

# Web Enumeration Tool

BSc. Hons. Ethical Hacking and Cybersecurity, Softwarica College of IT and E-commerce ST5062CEM Programming and Algorithms 2

Dhirendra Bhatta Aug 08, 2023

Table of Contents

[Introduction 5](#_bookmark0)

[Aim 5](#_bookmark1)

[Objectives 5](#_bookmark2)

[Problem Statement 6](#_bookmark3)

[Features and Functionalities 6](#_bookmark4)

[Technology Detection 6](#_bookmark5)

[Exploit Search 6](#_bookmark6)

[Directory Fuzzing 7](#_bookmark7)

[Subdomain Fuzzing 7](#_bookmark8)

[File Fuzzing 7](#_bookmark9)

[DNS Enumeration 7](#_bookmark10)

[Port Scanning 7](#_bookmark11)

[Email Address Extraction 7](#_bookmark12)

[WHOIS Record 7](#_bookmark13)

[SSL Certificate Information 8](#_bookmark14)

[Generate a Comprehensive PDF Report 8](#_bookmark15)

[Scope of the Project 8](#_bookmark16)

[Development Methodology 9](#_bookmark17)

[Agile Methodology and Waterfall Methodology 9](#_bookmark18)

[Tools and Technology 9](#_bookmark19)

[Design 9](#_bookmark20)

[Architecture 9](#_bookmark21)

[Class Diagram 9](#_bookmark22)

[Runtime Architecture 10](#_bookmark24)

[Coding and Implementation 14](#_bookmark31)

[Testing 20](#_bookmark40)

[Version Control 23](#_bookmark44)

[Conclusion 23](#_bookmark45)

Table of Figure

[Figure 1: Class Diagram of Web enum 10](#_bookmark23)

[Figure 2: The program asks for a target 11](#_bookmark25)

[Figure 3: Program while running 11](#_bookmark26)

[Figure 4: Program while running searching for subdomain 12](#_bookmark27)

[Figure 5: Program while running and performing DNS lookup 12](#_bookmark28)

[Figure 6: files created by the program 13](#_bookmark29)

[Figure 7: pdf created by the program 14](#_bookmark30)

[Figure 8: Import of Libraries. 15](#_bookmark32)

[Figure 9: Functions define 15](#_bookmark33)

[Figure 10: Function for Fuzzing 16](#_bookmark34)

[Figure 11: Function to capture Screenshot. 17](#_bookmark35)

[Figure 12: Function for DNS and port enum 17](#_bookmark36)

[Figure 13: Function to get email 18](#_bookmark37)

[Figure 14: Function to get whois record and SSL certificate. 19](#_bookmark38)

[Figure 15: Function to generate report. 20](#_bookmark39)

[Figure 16: Unit testing of get domain and other function 21](#_bookmark41)

[Figure 17: Unit testing of search exploit. 22](#_bookmark42)

[Figure 18: Successful test pass. 23](#_bookmark43)

# Introduction

Web enumeration is an important step in ethical hacking and cyber security. It involves gathering information about a web application or website that is the target to find security risks and vulnerabilities. The goal of this project is to make a web enumeration tool that automates different enumeration tasks. This will make it easier for cybersecurity professionals and ethical hackers to do thorough assessments of target URLs. This can also help people who aren't proficient with technology learn more about their website.

# Aim

The goal of this project is to make a web enumeration tool that makes it easier and faster to gather information about a specific website or web application. The main goal of the tool is to help security professionals find any vulnerabilities, weaknesses, or security risks that might be linked to the target URL. By automating the process of web enumeration, the tool aims to improve the speed, accuracy, and completeness of security assessments. This will help improve the security of web-based systems. By cutting down on the time needed for enumeration, we can find bugs faster and make our website safer.

# Objectives

The main goal of the tool is to make a powerful and easy-to-use web enumeration tool that automates the process of getting information about web applications or websites that are being targeted. The tool uses various enumeration techniques quickly and well, reducing the amount of work that cybersecurity professionals have to do by hand. The tool tries to find out exactly what programming languages, frameworks, and content management systems are being used in the target URL. The tool helps with vulnerability assessment and risk reduction by looking for known exploits and holes in these technologies. It will also use effective fuzzing techniques to find hidden or unprotected resources, like directories and files, that could be security risks.

Additionally, the tool will perform DNS enumeration to retrieve DNS records and port scanning to identify open ports and associated services, providing insights into the network configuration.

Retrieving WHOIS records and SSL certificate information further enhances the understanding of domain ownership and security measures in place. To facilitate easy analysis and reporting, the tool will generate a comprehensive PDF report summarizing the collected information.

# Problem Statement

The manual process of web enumeration for security assessments is time-consuming, labor- intensive, and prone to human errors, hindering the efficiency and accuracy of identifying potential vulnerabilities and security risks in web applications. Security professionals often face challenges in detecting the underlying technologies, searching for known exploits, conducting comprehensive fuzzing, and retrieving essential information like DNS records and SSL certificates. Furthermore, the lack of an automated and standardized approach for web enumeration leads to inconsistencies in results and difficulties in generating comprehensive reports.

Our goal is to develop a comprehensive and automated web enumeration tool that surpasses manual enumeration processes. Our tool should ensure accuracy, generate detailed reports, and help detect vulnerabilities while enhancing web application security.

# Features and Functionalities

Features are distinctive characteristics or capabilities of software or tools that provide specific functionalities to users. Functionalities refer to the tasks and operations that the tool can perform based on its features. The web enumeration tool will offer the following features and functionalities: **Technology Detection**

The tool will accurately detect the technologies used in the target URL, including programming languages, frameworks, content management systems, web servers, and more.

# Exploit Search

It will search for known exploits and vulnerabilities associated with the identified technologies by accessing relevant databases and repositories.

# Directory Fuzzing

The tool will perform directory fuzzing to discover hidden or unprotected resources by trying a wide range of common directory names.

# Subdomain Fuzzing

It systematically explores various subdomains by appending common subdomain names, helping to uncover additional entry points or services hosted on different subdomains.

# File Fuzzing

It systematically tries common file names and extensions on the web server, revealing files that may contain sensitive information or pose security risks if accessed by unauthorized users.

# DNS Enumeration

It fetches DNS records, including A, AAAA, MX, and NS records, to determine the target's domain name resolution, mail servers, and authoritative name servers.

# Port Scanning

It scans a range of ports on the target's IP address to determine which ports are open and the services running on them, helping in understanding the network configuration and potential entry points for attackers.

# Email Address Extraction

It will parse the content of the web application and identify valid email addresses, providing insights into potential points of contact and aiding in email security assessment.

# WHOIS Record

The tool retrieves WHOIS records to obtain domain ownership and registration details. It fetches domain registration information, including registrant contact details, registration dates, and administrative contacts, providing valuable insights into the domain's ownership.

# SSL Certificate Information

It retrieves SSL certificate details, including certificate issuer, expiration date, and encryption strength, to evaluate the SSL security of the target URL.

# Generate a Comprehensive PDF Report

It compiles all collected information, including technology details, identified vulnerabilities, DNS records, port scanning results, WHOIS data, and SSL certificate information, into a comprehensive PDF report for easy analysis and reporting.

By incorporating these features and functionalities, the web enumeration tool aims to provide a comprehensive, efficient, and user-friendly solution for security professionals to conduct web application security assessments effectively.

# Scope of the Project

The scope of the web enumeration tool is to provide a comprehensive and efficient solution for conducting web application security assessments. The tool aims to assist security professionals in identifying potential vulnerabilities, misconfigurations, and security weaknesses within web applications. It will offer a range of features and functionalities, including technology detection, exploit search, directory, subdomain, file fuzzing, DNS enumeration, port scanning, WHOIS record retrieval, SSL certificate information, email address extraction, and PDF report generation.

The tool is designed to work with various types of URLs, accommodating both HTTP and HTTPS protocols, making it versatile for different web applications. Leveraging builtwith and relevant APIs, it will accurately detect the technologies used in the target web application, allowing for targeted exploit

searches based on the identified technologies. Systematic fuzzing for directories, subdomains, and files will help uncover hidden resources and potential entry points for attackers.

# Development Methodology

The development methodology for the web enumeration tool will follow an iterative and incremental approach, combining elements of Agile and Waterfall methodologies. The goal is to ensure efficient development, frequent feedback, and continuous improvement while maintaining a structured and well-documented process.

# Agile Methodology and Waterfall Methodology

Agile methodology focuses on iterative and incremental development, collaboration, and responsiveness to changing requirements. Key aspects of Agile that have been applied to the web enumeration tool include Iterative Development and Continuous Improvement.

Waterfall methodology is a linear and structured approach to development, where each phase is completed before moving to the next. For the web enumeration tool, certain aspects of the Waterfall methodology have been incorporated to ensure a well-planned and documented development process. i.e., Requirements Gathering, Design and Planning, and testing.

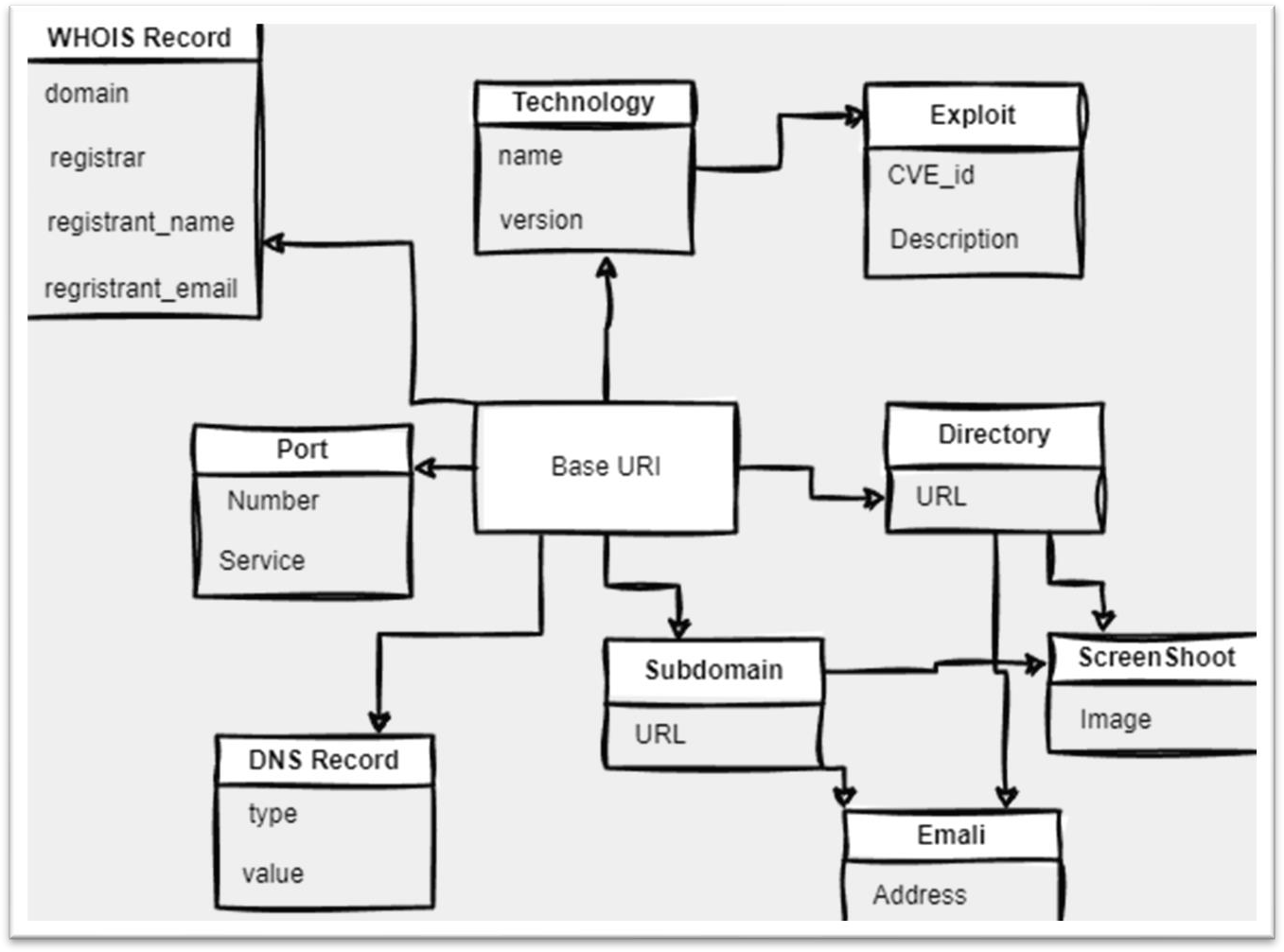
# Tools and Technology

The web enumeration tool is developed using Python as the primary programming language, complemented by essential libraries and modules such as Requests, Builtwith, Selenium, dns.resolver, Whois, SSL, and ReportLab. Version control is managed using Git, while Visual Studio code is used as IDEs. These tools and technologies ensure an efficient and effective development process, resulting in a reliable and valuable web enumeration tool.

# Design

# Architecture

## Class Diagram

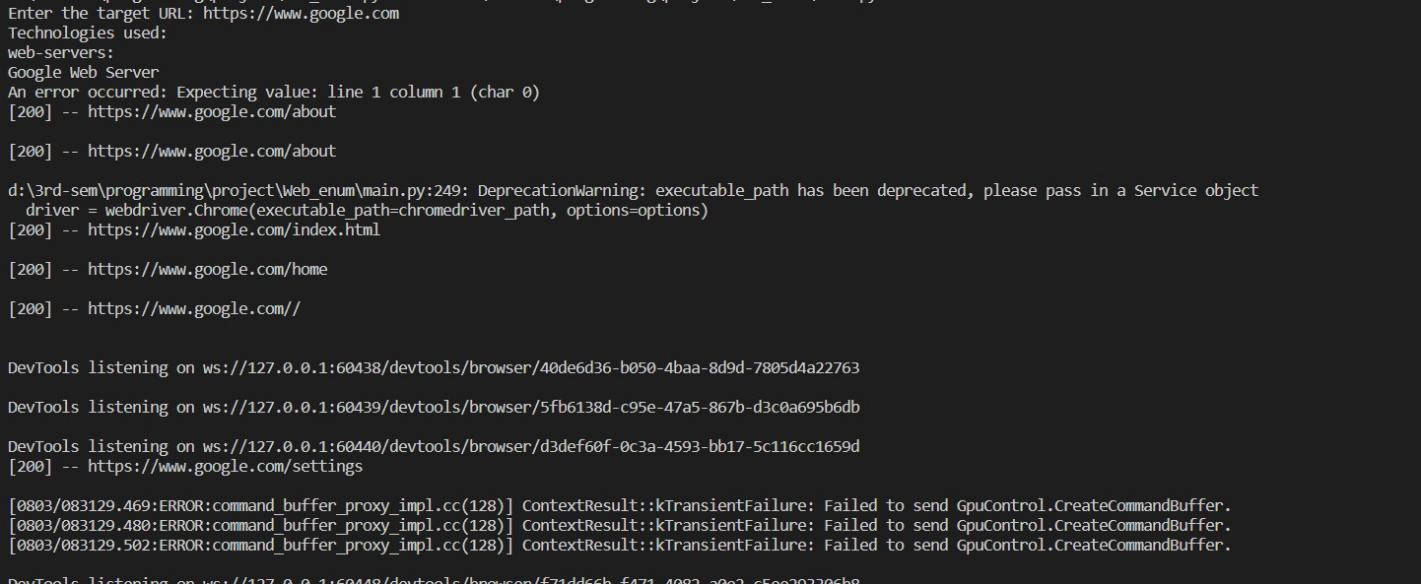


*Figure 1: Class Diagram of Web enum*

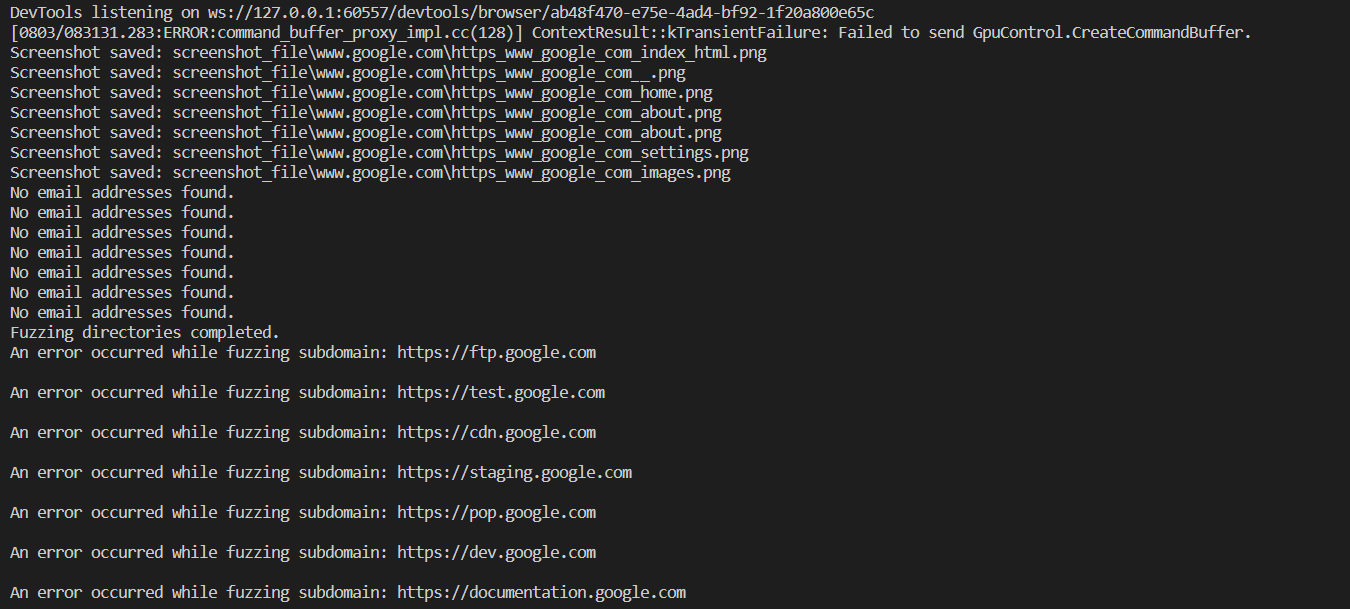
The Class Diagram for the web enumeration tool represents the classes, attributes, and methods involved in the tool's implementation.

# Runtime Architecture

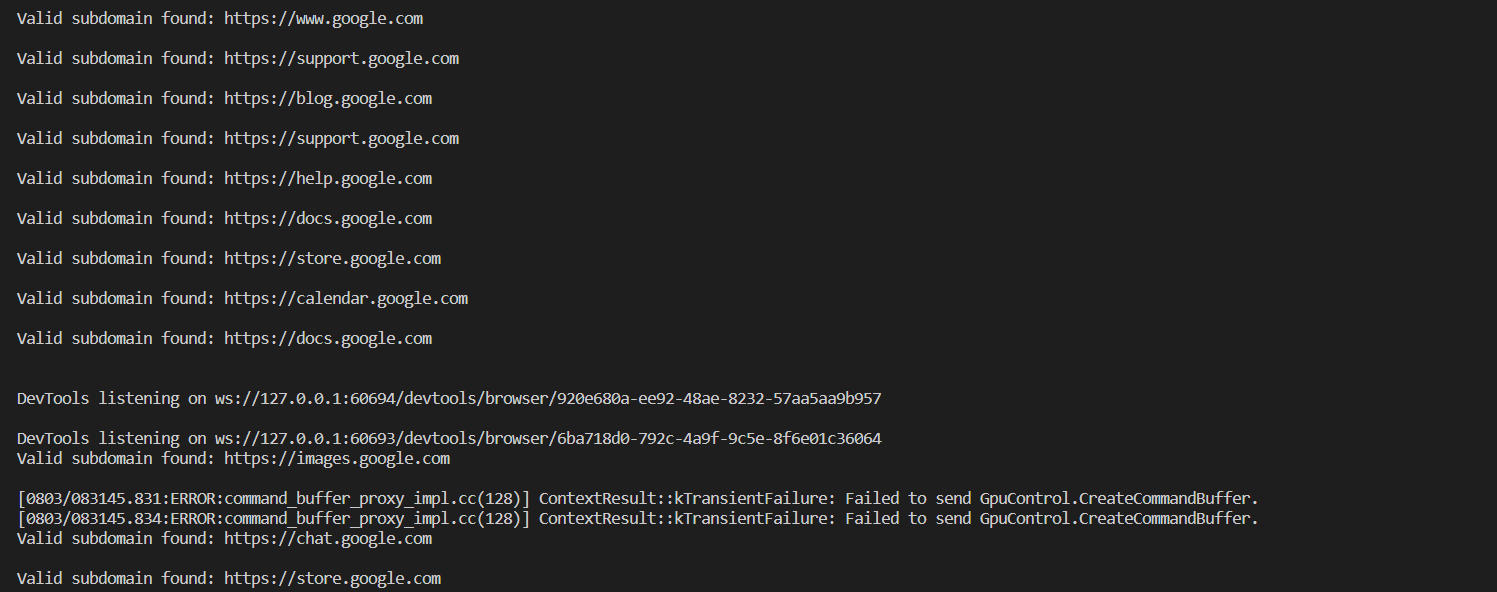
The Dynamic Architecture of the web enumeration tool focuses on the runtime behavior and interactions between various components during the execution of the tool. It describes how different modules and functionalities collaborate to achieve the intended functionality of the tool.



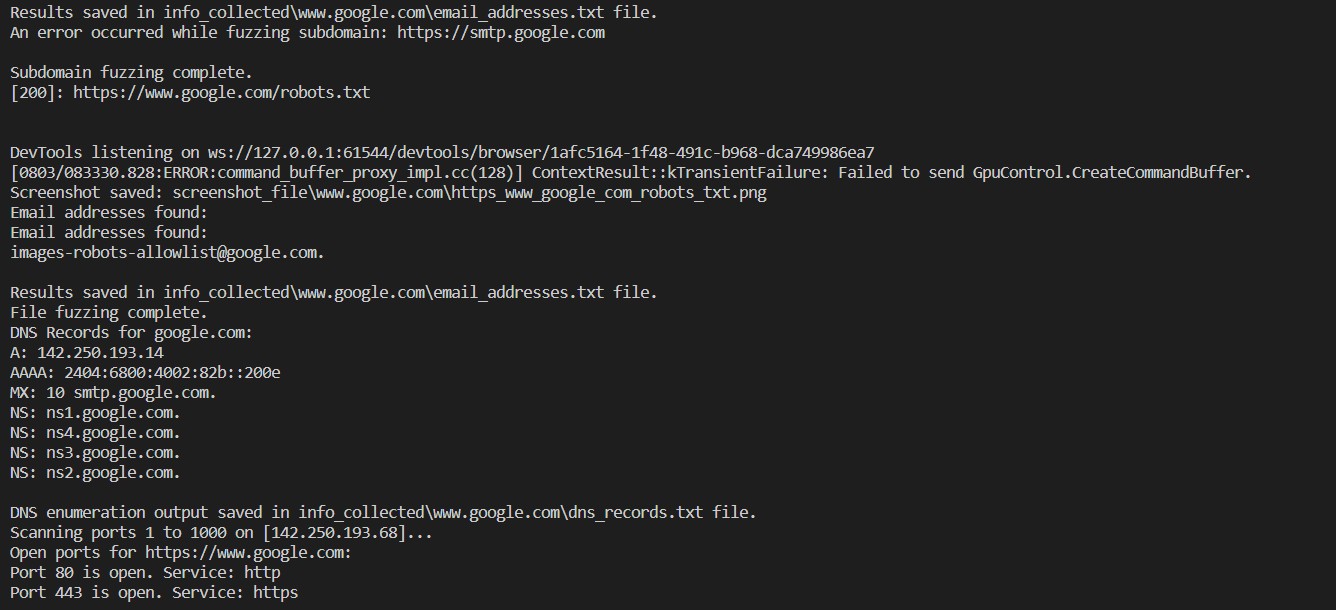
*Figure 2: The program asks for a target.*



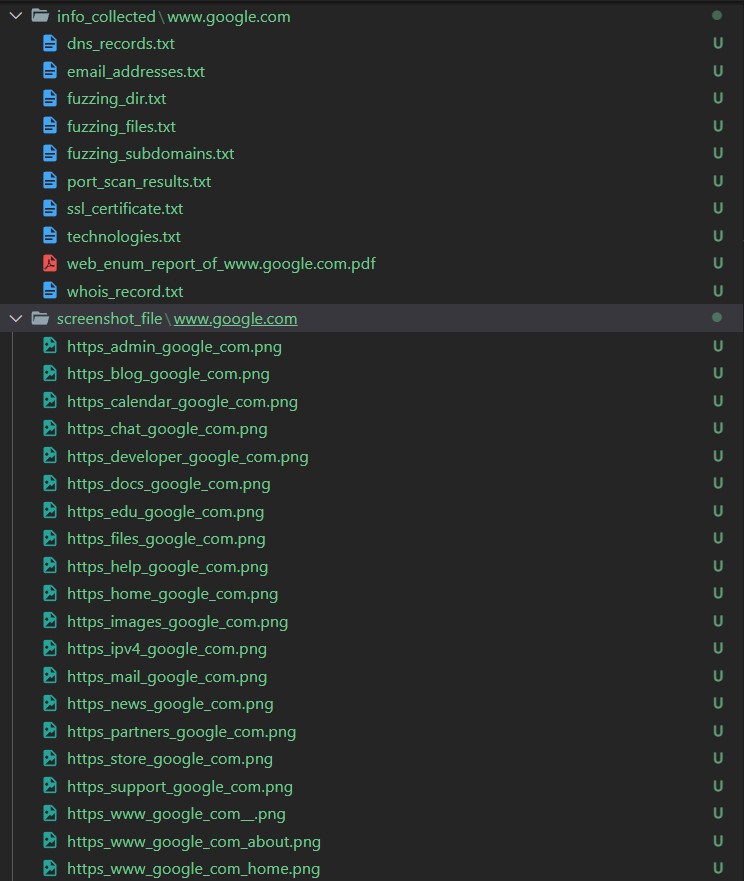
*Figure 3: Program while running.*



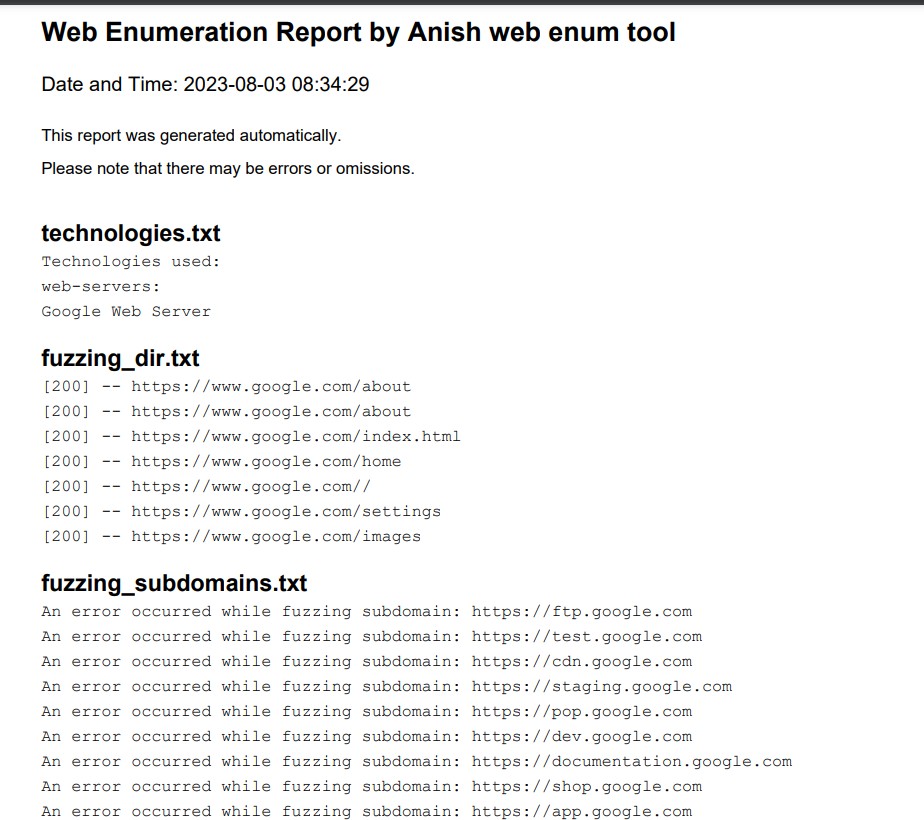
*Figure 4: Program while running searching for subdomain.*



*Figure 5: Program while running and performing DNS lookup.*

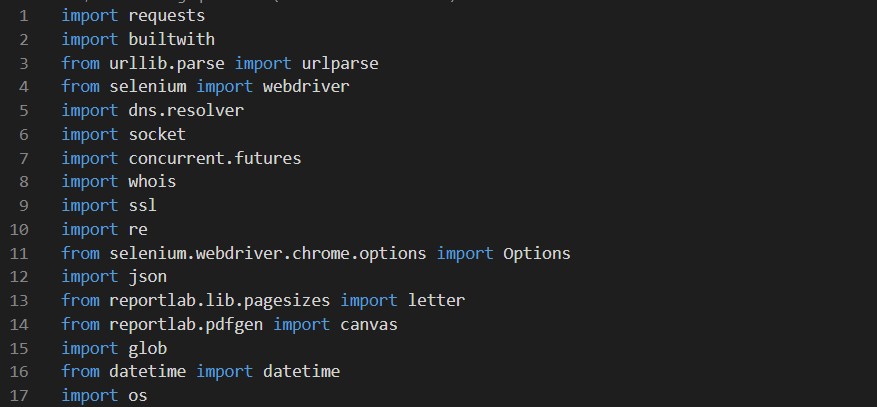


*Figure 6: files created by the program.*



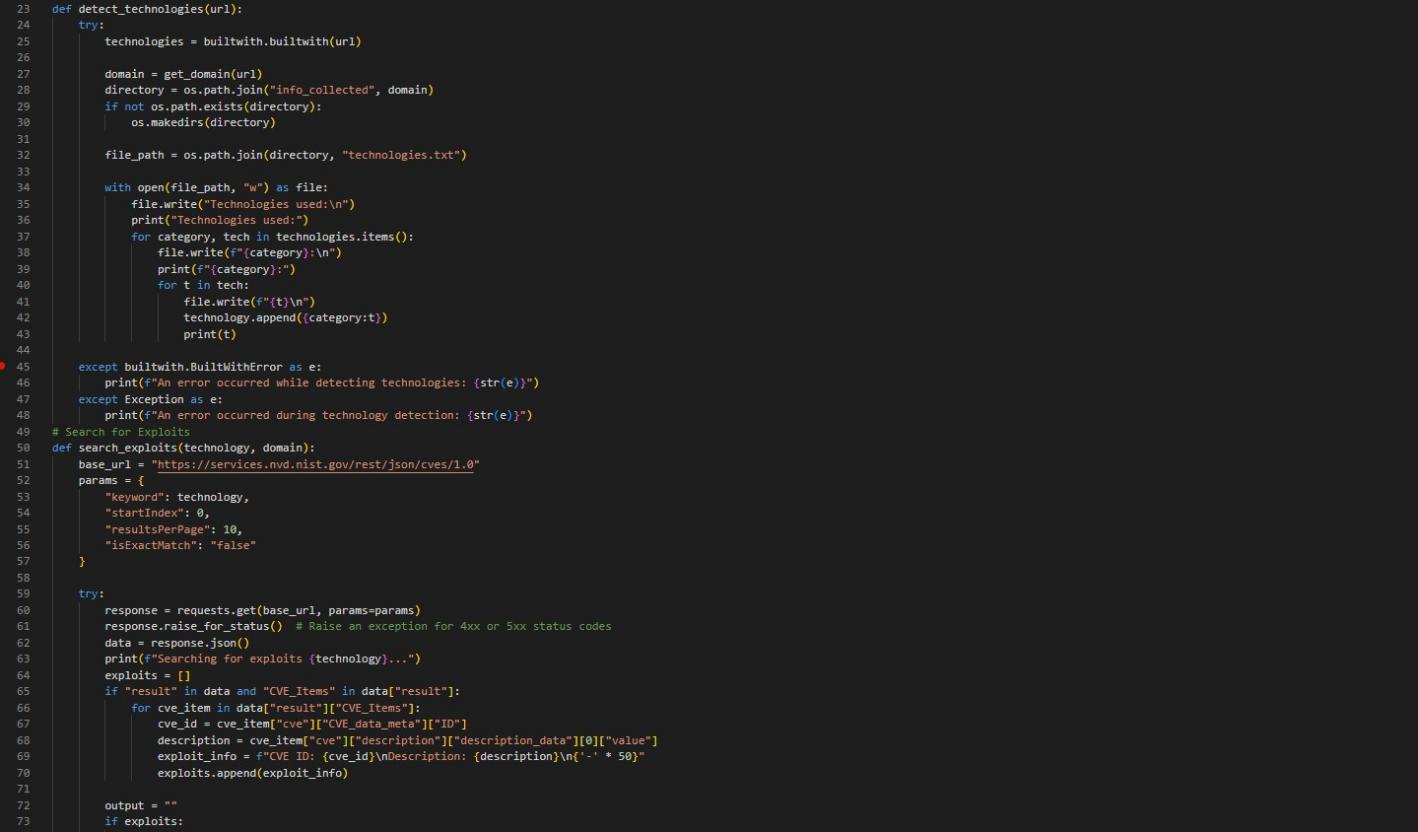
*Figure 7: pdf created by the program*

# Coding and Implementation



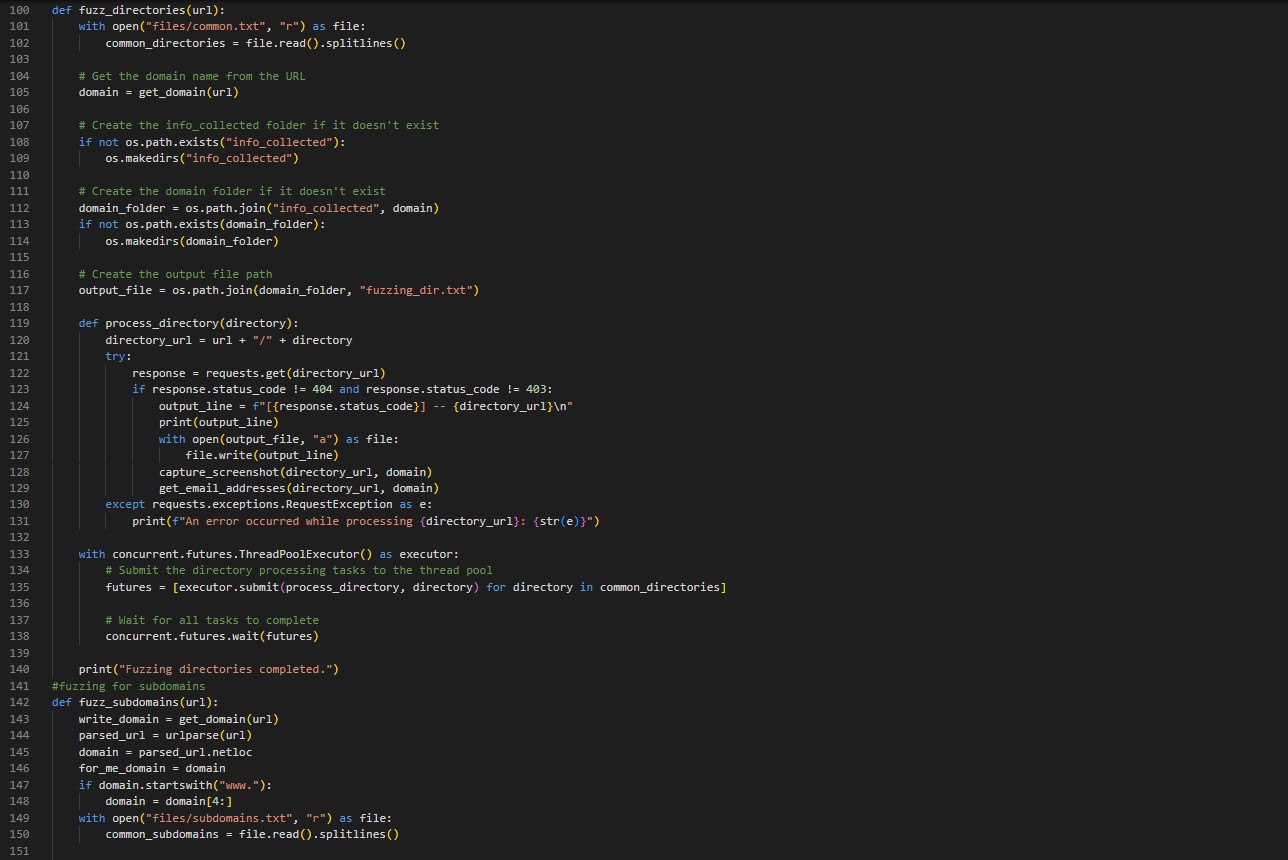
*Figure 8: Import of Libraries.*

The following libraries were imported.



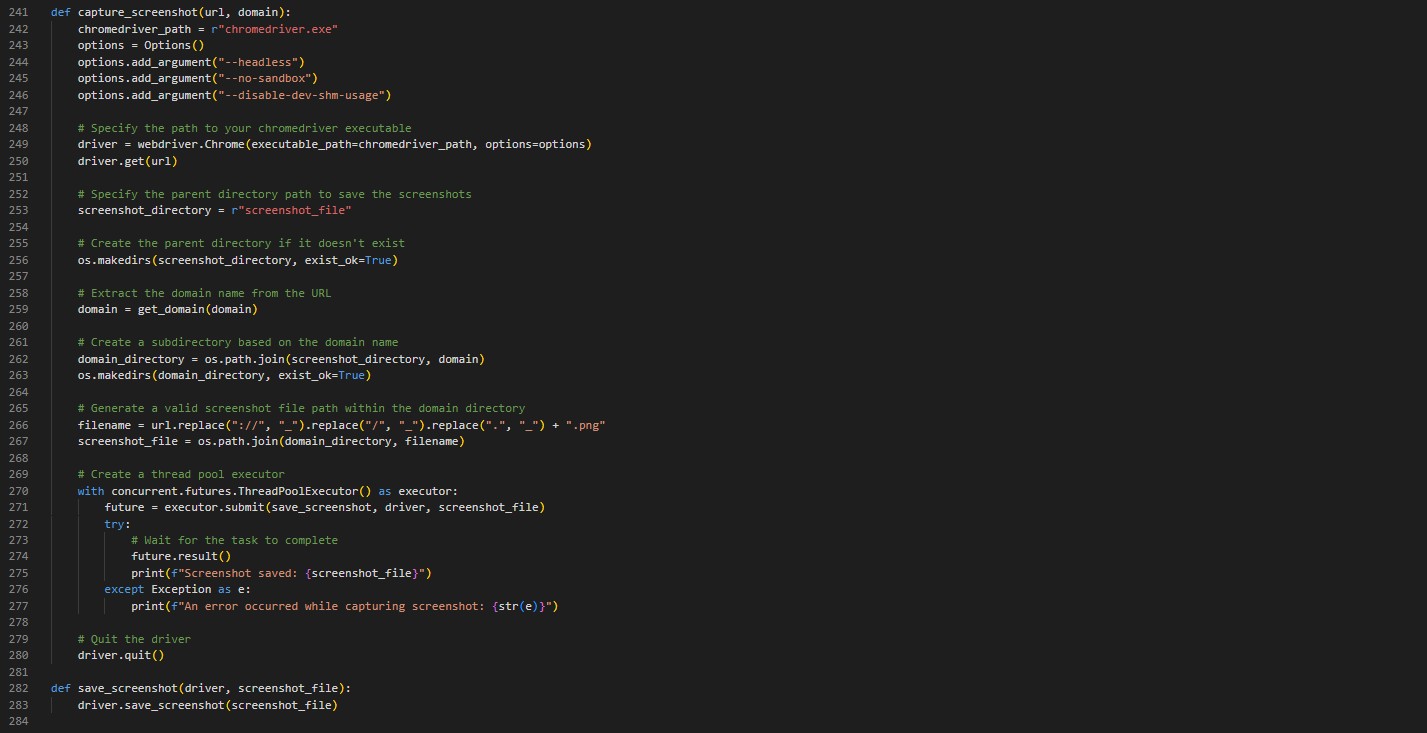
*Figure 9: Functions define*

These functions will detect the technology used and exploit related to those technologies.



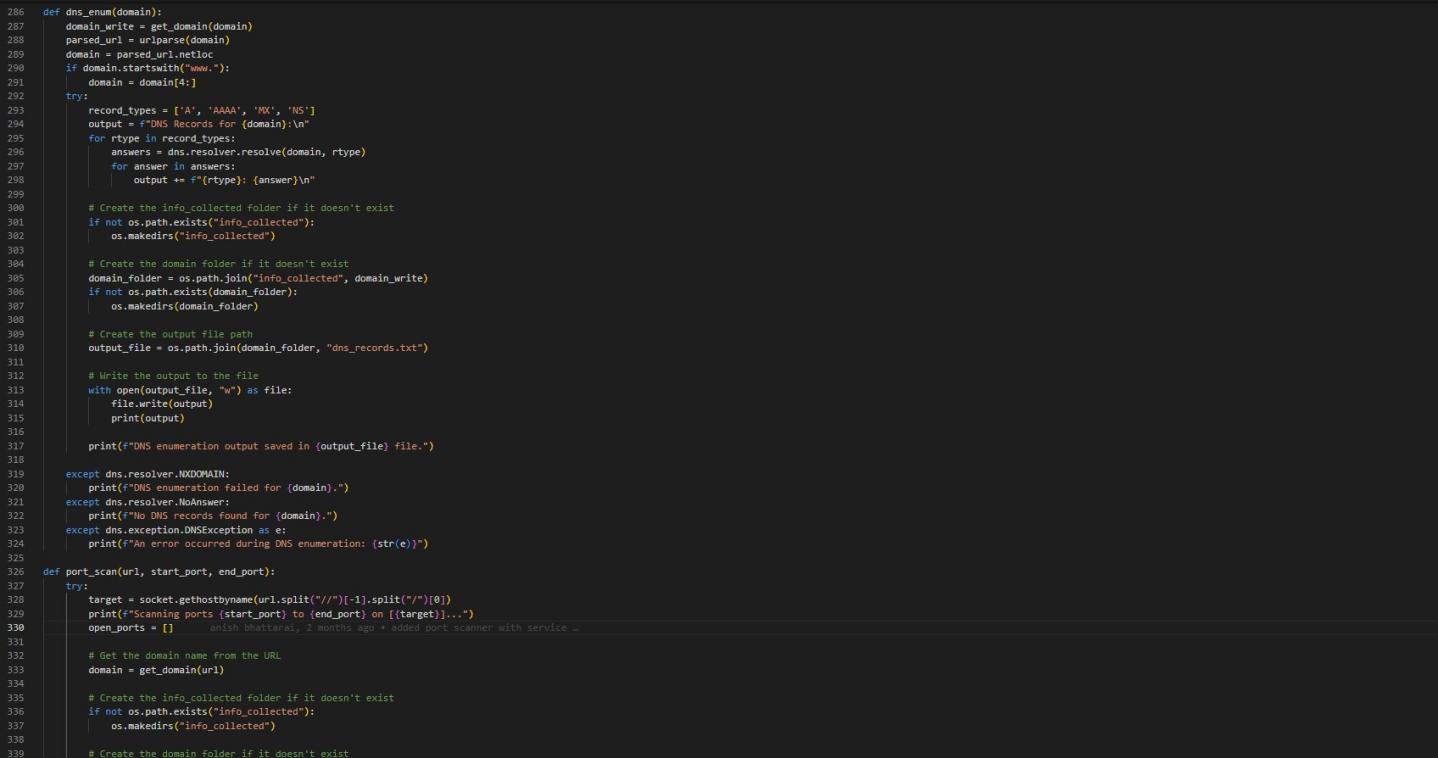
*Figure 10: Function for Fuzzing.*

These functions will fuzz for directories and subdomains as well as files.



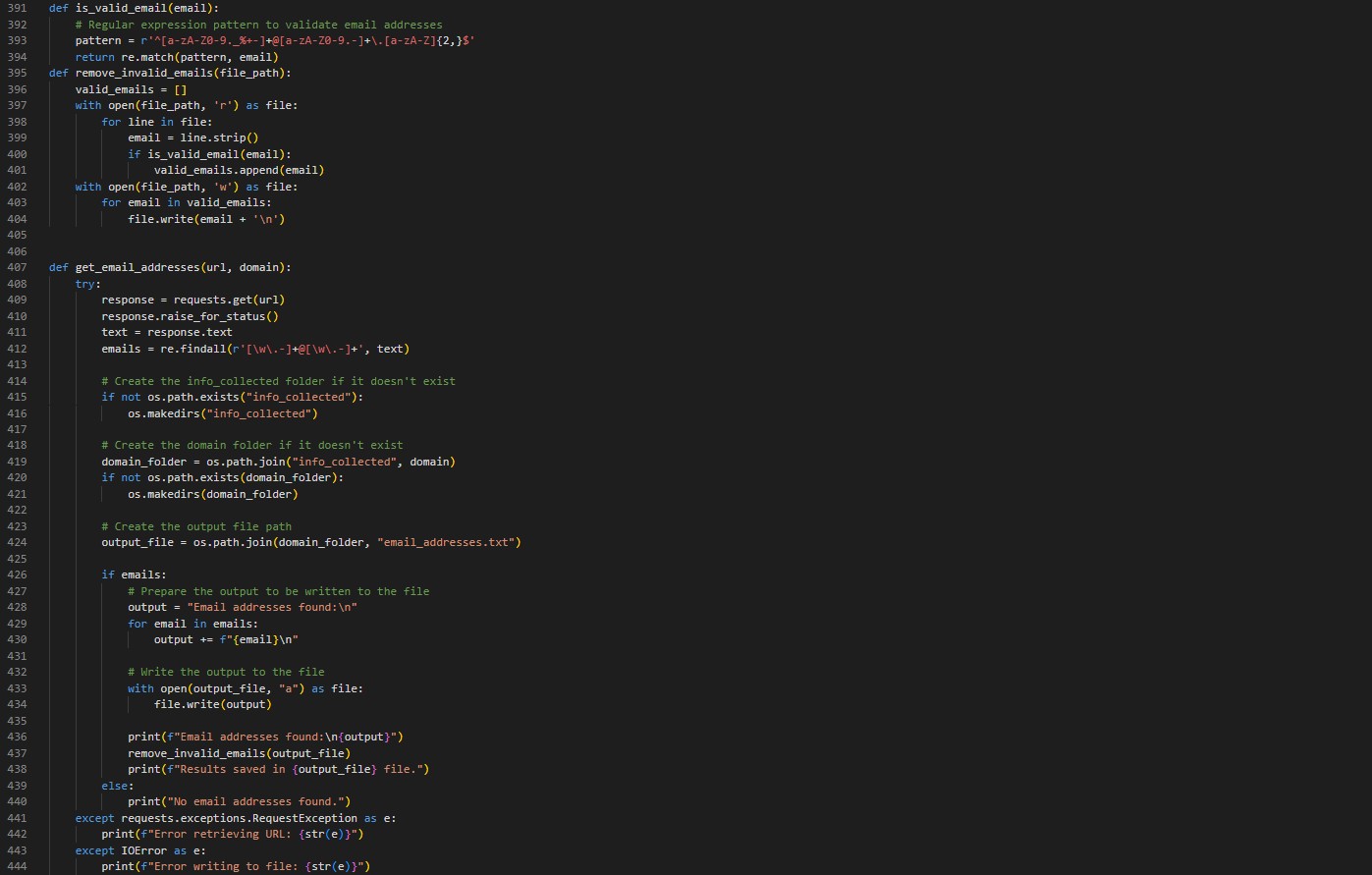
*Figure 11: Function to capture Screenshot.*

This function will capture the screenshot of the URL and save it in a file.



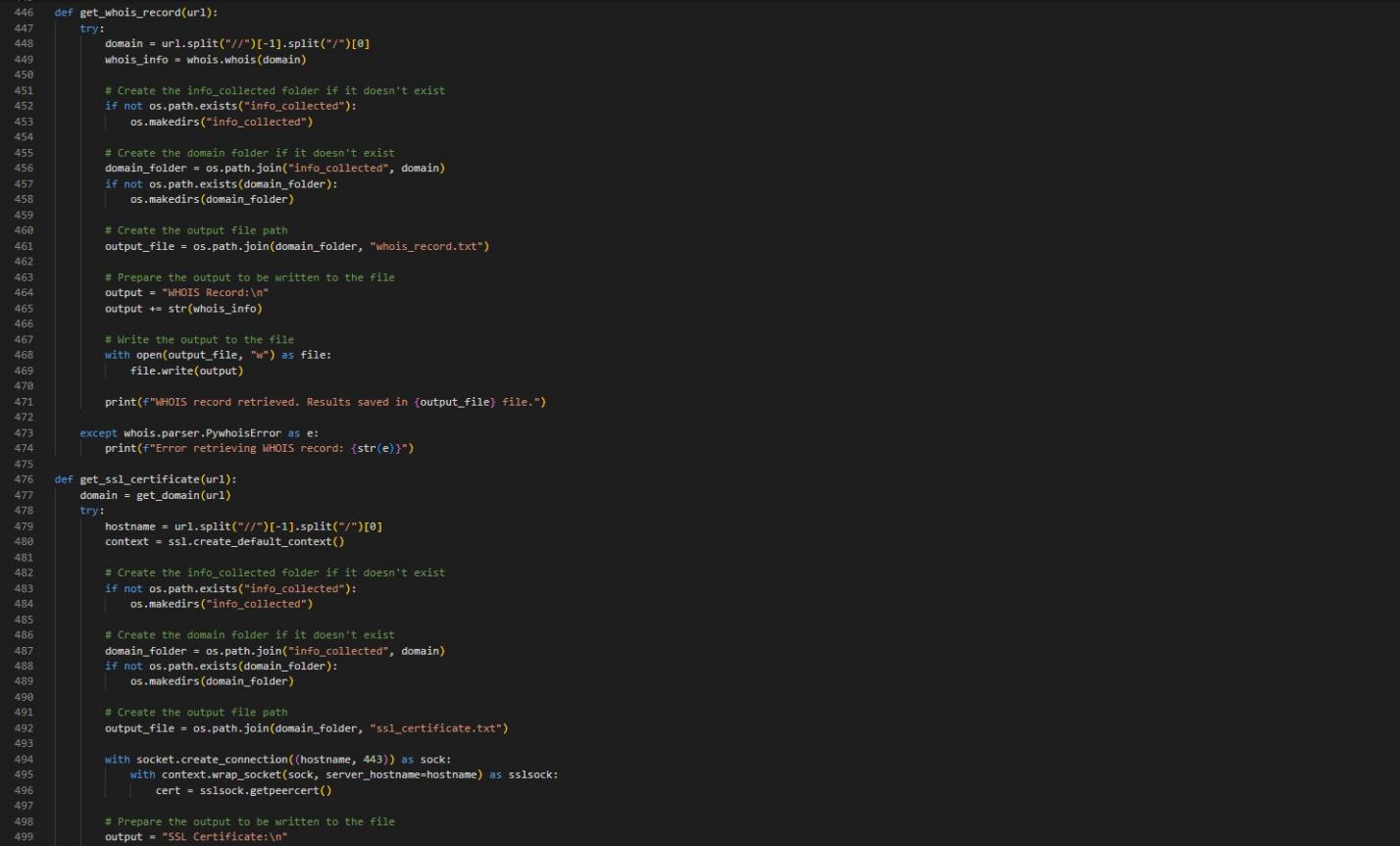
*Figure 12: Function for DNS and port enum.*

These functions will do DNS queries and scan for open ports.



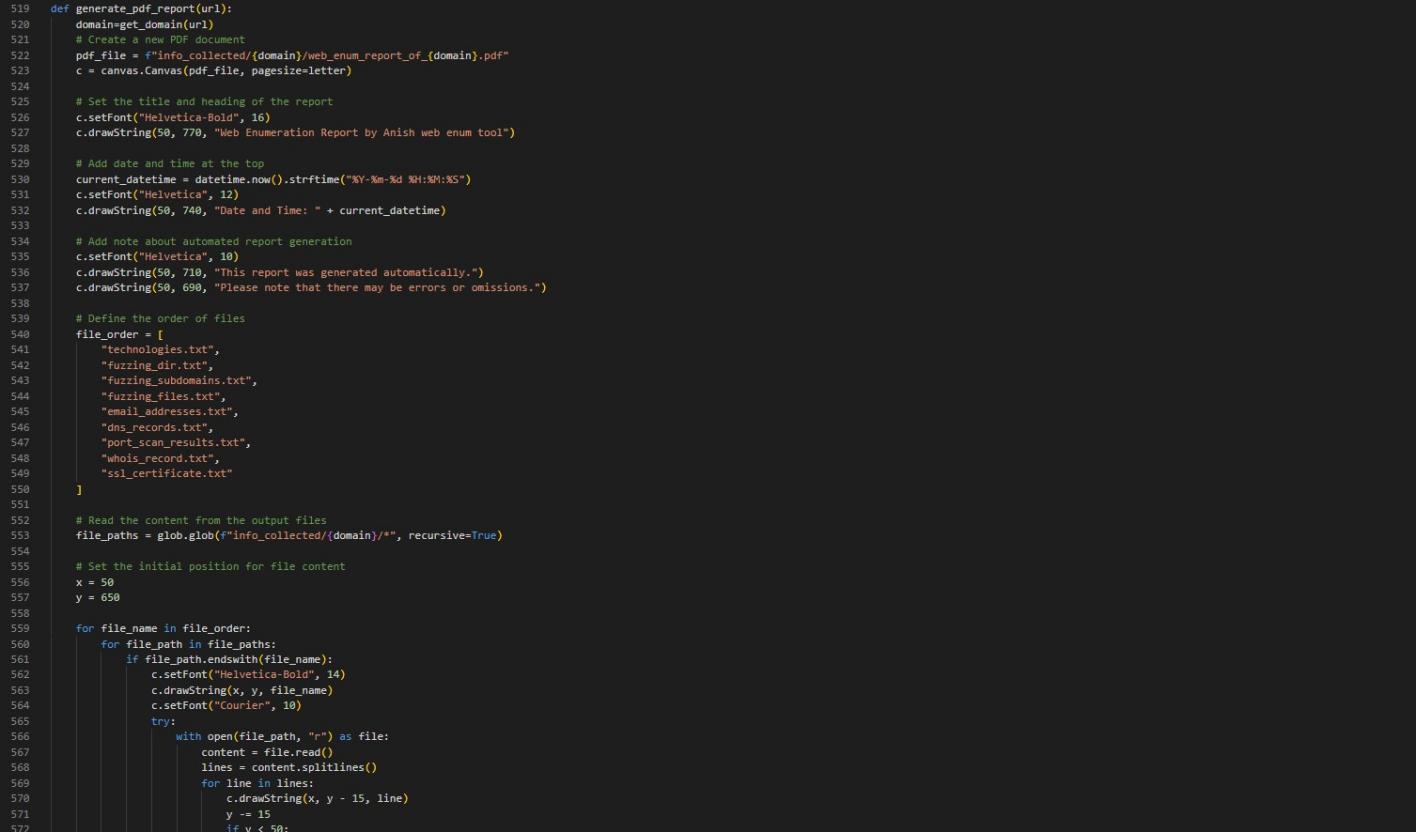
*Figure 13: Function to get email.*

These functions will find an email and also verify if it is valid or not.



*Figure 14: Function to get whois record and SSL certificate.*

These functions will get the whois record and SSL certificate of the given domain.

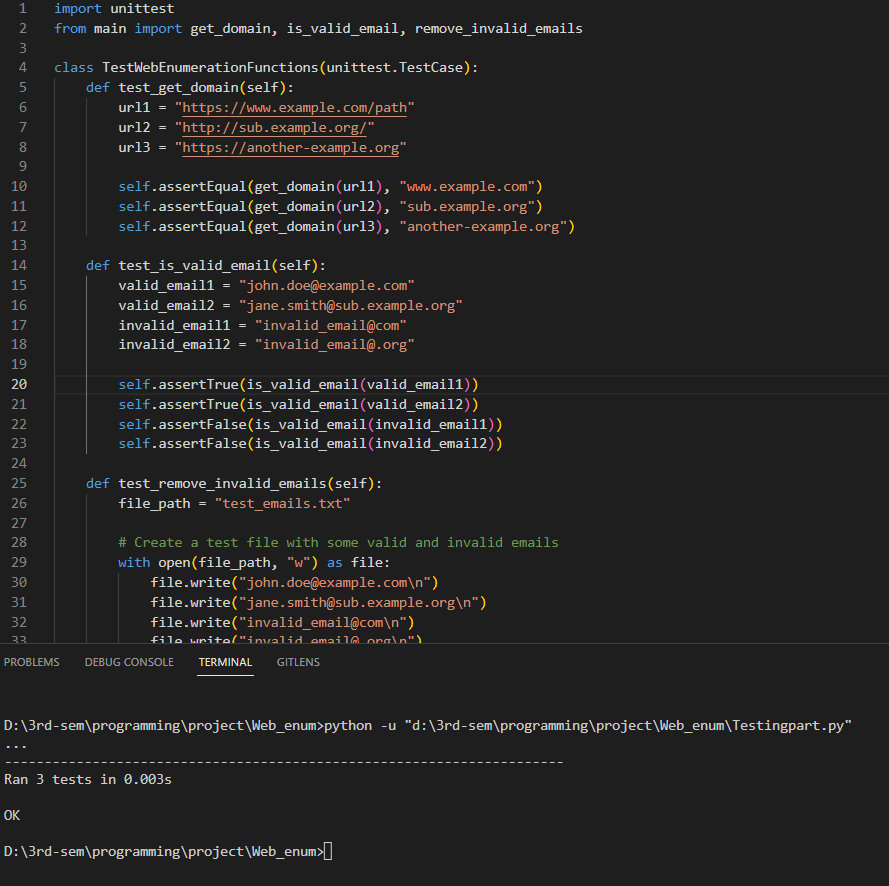


*Figure 15: Function to generate report.*

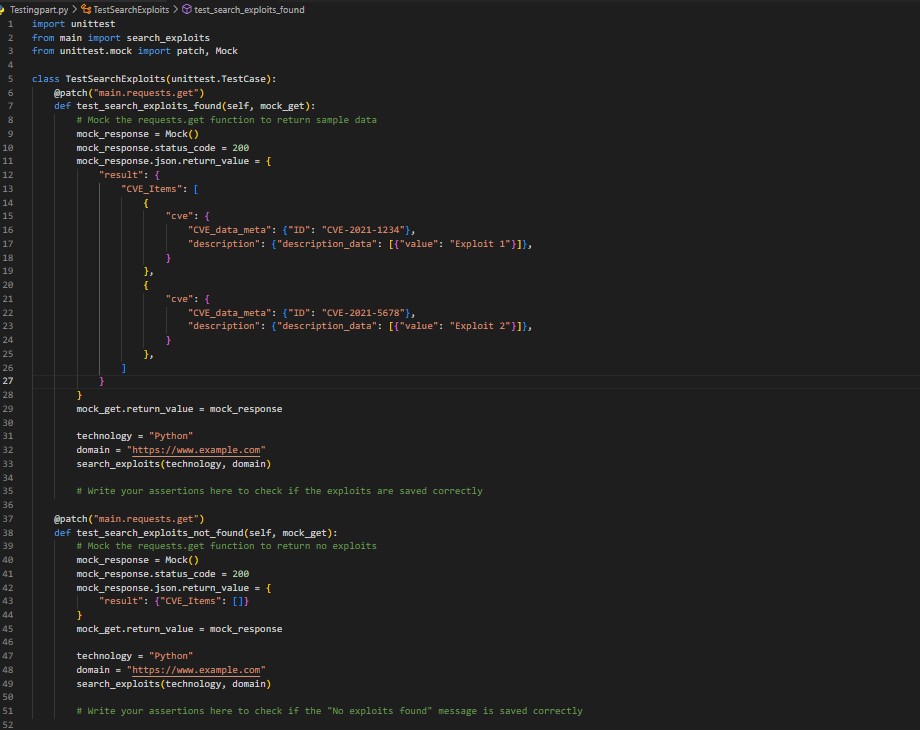
Finally, this function will generate a pdf report.

# Testing

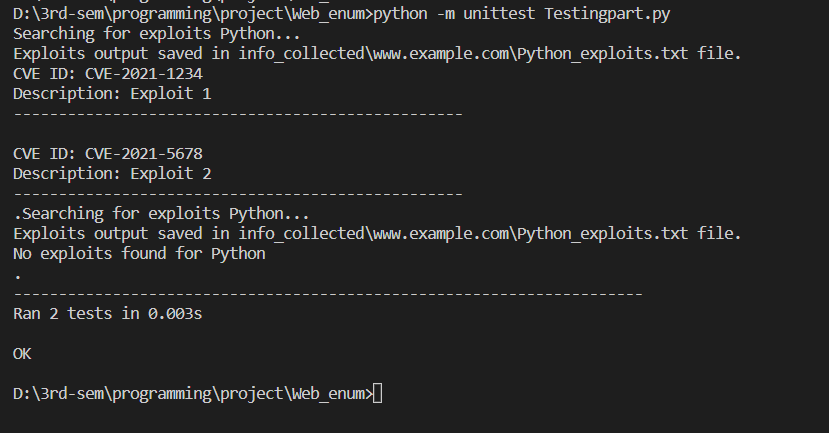
In the Testing phase of our web enumeration tool, we need to ensure that the implemented functionalities work correctly and as expected. We'll perform Unit Testing to validate the individual units of code and their interactions.



*Figure 16: Unit testing of get domain and other function.*



*Figure 17: Unit testing of search exploit.*



*Figure 18: Successful test pass.*

Many of the other functions rely on these functions. Therefore, by properly testing these functions, we can ensure that the code's design is correct.

# Conclusion

In conclusion, our web enumeration tool is a powerful and versatile asset for gathering vital information about a target website or domain. Through the implementation of various key functionalities, we can effectively perform DNS enumeration, port scanning, WHOIS lookups, SSL certificate analysis, technology detection, fuzzing of subdomains, directories, and files, as well as email

harvesting. The tool compiles all the collected data into a well-structured PDF report, presenting DNS records, port scan results, technologies used, discovered subdomains, directories, files, and more.

Security professionals can utilize this comprehensive report to assess potential risks, identify vulnerabilities, and enhance the target's overall security. However, it is crucial to use this tool responsibly and ethically, ensuring it is solely employed for legitimate security testing and not for any malicious purposes.

# Reference

*Welcome to Python.org*. (2023, August 2). Python.org; Python.org. <https://www.python.org/>

*Automating The Web Application Reconnaissance Process -All In One Recon*. (n.d.). Retrieved August 3, 2023, from <https://ijcrt.org/papers/IJCRT2205171.pdf>

Reichinger, Kurt & Baumgartner, Robert. (2023). SEMNUM RDF Vocabulary Specification v.

01.

Reichinger, K., & Baumgartner, R. (n.d.). *INTRODUCING ENUM TO THE SEMANTIC WEB*.

Retrieved August 3, 2023, from <https://www.dbai.tuwien.ac.at/proj/semnum/documents/494-048.pdf>

son, do. (2021, October 5). *kenzer v3.35 releases: Automated web assets enumeration & scanning*. Penetration Testing. [https://securityonline.info/kenzer-automated-web-assets-enumeration-](https://securityonline.info/kenzer-automated-web-assets-enumeration-scanning/) [scanning/](https://securityonline.info/kenzer-automated-web-assets-enumeration-scanning/)

*Webdiscover Automate The Web Enumeration Process And Search For Exploits*. (2022, January 2). GeeksforGeeks; GeeksforGeeks. [https://www.geeksforgeeks.org/webdiscover-](https://www.geeksforgeeks.org/webdiscover-automate-the-web-enumeration-process-and-search-for-exploits/) [automate-the-web-enumeration-process-and-search-for-exploits/](https://www.geeksforgeeks.org/webdiscover-automate-the-web-enumeration-process-and-search-for-exploits/)

*OWASP Automated Threat Handbook Web Applications*. (n.d.). [https://owasp.org/www-pdf-](https://owasp.org/www-pdf-archive/Automated-threat-handbook.pdf) [archive/Automated-threat-handbook.pdf](https://owasp.org/www-pdf-archive/Automated-threat-handbook.pdf)

Singh, N., Bajpai, P., & Ranjan, R. (2022). *Web Application Penetration Automation Testing Tool - WAPATT*. *8*. <https://ijirt.org/master/publishedpaper/IJIRT154789_PAPER.pdf>

Oliveau, A. (n.d.). *OFFENSIVE ENUMERATION*. Retrieved August 3, 2023, from <https://competitivecyber.club/past-talks/MasonCC-S20-Offensive-Enumeration.pdf>

AUTOMATION IN MANUAL PENETRATION TESTING USING BASH SHELL SCRIPT.

(2023). *International Research Journal of Modernization in Engineering Technology and Science*. <https://doi.org/10.56726/irjmets40392>