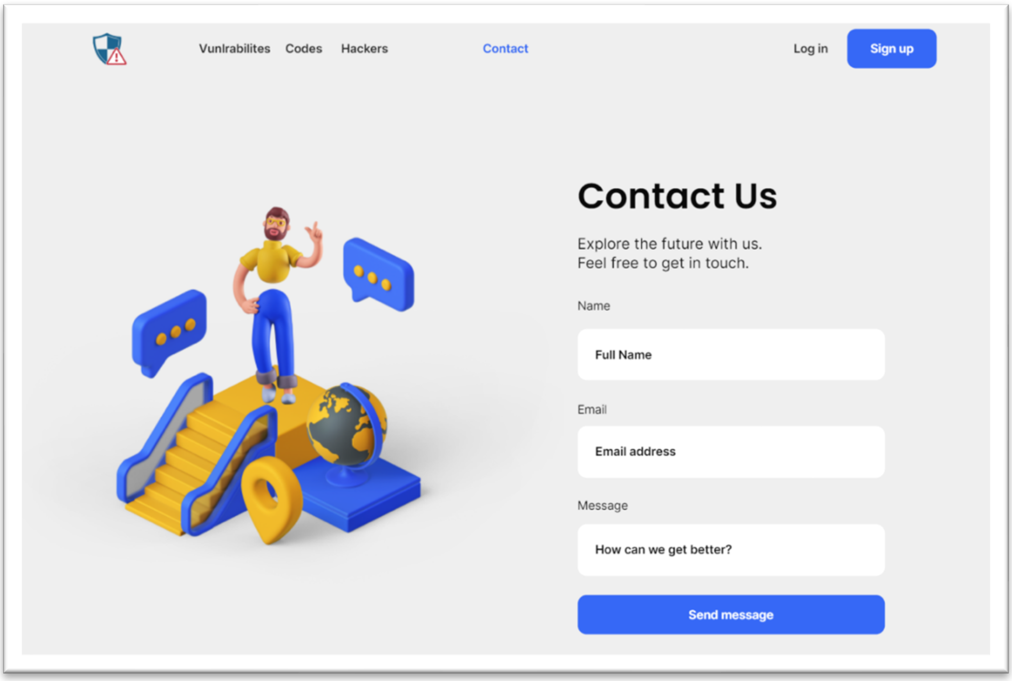

SQL Injection AND Vulnerability Detector
Guest
Login
Sign Up
Add New Vulnerability & Solution & Avoidance
Modify New Vulnerability & Solution & Avoidance
Add OR Modify Python Codes
Download Codes
Profile Info
Open Online CHAT
Offering
Read & Check Vulnerabilities News & Solutions
ADMINISTRATOR
User
Hacker

Figure 4-4 Use Case Diagram

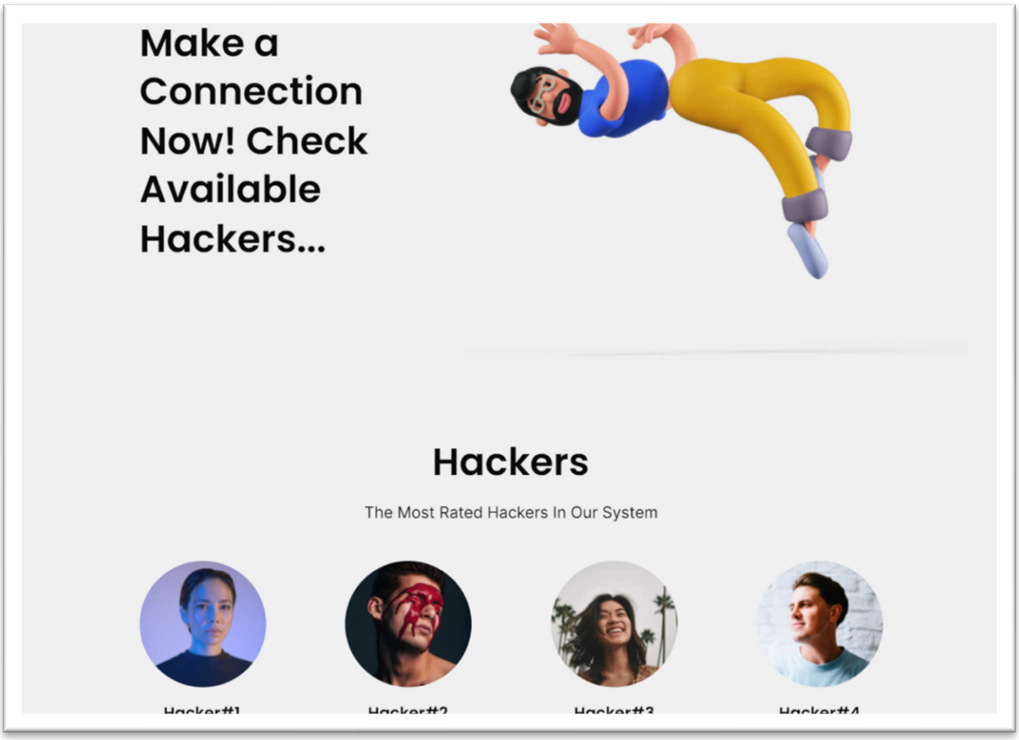
4.4. Interface Design



Contact Us

Explore the future with us.
Feel free to get in touch.

Figure 4-5 Contact Page

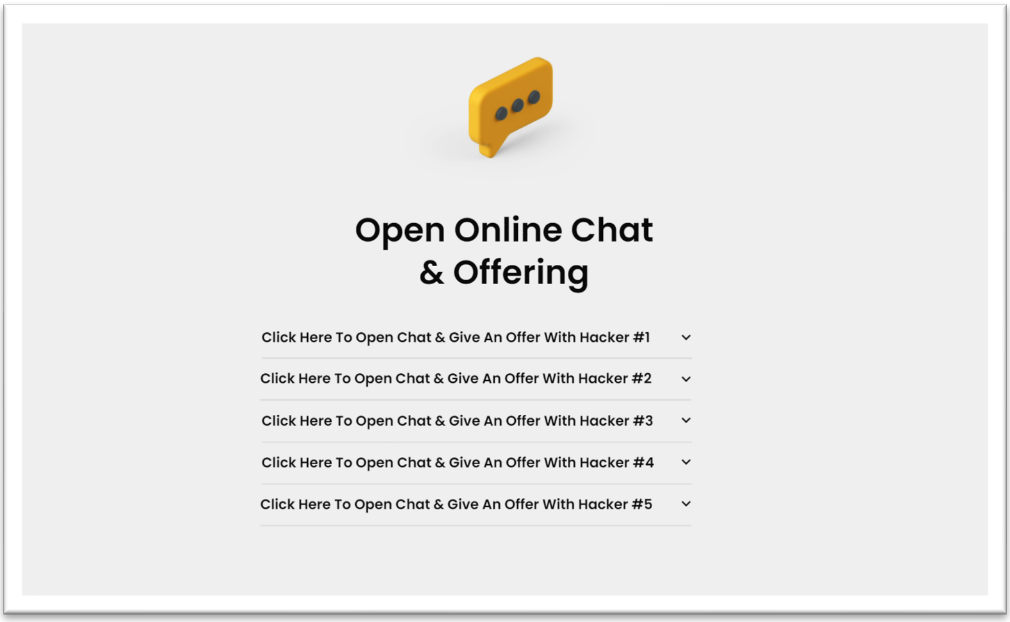


Make a Connection Now! Check Available Hackers...

Hackers

The Most Rated Hackers In Our System

Figure 4-6 Hacker Most-Rated Page



Open Online Chat
& Offering

Click Here To Open Chat & Give An Offer With Hacker #1 ⌄

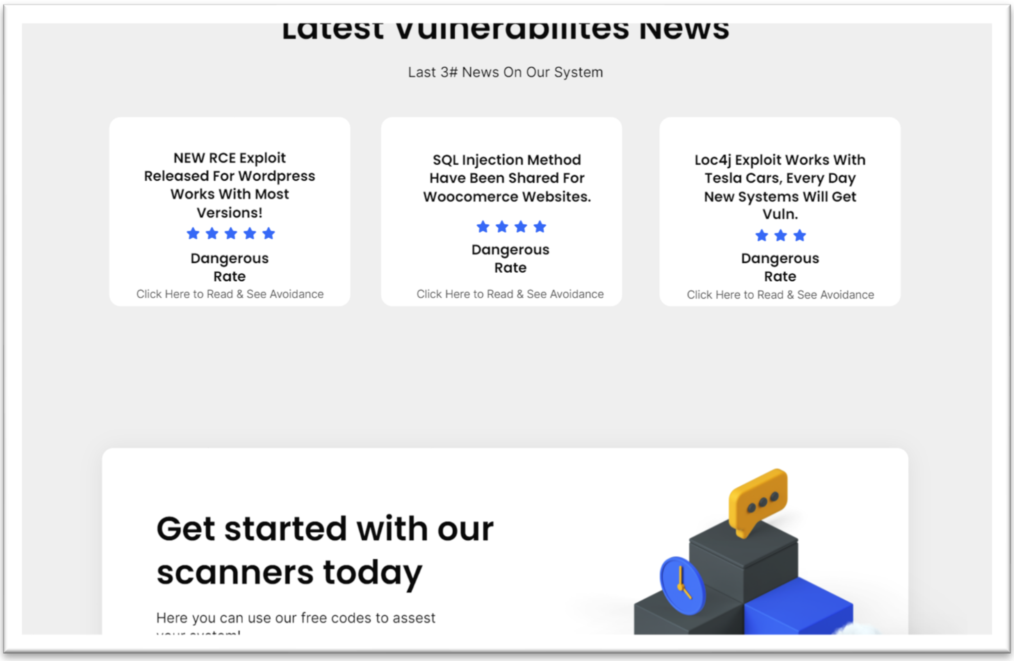
Click Here To Open Chat & Give An Offer With Hacker #2 ⌄

Click Here To Open Chat & Give An Offer With Hacker #3 ⌄

Click Here To Open Chat & Give An Offer With Hacker #4 ⌄

Click Here To Open Chat & Give An Offer With Hacker #5 ⌄

Figure 4-7 Online Chat & Offering Page



Latest Vulnerabilites News

Last 3# News On Our System

NEW RCE Exploit Released For Wordpress Works With Most Versions!
★★★★★
Dangerous Rate
Click Here to Read & See Avoidance

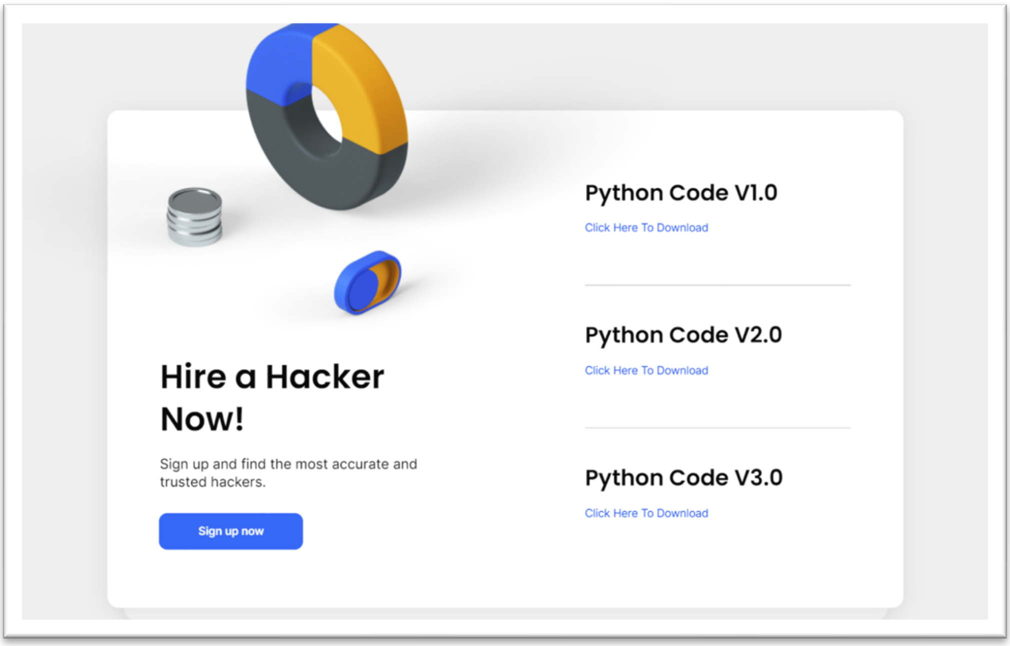
SQL Injection Method Have Been Shared For Woocomerce Websites.
★★★★
Dangerous Rate
Click Here to Read & See Avoidance

Loc4j Exploit Works With Tesla Cars, Every Day New Systems Will Get Vuln.
★★★
Dangerous Rate
Click Here to Read & See Avoidance

Get started with our scanners today

Here you can use our free codes to assest your system!

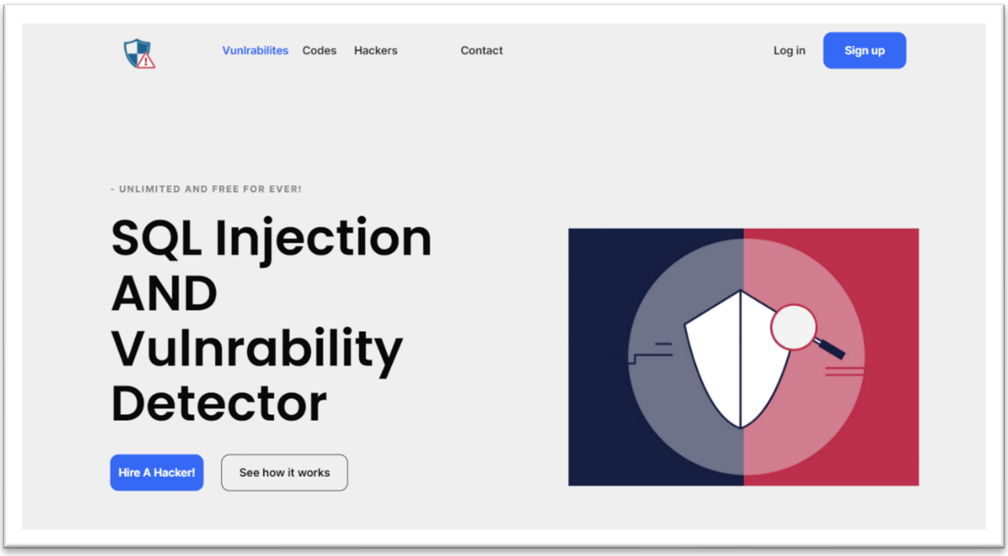
Figure 4-8 Last Three Vulnerability & Solutions Page



Hire a Hacker Now!

Sign up and find the most accurate and trusted hackers.

Figure 4-9 Download Python Codes Page



SQL Injection AND Vulnrability Detector

Figure 4-10 Main and Vulnerability Page

4.5. Chapter Summary

Finally, by reaching this point there is several goals and achievements have been done which is selecting the entire design with the combination of common diagram like UML Diagram and class diagram and also the prototype etc. to the project and explaining each part of the system by providing a clear connection through the diagrams and UML Design also the most important one which is prototype. for each of them furth more there is different type of diagrams stated that could be necessary for this project also here is numerous design tools used for that, in the chapter 5 there would be more things and giving a summary to the entire system will be one of them.

Chapter 5

Implementation, Testing, Results, and Discussion

5.1. Introduction

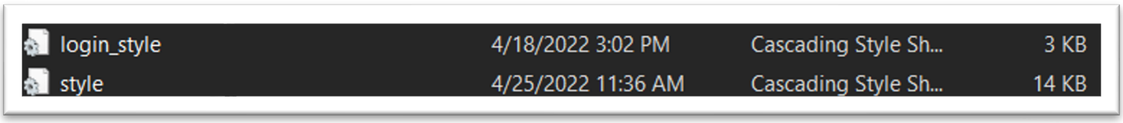
From this chapter we will focus on some different and main categories compare to the previous ones, because we will mostly talks about the way that we've coded the website and how we process everything also how is the analysis besides that we will going to explain all the main parts of the website one by one and how they works also we will do some tests like white box testing also most important user testing also since the beginning of the project we have taken advantage of many libraries and different languages to code the project so we're going to explain them as well in deeply information.

5.2. Coding of System Main Functions

The following has been used to the project:

1. HTML:
   Hypertext Markup Language is abbreviated as HTML. It is the most basic language, and it is simple to learn and modify. It is a cross between hypertext and markup language. It consists of features that may alter or develop the design and content of a web page. In contrast, HTML creates or specifies the structure of web pages. We can create HTML webpages that can be seen on internet-connected devices such as laptop computers and Android phones.
2. CSS:
   Cascading Style Sheets is referred to as CSS. We are able to make our web pages available to individuals thanks to the language used to specify how Web

pages are presented, including colors, layout, and fonts. Web-based style sheets are made using CSS. It may be used with any XML-based markup language and is not dependent on HTML.

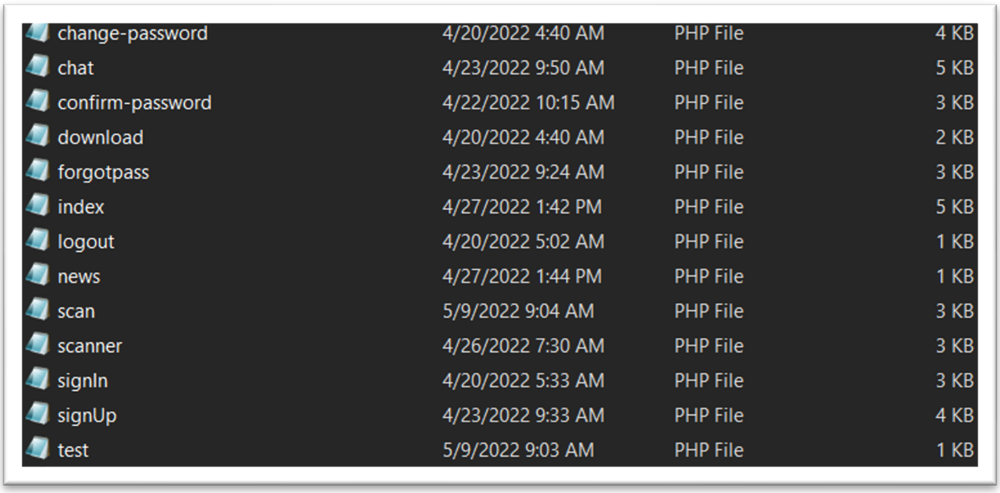


login_style	4/18/2022 3:02 PM	Cascading Style Sh...	3 KB
style	4/25/2022 11:36 AM	Cascading Style Sh...	14 KB

Figure 5-1 CSS Files

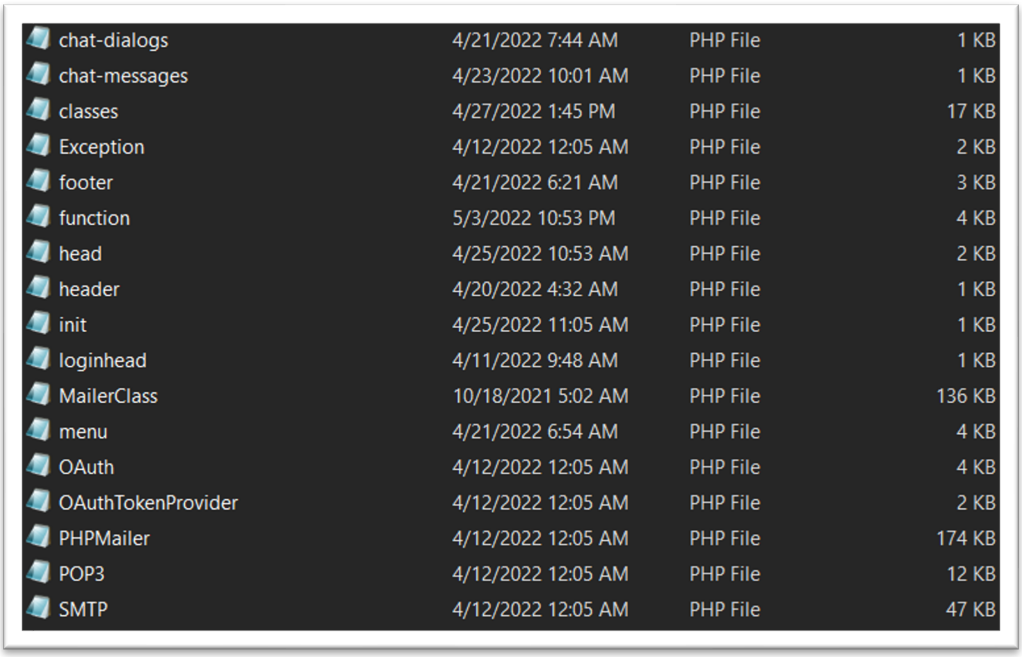
3. PHP:

PHP is a general-purpose server-side programming language that is ideal for web development. PHP stood for Personal Home Page at first. It now stands for Hypertext Preprocessor. Because the first word is likewise an acronym, it's a recursive acronym.



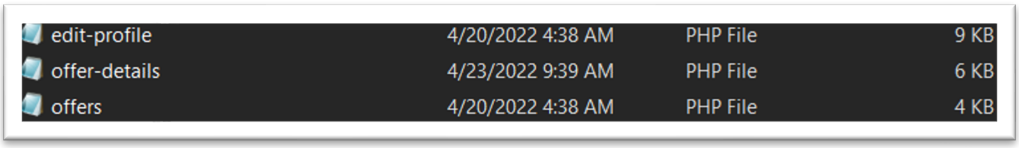
change-password	4/20/2022 4:40 AM	PHP File	4 KB
chat	4/23/2022 9:50 AM	PHP File	5 KB
confirm-password	4/22/2022 10:15 AM	PHP File	3 KB
download	4/20/2022 4:40 AM	PHP File	2 KB
forgotpass	4/23/2022 9:24 AM	PHP File	3 KB
index	4/27/2022 1:42 PM	PHP File	5 KB
logout	4/20/2022 5:02 AM	PHP File	1 KB
news	4/27/2022 1:44 PM	PHP File	1 KB
scan	5/9/2022 9:04 AM	PHP File	3 KB
scanner	4/26/2022 7:30 AM	PHP File	3 KB
signIn	4/20/2022 5:33 AM	PHP File	3 KB
signUp	4/23/2022 9:33 AM	PHP File	4 KB
test	5/9/2022 9:03 AM	PHP File	1 KB

Figure 5-2 PHP files 1



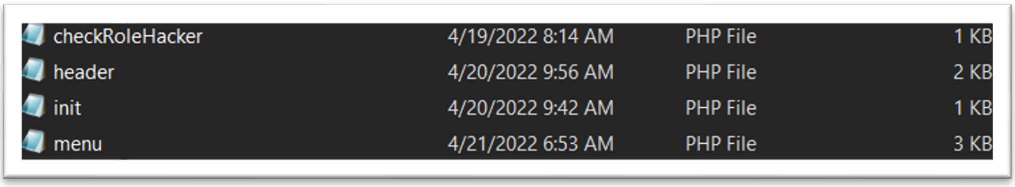
chat-dialogs	4/21/2022 7:44 AM	PHP File	1 KB
chat-messages	4/23/2022 10:01 AM	PHP File	1 KB
classes	4/27/2022 1:45 PM	PHP File	17 KB
Exception	4/12/2022 12:05 AM	PHP File	2 KB
footer	4/21/2022 6:21 AM	PHP File	3 KB
function	5/3/2022 10:53 PM	PHP File	4 KB
head	4/25/2022 10:53 AM	PHP File	2 KB
header	4/20/2022 4:32 AM	PHP File	1 KB
init	4/25/2022 11:05 AM	PHP File	1 KB
loginhead	4/11/2022 9:48 AM	PHP File	1 KB
MailerClass	10/18/2021 5:02 AM	PHP File	136 KB
menu	4/21/2022 6:54 AM	PHP File	4 KB
OAuth	4/12/2022 12:05 AM	PHP File	4 KB
OAuthTokenProvider	4/12/2022 12:05 AM	PHP File	2 KB
PHPMailer	4/12/2022 12:05 AM	PHP File	174 KB
POP3	4/12/2022 12:05 AM	PHP File	12 KB
SMTP	4/12/2022 12:05 AM	PHP File	47 KB

Figure 5-3 PHP Files 2



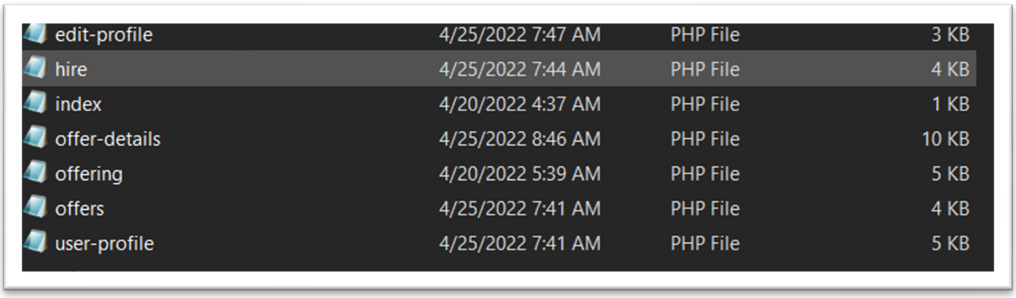
edit-profile	4/20/2022 4:38 AM	PHP File	9 KB
offer-details	4/23/2022 9:39 AM	PHP File	6 KB
offers	4/20/2022 4:38 AM	PHP File	4 KB

Figure 5-4 PHP Files 3



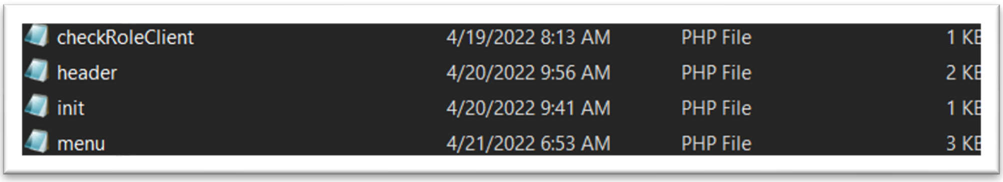
checkRoleHacker	4/19/2022 8:14 AM	PHP File	1 KB
header	4/20/2022 9:56 AM	PHP File	2 KB
init	4/20/2022 9:42 AM	PHP File	1 KB
menu	4/21/2022 6:53 AM	PHP File	3 KB

Figure 5-5 PHP Files 4



edit-profile	4/25/2022 7:47 AM	PHP File	3 KB
hire	4/25/2022 7:44 AM	PHP File	4 KB
index	4/20/2022 4:37 AM	PHP File	1 KB
offer-details	4/25/2022 8:46 AM	PHP File	10 KB
offering	4/20/2022 5:39 AM	PHP File	5 KB
offers	4/25/2022 7:41 AM	PHP File	4 KB
user-profile	4/25/2022 7:41 AM	PHP File	5 KB

Figure 5-6 PHP Files 5



checkRoleClient	4/19/2022 8:13 AM	PHP File	1 KB
header	4/20/2022 9:56 AM	PHP File	2 KB
init	4/20/2022 9:41 AM	PHP File	1 KB
menu	4/21/2022 6:53 AM	PHP File	3 KB

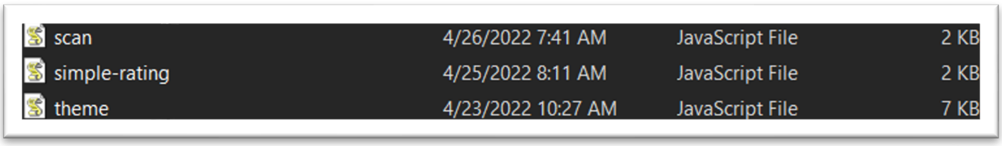
Figure 5-7 PHP Files 6

4. jQuery:

   Using JavaScript on your website will be a lot simpler thanks to jQuery. jQuery wraps a number of common activities into methods that you may call with only one line of code instead of the several lines of JavaScript code needed to complete them.

5. JavaScript:

   JavaScript, commonly referred to as the scripting language for websites, is a portable, cross-platform, interpreted computer language. It is widely used in non-browser situations and is well recognized for web page building. Both client-side and server-side programming may be done using JavaScript.



scan	4/26/2022 7:41 AM	JavaScript File	2 KB
simple-rating	4/25/2022 8:11 AM	JavaScript File	2 KB
theme	4/23/2022 10:27 AM	JavaScript File	7 KB

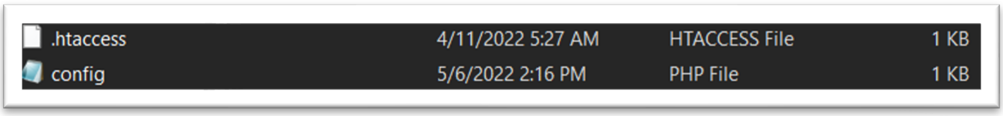
Figure 5-8 JS Files

6. Bootstrap:

   It is an accessible and free CSS framework that aids in guiding a front-end web page development tool that is mobile-first and responsive to devices. To cope with typography, the implementation of buttons, forms, and numerous other user interface components, Bootstrap contains CSS (Cascading Style Sheets), as well as an optional JavaScript enabled design template (plug-ins). This framework enables developers in producing responsive web pages more quickly and speeds up web development.

7. MySQL:

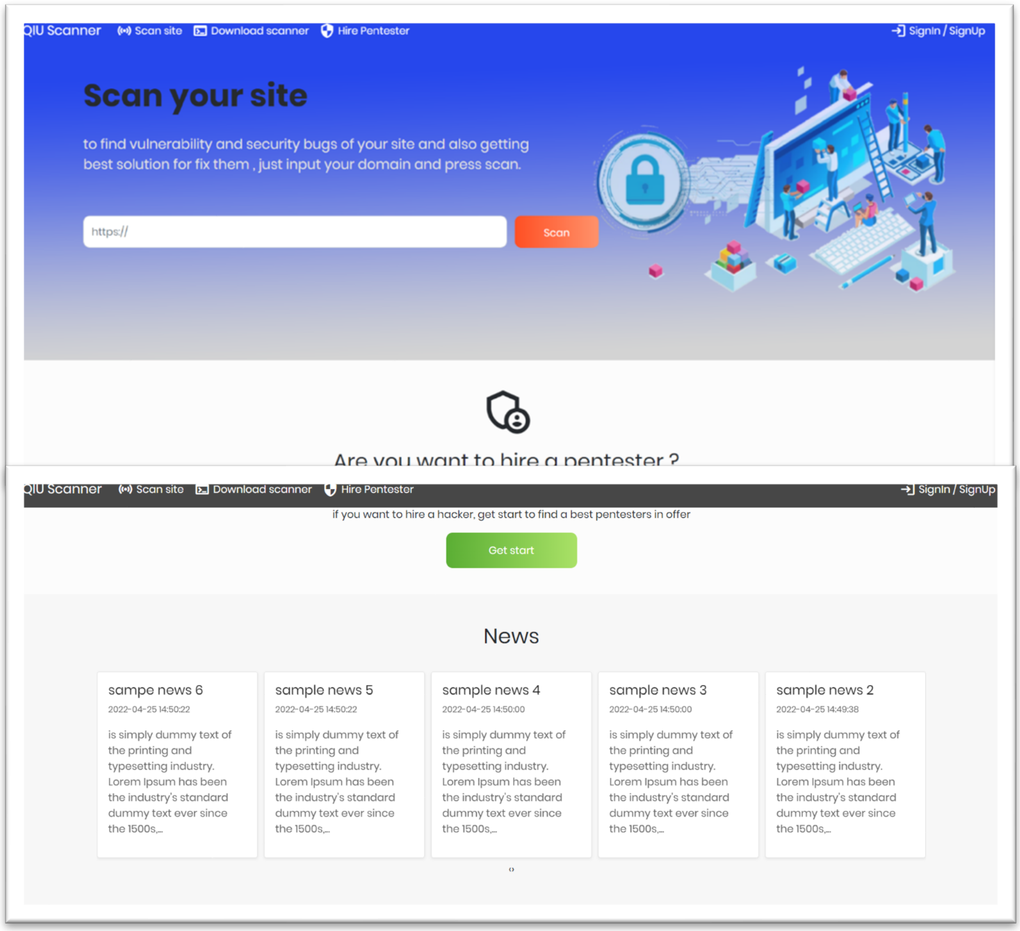
An open-source relational database management system is called MySQL (RDBMS). It is the most often used database type for PHP. Oracle Corporation creates, distributes, and supports MySQL.



.htaccess	4/11/2022 5:27 AM	HTACCESS File	1 KB
config	5/6/2022 2:16 PM	PHP File	1 KB

Figure 5-9 MySQL Files

5.3. Interfaces of System Main Functions



Scan your site

to find vulnerability and security bugs of your site and also getting best solution for fix them , just input your domain and press scan.

https://

Are you want to hire a pentester ?

if you want to hire a hacker, get start to find a best pentesters in offer

News

sampe news 6
2022-04-25 14:50:22
is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s,..

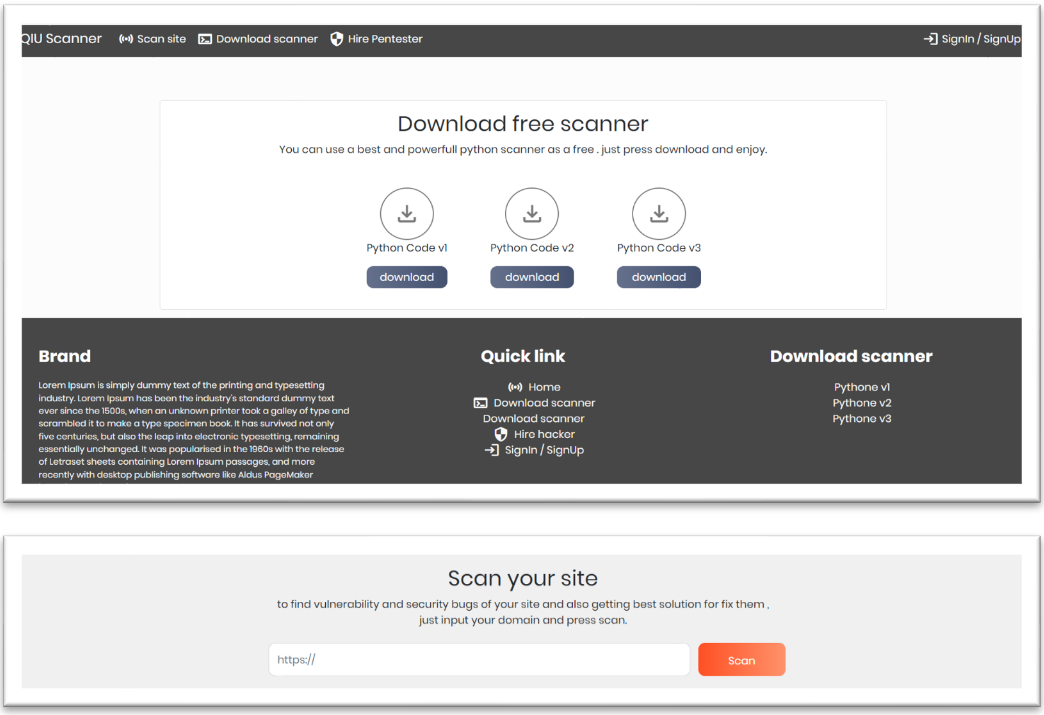
sample news 5
2022-04-25 14:50:22
is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s,..

sample news 4
2022-04-25 14:50:00
is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s,..

sample news 3
2022-04-25 14:50:00
is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s,..

sample news 2
2022-04-25 14:49:38
is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s,..

Figure 5-10 Guest Access



QIU Scanner   Scan site   Download scanner   Hire Pentester   SignIn / SignUp

Download free scanner

You can use a best and powerfull python scanner as a free . just press download and enjoy.

Python Code v1 download   Python Code v2 download   Python Code v3 download

Brand

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker

Quick link

Home
Download scanner
Download scanner
Hire hacker
SignIn / SignUp

Download scanner

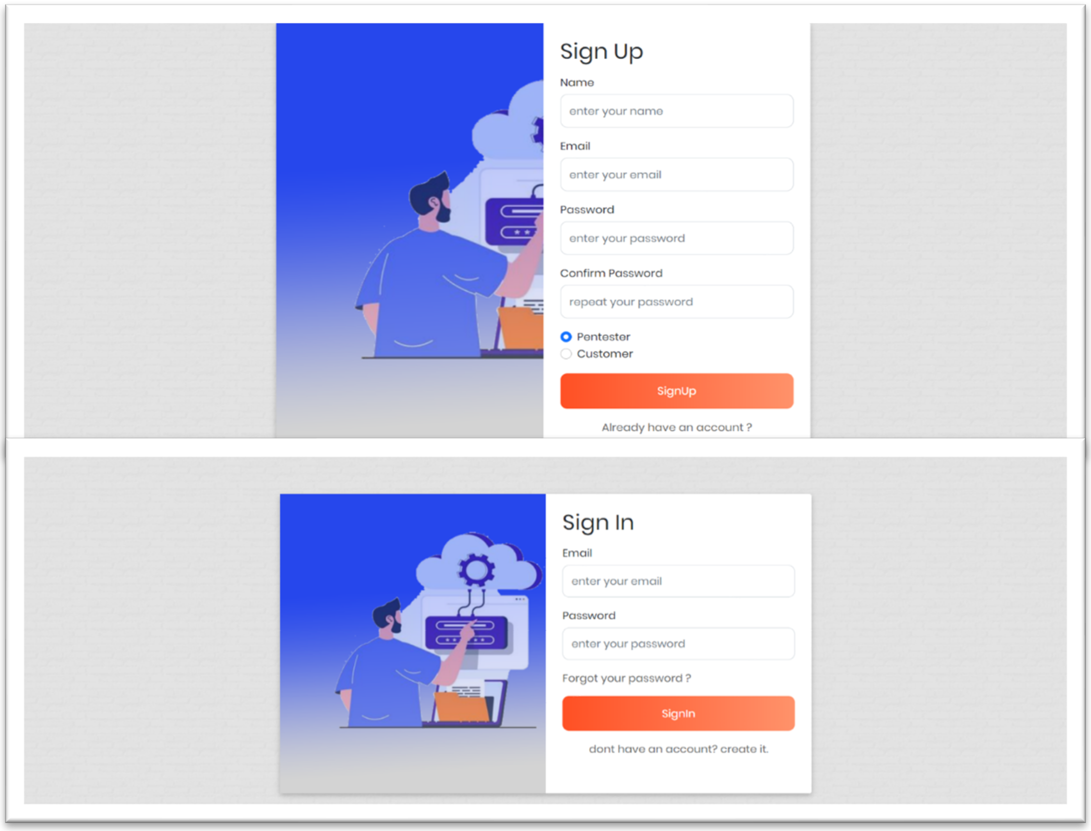
Pythone v1
Pythone v2
Pythone v3

Scan your site

to find vulnerability and security bugs of your site and also getting best solution for fix them ,
just input your domain and press scan.

https://   Scan

Figure 5-11 Guest Access



Sign Up

Name: enter your name
Email: enter your email
Password: enter your password
Confirm Password: repeat your password

● Pentester
○ Customer

SignUp

Already have an account ?

Sign In

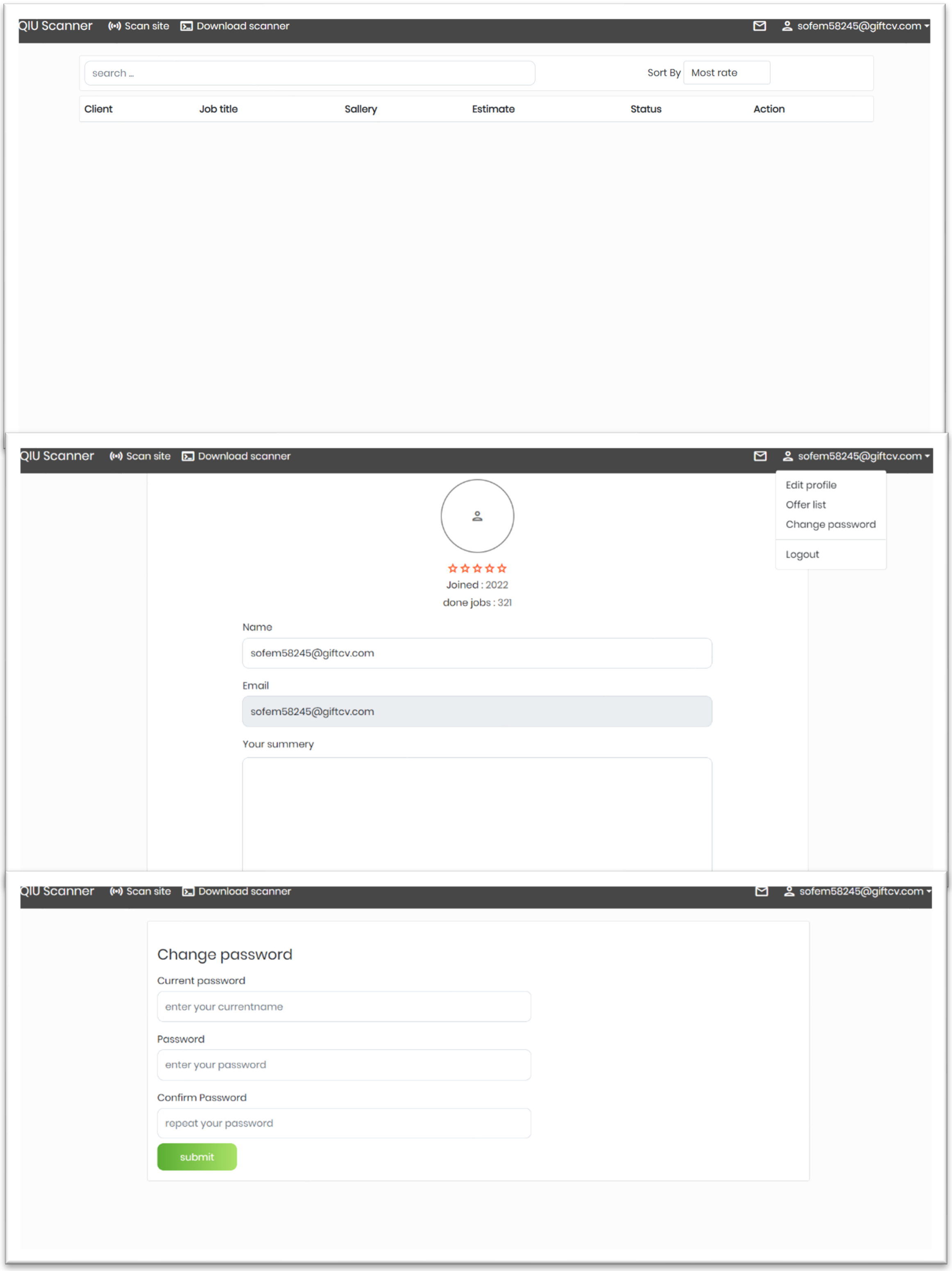
Email: enter your email
Password: enter your password

Forgot your password ?

SignIn

dont have an account? create it.

Figure 5-12 Login & Signup



Joined : 2022

done jobs : 321

Name: sofem58245@giftcv.com

Email: sofem58245@giftcv.com

Your summery

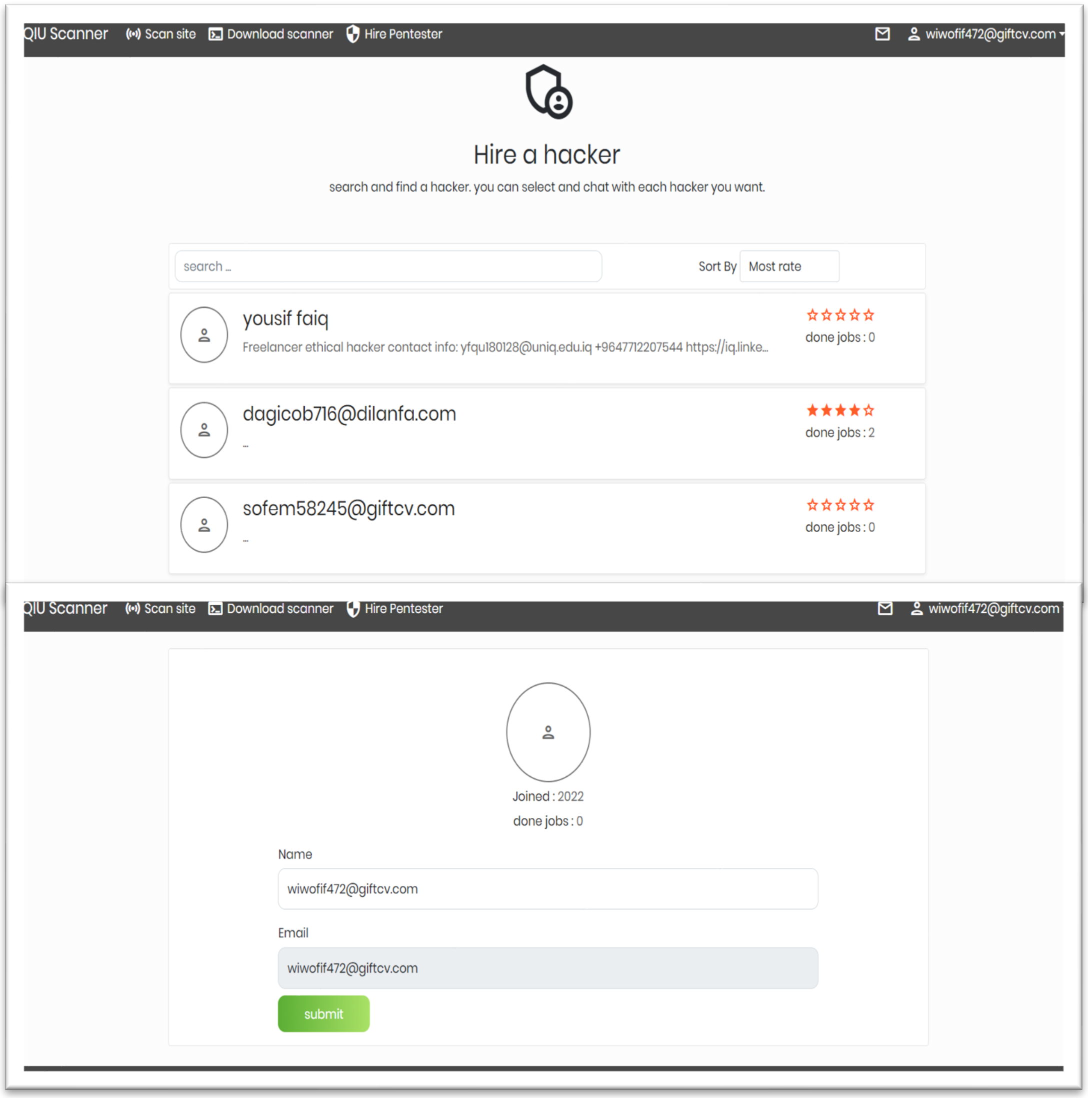
Change password

Current password: enter your currentname

Password: enter your password

Confirm Password: repeat your password

Figure 5-13 Pen tester Access After Log inning.



Hire a hacker

search and find a hacker. you can select and chat with each hacker you want.

search ..

Sort By Most rate

yousif faiq
Freelancer ethical hacker contact info: yfqu180128@uniq.edu.iq +9647712207544 https://iq.linke...
☆☆☆☆☆
done jobs : 0

dagicob716@dilanfa.com
-
★★★★☆
done jobs : 2

sofem58245@giftcv.com
-
☆☆☆☆☆
done jobs : 0

Joined : 2022
done jobs : 0

Name
wiwofif472@giftcv.com

Email
wiwofif472@giftcv.com

Figure 5-14 Customer Access After Log inning.

5.4. Testing The System

5.4.1. White Box Testing

Testing in which the tester can view the code is known as white box testing. These tests are mostly used to examine the inner workings of the program, bolster its security, and enhance its usability and design.

As the tester selects the inputs to test and tracks their progress through the software to get the desired results, this is sometimes referred to as structural testing. In the unit, integration, and systems testing phases of software development, white box testing is utilized.

Although this testing approach is effective for identifying defects in various software components, it has the potential to overlook other issues in areas that the tester did not examine.

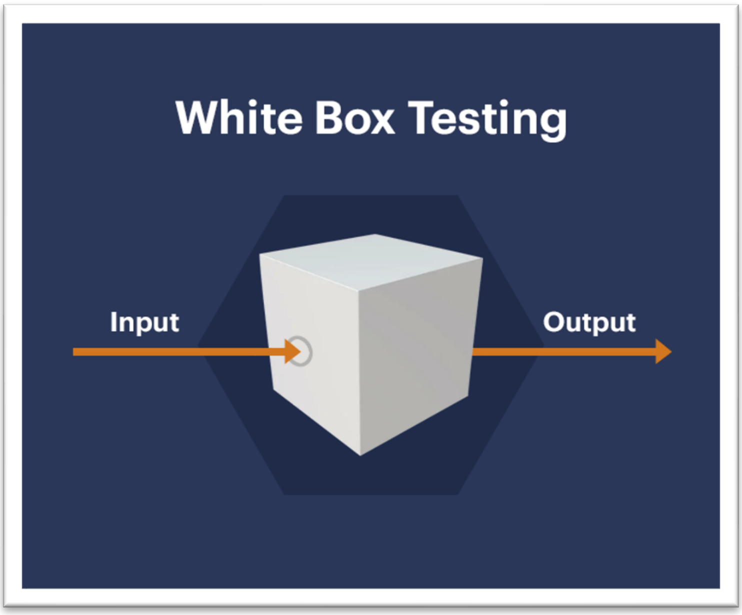


Figure 5-15 White Box Testing

Table 5-1 White Box Testing

Test Number	Test Type	Test Data	Reason	Expected Outcome	Actual Outcome	Pass OR fail?
#1	Valid	txtEmail = b@a.a	Enter a valid email address to check if it says valid	Message box displays “VALID”	Message box displays “VALID”	PASS
#2	Valid	txtEmail = cc22@c44.d1	Enter another valid email to check if it says valid	Message box displays “VALID”	Message box displays “VALID”	PASS
#3	Invalid	txtEmail = @pa.c	Enter an invalid email address to check if it says invalid	Message box displays “INVALID”	Message box displays “INVALID”	PASS
#4	Invalid	txtEmail = 321.n@pow	Enter another invalid email address to check if it says invalid	Message box displays “INVALID”	Message box displays “INVALID”	PASS
#5	Null Value	txtEmail = nothing entered	To see if it will ask to enter an email while nothing entered	Message box displays “INVALID”	Message box displays “INVALID”	PASS

5.4.2. User Acceptance Testing

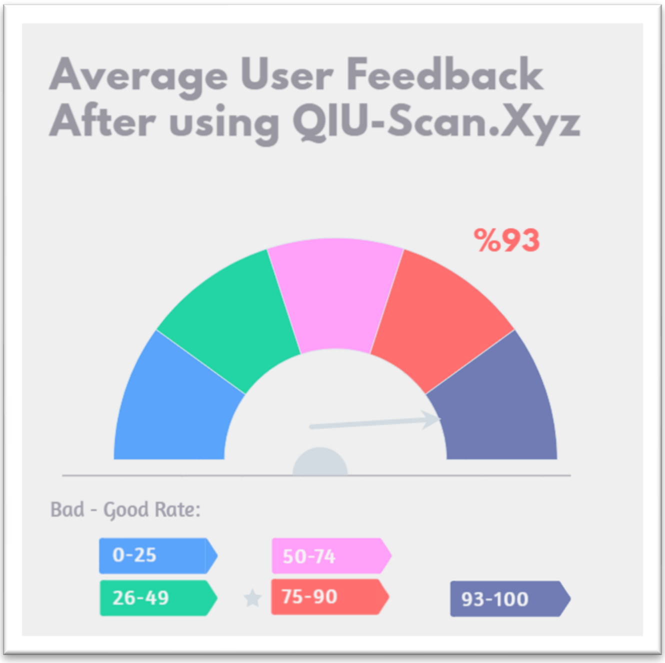


Figure 5-16 Average Good Rate Feedback %93

User testing encompasses the complete spectrum of a customer's interaction with your product, prototype, or feature. This comprises all of their perceptions, feelings, preferences, attitudes, and behaviors in regard to that thing from the time they acquire it until they cease using it.

Table 5-2 User Acceptance Table

Main-Functions TESTS	User1	User2	User3	User4	User5	User6	User7
Successfully platform launched?	YES	YES	YES	YES	YES	YES	YES
Does the scan site work well?	YES	YES	YES	YES	YES	YES	YES
giving offers working?	YES	YES	YES	YES	YES	YES	YES
chatting is accurate and responsive?	YES	YES	YES	YES	YES	YES	YES
all the three scanners can be downloaded?	YES	YES	YES	YES	YES	YES	YES
sign/sign up works?	YES	YES	YES	YES	YES	YES	YES
forget password works?	YES	YES	YES	YES	YES	YES	YES
giving feedback & rating to the pen tester works?	YES	YES	YES	YES	YES	YES	YES
modifying profile info or changing password works perfectly?	YES	YES	YES	YES	YES	YES	YES
give a percentage about accuracy of SQL Injection live detector.	%91	%94	%93	%91	%95	%92	%94

5.5. Chapter Summary

Lastly, from end of this chapter we've completed the entire process to the project and we have explained everything that used from the beginning of the project until last thing which is the test and we've done it with some different steps first we have started with white box then finally we've made a test from users to get result for our project, besides all of this we have explained all the codes and languages used in this project also we have screened the files for each language used if exists.

Chapter 6

Conclusion

6.1. Introduction

A vulnerability assessment is a methodical evaluation of safety weaknesses in a data system. It measures whether the system or website is vulnerable to any recognized vulnerabilities, assigns the degree of cruelty to these vulnerabilities, and comments on remedies or reasons when needed. The penetration exam is a full review of a datum system's security faults. It controls if the system is vulnerable to any known vulnerabilities, gives severity assessments to those vulnerabilities, and, if and when essential, offers therapy or mitigation. The goal of this phase is to make a complete list of vulnerabilities in a submission. Security experts use automated tools to scan applications, servers, and other programs, or perform physical tests and evaluations on them to determine their safety and health. Vulnerability files, vendor vulnerability announcements, strength management systems, and danger intelligence feeds are also used by specialists to detect security flaws.

6.1.1. Objectives

The objectives of execution a Vulnerability detector is to make an overview of the security threats to a network or a web application and then use that overview as a guide to resolution those threats which is:

- Performing fixed assessments and regularly resolving all security risks offers a baseline security for the network.

- Managers and users can feel self-assured that potential attackers will be powerless to exploit vulnerabilities on their system.
- A vulnerability valuation is a methodical evaluation of security weaknesses in an evidence system.
- It determines if the system is vulnerable to any known flaws, assigns severity ratings to those flaws, and suggests remediation or change if and when necessary.

Figure 6-1 Objectives

6.2. Achievements

This project will mostly focus to vulnerabilities and explains how dangerous they're to the community and organizations, also depending on my experience I will clarifies and provides the major and famous vulnerabilities like SQL injection then affords the solutions to fix them by combining and putting them into a modern website afterward I'm going to share some of my python codes that people could use them to scan their website and found the loopholes automatically using my code besides that I've planned to specialize a different section for penetration testing with some good offers that people and organizations could pay and own me to Pen-testing their website and give the solutions for closing the vulnerability and to stop being attacked and exploits by others.

And to protect a website or a server it's necessary to know where you buy a domain or resellers and webhosting plus the script you're using to code your website if it's an instant one then it's so important to have a review to previews exploits and loopholes in that script to avoid repeating the same mistake otherwise if you're coding it from zero to end still you should have a review and not letting the same Vulnerability to happen and give a chance to hackers to exploit it. To get a better solution it'll be better to prevent using WordPress and the other instant websites because there is still a chance to have a vulnerability in the future especially by having those much plugins to install, So, to have a better solution there will be not the same mistakes that have done before for example there will be no use of instant open-source sites like WordPress, Joomla, OpenCart, Presta-shop etc. because there is a lot of exploits every year and the patch takes so longer time than having your own script also fixing it by itself. And in this project, the secured webhosting websites and resellers will be recommended to have less chance of affection by bulk exploits because there are many hosting sites that may let the hacker to jump from the affected site to another site that does not have any bugs. Furth more, hackers can make money and have better chance of making connection with organizations and even any kind of people in any career that needs to make contact with a hacker and ask for assessment his/her system besides there is free codes available to do scanning with no payment or credit card requirement also people can read and see the solutions of new vulnerabilities or even old ones.

Figure 6-2 Achievements

6.3. Suggested Plans for Project

To be honest in this level after finishing a big part of the project anyone may have a confusion or being stress but fortunately in PSM2 it will be a great pleasure to have this project in a functional one and doing the entire project from first chapter until last one which is this one chapter five to convert it into real project so it'll be a big achievement if the project going to use by the people and giving at least some benefit to this people who are experienced or want to get experience in this kind of subject, So. In near future the chapter 6 will begins and the most important section is mentioning future improvements to the project and this can be achieved through surveys which other people can provide and share his/her ideas that could have a great result by the end of it. And to be more clarified this project have several sections that could have very great benefit to different parts of society, the first one is people and users can have free codes to scan their websites plus detecting vulnerabilities without needing help of others and the second one is hackers. So, they can make money in legal way without disadvantaging others, and the third one is customers and clients can read news about latest and common vulnerabilities also how to fixing them and how to avoidance from them.

REFERENCES

Antunes, N. also Vieira, M., 2014. Surveying and contrasting weakness identification apparatuses for web administrations: Benchmarking approach and models. IEEE Transactions on Services Computing, 8(2), pp.269-283.

Liu, B., Shi, L., Cai, Z. what's more Li, M., 2012, November. Programming weakness revelation procedures: A review. In 2012 fourth worldwide gathering on mixed media data systems administration and security (pp. 152-156). IEEE.

Shah, S. also Mehtre, B.M., 2015. An outline of weakness appraisal and entrance testing strategies. Diary of Computer Virology and Hacking Techniques, 11(1), pp.27-49.

Petukhov, A. also Kozlov, D., 2008. Distinguishing security weaknesses in web applications utilizing dynamic investigation with infiltration testing. Processing Systems Lab, Department of Computer Science, Moscow State University, pp.1-120.

Antunes, N. also Vieira, M., 2013. Infiltration testing for web administrations. PC, 47(2), pp.30-36.

Suteva, N., Zlatkovski, D. what's more Mileva, A., 2013. Assessment and testing of a few free/open-source web weakness scanners.

Nilsson, J. what's more Virta, V., 2006. Weakness scanners. Imperial Institute of Technology, Stockholm.

Antunes, N. what's more Vieira, M., 2009, November. Looking at the viability of entrance testing and static code examination on the identification of sql infusion weaknesses in web administrations. In 2009 fifteenth IEEE Pacific Rim International Symposium on Dependable Computing (pp. 301-306). IEEE.

Fonseca, J., Vieira, M. what's more Madeira, H., 2007, December. Testing and looking at web weakness checking instruments for SQL infusion and XSS assaults. In thirteenth Pacific Rim worldwide discussion on reliable processing (PRDC 2007) (pp. 365-372). IEEE.

Antunes, N. what's more Vieira, M., 2009, September. Recognizing SQL infusion weaknesses in web administrations. In 2009 Fourth Latin-American Symposium on Dependable Computing (pp. 17-24). IEEE.