Palestine Polytechnic University

College of Information Technology and Computer Engineering

Graduation Project-Software Security

"Test Your website"

Project Team:

Nagham Nassar

Yara Sarahna

supervisor:

Dr.Khalid daghameen

2022-2023

Acknowledgement

All thanks and appreciation to those who contributed to our education until we reached what we have achieved

We also thank our supervisor for this project Dr.Khalid daghameen

Abstract

Recently, the number of people trying to hack websites has increased with the increase in the number of security vulnerabilities and the lack of security awareness among programmers, and website programmers focus only on the content and form of the website and not paying attention to the security dimensions that threaten these websites and may lead to their downfall. New companies are negligent in hiring someone. In the field of information security to carry out the initial and periodic examination, in addition to the lack of awareness of programmers and employees in the field of information technology in the field of site and information security ,Therefore, we decided to help the beginners in the field of website programming and new startups in examining their websites and discovering the vulnerabilities that threaten them, in addition to the feature of checking two-factor authentication for social media sites .for people interested in the field of ethical hacking Also through this site can help , small and new companies can save the cost of bringing someone to check The site has its own in addition to saving time on the beneficiary category.

مؤخراً ازداد عدد الأشخاص الذين يحاولون اختراق المواقع الالكترونية مع ازدياد اعداد الثغرات وقلة الوعي الأمني لدى المبرمجين , وتركيز مبرمجين المواقع الالكترونية فقط على فحوى الموقع وعلى شكله وعدم الانتباه الى الأبعاد الأمنية التي تهدد هذه المواقع وقد تؤدي الى سقوطها .وتهاون الشركات الجديدة في توظيف شخص في مجال امن المعلومات ليقوم بالفحص الأولي والدوري , بالإضافة لقلة وعي المبرمجين والموظفين في مجال تكنولوجيا المعلومات في مجال أمن المواقع وأمن المعلومات .لذلك قررنا مساعدة الصاعدين في مجال برمجة المواقع الالكترونية والشركات الناشئة الجديدة في فحص مواقعها الالكترونية واكتشاف ما يهددها من ثغرات بالإضافة لميزة فحص المصادقة الثنائية لمواقع التواصل الاجتماعي للأشخاص المهتمين بمجال الاختراق الاخلاقي .وايضاً من خلال هذا الموقع يمكن التوفير على الشركات الصغيرة والجديدة تكلفة احضار شخص لفحص الموقع خاصتها بالإضافة لتوفير الوقت على الفئة المستفيدة .

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

- Overview
- Problem Definition
- Motivation
- General objectives
- Scope of the system
- System Requirements
- Procedure to achieve
- Conclusion

1.1Overview

At some point, website users and developers in general must verify that they have a safe and comfortable experience using these websites (https://www.w3schools.com/, 2022). This project aims to develop a simple website that checks some security vulnerabilities in other websites to reflect security approach and improve security functionality in terms of CIA / AAA (Iyad Hraini, 2021; Badran, Arman, & Farajallah, 2021)

The website will make it easier for university students, website developers and small business owners to verify websites that seem a little complicated for all parties, and it will save time and effort in addition to a comfortable experience for its users (https://github.com, 2022).

1.2Problem Definition

As we are information security searchers, we recognize the real problem that face all designer and websites admins, and their need to protect their website from the electronic crimes. We introduce a suitable solution, which is am website is able to check if there are gaps in the other websites and give suggestion solutions which may reduce these gaps and protect the net security .And those errors which weaken the website and harm their owners if they are discovered after a while. which means exposes website to hacking, by beginners in hacking or amateur especially if the owner of the website is weak in information security field.

1.3Motivation

Through experience and the project team's research about modern problems in the security field and asked people around us with different ages, we found that website users and developers suffer from the same security problems when they use unsafe websites.

1.3.1For small business owners:

- They usually pay a computer engineer who checks their websites.
- They face the problem of not knowing the solutions to the security vulnerabilities that may exist in their sites, when they use other scanning websites.

- The security ignorance from website administrators and companies often causes the a lineation of customers from any website after problems occur as a result of the security weakness of the site.

1.3.2For normal users of internet and students:

- Security vulnerabilities scanners websites are often paid.
- Some other scanner websites ignore user interface which may be a source of attraction for a number of customers.
- Some scanning sites are so complex that only security professionals can use them.

1.3.3For developers:

- They need instant and quick scanning of their own websites.
- They will work better when they use test websites without ads or complicated steps.

Accordingly, it was suggested to develop a vulnerabilities security scanner website that will make a difference and help the three parties in using websites safe use. We chose just five vulnerabilities for our project to make the ideas clearer and more specific.

1.4General Objectives

- Providing an unpaid website that checks security vulnerabilities.
- Enable users to get check services without adds.
- Enable users to check any website from vulnerabilities without need any computer engineer or professional.
- Save time, effort and money for small business owners.
- Giving an easy way for beginners in hacking to test any website.
- Detect the problem with proposing the solution in one website.

1.5Scope of the system

The system will target university students, Designers, websites admins, Ethical hacker, Normal users of the internet, beginners in hacking or amateur and developers.

1.6System Requirements

At this stage, we will talk about an important part of the analysis process for our project, which are the requirements, which are divided into functional and non-functional requirements, and security requirements.

1.6.1Website functional requirements

- The user shall enter the link of the website to be checked
- The website must receive the link of the website to be checked.
- The website must check the website entered link for security vulnerabilities.
- The Website shall display the results of the scan process on the user interface
- The website shall suggestion solutions for Vulnerabilities resulting from checking websites.

1.6.2Non-functional requirements

1.6.2.1Product requirements

- The website is available for all users are concerned about the security of their websites and for beginners in security field.
- The website must be usable, so users can deal with it easily without any problem (user friendly interface).
- The website shall provide solutions for Vulnerabilities resulting from checking websites.
- The website must have an internet connection in order to keep up with the information online and deal with the site that will be checked.
- The users will be given real time service.

1.6.2.2Organizational requirements

- The front end of the website is written in React Frame work programming language.
- The backend of website is written in python programming language using "visual studio code" due to good tools that help the programmer to code and easy packing downloading.

1.6.2.3External requirements

- The website must respect engineering ethics, so that it supporting ethical hacking only.

1.3.1.1 Security requirements

The website must test Specific security vulnerabilities, which are:

- SQL Injection
- Cross-Site Scripting (XSS) Injection
- HTTP security headers(x-xss, non-snif, x-frame and policy)
- Scan ports

1.7Procedure to achieve

The research team relied on the systems engineering process which begins with the planning of the system, then analysis of requirements followed by the design of the system, then development operation, and finally testing. We also relied on scrum framework.

1.8Conclusion

In this chapter, we have talked about the research problem and solution, the objectives of the system, and how it is important, and system requirements specifications, This introduction will be the basis of starting to talk about the second chapter which includes the literature review and similar work done by others in the past.

Chapter 2

Background and Review of Literature

- Introduction
- literature review
- Similar work done by others
- Basic security background

2.1 Introduction

This chapter includes previous studies on our topic, summarized scientific papers, and previous works similar to our project, and we studied two examples of them. And finally basic security background with citations to references containing these issues.

2.2 literature review

Each website is created using a series of codes to be able to display data that is public accessible to everyone. However, usually on the server computer where the website is stored, there are also data that are confidential or private, so it is not allowed to be accessed by the public. This research is conducted to analyze various techniques and ways of attack that usually done on the internet website, in order to implement various ways of handling so that the existing website can be more secure against the attack . The results have been obtained that is known some weaknesses and attacks that occur on a website (FARAJALLAH, 2022).

The" Web vulnerability analysis and implementation" study also mentioned that XSS is one of the weaknesses that is often exploited by it attacker, but many service providers who do not recognize the weakness .for a website that has implemented a security system, vulnerability can still occur because there is the possibility missed in one side of the security of the web not previously considered during the design or construction of the system, or also because of the ability of hackers or crackers ability increases (Farajallah, Gautier, Hamidouche, Déforges, & Assad, 2022).

according to figure2.1.

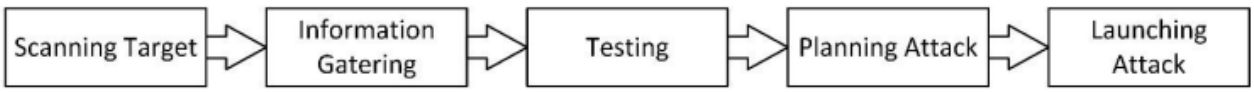


Figure2.1

Stages of web attack system, start from scanning process until launching the attack by the attacker.

Research team opinion: Any internet user must to check all the websites we use, even if they seem safe ,And how to discover vulnerabilities in websites for beginners may seem a bit daunting, Especially at the beginning of learning the basics of programming. Each underestimated vulnerability indicates a hacking attempt to gain access to the site's database.

The security vulnerabilities in the websites also reflect the weaknesses in this site and its entire system Thus often any beginner seeks improves in his website to makes it safe.

2.3 Similar work done by others

The research team studied many websites similar to the project system

And here is an example HostedScan

2.3.1 HostedScsn

HostedScan provides vulnerability scanning, continuous monitoring, and risk management for your websites.

- 24 vulnerability scanning
- Automated alerts when something changes
- Comprehensive yet lightweight risk management
- Industry standard and open source scans, such as NMAP Port Scan.
- And here research team experience of HostedScan :

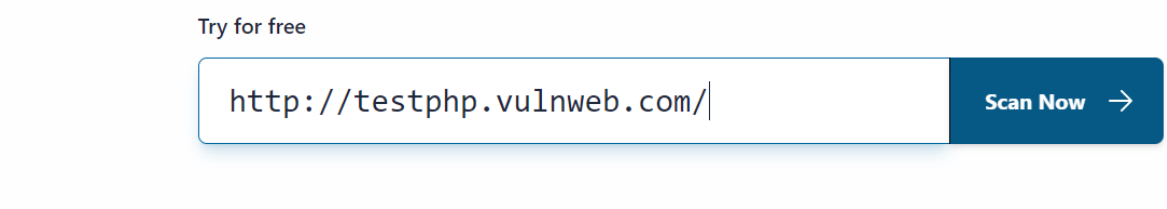


Figure 2.2

Then it request an email to send the scanning result

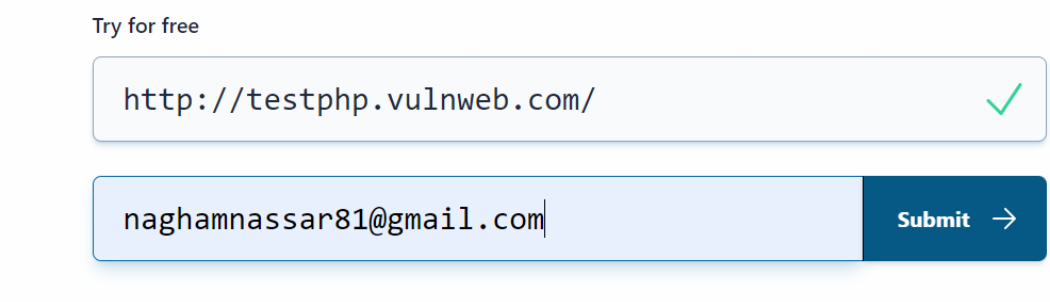


Figure 2.3

Here user receive a notification on email :

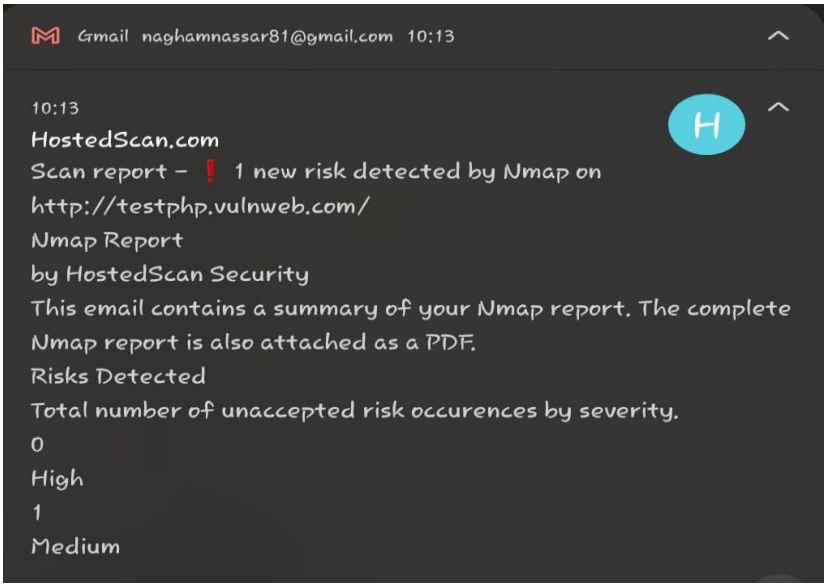


Figure 2.4

positives

Ease of use, the user interface is suitable for any user, the way to send a detailed result to the e-mail is good, it checks a large number of security vulnerabilities.

downsides

It takes more than 15 minutes to finish scanning , which is a relatively long time for some. Users are not allowed to give feedback.

2.4 Basic security background

In fact, the research team found a huge number of cybercrimes recently, after research and study a number of cybersecurity statistics 2019to 2022.

Studies indicate that cyber threats have become more dangerous and occur at a high rate, Arkoses labs study estimated that in august 2020 almost 445 million global cyber-attack had occurred . this statistic shows that this number is the double number of attacks comparing with 2019 attacks, this indicates the rapid increase in cybercrime on a global scale .adding to another study conducted by the austral ion cyber security center agency ,about 164 cybercrimes occur daily which is approximately one crime every 10 minutes .

Chapter 3

Design

- Introduction
- Context Diagram
- Use Case Diagram
- Use Case Description
- Activity Diagram
- Sequence Diagram

3.1 Introduction

This chapter includes an explanation of the design and structure of the project, where the components and the parts of the system will be detailed so that we give a complete idea for all parts of the system. In terms of its design and internal components.

3.2 Context Diagram

It shows the interactions between a system and the actors.

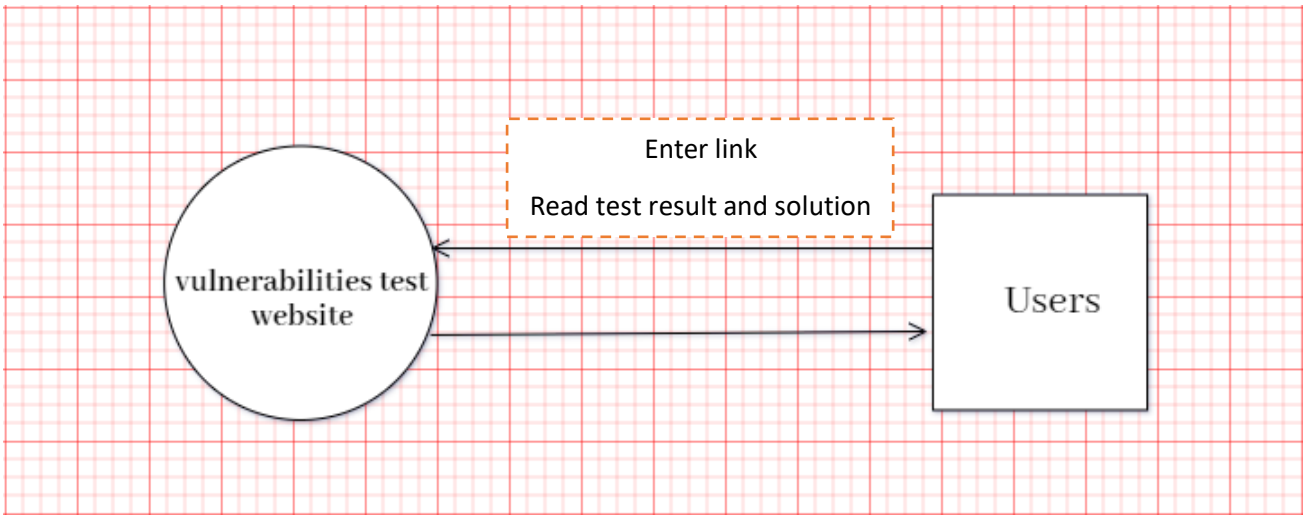


Figure 3.1 Context Diagram

3.3 Use Case Diagram

It explains the user's interactions with the system:

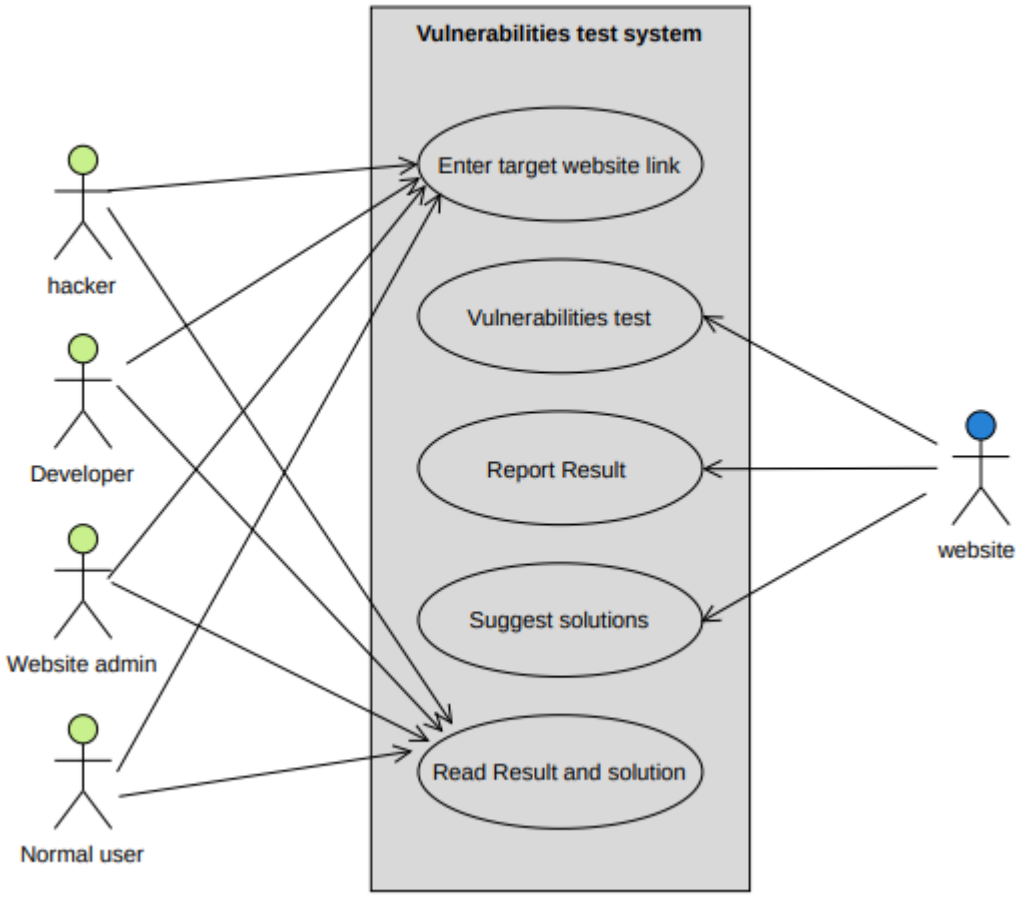


Figure3.2Use Case Diagram

3.4 Use Case Description

Use case	Security Vulnerabilities Test
Actors	Users (Hackers, Website admins, Developers, Normal Users of Internet) And Vulnerabilities Test Website.
Goal	Scan The target website from vulnerabilities.
Use Case Description	The project team website will scan the target website then show the result to the user
Pre-Condition	The user must copy link of target website.
Scenario	1. The user enter link of target website. 2. The user presses the "scan" button. 3. If the link is not valid, the website will show message "nothing to view". 4. If the link is valid, it will send via (post request) from API/create from Frontend to the backend to API/create. 5. The backend received the link as json (object). 6. The link passes to python functions for processing. 7. After processing, result sent via API to frontend (API response). 8. The user read security vulnerabilities testing result.
Post Condition	The User read testing result, and solution

Table3.1Use Case Description

3.5 Activity Diagram

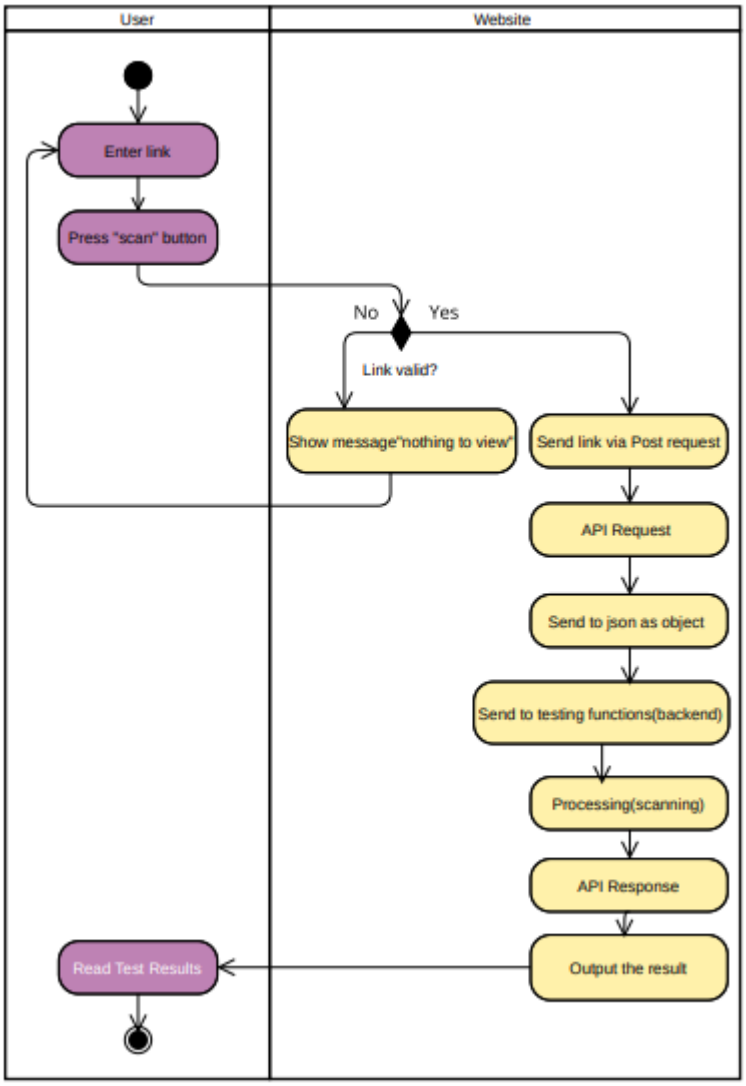


Figure3.3Activity Diagram

3.6 Sequence Diagram

It describes the main functions, and how the system objects (Frontend and Backend) work together:

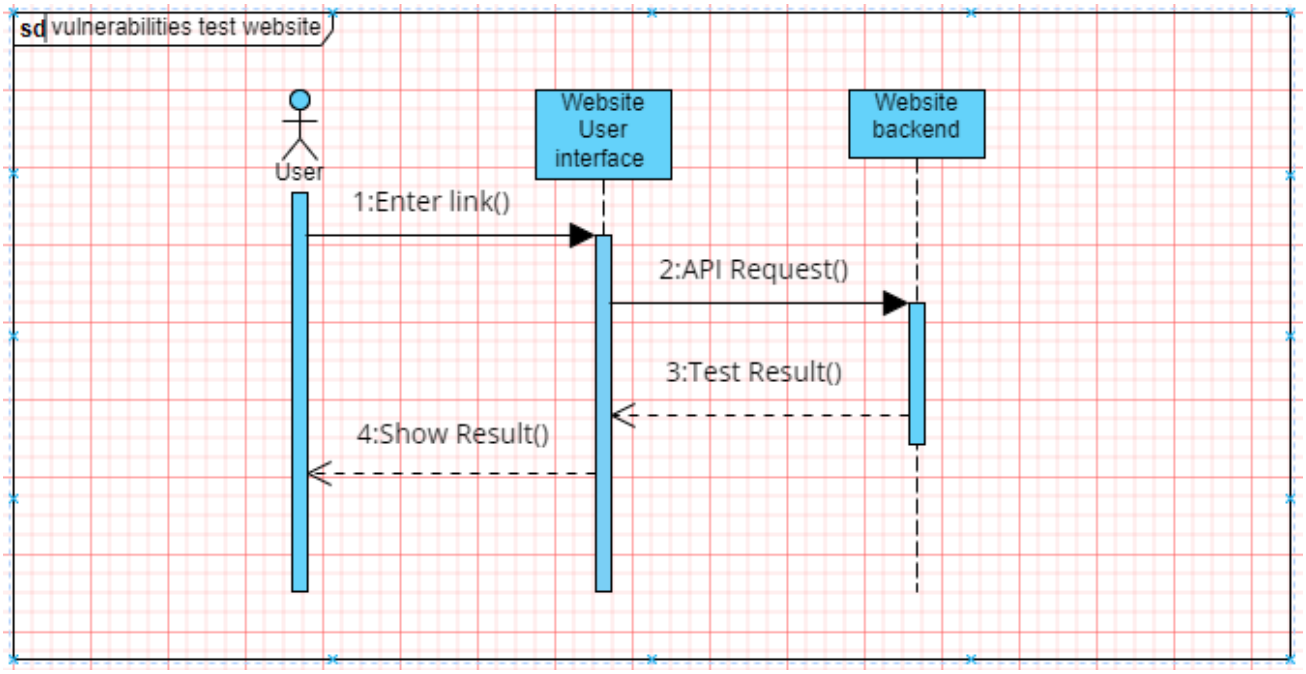


Figure3.4SequanceDiagram

Chapter 4

Software Implementation

- Introduction
- Software needed for development stage
- Backend programming
- System interface

4.1 Introduction

In this chapter, we will discuss how the system was built. The system implementation stage is one of the most important stages, through which the transition from the theoretical stage, which is the preparatory stage of the system to the practical stage, and then start programming and building the system. We will learn about the tools and programs necessary to develop the system and operate it fully and effectively, and the software that was used.

4.2 Software needed for development stage

Figure4.1software Needed For Development Stage

We first start writing down the project documentation using Google Tools (Google Docs, and Google Drive) then the diagrams that are attached to the documentation were created with Visual Paradigm. In developing the Website, React was used as a Frontend, and Python (Flask Framework) as a Backend. Bootstrap were needed in our Frontend code. Tasks were divided among the group members, and Scrum meetings were held with project group during the developing period. The code was written using Visual Studio Code (VS Code).

4.3 Backend programming

In the beginning, we started learning the basics of Python, and then we researched how the scanning process takes place by processing website files, and based on that, we created software codes that scan several security vulnerabilities in websites.

And we used the vscode program to write the code and we tested it on websites that are allowed to work on it.

4.4 System Interface (Frontend)

We used react framework, and used the principle of the component to facilitate modification and addition to the code ,we made several parts that serve our website, The website interface contain several pages, one for the open ports , another for vulnerabilities test result , and other pages that provide information about vulnerabilities that are scanned.

And we put a place to enter the link and a button to start the scanning process with instructions for the type of link to be entered.

Then this link is sent from the front via the API to the backend so that it can be processed and the result returned and displayed within less than a minute under good internet conditions.

We used the API to create Python flask,This is due to its suitability for the way we work.

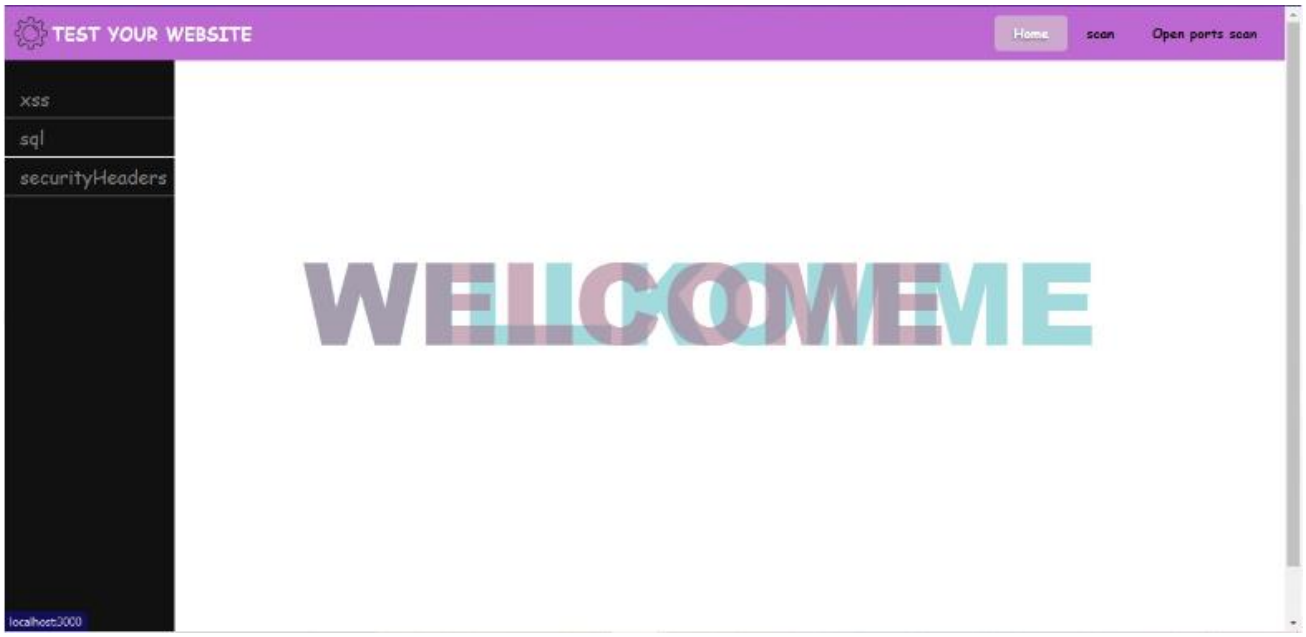


Figure4.2User Interface

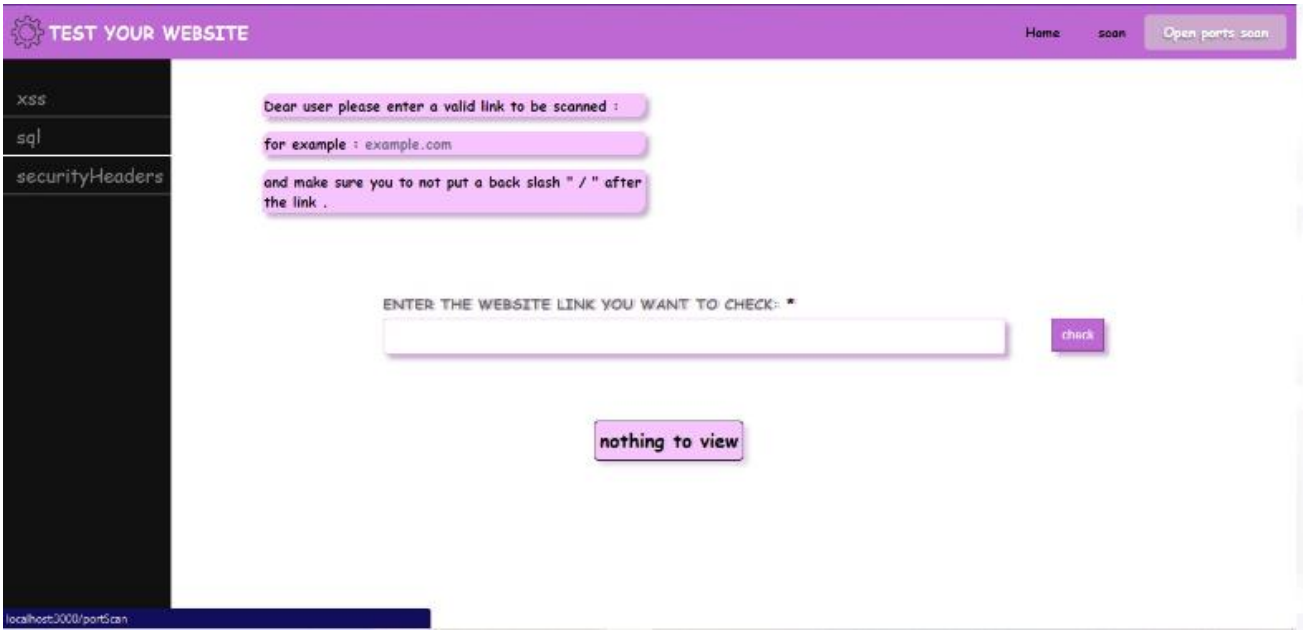


Figure4.3User Interface

Figure4.4Uer Interface

Chapter 5

Testing

- Introduction
- Validation
- API Request Testing

5.1 Introduction

In the stage of testing the system, we make sure that the system works correctly without any problems, and we also make sure that the functional and non-functional requirements of the project are completed, and that the system works with accuracy and high speed in completing tasks and displaying information. The stage of testing comes after the design and implementation of the system.

5.2 Validation

The only user input in the system is website link, it tested to ensure that the data entered by the user matches all conditions as follows:

- Customize the field in proportion to the entry
- The process will not be executed if wrong data is entered.

As for the output of the system, it is the result of testing the website of the link entered by the user for security vulnerabilities.

More than one website has been tested in the system and the results have been monitored to ensure that the functional, non-functional and security requirements of the system are met.

As table shows , implementation satisfies each requirements as listed in introduction part

Requirements Type	Requirements	Pass	Fail
Functional	Check if the link is valid or not	•	
	Vulnerabilities Test	•	
Security	SQL Injection Test	•	
	XSS Test	•	
	Scan Ports	•	
	Header of xxss	•	
	Header of nonsnif	•	
	Header of x-frame	•	
	Header of policy	•	
	Header of hsts	•	

Non-functional	Show an explanation of the vulnerabilities and solutions	•	
	Friendly user interface	•	
	Real time service	•	

5.3 API Request Testing

The project team tested 10 different websites and below are screenshots showing the results

ENTER THE WEBSITE LINK YOU WANT TO SCAN : *

https://www.hackthebox.com/ scan

is the header of xxss exist | False

is the header of X-Content-Type-Options (nonsnif) exist | False

is the header of x-frame exist | False

is the header of policy exist | False

is the header of hsts exist | False

is it vulnarable to xss | False

is it vulnarable to sql injction | no files to scan

ENTER THE WEBSITE LINK YOU WANT TO SCAN : *

http://www.itsecgames.com/ scan

is the header of xxss exist | False

is the header of X-Content-Type-Options (nonsnif) exist | False

is the header of x-frame exist | False

is the header of policy exist | False

is the header of hsts exist | False

is it vulnarable to xss | False

is it vulnarable to sql injction | no files to scan

ENTER THE WEBSITE LINK YOU WANT TO SCAN : *

https://google-gruyere.appspot.com/ scan

is the header of xxss exist | False

is the header of X-Content-Type-Options (nonsnif) exist | False

is the header of x-frame exist | False

is the header of policy exist | False

is the header of hsts exist | False

is it vulnarable to xss | False

is it vulnarable to sql injction | no files to scan

ENTER THE WEBSITE LINK YOU WANT TO SCAN : *

https://www.cybrhome.com/website/hellboundhackers.org/ scan

is the header of xxss exist | False

is the header of X-Content-Type-Options (nonsnif) exist | False

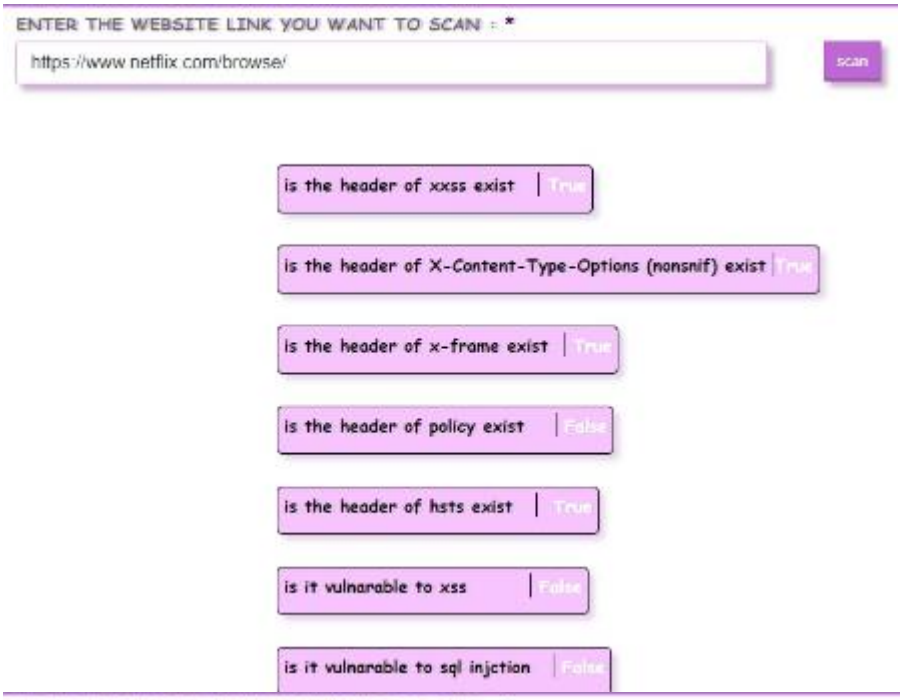
is the header of x-frame exist | False

is the header of policy exist | False

is the header of hsts exist | False

is it vulnarable to xss | False

is it vulnarable to sql injction | no files to scan


ENTER THE WEBSITE LINK YOU WANT TO SCAN : *
https://www.netflix.com/browse/
scan
is the header of xxss exist | True
is the header of X-Content-Type-Options (nonsnif) exist | True
is the header of x-frame exist | True
is the header of policy exist | False
is the header of hsts exist | True
is it vulnarable to xss | False
is it vulnarable to sql injction | False


ENTER THE WEBSITE LINK YOU WANT TO SCAN : *
https://www.facebook.com/
scan
is the header of xxss exist | True
is the header of X-Content-Type-Options (nonsnif) exist | True
is the header of x-frame exist | True
is the header of policy exist | False
is the header of hsts exist | True
is it vulnarable to xss | False
is it vulnarable to sql injction | False


ENTER THE WEBSITE LINK YOU WANT TO SCAN : *
https://www.pinterest.com/
scan
is the header of xxss exist | True
is the header of X-Content-Type-Options (nonsnif) exist | True
is the header of x-frame exist | True
is the header of policy exist | True
is the header of hsts exist | True
is it vulnarable to xss | False
is it vulnarable to sql injction | no files to scan


ENTER THE WEBSITE LINK YOU WANT TO SCAN : *
https://www.bing.com/
scan
is the header of xxss exist | False
is the header of X-Content-Type-Options (nonsnif) exist | False
is the header of x-frame exist | False
is the header of policy exist | False
is the header of hsts exist | True
is it vulnarable to xss | False
is it vulnarable to sql injction | False

- Open ports scanning for same websites:

Chapter 6

Conclusion

- Recommendations
- Future work
- References

6.1 Recommendations

In light of the technological development and electronic crimes that our current era is going through, we advise students, website developers, and small business owners, who need to use websites frequently, to take advantage of this system for ease of dealing with it, as it facilitates the safe and comfortable browsing process for them, through one simple step.

We recommend that the system be used by the scope of the system at least once, noting the problems that result from using the system and working on resolving them.

6.2 Future work

In the future, we are looking forward to adding many features to the current system such as:

- Adding a live chatting feature that facilitates the communication between the user and our website developers.
- Adding a notification feature whenever a new security vulnerability is detected globally.
- Allowing the user to create an account on our website in order to save the examination results and not have to repeat the examination process each time.
- Adding some courses on cybersecurity, encryption and other security topics.
- Expanding the website to be able to scan more than five vulnerabilities.

المراجع

https://github.com.(2022) .

https://www.w3schools.com.(2022) ./

MOUSA FARAJALLAH .(2022 ,8 15) .LIGHTWEIGHT CHAOTIC BLOCK CIPHER FOR IOT APPLICATIONS . *Journal of Theoretical and Applied Information Technology*.5436-5426 الصفحات ،

Mousa Farajallah, Nabil Arman, Wassim Hamidouche Iyad Hraini .(2021 ,11 30) .Joint crypto-compression based on selective encryption for WMSNs .*IEEE Access*.161282-161269 الصفحات ،

Mousa Farajallah ،Guillaume Gautier ،Wassim Hamidouche ،Olivier Déforges و ،Safwan El Assad ,2 7) . .(2022Selective Encryption of the Versatile Video Coding Standard .*IEEE Access* - 21821 الصفحات ، .21835

Sultan Badran ،Nabile Arman و ،Mousa Farajallah .(2021) .An Efficient Approach for Secure Data Outsourcing using Hybrid Data Partitioning *2021 .International Conference on Information Technology (ICIT)*.423-418 الصفحات ،

6.3 Biography

- https://www.youtube.com/
- https://www.thepythoncode.com/
- https://reactjs.org/
- https://hostedscan.com/
- https://iopscience.iop.org/article/10.1088/1757-899X/407/1/012081/meta
- https://www.websiterating.com/ar/research/cybersecurity-statistics-facts/
- https://flask.palletsprojects.com/en/2.2.x/
- https://developer.mozilla.org/en-US/