

UNIVERSITY OF BUCHAREST

FACULTY OF MATHEMATICS AND INFORMATICS

SECURITY AND APPLIED LOGIC

DISSERTATION PAPER

Python Web Scanner

SCIENTIFIC COORDINATOR: GRADUATE:

LECT.DR. SILVIU LAURENȚ VASILE NĂIBOIU TEODOR

BUCHAREST, SEPTEMBER 2024

Contents

[I. Introduction 6](#_Toc174469696)

[I.1 Motivation 6](#_Toc174469697)

[I.2 Personal contribution 7](#_Toc174469698)

[I.3 Structure 8](#_Toc174469699)

[II. Technologies 9](#_Toc174469700)

[II.1 Python 9](#_Toc174469701)

[II.2 Requests 9](#_Toc174469702)

[II.3 Urllib 10](#_Toc174469703)

[II.3.1 Urllib.parse 10](#_Toc174469704)

[II.3.2 Urllib.requests 10](#_Toc174469705)

[II.4 BeautifulSoup 11](#_Toc174469706)

[II.5 Threading 11](#_Toc174469707)

[II.6 OS 11](#_Toc174469708)

[II.7 ConfigParser 11](#_Toc174469709)

[II.8 RE 12](#_Toc174469710)

[II.9 ArgParse 12](#_Toc174469711)

[II.10 HTML 12](#_Toc174469712)

[II.11 JINJA2 13](#_Toc174469713)

[II.12 DVWA 13](#_Toc174469714)

[II.13 Bee-Box 13](#_Toc174469715)

[II.14 Other technologies 14](#_Toc174469716)

[III. Vulnerabilities and Misconfigurations 15](#_Toc174469717)

[III.1 Injections 15](#_Toc174469718)

[III.1.1 SQL Injections 16](#_Toc174469719)

[III.1.2 XSS Injections 16](#_Toc174469720)

[III.1.3 HTML Injections 17](#_Toc174469721)

[III.1.4 Command Execution Injections 17](#_Toc174469722)

[III.1.5 iFrame Injections 17](#_Toc174469723)

[III.1.6 Javascript Injections 18](#_Toc174469724)

[III.1.7 IDOR Injections 18](#_Toc174469725)

[III.1.8 LFI Injections 18](#_Toc174469726)

[III.1.9 PHP Injections 19](#_Toc174469727)

[III.1.10 SSI Injections 19](#_Toc174469728)

[III.1.11 SSRF Injections 19](#_Toc174469729)

[III.1.12 XML Injections 20](#_Toc174469730)

[III.2 Security Misconfigurations 20](#_Toc174469731)

[III.2.1 Weak Browser Cache Configurations 21](#_Toc174469732)

[III.2.2 CORS 21](#_Toc174469733)

[III.2.3 Host Header 21](#_Toc174469734)

[III.2.4 HSTS 22](#_Toc174469735)

[III.2.5 RIA 22](#_Toc174469736)

[III.2.6 Robots.txt 22](#_Toc174469737)

[III.2.7 Cookies 22](#_Toc174469738)

[III.3 CVEs 23](#_Toc174469739)

[IV. Application Architecture and Implementation 24](#_Toc174469740)

[IV.1 The configuration files 25](#_Toc174469741)

[IV.2 The Payload files 26](#_Toc174469742)

[IV.3 The Report files 26](#_Toc174469743)

[IV.4 The Core files 27](#_Toc174469744)

[IV.4.1 Confidence 27](#_Toc174469745)

[IV.4.2 DataStorage 28](#_Toc174469746)

[IV.4.3 ScanConfig 30](#_Toc174469747)

[IV.4.4 Utilities 31](#_Toc174469748)

[IV.5 The Test files 36](#_Toc174469749)

**Abstract**

The following project represents the implementation methods and techniques used for a scanner software application written in Python programming language, designed to aid developers, white hat hackers (security researchers, red-teamers, bug-bounty hunters) and other cybersecurity enthusiast in detecting vulnerabilities and assessing the attack surface and risk exposure of a Web Application. This new implementation is a redesigned and enhanced version of my previous Web Application Vulnerability Scanner software presented in Bachelor's thesis [1]. This new implementation is designed for Linux ***O****perating* ***S****ystem* (OS) usage only. Users can interact with the application through the ***C****ommand* ***L****ine* ***I****nterface* (CLI) and by providing the scanning arguments such as the target website, scan type and login details.

The new scanner functionality has been enhanced by refining more accurate detections and by adding new features such as rogue comment identification, hierarchical site map graph, external ***U****niform* ***R****esource* ***L****ocators* (URLs) references, hidden URL paths and ***C****ommon* ***V****ulnerabilities and* ***E****xposures* (CVE) detection. The reporting method has also been changed to a ***H****yper****T****ext* ***M****arkup* ***L****anguage* (HTML) report. The new version has been built for scalability and ease of access, as the number of prerequisite configurations has been decreased compared to the previous version. Additionally, the majority of ‘future enhancements’ mentioned in the previous thesis were implemented in this version along a completely new method of scanner-website interaction logic that increases reliability and decreases the time of execution.

# Introduction

*“*Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use*”* [2]. This formal definition of cybersecurity can be visualized as a tug-of-war battle between two opposing forces whose common purpose is to dominate each other’s’ territory. Over the last years, the need of understanding and educating people on cyber security has been increasing. Nowadays, not only people working in the **I**nformation **T**echnology (IT) industry are impacted by digital data polluted with malicious additions, but any other person with a smart device connected to the internet can be a victim of the attackers’ bad intentions, either directly or, as most of the time, coincidentally.

Currently, more and more solutions are transitioning to web applications designed to provide the users with a fast resolution for everyday activities (e.g., buying a bus ticket, ordering a meal from the local restaurant, tracking your parcels or accessing your bank balance). “On average every day, approximately 30000 new websites fall to hacking attacks” [3]. As the numbers of websites is increasing due to demand and digitalization, so are the attacks aimed at stealing data by exploiting misconfigurations, vulnerabilities or by simple social engineering attacks facilitated by lack of access restrictions. Due to this reason, numerous websites are storing sensitive user data that can be worth lots of money in the hands of the wrong people. So, protecting the web applications and their data has become one of the most important security issues of our times, as today, compromising such an application can provide valuable data for further elaborated attacks.

## Motivation

I have decided to continue my previous implementation of the web application vulnerability scanner and to enhance its functionality due to my ongoing passion for web application security and for my personal projects. “A web application is a computer program stored on a remote server and run by its users via a web browser” [4]. “A web browser is a computer program used for accessing sites or information on a network (such as the World Wide Web)”[5]. As the web application is designed to be publicly accessible, attackers have an easy target available to lock on their scanners to and wait for immediate and easy to reach security weaknesses. Due to this reason, I have aimed to develop a scanner tool that simulates attackers’ tactics to proactively identify the latest emerging threats.

As information is constantly changing, so are software solutions and their configurations. Due to the ongoing modifications in web application service configurations and their increased complexity, researchers and ethical hackers can have difficulties in detecting vulnerabilities in a timely manner. This also causes automated vulnerability detection tools to become deprecated really fast. As my project is an automated detection tools as well, I have decided to further continue its development and update the detection capabilities to keep up the latest security risks and recommendations while also keeping track of scalability and performance. In the following pages, I will present the new features of this tool, as well as the implementation methods I have chosen for this new and enhanced web applications scanner.

## Personal contribution

While the previous version was much more focused on the ***O****pen* ***W****orldwide* ***A****pplication* ***S****ecurity* ***P****roject* (OWASP) Top 10 Standards [6], the new version is based on my work experience as a Security Analyst and on ***C****apture* ***T****he* ***F****lag* (CTF) competitions experience and observations, over the last 3 years.

“CTFs are gamified competitive cybersecurity events that are based on different challenges or aspects of information security” [7]. The focus was shifted from a OWASP Top 10 approach to a more subjective means of detections based on my past observations from live models of vulnerable web applications. Almost all of the detection methods and capabilities were implemented based on my best judgement instead of generic approaches. This was done to further increase the accuracy of detections and to decrease the false-negative findings. Due to this approach, there might be a significant number of false-positive findings as well, hence the scanner results should be confirmed by manual replication.

Furthermore, I have decided to bring this scanner up to a competitive level by lowering the number of prerequisite configurations needed, and by providing a human readable report with dynamic and intuitive ***U****ser* ***I****nterface* (UI).

## Structure

TBD after chapters

# Technologies

Compared to the previous scanner version which was running Python version 3.2, the new version was implemented in Python version 3.9. Python is one of the best programming languages to use for automated sequential or parallel instructions, since it is easy to learn, to read and to understand [8]. Additionally, what makes Python great for automations is the big number of modules and libraries available and easily compatible with numerous software applicability (web and desktop applications, data structures and analysis, scripts, etc.).

For this project, the most important modules and components are the ones used to communicate with the website, such as *beautifulsoup* [9], *requests* [10], *urllib* [11]. In the following pages I will be describing the modules among other technologies and solutions used to build, run and test the new version of the scanner.

## Python

“Python is an interpreted, object-oriented, high-level programming language with dynamic semantics” [12]. Due to the great, easy to read and write syntax, Python is widely used for complex automated actions among cybersecurity enthusiasts. In projects similar with this one, Python is the best choice of any individual interested in ease of use and versatility. Web applications are constantly changing their structure and code, due to this reason, automated scanning tools need to be implemented in easy to maintain solutions that can handle large amount of data and also be compatible with other tools and technologies [13].

## Requests

The *requests* module is used for transferring data from a client (*Web Browser*) to a *Web Server* using the ***H****yper****t****ext* ***T****ransfer* ***P****rotocol* (HTTP) protocol and ***U****niform* ***R****esource* ***L****ocators* (URLs) [10]. There are a total of nine requests type (*GET, HEAD, POST, PUT, DELETE, CONNECT, OPTIONS, TRACE, PATCH*). During the development of this project, I have used four types of requests:

**GET** – This is one of the principal types of requests as it represents the action of requesting data from the server. This request type is used for receiving data according to the provided parameters.

**POST** – Another principal request method used to send data to the server. This method can be used for creating new data on the server and for updating already existing data.

**PUT** – Method used for creating or changing the representation of a resource according to the data provided in the request payload.

**TRACE** – Method generally used for debugging purposes. This method provides information on the path the requests take to the target destination.

The *requests* module is not only used for exchanging data with the server, but is also used for creating the session to maintain persistent communication with the Web Server during the testing procedures. This module also provides custom request creation functionalities and HTTP error handling methods.

## Urllib

Urllib module is used generally for URL manipulation [11]. From this module, I have used two functionalities:

### Urllib.parse

The *.parse* module from *Urllib* is generally used for combining strings back into URL format. In this project, the module has been used for combining actions, extracting certain strings of interest and fragment parts of URLs into variables [14].

### Urllib.requests

The *.requests* module from *Urllib* is similar with the *requests* module. The difference between the two is that this module provides some more advanced HTTP actions. In this project, this module was used for opening and reading URLs [15].

## BeautifulSoup

One of the most popular modules used for interaction with ***H****yper****t****ext* ***M****arkup* ***L****angua*ge (HTML), ***E****xtensible* ***M****arkup* ***L****anguage* (XML) components and ***D****ocument* ***O****bject* ***M****odel* (DOM) of a page. It provides a wide array of functions that help with pulling data from web pages, navigation, modifying and parsing different values available on a website [9]. This module is responsible for any interaction between the scanner and the targeted web page content.

## Threading

Threading is used for changing the flow of execution from a sequential flow to a parallel flow by creating a separate line of execution that can run simultaneously. Threading is useful for applications that handle large number of independent instructions and in which execution time is also important. The CPU is used for allocating divisions of the physical core into virtual components or codes, these virtual components are called *threads* [16]. Threading was implemented for decreasing the execution time of the project by running multiple tests for multiple URLs in parallel.

## OS

The ***O****perating* ***S****ystem* (OS) module is used any interaction with the operating system. Actions such as creating, reading, modifying, opening and closing files and directories are performed through the usage of this module [17]. This module can also be used for more advanced interactions with the OS such as accessing environments variables, process information, managing registries and other system related functions. In this project, the module is responsible for file interaction.

## ConfigParser

Configuration files are a necessary part of an application that interacts with multiple pieces of data and complex logic. Configuration files are code structures with the *.ini* file extension that can be easily modified by experienced and beginner users without the need of any application architecture knowledge. A configuration file contains custom variables that are usually depended on the execution environment or purpose of the application [18].

The *ConfigParser* module is responsible with the interaction between the configuration file and the application Python code. This module is used to access and import the configuration values in the code and execution logic.

## RE

***R****egular* ***E****xpressions* (RE or Regex) are recognition rules based on symbols and characters that form search patterns in order to detect any certain characters or string of characters inside other strings based on that searching rule [19]. Once a pattern is defined, a string can be manipulated in any way the user wants, those include edits, deletions, word substitutions, character(s) extractions from any string of characters that contains that pattern.

The RE module is the Python implementation of Regex functionality. Regex has been extensively used across this project for vulnerability detection checks, result confirmation, URL manipulation and others.

## ArgParse

ArgParse is a module that is used for Python applications that require user interaction through ***C****ommand* ***L****ine* ***I****nterface* (CLI). ArgParse is the link between *sys.argv* (the list of commands passed to the script using the CLI) and the Python code [20]. The advantage of using ArgParse is that it provides a user-friendly CLI while also automatically generating the *–help* menu used for displaying all the available arguments. From a programming point of view, this module also provides an easier method to manipulate the arguments passed via CLI into the code logic. Since this new scanner version is based on CLI interaction, this module is needed for parsing the user arguments to the application logic.

## HTML

This is a simple module used for manipulating HTML entities. The submodules used from HTML are the modules that *escape* and *unescape* characters. An *escaped* *character* is a character that uses an alternative interpretation of the same character [21]. For Web Application scanning, certain characters need to be escaped when a set of data is sent to the website and others need to be unescaped when data is received. Across this project, data sent and received to, respectively from the application, needs to be escaped for further processing down the test logic.

## JINJA2

The Jinja2 module is responsible for HTML template creation and manipulation through Python code [22]. This module is used for creating the final HTML report file based on an already created template which serves as a starting point for the report output data and format. All scanning results are parsed through Jinja2 to the templating functions that handle the data. The data is then added to the report, through Jinja2 methods, along with the HTML tags required for the HTML page to be correctly interpreted and displayed.

## DVWA

***D****amn* ***V****ulnerable* ***W****eb* ***A****pplication* (DVWA) is a PHP/MySQL web application that is left intentionally vulnerable with the main goal of helping security enthusiasts, web developers, students and teachers to use test their tools, practice their cybersecurity skills and understand web application security better, in a controlled, isolated and legal environment [23].

This application is one of the two web servers used in this project for testing the scanner and simulating real life scenarios. The web server contains numerous different vulnerabilities and misconfigurations which allow a comprehensive coverage of the most frequently found vulnerabilities in the wild. This application was hosted in a controlled virtual environment using the Linux Distribution – Kali Linux.

## Bee-Box

Bee-Box or BWapp is also a PHP/MySQL web application left intentionally vulnerable that follows the same purpose as DVWA. Bee-Box contains over one hundred web vulnerabilities and it covers all the major known web weaknesses and bugs along with the ones from OWASP Top 10 project [24].

This is the second web server used for testing the scanner progress and detections in this project. This web server was hosted in a controlled virtual environment using the Linux Distribution – Ubuntu.

## Other technologies

Below are some of the less utilized but still important modules that were used for implementing the web application scanner.

The *random* module is used for generating pseudo-random numbers or choices for various purposes [25]. In this project, the module was used for choosing a pseudo-random web user agent from a list. A web user agent is a characteristic string of data that helps servers identify the application, operating system, vendor of the requesting source [26].

The *datetime* module is used for accessing the calendar’s date and time. Using this module, I have provided date and time details in the resulting report with the format *YYYY:MM:DD HH:MM:SS* [27]*.*

The *math* module provides access to mathematical operations and functions [28]. In this project, the module was used to perform rounding on list length divisions used to split the data for threading purposes.

The *colorama* module is used to color the output text to terminal [29]. In this project the module was used to color the output text when the error file is not available due to any reason.

The *json* module is used to import **J**ava**S**cript **O**bject **N**otation (JSON) data interpretation. JSON is a standardized format for data that can be easily interpreted and read both by humans and computers [30]. In this project, the *json* module was used for creating and manipulating the URL graph map.

The *warning* module provides warning control functions. Warnings are issued in situations in which the script does not raise a condition that terminates the program, but the user should be aware of the event. In this project, the *warning* module was used only to suppress character encoding warnings for HTML received data.

# Vulnerabilities and Misconfigurations

The following sections are necessary for better understanding vulnerabilities and common misconfigurations a web application usually has. This chapter covers the theoretical implementation of the scanner. The below pages present all the information necessary for understanding the detection capabilities of the scanner and its final report.

“A vulnerability, is a flaw in code or design that creates a potential point of security compromise for an endpoint or network”[31]*.* Usually, thereason a vulnerability exists is due to a misconfiguration. These misconfigurations are usually incorrect setups of data in the system or environment. Misconfigurations can be caused by lots of variables, both from a technical point of view to business logic.

Vulnerabilities represent attack opportunities for adversaries. There are multiple methods of abusing vulnerabilities for gaining access to the weakened system. Depending on the type and motives, attackers can leverage them for unauthorized access in the environment. Both *white-hat hackers* and *black-hat hackers* are constantly searching for these vulnerabilities as they represent the initial key of access to any system. The notion of *white-hat hacker* is used to refer to a person motived by legal and ethical reasons to find and report such misconfigurations. The *black-hat hacker* term is used to describe people motivated by and not limited to financial gain or by seeking reputation from their community while disregarding the legal and moral constrictions [32].

In the following pages I will be describing some of the vulnerabilities and misconfigurations that can be detected using this scanner, with the mention that the new scanner version is no longer following the OSWASP Top 10 Standards, hence the vulnerabilities will be more biased towards personal criteria of exploitability, severity and importance.

## Injections

“Injections based vulnerabilities are still one of the most abused and widely spread ones, due to this reason, injections are considered a critical threat to cybersecurity” [33]. Injections rely on user input fields. The provided data always needs to be interpreted by the application; hence the application is susceptible to any malicious instruction if the input field is not properly sanitized. There are multiple types of Injection attacks, with the majority of them depending on the software solutions running on the application server.

The following types of injections are the most spread injections in the wild and also the ones detectable by the new scanner version.

### SQL Injections

***“S****tructured* ***Q****uery* ***L****anguage* (SQL) is the most common language for interacting with data stored in a relational database” [34]. These injections rely on misconfigurations in the input fields connected to the SQL Database running in the back-end of the web application. Attackers can leverage these vulnerabilities to arbitrarily tamper with any piece of data stored in the application. SQL Injections can be blind or reflected. With reflected SQL Injections, feedback is provided back to the client according to the provided set of SQL data. Blind injections do not provide any feedback back to the client; hence more difficult to detect.

### XSS Injections

***“Cross****-****S****ite* ***S****cripting* (XSS) injections refer to the practice of sending malicious scripts, in the form of a browser side script to a target victim using a web application” [35]. The victim’s web browser will execute the code as part of the legitimate website. XSS attackers are used when attackers want to execute code on behalf of another user in their browser. The executed code will have all the privileges and access rights the victim has at the moment the malicious script is executed. There are multiple types of XSS attacks.

#### Reflected XSS

Reflected XSS attacks are the most common XSS attack in the wild. This type of attack relies on single execution of the malicious script and requires user interaction. The malicious code is not stored in the browser and can only be executed once, this applies to both requests and response transmitted malicious code [36].

#### Stored XSS

Stored XSS is one of the most dangerous XSS attack as it does not require any user interaction. This attack is based on injecting XSS code directly into the database through the vulnerable inputs. The malicious code gets stored on the affected page and gets executed each time the page is accessed, hence affecting all users visiting the website [37].

### HTML Injections

This injection is a type of attack in which HTML tags are injected directly in the DOM of the website. This attack is different than others as it does not exploit the back-end of the server, but the structure and content of web page. Similar with the XSS, this type of Injection can also have a single time execution (Reflected HTML Injection) or a persistent injection (Stored HTML Injection) [38].

### Command Execution Injections

Also called ***R****emote* ***C****ode* ***E****xecution* (RCE), code injection is a method that allows attackers to remotely execute unauthorized code on targeted systems with the end goal of executing commands. The targeted server executes OS commands received through the web application inputs. Similar with the SQL Injection, Command Injection can also be reflected or blind.

### iFrame Injections

“iFrame is short for inline frame and is used to embed content from another website into the current page” [39]. iFrames injection is the practice of injecting malicious code into a webpage in the form of an iFrame element in the HTML page. Once an iFrame is injected, attackers can add their own controlled domain snippet to the targeted app, this can cause numerous security issues as iFrames provide full view of the embedded domain to the body of the compromised webpage.

### Javascript Injections

“JavaScript is the most powerful and versatile web programming language used for building interactive websites through implementation of animations, interactive forms and dynamic content to web pages” [40]. Javascript injections are a type of injections in which attackers inject malicious Javascript code into the client side of the application, usually a web browser. Through this attack, adversaries can steal sensitive information such as personal user data, credentials, sessions, cookie settings and any other data available in the target’s browser. They can also manipulate the targeted website, redirect the users to other attacker-controlled domains or install malicious extensions in the victim’s browser.

### IDOR Injections

“***I****nsecure* ***D****irect* ***O****bject* ***R****eference* (IDOR) is a vulnerability that arises when attackers can access or modify objects by manipulating parameters used in a web application” [41]. This type of attack allows adversaries to access unauthorized data through URL tampering or DOM body manipulation by modifying the vulnerable fields with custom values that link different objects in the back-end or database. This vulnerability is most commonly abused for horizontal privilege escalation, but it can be used for vertical privilege escalation as well. The term of horizontal privilege escalation refers to the practice of tampering with data of users with the same access level as the attacker’s. Vertical privilege escalation refers to the practice of accessing a higher level of privilege than the one they initially possess.

### LFI Injections

***“L****ocal* ***F****ile* ***I****nclusion* (LFI) allows an attacker to include files on a server through the web browser” [42]. Local files are files that are already present on the server that is running the web application. Accessing such files can lead to information disclosure, RCE or XSS. This vulnerability can be easily abused by providing filenames or file paths as inputs in the URL parameters or in the body of a website. Using this vulnerability, an attacker can perform a Directory Transversal attack and access any file from the server. Path or Directory transversal is a type of vulnerability in which the attacker is navigating the file hierarchy on the targeted system through CLI compatible commands such as *‘../../etc/passwd*’ used for navigating two folders back and accessing the account passwords in UNIX based systems.

### PHP Injections

“PHP (recursive acronym for PHP: Hypertext Preprocessor) is a widely-used open-source, general-purpose scripting language that is especially suited for web development and that can be embedded into HTML” [43].PHP Injections are very similar to Javascript or Code Injections as it requires an attacker to send malicious PHP code to an application running PHP. The provided code then gets executed successfully on the back-end server.

### SSI Injections

***“S****erver-****s****ide* ***I****ncludes* (SSIs) are directives found within a web application’s HTML code and are used to provide an HTML page with dynamic content***.*** SSI injections are a server-side exploit that enables an attacker to inject code into a web server and execute it upon the page load” [44]. The SSI syntax is *<! --#directive parameter=value parameter=value -->.* Directives are instructions that can be interpreted by the web server for providing dynamically generated content on a web page.

### SSRF Injections

**“S**erver-**S**ide **R**equest **F**orgery (SSRF) attacks allow adversaries to trick the server-side application to allow access to the server resources. The attack can be performed if the target application supports data imports or reads data from URLs without proper validation” [45]. SSRF Injections are performed by injecting an arbitrary domain into the URL or replacing the URL altogether on the targeted web application. The resulted HTTP requests can be abused for unauthorized access or actions over the web server or any other external server with which the web application communicates.

### XML Injections

***E****xtensible* ***M****arkup* ***L****anguage* (XML) is used to store, transport and exchange data. The difference between HTML and XML is that HTML is oriented towards displaying data and can be managed only with predefined tags, whereas XML is more focus on data manipulation and allows the users to define their own tags. Due to this reason XML can be abused by adversaries by creating custom ***X****ML* ***e****xternal* ***e****ntities* (XEE) with specific tags designed to allow access to view files on the server filesystem and to interact with any other back-end or external system that the web application has access to and communicates with [46].

The majority of the above injections can be mitigated by implementing input validation and sanitization. Developers need to ensure that all available inputs are validated, sanitized and that the outputs are properly encoded. There are a multitude of methods depending on the frameworks and software solutions used by the web application that need to be properly configured, such as parameterized queries for SQL interaction, pre-compiled and stored objects for databases, restrictive access and error handling.

## Security Misconfigurations

“Security misconfigurations represent any error or vulnerability in the configuration of the code that allows attackers to access sensitive data” [47]. Almost all vulnerabilities are, to some level, misconfigurations caused by either human or software error or due to deviations from best-practices. There are multiple types of misconfigurations that either represent full vulnerabilities or can lead to opportunities by allowing prerequisite configurations for defense impairment.

Due to their nature, misconfigurations are difficult to detect due to the high number of places they can found. It is a very difficult job for *ethical hackers* and *developers* to correctly identify and mitigate, in a timely manner, all security misconfigurations present in a web application. Due to this reason, I have decided to cover the most frequent and common misconfigurations found in the wild and some other that are not that popular. Detecting misconfigurations as soon as possible is the key to keeping attackers away and to discourage them for further targeting specific web servers.

### Weak Browser Cache Configurations

Browsers can store information for purposes of caching and history. Caching is used to improve performance, so that previously displayed information doesn’t need to be downloaded again [48]. Caching issues can lead to vulnerabilities such as Cache Poisoning and Cache Deception or sensitive data disclosure by abusing other vulnerabilities such as XSS along with the caching misconfiguration. Cache Poisoning refers to the practice of injecting malicious code into the cache. On requests, the malicious content gets served to other web applications users. Cache Deception is more oriented towards sensitive data access, the attacker causes the web application to store sensitive content in the cache, the content can be later access by adversary [49].

Generally, for web pages with sensitive content or information, the cache should be disabled.

### CORS

***C****ross-****O****rigin* ***R****esource* ***S****haring* (CORS) is a protocol that enables scripts running on a browser client to interact with resources from a different origin [50]. CORS is usually used for web application that rely on third-party APIs or embedded content from other websites. This attack relies on the bad validation of the proper origin of the request. An attacker can create a custom script that sends requests to an application and then execute it from their controlled malicious domain. Without proper validation, the targeted application can provide the attacker with access to its resources [51].

### Host Header

The Host header is a crucial part of the HTTP protocol and is used by web servers to determine which virtual host or website the client is requesting [52]. The Host Header misconfiguration provide an attacker the opportunity to inject malicious code into the targeted application Host Header. Similar with other misconfigurations, this attack also relies on the improper validation of the Host input.

### HSTS

***H****TTP* ***S****trict* ***T****ransport* ***S****ecurity* (HSTS) governs the connection method of a web browser to a web application. This configuration is responsible for ensuring the web server is only communicating with clients through the HTTPS (HTTP Secure) protocol by upgrading the connection from the HTTP protocol to HTTPS through a redirect. HTTP connections are vulnerable to ***M****an-****I****n-****T****he-****M****iddle* (MITM) attacks and other data sniffing techniques and are generally considered unsafe. HSTS flag should be generally enabled in the headers of a request to avoid the usage of HTTP communication [53].

### RIA

***“R****ich* ***I****nternet* ***A****pplications* (RIAs) refer to web applications that offer dynamic content and interactions, often inaccessible to users who rely on screen readers or other assistive technologies” [54]. RIA uses Adobe *crossdomain.xml* to allow cross domain access to the web server resources required for RIA good functionality. Restrictive permissions need to be set up to prevent attackers from abusing RIA function to access sensitive data on the server.

### Robots.txt

“The robots.txt file tells search engine crawlers which URLs the crawler can access on a website” [55]. The file is a text base field that contains numerous web paths allowed or disallowed from search engine indexing. Due to this reason, there is a chance that sensitive paths such as */admin* or */administrator* can accidentally leaked. As those paths are not designed for public access, they can lack the necessary access restriction a usual path would have.

### Cookies

“Cookies are small files of information that a web server generates and sends to a web browser” [56]. Cookies are mostly used for tracking and tailoring the users experience over the web application. Depending on the website, cookies can be set as flags for numerous access rights or for storing relevant user data such as the session ***id****entification* (ID). If not properly secured, attackers can access the cookies and steal or modify relevant data that can lead to website compromission. Cookies can be left frequently misconfigured by not protecting the user’s session cookies with appropriate attributes and by permitting stored cookies to persist indefinitely in the user's browser [57].

## CVEs

*“****C****ommon* ***V****ulnerabilities and* ***E****xposures* (CVEs) is an international framework and effort to maintain an updated registry of all known computer security vulnerabilities and exposures” [58]. CVEs can be applied to any piece of software running in any environment. Modern web applications are very complex with many third-party integrations and frameworks embedded. “A framework is a collection of reusable software components that make it more efficient to develop new applications” [59]. Due to the multiple pieces of individual components that now form a web application, a potential CVE identified in one solution running on a web server can be exploited for full compromission of the whole server. It is very important for web server owners to manage and be up to date with the latest CVEs for the software running in their environment.

In this project I have also implemented methods for automatic CVE detection using the ***A****pplication* ***P****rogramming* ***I****nterface* (API) from ***N****ational* ***I****nstitute of* ***S****tandards and* ***T****echnology* (NIST) ***N****ational* ***V****ulnerability* ***D****atabase* (NVD). “An API is a collection of communication protocols and subroutines used by various programs to communicate between them” [60]. “NIST NVD is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP)” [61].

# Application Architecture and Implementation

Unlike the previous version of this scanner, the new one has been split amongst multiple folders according to their code and purpose. The previous version was implemented on a single Python file too big to manage and difficult to keep up to date due to amount of lines. The new version is easier to maintain and update due to the module-like approach. The filenames have descriptive names according to their role in the application logic.

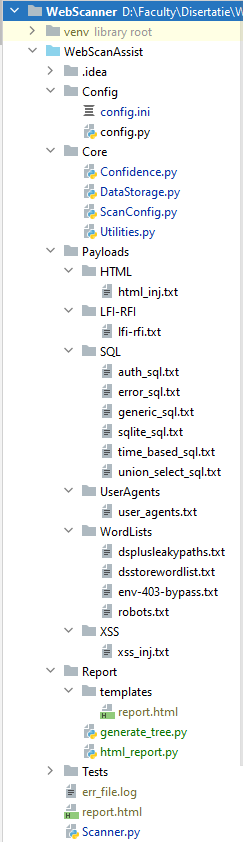


Figure 4.1. Application file hierarchy

## The configuration files

The configuration files are stored in the ‘Config’ folder. The folder contains the Python code file ‘config.py’ required for reading and parsing the configurations from the ‘config.ini’ configuration file stored under the same folder.

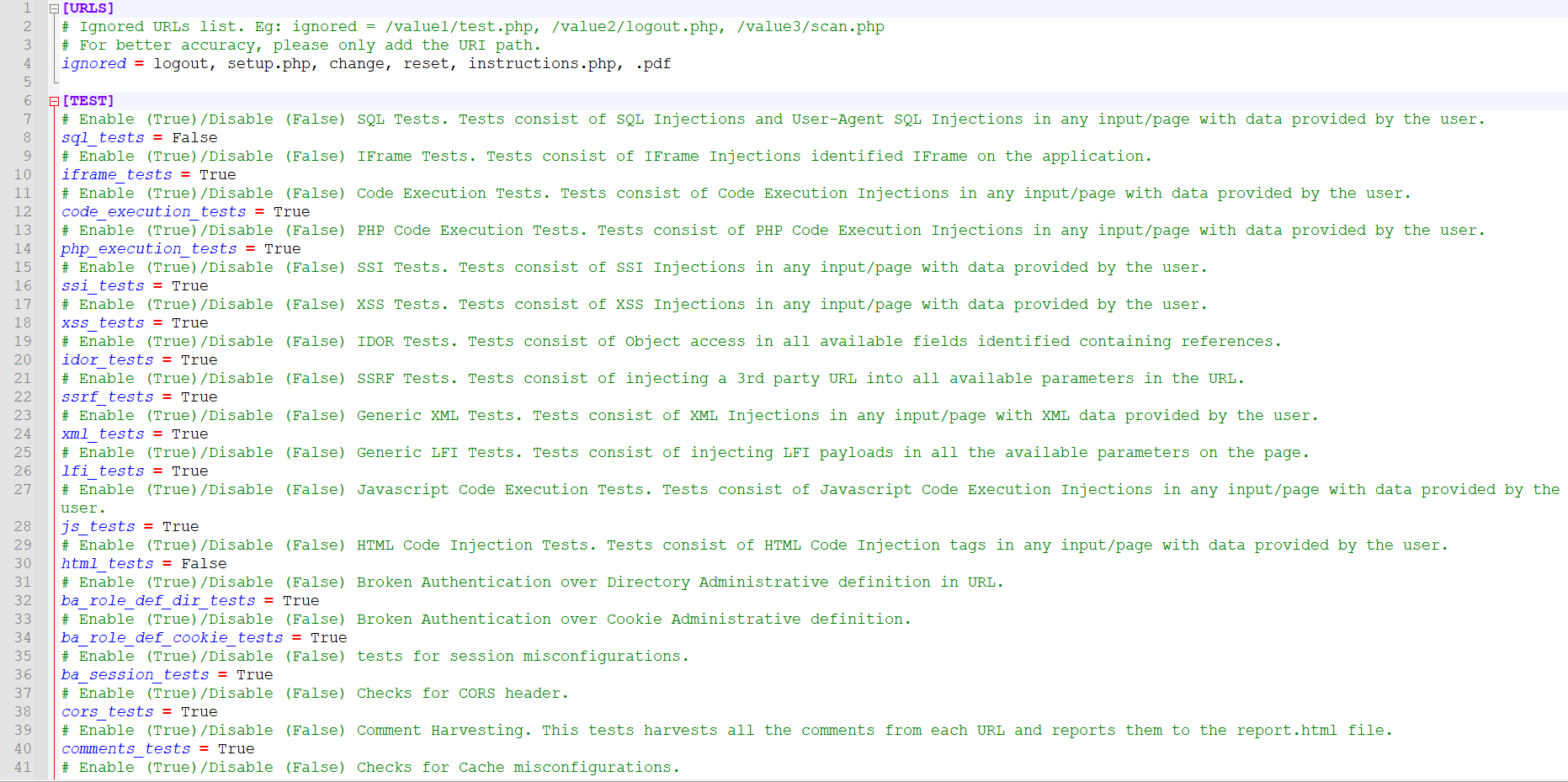
class Config:  
 def \_\_init\_\_(self):  
 try:  
 self.config\_object = ConfigParser()  
 self.config\_object.read("Config/config.ini")  
 except Exception as e:  
 print(e)

Figure 4.2. Configuration file contents (partial capture)

The configuration file ‘config.ini’ contains the following options: variables for enabling/disabling specific tests, the ignored URL string list required for ignoring specific URL keywords (e.g., logout.php) and the API private key required for NIST interaction for CVE identification.

## The Payload files

“A payload in cybersecurity is a code that is designed to perform malicious activities on a victim’s computer or network” [62]. In this project, the ‘Payloads’ folder contains the necessary strings and data required for testing and validating the vulnerability state of the targeted input.

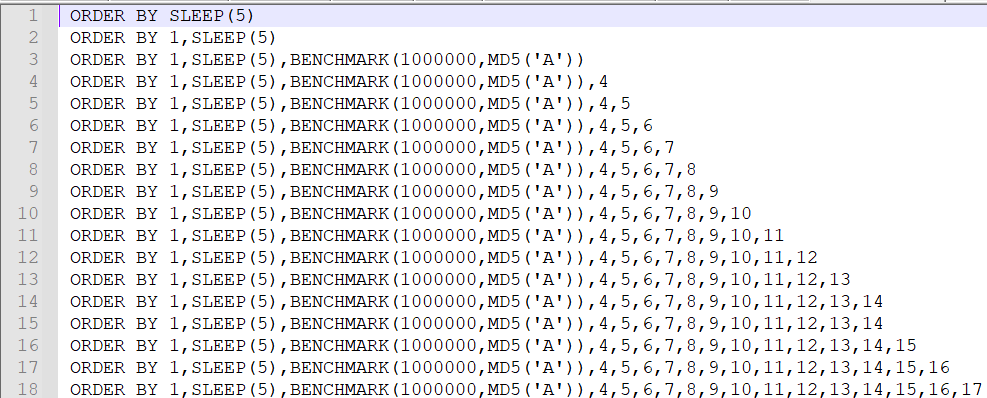
 As observed in the *Figure 4.1 Application file hierarchy* each file and folder name are descriptive for their purpose. These files are dictionary of words from the most popular and up to date Payload repositories over the internet [63] [64] [65] [66] [67]. Unlike other scanner applications that rely on static and hard-coded out-of-reach dictionary of payloads, this format allows the user to provide his own dictionary of words or payloads required for testing the targeted application.

Figure 4.3. Contents of union\_select\_sql.txt (partial capture)

## The Report files

The ‘Report’ folder contains the necessary files for dynamically generating the final .HTML report file.

As also observed in *Figure 4.1 Application file hierarchy* the folder contains a subfolder named ‘templates’ with the ‘report.html’ template. This template contains the necessary HTML and JINJA2 tags required for dynamically generating and displaying the final report based on the lists of data populated by the executed testing methods results. This file contains the ***C****ascading* ***S****tyle* ***S****heet* (CSS) code required for styling the report to an easy to navigate and read format, the Python code necessary for parsing and displaying the results from the testing procedures and the Javascript code required for the generation of the hierarchical site map graph and for the animations.

The ‘generate\_tree.py’ and ‘html\_report.py’ files contain the Python side logic for forwarding the testing and the site map graph data to the HTML template. These files are required for correctly parsing and formatting the data for compatibility with the display code in the HTML file. More on the generated report and methods used in Chapter XXX.

## The Core files

The Core folder contains the four main files with no testing logic, but with various methods used for interacting with the web application, generating confidence, opening and closing files, setting up prerequisites, error handling, sending requests and managing responses and others.

### Confidence

This file contains the code necessary for dynamically assigning a confidence level based on a test result. The logic relies on four arguments (severity, past\_occurences, exploitability and impact) provided during each test result. All arguments accept values between ‘0.1’ and ‘1’ depending on the test logic.

class Confidence:  
 def \_\_init\_\_(self, severity=0, past\_occurrences=0, exploitability=0, impact=0):  
 self.severity = severity  
 self.past\_occurrences = past\_occurrences  
 self.exploitability = exploitability  
 self.impact = impact  
  
 def add\_confidence(self, severity=0, past\_occurrences=0, exploitability=0, impact=0):  
 self.severity += severity  
 self.past\_occurrences += past\_occurrences  
 self.exploitability += exploitability  
 self.impact += impact  
  
 def calculate\_confidence(self):  
 score = (self.severity \* 0.3) + \  
 (self.past\_occurrences \* 0.3) + \  
 (self.exploitability \* 0.2) + \  
 (self.impact \* 0.1)  
  
 if score >= 0.75:  
 return "Critical"  
 elif score >= 0.5:  
 return "High"  
 elif score >= 0.25:  
 return "Medium"  
 else:  
 return "Low"

During execution of a test, the ‘Confidence’ object is initialized with the default initial values (0). For each new payload that successfully exploits an input, the ‘add\_confidence’ method is called and the values are increased accordingly. At the end of the test, the ‘calculate\_confidence’ method is called and the vulnerability score is determined based on the previous values.

For example, the below vulnerability confidence logic is used for the LFI identification tests:

At the beginning of the testing function, the confidence object is created:

sql\_test\_confidence = Confidence()

Then, if the target is vulnerable to LIF, the ‘add\_confidence’ method is called with arbitrary values dependent of the testing conditions and the number of times the application is found vulnerable to different inputs.

if "root:" in response.text.lower():  
 sql\_test\_confidence.add\_confidence(severity=0.8, past\_occurrences=0.1, exploitability=0.7, impact=0.7)  
 confidence += 1

After the true positive condition is met, the application calculates the final vulnerability score and returns it to the calling method:

if confidence >= 1:  
 if new\_url:  
 return lfi\_script, new\_url, sql\_test\_confidence.calculate\_confidence()

Each testing method has different confidence values depending on the testing logic used.

### DataStorage

The ‘DataStorage.py’ file contains the Python code for accessing the local data in the ‘Payloads’ folder.

The most important method is the one that accesses the relevant payloads based on the provided input:

@staticmethod  
def payloads(p\_type): *# returns a list of payloads depending on the chosen type* try:  
 *# Get the payload type from the Payload Local Repo.* if p\_type == 'SQL':  
 for filename in os.listdir(os.getcwd() + '/Payloads/SQL'):  
 with open(os.path.join(os.getcwd() + '/Payloads/SQL', filename), 'r', encoding="utf8") as f:  
 DataStorage.sql\_dict[filename.split('.')[0]] = f.read().splitlines()  
 f.close()  
 all\_sql\_values = []  
 for value in DataStorage.sql\_dict.values():  
 if isinstance(value, list):  
 all\_sql\_values.extend(value)  
 else:  
 all\_sql\_values.append(value)  
 return all\_sql\_valueselif p\_type == 'HTML':  
 for filename in os.listdir(os.getcwd() + '/Payloads/HTML'):  
 with open(os.path.join(os.getcwd() + '/Payloads/HTML', filename), 'r', encoding="utf8") as f:  
 DataStorage.html\_inj = f.readlines()  
 f.close()  
 return DataStorage.html\_injelif p\_type == 'XSS':  
 for filename in os.listdir(os.getcwd() + '/Payloads/XSS'):  
 with open(os.path.join(os.getcwd() + '/Payloads/XSS', filename), 'r', encoding="utf8") as f:  
 DataStorage.xss\_inj = f.readlines()  
 f.close()  
 return DataStorage.xss\_inj  
 elif p\_type == "WORDS":  
 for filename in os.listdir(os.getcwd() + '/Payloads/WordLists/'):  
 if 'robots' in filename:  
 continue  
 with open(os.path.join(os.getcwd() + '/Payloads/WordLists/', filename), 'r', encoding="utf8") as f:  
 DataStorage.word\_list.extend(f.readlines())  
 f.close()  
 return DataStorage.word\_list  
 elif p\_type == "LFI":  
 for filename in os.listdir(os.getcwd() + '/Payloads/LFI-RFI'):  
 with open(os.path.join(os.getcwd() + '/Payloads/LFI-RFI', filename), 'r', encoding="utf8") as f:  
 DataStorage.rfi\_inj = f.readlines()  
 f.close()  
 return DataStorage.rfi\_inj  
 elif p\_type == "ROBO":  
 with open(os.path.join(os.getcwd() + '/Payloads/WordLists/', 'robots.txt'), 'r', encoding="utf8") as f:  
 DataStorage.robots\_list = f.readlines()  
 f.close()  
 return DataStorage.robots\_list

On each call, the method accepts the payload type parameter ‘p\_type’ and according to its value, it provides the list, set or dictionary required for test usage.

This method also contains a special function for the SQL Injection payloads designed to also return the type of SQL Injection used, for better detailing in the report:

@staticmethod  
def inject\_type(p\_type):  
 try:  
 *# Based on filename, get the injection type, used for SQL.* for key, value in DataStorage.sql\_dict.items():  
 if isinstance(value, list) and p\_type in value:  
 return key  
 return None

### ScanConfig

The Scanning Configuration file ‘ScanConfig.py’ contains the logic for the preliminary tests and setups for the scanner. It contains the ‘ScanConfig’ object that once called, initializes the initial parameters (session, lists for errors, the ignored\_links, the DataStorage variable and the configuration variable).

class ScanConfig:  
 *# Initialize Session for current run* session = requests.Session()  
 *# Initialize the ignored links and errors file parameters* err\_file = None  
 ignored\_links = None  
 config\_params = config.Config().config\_object  
  
 def \_\_init\_\_(self, url):  
 try:  
 *# Initialize Scanner Configuration Parameters.* self.url = url  
 *# Initialize Data Storage.* self.DataStorage = DataStorage()  
 *# Empty list of links pairs used for hierarchy.* self.link\_pairs = []  
 *# Setup initial requirements and prepare files.* self.setup()

This class is also responsible for setting up the original connection and testing it in the ‘setup()’ method.

def setup(self):  
 try: *# Test connection* test\_get = self.session.get(self.url)  
 if test\_get.status\_code == 404: *# If page is not found, scanner will not start.* print("[Error] Bad URL provided (404). Quitting..")  
 quit()  
 except requests.ConnectionError: *# If ConnectionError identified, try to change the HTTP protocol.* try: *# Switch to HTTP if HTTPs is unsupported* self.url = self.url.replace("https://", "http://")  
 self.session.get(self.url)  
 except requests.ConnectionError: *# Switch to HTTPs if HTTP is unsupported* self.url = self.url.replace("http://", "https://")  
 self.session.get(self.url)

The setup method will also correct the URL and try to switch the protocols if the provided one is unsupported. This was done in an effort to allow users to use the scanner even if the application is not publicly available nor has a valid ***S****ecure* ***S****ockets* ***L****ayer* (SSL) certificate. The session variable is the one that will be used across the scanner to maintain communication and interact with the application responses.

### Utilities

The ‘Utilities.py’ method is one of the most referenced across the application. This method contains all the major logic for interaction with the web application and all its components. It also contains methods that are used during testing procedures but are not generally applicable to one test, such as the ones used for formatting strings, URLs, accessing cookies, escaping html or processing the login sequences.

The first implemented method is the ‘spider’ function used for harvesting all the available URLs in the application and appending them to the relevant lists (main URL scan list, the link pair hierarchy used for creating the URL graph map and the URLs referencing external domains). At the first call, the provided URL is added to the ‘main URL scan list’ and the ‘link pair list’ as a starting point for the crawling process, for future calls, the application continues with the crawling process for the provided ‘url’ variable. This method is called recursively.

def spider(self, url):  
 try:  
 *# Check if this is the first call, and if it is, add the provided URL to the list.* global firstCallSpider  
 if firstCallSpider:  
 self.link\_pairs.append(['-1', url])  
 response = self.session.get(url)self.DataStorage.urls.add(url)  
 firstCallSpider = 0  
 else:  
 response = self.session.get(url)

Then, the method searches for HTML Anchor tags and verifies if the newly identified URL is part of the target application. The verification is based on a regex expression designed to match the provided URL domain with the extracted one.

if response.status\_code == 200:  
 soup = BeautifulSoup(response.text, "html.parser")  
 *# Build up URls list by extracting all hrefs and anchors* for link in soup.find\_all('a'):  
 href = link.get('href')  
 if href and not href.startswith('#'):  
 extracted\_url = urllib.parse.urljoin(url, href)  
 *# Ensure the app does not scan other webapps by checking if the harvested URL has the same domain as the URL provided by user.* if re.search("^(?:https?:\/\/)?(?:[^@\/\n]+@)?(?:www\.)?([^:\/?\n]+)", extracted\_url).group(1) == re.search("^(?:https?:\/\/)?(?:[^@\/\n]+@)?(?:www\.)?([^:\/?\n]+)", self.url).group(1):  
 *# Adds URLs to main list object, ignore the user - ignored ones.  
 # [[a.html,b.html], [b.html,c.html], [a,d], [a,g], [g,h], [b,j]]* if extracted\_url not in self.DataStorage.urls:  
 self.link\_pairs.append([url, extracted\_url])  
 if extracted\_url not in self.DataStorage.urls and not any(ignored.replace(" ", "") in extracted\_url for ignored in self.ignored\_links):  
 self.DataStorage.urls.add(extracted\_url)  
 self.spider(extracted\_url)  
 else: html\_report.add\_external\_link(extracted\_url)

Based on the result, if the URL is internal, it is added to the ‘graph URL map list’ and to the ‘main URL to scan list’. The external URLs are added to the ‘external URL list’.

Other methods present under ‘Utilities’ class manage interactions between the scanner and the ‘inputs’ and ‘forms’ on the web application. The method used for extracting the forms uses the ‘BeautifulSoup’ parser to find and extract all the data under each ‘form’ tag identified on the provided URL.

def extract\_forms(url):  
 try:  
 *# Extract all forms from an URL.* response = ScanConfig.session.get(url, timeout=25)  
 response.raise\_for\_status()  
 parsed\_html = BeautifulSoup(response.content, "html.parser")  
 return parsed\_html.findAll("form")

The same type of logic is used for extracting the ‘inputs’ as well. The ‘input’ tags can be under ‘form’ tags or have no ‘form’ parent. Due to this reason, a separate method is used for extracting all identified inputs as well.

def extract\_inputs(url):  
 try:  
 *# Extract Inputs the same way forms are extracted* response = ScanConfig.session.get(url, timeout=300)  
 response.raise\_for\_status()  
 parsed\_html = BeautifulSoup(response.content, "html.parser") *# , from\_encoding="iso-8859-1")* return parsed\_html.findAll("input")

For extracting data out of ‘form’ tags and to determine potential injection points, few additional methods are used. This was done in an effort to ensure the scanner is able to recognize and extract as much injection opportunities as possible for better test coverage.

The scanner attempts to extract the following tags from a ‘form’: ‘input’, ‘button’, ‘select’ and ‘textarea’. The method creates and returns a ‘form\_data’ dictionary variable in which the key is the field name and the attribute is left blank (the ‘button’ and ‘input’ tags are additionally checked for the common values needed for web application good functionality [e.g., ‘submit’]).

Inputs:

input\_fields = form.find\_all('input')  
for field in input\_fields:  
 if field.get('name'):  
 if (str(field.get('name')).lower() == 'submit') or (str(field.get('type')).lower() == 'submit') or (str(field.get('name')).lower() == 'user\_token'):  
 form\_data[field.get('name')] = field.get('value')  
 continue  
 form\_data[field.get('name')] = ''

Buttons:

form\_fields = form.find\_all('button')  
for field in form\_fields:  
 if field.get('name'):  
 if (str(field.get('name')).lower() == 'submit') or (str(field.get('type')).lower() == 'submit') or (str(field.get('name')).lower() == 'user\_token'):  
 form\_data[field.get('name')] = field.get('value')  
 continue  
 form\_data[field.get('name')] = ''

Selects:

form\_option = form.find\_all('select')  
for field in form\_option:  
 if field.get('name'):  
 form\_data[field.get('name')] = ''

Textareas:

form\_textarea = form.find\_all('textarea')  
for field in form\_textarea:  
 if field.get('name'):  
 form\_data[field.get('name')] = ''

This class also contains the necessary methods used for sending data to the application. The method used for submitting the form with the payload data for testing is also implemented here.

def submit\_form(url, form, form\_data):  
 try:  
 *# Get the action (URL or PATH)* action = form.get("action")  
 *# Get the method (GET, POST, PUT etc.)* if form.get("method"):  
 method = form.get("method").upper()  
 else:  
 return 0  
 *# Check if action is URL or if it is path relative to URL.* if action:  
 if action.startswith('http'):  
 action\_url = action  
 else:  
 action\_url = urllib.parse.urljoin(url, action)  
 else:  
 action\_url = url  
 *# Send data accordingly to method.* if method == 'GET':  
 response = ScanConfig.session.get(action\_url, params=form\_data, timeout=30)  
 else:  
 response = ScanConfig.session.post(action\_url, data=form\_data, timeout=30)  
 response.raise\_for\_status()  
 return response

The ‘submit\_form’ method is used for checking the request type and the destination of data based on the provided URL, then, after all the checks are performed, the payload data is sent to the application according to the identified method and action.

In certain situations, injection fields cannot be extracted from newly extracted ‘form’ tags, so another method is used to extract them based on the form data already present in the scanner memory by providing it as an argument.

def extract\_injection\_fields\_from\_form(form\_data):  
 try:  
 keys\_to\_populate = []  
 *# Find the emtpy form values, meaning they await user input, add them to a list and return the list* for key, value in form\_data.items():  
 if form\_data[key]:  
 continue  
 else:  
 keys\_to\_populate.append(key)  
 return keys\_to\_populate

This method receives the ‘form\_data’ as an argument, then it iterates through the available tags. If an empty tag is found, a list with the injection field names is populated and returned.

Another method used for attempting to find injection points is the ‘extract\_non\_form\_inputs’.

def extract\_non\_form\_inputs(self, url):  
 try:  
 name\_list = []  
 action\_urls = []  
 input\_list = self.extract\_inputs(url)  
 for input in input\_list:  
 name\_list.append(self.extract\_name\_value(input))  
 for name in name\_list:  
 action\_urls.append(str(url + '?' + str(name) + '='))  
 return action\_urls

This method is used to extract all the ‘input’ tag names and force them into URL parameters.

The last major method of this class is the method used for extracting special inputs either under ‘form’ tags or in the URL path.

def no\_form\_input\_content(url, payload):  
 try:  
 *# Extract inputs outside of form or with no method/action in form* input\_list\_fin = set()  
 form\_data = {}  
 response\_list = []  
 soup = BeautifulSoup(ScanConfig.session.get(url, timeout=300).content, 'html.parser')  
 input\_list = soup.findAll('input')  
 *# Get all inputs that have a form parent but no action or button.* for input in input\_list:  
 if input.find\_parent('form'):  
 parent\_attr = input.find\_parent('form').attrs  
 if not (('action' in parent\_attr) or ('button' in parent\_attr)):  
 input\_list\_fin.add(input)  
 else:  
 *# Get inputs with no form parent* input\_list\_fin.add(input)  
  
 if input\_list\_fin:  
 for field in input\_list\_fin:  
 if field.get('name'):  
 form\_data[field.get('name')] = payload

This method searches for inputs with a ‘form’ parent but with no action or method defined in the HTML DOM. The inputs are added to a list and returned.

The ‘Utilities’ class also contains more additional methods used for various purposes such as extracting the headers, preparing XML entities for injections, changing the User-Agent, extracting cookies, finding hidden inputs under DOM, printing the exception messages in color and formatting them based on time and date, extracting XML tags, escaping HTML encoded characters, creating average response time based on request dwell time. All of these methods will be referenced in the following Sub-Section under each related testing procedure.

## The Test files

Each test has a designated python file in which all the logic relevant to that test is contained. The testing methods apply the principles presented in the *Chapter III. Vulnerabilities and Misconfigurations* All the implemented testing functions apply the identification methods used by white-hat hackers but also by the attackers’ automated scanning tools. Each test has a major method called ‘run()’ used to call the testing logic for the specific file. Each file can have one or more additional methods used for various testing practices.

### SQL Tests

The SQL test file contains four methods used to identify the presence of SQL vulnerabilities. The first method is the standard method predominantly used in all future injection tests. This method contains the logic required for extracting forms and inputs from the provided URL using the ‘Utilities’ module.

def t\_i\_sql(url, form, form\_data):

injection\_keys = Utilities.extract\_injection\_fields\_from\_form(form\_data)

for sql\_payload in DataStorage.payloads("SQL"):  
 *# Populate injection keys with payloads.* for injection\_key in injection\_keys:  
 form\_data[injection\_key] = sql\_payload

Each payload from the DataStorage payload list is attempted as an test string. Depending on the response results, two types of SQL vulnerabilities can be found. The reflected type is usually containing a message with error or the injected payload itself.

if ("error" in response\_injected.text.lower() and 'error' not in ScanConfig.session.get(url)) or (  
 'error' in ScanConfig.session.get(url) and sql\_payload in response\_injected.text.lower()):  
 confidence += 1

The time-based test is done using the average response time. The testing payload contains instructions designed to make the SQL database hang execution (sleep) for minimum two seconds.

if payload\_response\_time > avg\_response\_time and payload\_response\_time > 2:  
 *# Vulnerable to Time based SQL type X, increase confidence* sql\_test\_confidence.add\_confidence(severity=0.8, past\_occurrences=0.1, exploitability=0.4, impact=0.4)  
 confidence += 1

To prevent the scanner from over-testing, a threshold of maximum four true positive reflected and one time-based attempt is conditioned as a stop flag.

if confidence == 4:  
 forms, form\_data = Utilities.extract\_from\_html\_string('form', response\_injected.text)  
 return sql\_payload, sql\_type\_list, forms, sql\_test\_confidence.calculate\_confidence()  
  
if confidence >= 1:  
 return sql\_payload, sql\_type\_list, form, sql\_test\_confidence.calculate\_confidence()

The SQL test method returns the SQL payload used, the SQL payload type, the vulnerable form and the test confidence (note: the ‘confidence’ variable is used just for threshold purposes and does not influence the actual confidence presented in the final report).

The second type of SQL testing is the one using the ‘non-form input’ testing method from the Utilities class. The same type of logic is applied here as well, with the only exception being the input fields the tests are performed for.

def t\_i\_sql\_nfi(url):

response\_injected = Utilities.no\_form\_input\_content(url, sql\_payload)  
if not response\_injected:  
 continue  
for response\_inj in response\_injected:  
 if response\_inj.elapsed.total\_seconds() > 4.5:  
 sql\_test\_confidence.add\_confidence(severity=0.8, past\_occurrences=0.1, exploitability=0.5, impact=0.7)  
 return sql\_payload, sql\_test\_confidence.calculate\_confidence()

The third SQL testing method is based on User-Agent. For this attempt, the scanner injects the testing payloads into the headers of the request. The identification conditions are the same with the above methods.

for sql\_payload in DataStorage.payloads("SQL"):  
 *# Inject headers with payloads* headers = Utilities.custom\_user\_agent(sql\_payload)  
 try:  
 response = ScanConfig.session.get(url, timeout=30, headers=headers)

The last type of SQL test method is the XML injection with a SQL Payload. For this attempt, the scanner attempts to identify and inject XXE prepared data with SQL payloads into the request. For this, the testing method uses the ‘prepare\_xml\_inj’ method from the Utilities class, this method is used only for SQL and XML injection tests. The’‘prepare\_xml\_inj’ method has two parameters (URL and payload). This method uses RegEx to attempt to extract XML object from the page (using the ‘extract\_xml\_tags()’ method from Utilities module), modify them according to the provided parameters and return them back to the SQL testing method.

Extraction:

pattern\_tags = r'xmlHttp\.send\("([^"]+)"\);'  
pattern\_uri = r'xmlHttp\.open\("POST","([^"]+)"'  
match\_tags = re.search(pattern\_tags, ScanConfig.session.get(url).text, re.DOTALL)  
match\_uri = re.search(pattern\_uri, ScanConfig.session.get(url).text, re.DOTALL)

Preparing the SQL XXE payload:

This method also handles the situation if the application requires a specific URL to send the XML data.

if extracted\_uri and extracted\_tag:  
 *# Get the first content of the first identified tag and inject it with the custom XXE variable* prepared\_tag = re.sub(r'(<[^>]+>)([^<]+)(</[^>]+>)', r'\1' + '&XXE;' + r'\3', extracted\_tag, count=1)  
 *# Prepare the payload with specific requirements such as identified tags.* xml\_payload = '''<?xml version="1.0" encoding="utf-8"?>  
 <!DOCTYPE root [<!ENTITY XXE SYSTEM "{}"> ]>  
 {}'''.format(payload, prepared\_tag)  
  
 *# Prepare URL for injection, URL consist of custom POST request of XML.* pattern\_url = r'(.\*/)[^/]+$'  
 prepared\_url = re.sub(pattern\_url, r'\1' + extracted\_uri, url)  
  
 *# Return the pre-build URL and the custom XML payload* return prepared\_url, xml\_payload

SQL method sending XXE payload to custom URL:

if prepared\_url and custom\_payload:  
 try:  
 response = ScanConfig.session.post(prepared\_url, data=custom\_payload,  
 headers={'Content-Type': 'application/xml'})

After the data is sent to the application, the same verification conditions as in the previous SQL testing method are used to validate the SQL vulnerability.

All the previous testing methods are called in the ‘run()’ method under ‘InjectionSql’ file. The ‘run()’ method also handles the call to the report file providing the necessary information according to each test.

payload, xml\_url, confidence = t\_i\_xml\_sql(url)  
if payload:  
 payload = Utilities.escape\_string\_html(encoded\_single=payload)  
 html\_report.add\_vulnerability('SQL Injection in XML tag',  
 'SQL Injection in XML tag vulnerability identified on URL: {} using custom XML tags.'.format(  
 url), confidence, payload=payload, comment="Used custom URL for XML SQL Injection URL: {}.".format(xml\_url))

### XSS Tests

The XXS tests are very similar with the SQL ones. The only difference is that XSS does uses specific XSS payloads and does not test for XXE injections with XSS payloads, as XSS is only run in the client’s browser. The XSS vulnerability validation condition is based on the existence of the XSS payload into the application response. If the application response contains the unmodified payload string, it means that the data was successfully interpreted by the HTML page, since any tag on the page is valid for the HTML interpreter. Similar with the SQL test, this tests also has a threshold of four true positive identifications.

if (str(xss\_payload).lower() in str(response\_injected.text).lower()) or (  
 str(xss\_payload).lower() in str(html.unescape(response\_injected.text.lower()))) or str(html.unescape(str(xss\_payload).lower()) in str(response\_injected.text).lower()):  
 confidence += 1

### HTML Tests

Also, very similar with the previous two testing practice, the HTML Injection is also performed on the standard inputs and only on the ‘non-form inputs’. Due to their nature, HTML injection cannot be done on User-Agents or XXE tags, so testing for those is not required. The vulnerability validation is performed the same way the XSS one is, by confirming the existence of the HTML injected payload into the application response.

if html\_payload.lower() in response\_injected.text.lower():  
 confidence += 1

The same threshold rules apply to HTML injections as well.

### Code Execution Tests

Code execution tests are performed only for standard and ‘non-form’ inputs. Unlike the previous testing methods, the code execution test does not contain a DataStorage object for storing payloads. For this test, the injected payload is a UNIX command, preceded by a pipe (|), that once executed pings the loopback address (127.0.0.1) for 3 seconds.

code\_exec\_payload = "|ping -c 3 127.0.0.1"

The pipe (|) character is used to chain a series of commands under the same CLI line.

Since it is a time-based detection, this method will ensure that both reflected and time-based Code Execution vulnerabilities are detected:

for injection\_key in injection\_keys:  
 form\_data[injection\_key] = html.unescape(code\_exec\_payload)  
response = Utilities.submit\_form(url, form, form\_data)

The vulnerability validation is performed by comparing the average response time with the injected response one.

if response.elapsed.total\_seconds() > 1.5 and response.elapsed.total\_seconds() > avg\_response\_time:  
 forms, form\_data = Utilities.extract\_from\_html\_string('form', response.text)

This testing method does not require a threshold as this is the only attempted payload for this test.

### iFrame Tests

For iFrame testing, the application attempts to extract all available iFrames from the web page using the ‘extract\_iframe()’ method.

def extract\_iframes(url):  
 *# Extract iFrames the same way forms are extracted* response = ScanConfig.session.get(url, timeout=300)  
 response.raise\_for\_status()  
 parsed\_html = BeautifulSoup(response.content, "html.parser"return parsed\_html.findAll("iframe")

From the extracted iFrame, the source value in the URL is modified to a custom one provided as payload.

If iframe[‚src’] in url:  
 url = url.replace(iframe[‚src’], payload)

The payload value is actually the ‘https://www.google.com' URL. The testing method then sends a get request to the modified URL. For validation, the iFrame payload is searched in the response body. If the value is found, the application is vulnerable to iFrame injection on that specific URL.

if iframe\_payload in ScanConfig.session.get(iframe\_url).text.lower():  
 return iframe\_url

### Javascript Test

Javascript code injection tests are very similar with the Code Execution tests, the only difference is the payload used and the method of injection. For JS Injection, the URL is brute forced with the JS payload. The JS payload is provided as a parameter in the URL either by replacing already existing parameters or by concatenating the JS payload to the URL, as the payload already contains the parameter definition symbol (?).

js\_payload = '/?javascript:alert("testedforjavascriptcodeexecutionrn3284")'

if url[-1] != '/':  
 new\_url = url + js\_payload

else:  
 new\_url = url + js\_payload[1:]

For vulnerability validation, the JS payload is searched in the response body, if the payload is identified the application is considered vulnerable.

### IDOR Tests

**References**

|  |  |
| --- | --- |
| [1] | T. Naiboiu, Web Application Vulnerability Scanner, Bucharest: University Of Bucharest, 2021. |
| [2] | CISA, 1 February 2021. [Online]. Available: https://www.cisa.gov/news-events/news/what-cybersecurity. [Accessed 1 August 2024]. |
| [3] | BUGTI, "Website Hacking Statistics 2024," BUGTI, 07 05 2024. [Online]. Available: https://www.bugtiwallet.com/website-hacking-statistics-2024/. [Accessed 1 August 2024]. |
| [4] | A. Volle, "Web application," [Online]. Available: https://www.britannica.com/topic/Web-application. [Accessed 1 August 2024]. |
| [5] | W. I. a. W. Browser?. [Online]. Available: https://www.lifewire.com/what-is-a-browser-446234. [Accessed 1 August 2024]. |
| [6] | "OWASP," [Online]. Available: https://owasp.org/www-project-top-ten/. [Accessed 1 August 2024]. |
| [7] | K. Crawley, 10 06 2021. [Online]. Available: https://www.hackthebox.com/blog/what-is-ctf. [Accessed 1 August 2024]. |
| [8] | "What is Python?," [Online]. Available: https://www.qamadness.com/knowledge-base/python-for-automation-why-is-it-great-and-how-to-use-it/. [Accessed 1 August 2024]. |
| [9] | "Beautiful Soup Documentation," [Online]. Available: https://beautiful-soup-4.readthedocs.io/en/latest/. [Accessed 1 August 2024]. |
| [10] | "Requests: HTTP for Humans," [Online]. Available: https://docs.python-requests.org/en/latest/index.html. [Accessed 1 August 2024]. |
| [11] | "URL handling modules," [Online]. Available: https://docs.python.org/3/library/urllib.html. [Accessed 1 August 2024]. |
| [12] | "What is Python?," [Online]. Available: https://www.python.org/doc/essays/blurb/. [Accessed 1 August 2024]. |
| [13] | "Why is Python Important for Cybersecurity?," [Online]. Available: https://www.scaler.com/topics/cyber-security/cybersecurity-importance-for-python/. [Accessed 1 August 2024]. |
| [14] | "urllib.parse — Parse URLs into components," [Online]. Available: https://docs.python.org/3/library/urllib.parse.html#module-urllib.parse. [Accessed 1 August 2024]. |
| [15] | "urllib.request — Extensible library for opening URLs," [Online]. Available: https://docs.python.org/3/library/urllib.request.html#module-urllib.request. [Accessed 1 August 2024]. |
| [16] | "What are Threads in Computer Processor or CPU?," [Online]. Available: https://www.geeksforgeeks.org/what-are-threads-in-computer-processor-or-cpu/. [Accessed 1 August 2024]. |
| [17] | "os - Miscellaneous operating system interfaces," [Online]. Available: https://docs.python.org/3/library/os.html. [Accessed 1 August 2024]. |
| [18] | "configparser - Configuration file parser," [Online]. Available: https://docs.python.org/3/library/configparser.html. [Accessed 1 August 2024]. |
| [19] | "A Practical Guide to Regular Expressions," [Online]. Available: https://www.freecodecamp.org/news/practical-regex-guide-with-real-life-examples/. [Accessed 1 August 2024]. |
| [20] | "argparse — Parser for command-line options, arguments and sub-commands," [Online]. Available: https://docs.python.org/3/library/argparse.html. [Accessed 1 August 2024]. |
| [21] | "Escape sequences," [Online]. Available: https://en.cppreference.com/w/cpp/language/escape. [Accessed 1 August 2024]. |
| [22] | "Jinja," [Online]. Available: https://jinja.palletsprojects.com/en/2.10.x/. [Accessed 1 August 2024]. |
| [23] | "DVWA," [Online]. Available: https://www.kali.org/tools/dvwa/. [Accessed 1 August 2024]. |
| [24] | "BWapp - An extremely buggy web app!," [Online]. Available: http://itsecgames.com/. [Accessed 1 August 2024]. |
| [25] | "random - Generate pseudo-random numbers," [Online]. Available: https://docs.python.org/3/library/random.html. [Accessed 1 August 2024]. |
| [26] | "User-Agent," [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/User-Agent. [Accessed 1 August 2024]. |
| [27] | "datetime — Basic date and time types¶," [Online]. Available: https://docs.python.org/3/library/datetime.html. [Accessed 1 August 2024]. |
| [28] | "math — Mathematical functions," [Online]. Available: https://docs.python.org/3/library/math.html. [Accessed 1 August 2024]. |
| [29] | "colorama," [Online]. Available: https://pypi.org/project/colorama/. [Accessed 1 August 2024]. |
| [30] | "What Is JSON and How Do You Use It?," [Online]. Available: https://www.howtogeek.com/devops/what-is-json-and-how-do-you-use-it/. [Accessed 1 August 2024]. |
| [31] | TechTarget Contributor, "vulnerability (information technology)," [Online]. Available: https://www.techtarget.com/whatis/definition/vulnerability. [Accessed 03 August 2024]. |
| [32] | A. Ot, "What's the Difference Between Black-Hat and White-Hat Hackers?," [Online]. Available: https://www.makeuseof.com/what-are-black-white-hat-hackers/. [Accessed 03 August 2024]. |
| [33] | B. Lenaerts-Bergmans, "INJECTION ATTACKS," [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/injection-attack/. [Accessed 03 August 2024]. |
| [34] | S. Gupta, "What Is SQL & How Does It Work? A Guide to Structured Query Language," [Online]. Available: https://www.springboard.com/blog/data-analytics/what-is-sql/. [Accessed 03 August 2024]. |
| [35] | KirstenS, "Cross Site Scripting (XSS)," [Online]. Available: https://owasp.org/www-community/attacks/xss/. [Accessed 03 August 2024]. |
| [36] | A. Dizdar, "Reflected XSS: Examples, Testing, and Prevention," [Online]. Available: https://brightsec.com/blog/reflected-xss/. [Accessed 03 August 2024]. |
| [37] | A. Dizdar, "Stored XSS: Impact, Examples, and Prevention," [Online]. Available: https://brightsec.com/blog/stored-xss/. [Accessed 03 August 2024]. |
| [38] | "HTML Injection," [Online]. Available: https://www.imperva.com/learn/application-security/html-injection/. [Accessed 03 August 2024]. |
| [39] | J. Kent, "What Are iframe," [Online]. Available: https://www.cequence.ai/blog/api-security/what-are-iframe-injection-attacks/. [Accessed 04 August 2024]. |
| [40] | "JavaScript Tutorial," [Online]. Available: https://www.geeksforgeeks.org/javascript/. [Accessed 04 August 2024]. |
| [41] | "Insecure Direct Object Reference Prevention Cheat Sheet," [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Insecure\_Direct\_Object\_Reference\_Prevention\_Cheat\_Sheet.html. [Accessed 04 August 2024]. |
| [42] | Aptive, "Local File Inclusion (LFI) — Web Application Penetration Testing," [Online]. Available: https://medium.com/@Aptive/local-file-inclusion-lfi-web-application-penetration-testing-cc9dc8dd3601. [Accessed 04 August 2024]. |
| [43] | "What is PHP?," [Online]. Available: https://www.php.net/manual/en/intro-whatis.php. [Accessed 07 August 2024]. |
| [44] | M. Dahan, "SSI injection attacks and how to avoid them," [Online]. Available: https://www.comparitech.com/blog/information-security/ssi-injection-attacks/. [Accessed 07 August 2024]. |
| [45] | "Server-side request forgery (SSRF) attacks and how to prevent them," [Online]. Available: https://www.comparitech.com/blog/information-security/server-side-request-forgery-attacks/. [Accessed 07 August 2024]. |
| [46] | A. Jalli, "What Is XML?," [Online]. Available: https://builtin.com/data-science/xml. [Accessed 07 August 2024]. |
| [47] | K. Imtiaz, "Security Misconfiguration:," [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/security-misconfiguration/. [Accessed 07 August 2024]. |
| [48] | "Testing for Browser Cache Weaknesses," [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/latest/4-Web\_Application\_Security\_Testing/04-Authentication\_Testing/06-Testing\_for\_Browser\_Cache\_Weaknesses. [Accessed 07 August 2024]. |
| [49] | "Cache Poisoning and Cache Deception," [Online]. Available: https://book.hacktricks.xyz/pentesting-web/cache-deception. [Accessed 07 August 2024]. |
| [50] | S. Hobbs, "CORS Tutorial: A Guide to Cross-Origin Resource Sharing," [Online]. Available: https://auth0.com/blog/cors-tutorial-a-guide-to-cross-origin-resource-sharing/. [Accessed 07 August 2024]. |
| [51] | "Cross-Origin Resource Sharing (CORS) Vulnerability: Example and Prevention," [Online]. Available: https://medium.com/@tushar\_rs\_/cross-origin-resource-sharing-cors-vulnerability-example-and-prevention-588d299ff185. [Accessed 07 August 2024]. |
| [52] | "What is HHI (Host Header Injection) & How to Simply Test the Vulnerability," [Online]. Available: https://medium.com/mii-cybersec/what-is-hhi-host-header-injection-how-to-simply-test-the-vulnerability-4f1f74a36f9d. [Accessed 7 August 2024]. |
| [53] | A. Heddings, "What Is HSTS and How Do You Set It Up?," [Online]. Available: https://www.howtogeek.com/devops/what-is-hsts-and-how-do-you-set-it-up/. [Accessed 7 August 2024]. |
| [54] | "Rich Internet Applications," [Online]. Available: https://www.sciencedirect.com/topics/computer-science/rich-internet-applications. [Accessed 7 August 2024]. |
| [55] | "Introduction to robots.txt," [Online]. Available: https://developers.google.com/search/docs/crawling-indexing/robots/intro. [Accessed 7 August 2024]. |
| [56] | "What are cookies on websites?," [Online]. Available: https://www.cloudflare.com/learning/privacy/what-are-cookies/. [Accessed 7 August 2024]. |
| [57] | "Cookie Security," [Online]. Available: https://jscrambler.com/learning-hub/cookie-security. [Accessed 7 August 2024]. |
| [58] | A. Sharif, "What Is CVE?," [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/common-vulnerabilities-and-exposures-cve/. [Accessed 7 August 2024]. |
| [59] | "What is a Framework in Programming and Engineering?," [Online]. Available: https://aws.amazon.com/what-is/framework/. [Accessed 7 August 2024]. |
| [60] | "What is an API (Application Programming Interface)," [Online]. Available: https://www.geeksforgeeks.org/what-is-an-api/. [Accessed 11 August 2024]. |
| [61] | "National Vulnerability Database," [Online]. Available: https://nvd.nist.gov/. [Accessed 11 August 2024]. |
| [62] | "What is a Payload in Cyber Security? A Comprehensive Guide," [Online]. Available: https://networkinterview.com/what-is-a-payload-in-cyber-security/. [Accessed 11 August 2024]. |
| [63] | "SQL Payload List," [Online]. Available: https://github.com/payloadbox/sql-injection-payload-list. [Accessed 23 May 2024]. |
| [64] | "SQL Payload List," [Online]. Available: https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/SQL%20Injection/SQLite%20Injection.md. [Accessed 25 May 2024]. |
| [65] | "HTML Injection Payloads," [Online]. Available: https://github.com/InfoSecWarrior/Offensive-Payloads/blob/main/Html-Injection-Payloads.txt. [Accessed 26 May 2024]. |
| [66] | "XSS Injection Payloads," [Online]. Available: https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/XSS%20Injection. [Accessed 26 May 2024]. |
| [67] | "Other Payloads," [Online]. Available: https://github.com/swisskyrepo/PayloadsAllTheThings. [Accessed 26 May 2024]. |