CEH Module 6: System Hacking
Assignment - 03
(Marepalli Rakesh)

Given Lab Scenario

For a professional ethical hacker or pen tester, the first step in system hacking is to analyse the target system using information obtained and loopholes found in the system's access control mechanism. In this step, you will use various techniques such as password cracking, vulnerability exploitation, and social engineering to gain access to the target system. Password cracking is the process of recovering passwords from the data transmitted by a computer system or stored in it. It may help a user recover a forgotten or lost password or act as a preventive measure by system administrators to check for easily breakable passwords; however, an attacker can use this process to gain unauthorized system access.

Password cracking is one of the crucial stages of system hacking. Hacking often begins with password cracking attempts. A password is a key piece of information necessary to access a system. Consequently, most attackers use password-cracking techniques to gain unauthorized access. An attacker may either crack a password manually by guessing it or use automated tools and techniques such as a dictionary or brute-force method. Most password cracking techniques are successful, because of weak or easily guessable passwords. Vulnerability exploitation involves the execution of multiple complex, interrelated steps to gain access to a remote system. Attackers use discovered vulnerabilities to develop exploits, deliver and execute the exploits on the remote system. The labs in this exercise demonstrate how easily hackers can gather password information from your network and demonstrate the password vulnerabilities that exist in computer networks

Given Lab Objectives:

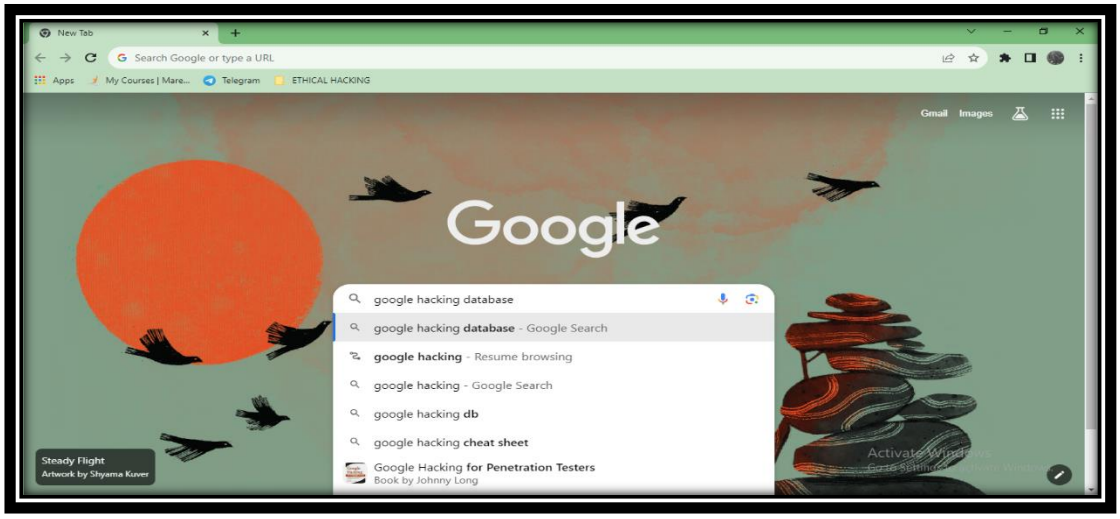
- Find vulnerabilities on exploit sites
- Intercept traffic using Burp suite software
- Perform vulnerability research using ZAP

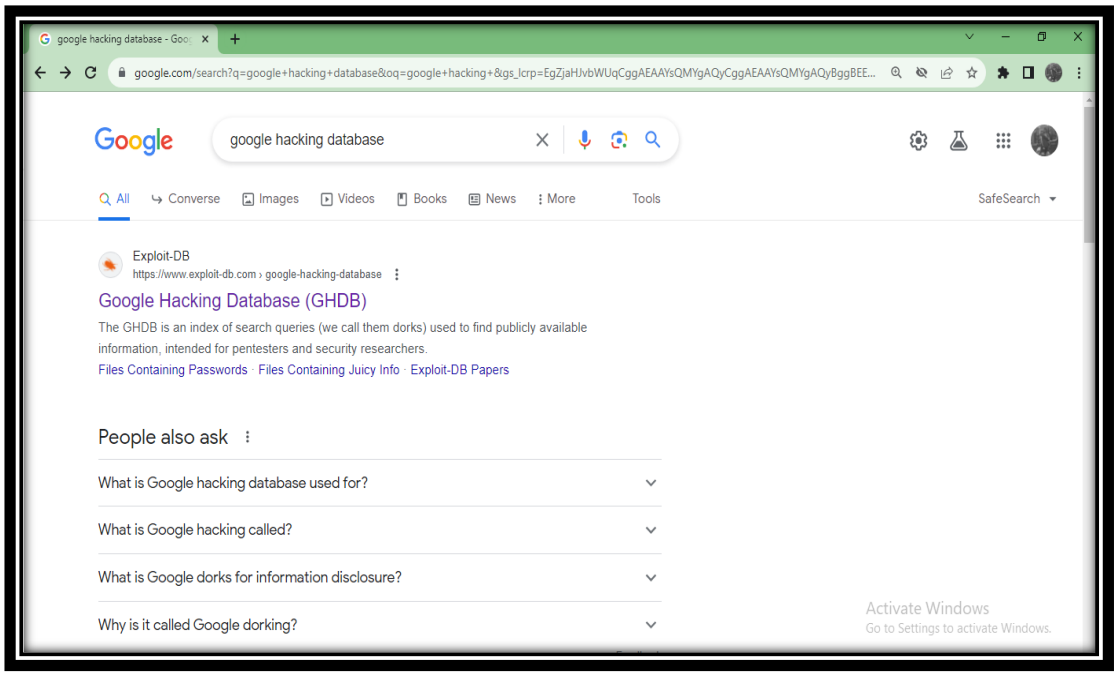
Objective: 01

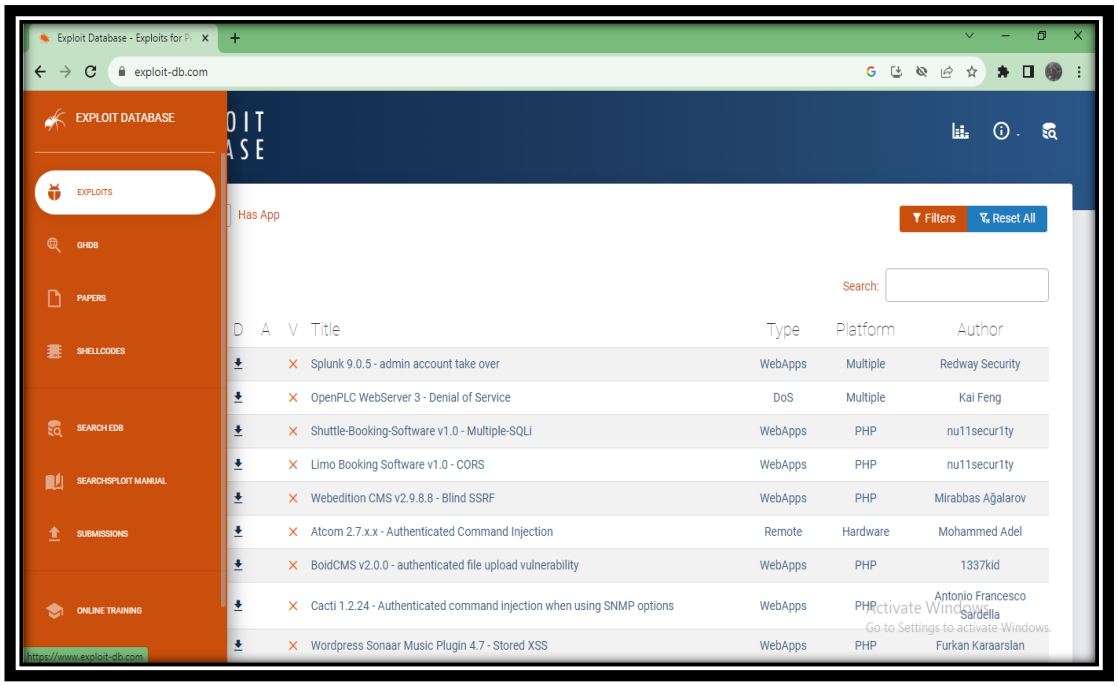
Find vulnerabilities on exploit sites

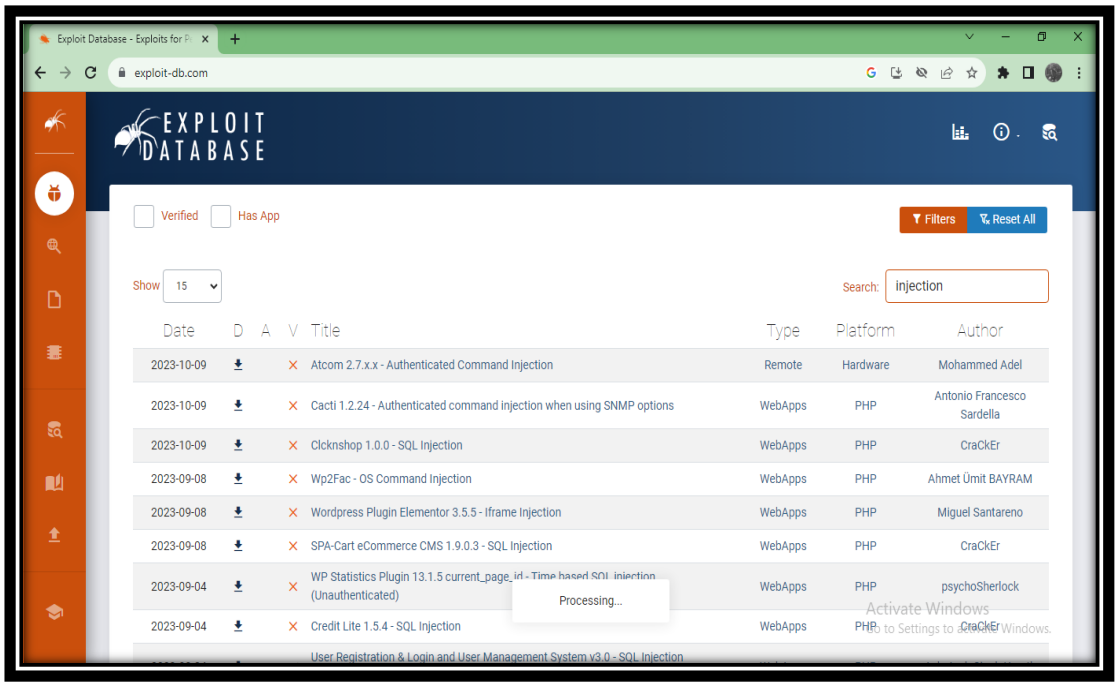
General:

- In the realm of cybersecurity, identifying and addressing vulnerabilities is of paramount importance. Vulnerabilities are potential weaknesses in software, systems, or networks that can be exploited by malicious actors, leading to security breaches or data compromises. One fertile ground for discovering and understanding vulnerabilities is through exploit sites.
- Exploit sites serve as virtual meeting points where security researchers, hackers, and enthusiasts exchange information about software vulnerabilities, known as "exploits," and share insights into their potential impact. This lab assignment focuses on the critical task of finding vulnerabilities within such exploit sites, with the goal of gaining deeper insights into the world of cybersecurity.
- The aim of this assignment was to explore vulnerabilities by utilizing online exploit databases, specifically the Google Hacking Database (GHDB) and the Common Vulnerabilities and Exposures (CVE) database.
- To commence the assignment, I opened a web browser and conducted a search for the Google Hacking Database (GHDB), a resource recognized for its extensive collection of vulnerabilities identified by security professionals. Also referred to as "exploit db," I accessed the GHDB and, on the left side of the interface, I located and clicked the 'Exploits' section. In the search bar, I entered the term "injection" as my focus was on identifying injection vulnerabilities, a common type. The GHDB yielded numerous injection vulnerabilities.

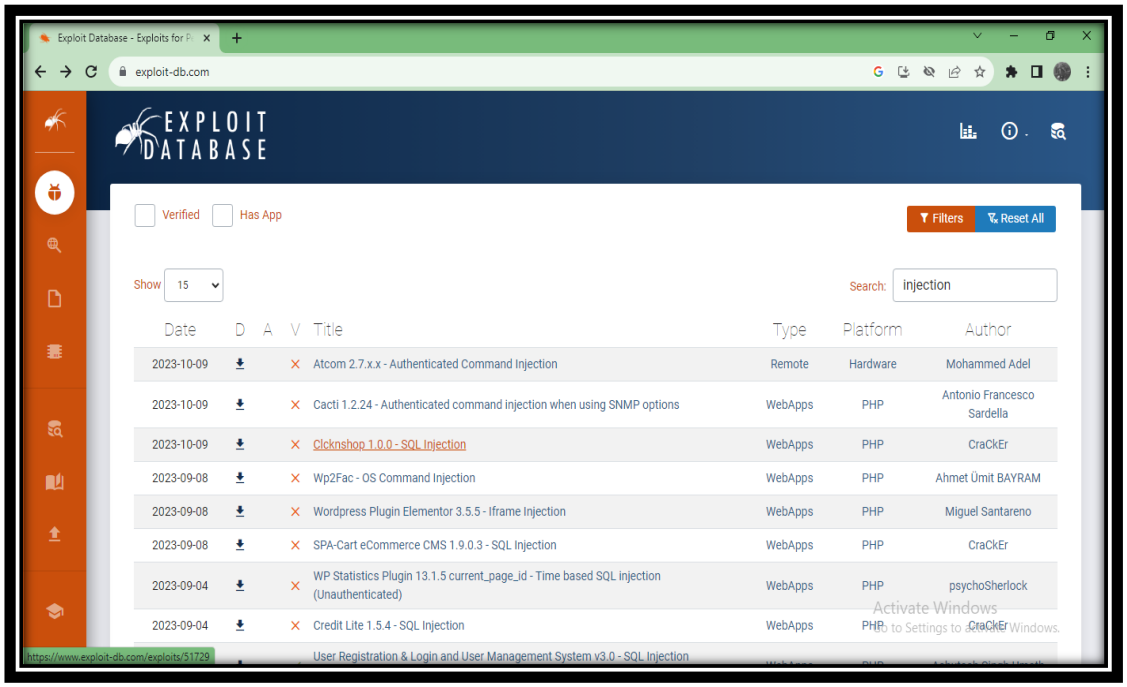


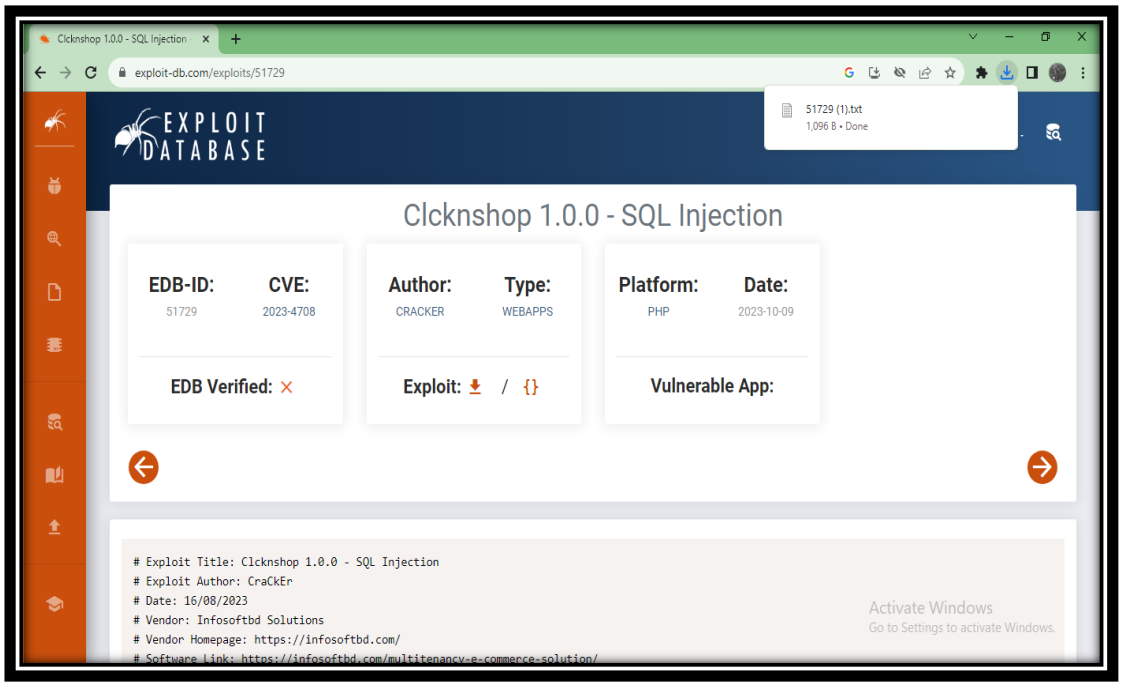

google hacking database - Goo
google.com/search?q=google+hacking+database&oq=google+hacking+&gs_lcrp=EgZjaHJvbWUqCggAEAAYsQMYgAQyCggAEAAYsQMYgAQyBggBEE...
Google
google hacking database
All
Converse
Images
Videos
Books
News
More
Tools
SafeSearch
Exploit-DB
https://www.exploit-db.com › google-hacking-database
Google Hacking Database (GHDB)
The GHDB is an index of search queries (we call them dorks) used to find publicly available information, intended for pentesters and security researchers.
Files Containing Passwords · Files Containing Juicy Info · Exploit-DB Papers
People also ask
What is Google hacking database used for?
What is Google hacking called?
What is Google dorks for information disclosure?
Why is it called Google dorking?
Activate Windows
Go to Settings to activate Windows.

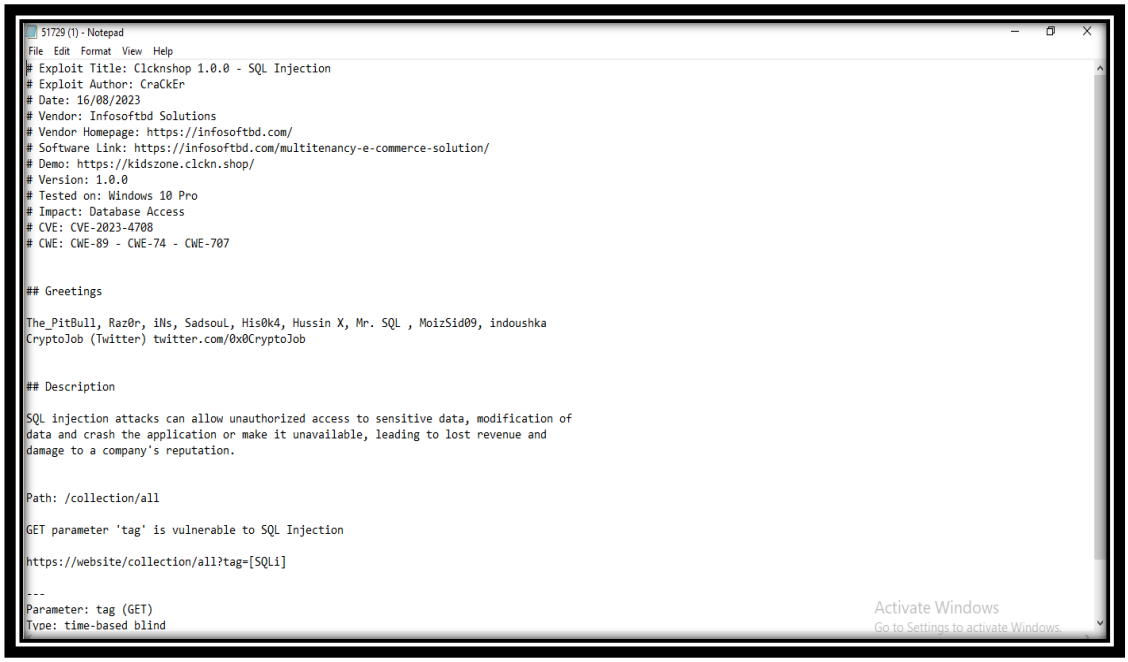

Exploit Database - Exploits for P
exploit-db.com
EXPLOIT DATABASE
EXPLOITS
GHDB
PAPERS
SHELLCODES
SEARCH EDB
SEARCHSPLOIT MANUAL
SUBMISSIONS
ONLINE TRAINING
Has App
Filters
Reset All
Search:
D A V Title Type Platform Author
Splunk 9.0.5 - admin account take over WebApps Multiple Redway Security
OpenPLC WebServer 3 - Denial of Service DoS Multiple Kai Feng
Shuttle-Booking-Software v1.0 - Multiple-SQLi WebApps PHP nu11secur1ty
Limo Booking Software v1.0 - CORS WebApps PHP nu11secur1ty
Webedition CMS v2.9.8.8 - Blind SSRF WebApps PHP Mirabbas Ağalarov
Atcom 2.7.x.x - Authenticated Command Injection Remote Hardware Mohammed Adel
BoidCMS v2.0.0 - authenticated file upload vulnerability WebApps PHP 1337kid
Cacti 1.2.24 - Authenticated command injection when using SNMP options WebApps PHP Antonio Francesco Sardella
Wordpress Sonaar Music Plugin 4.7 - Stored XSS WebApps PHP Furkan Karaarslan
Activate Windows
Go to Settings to activate Windows.



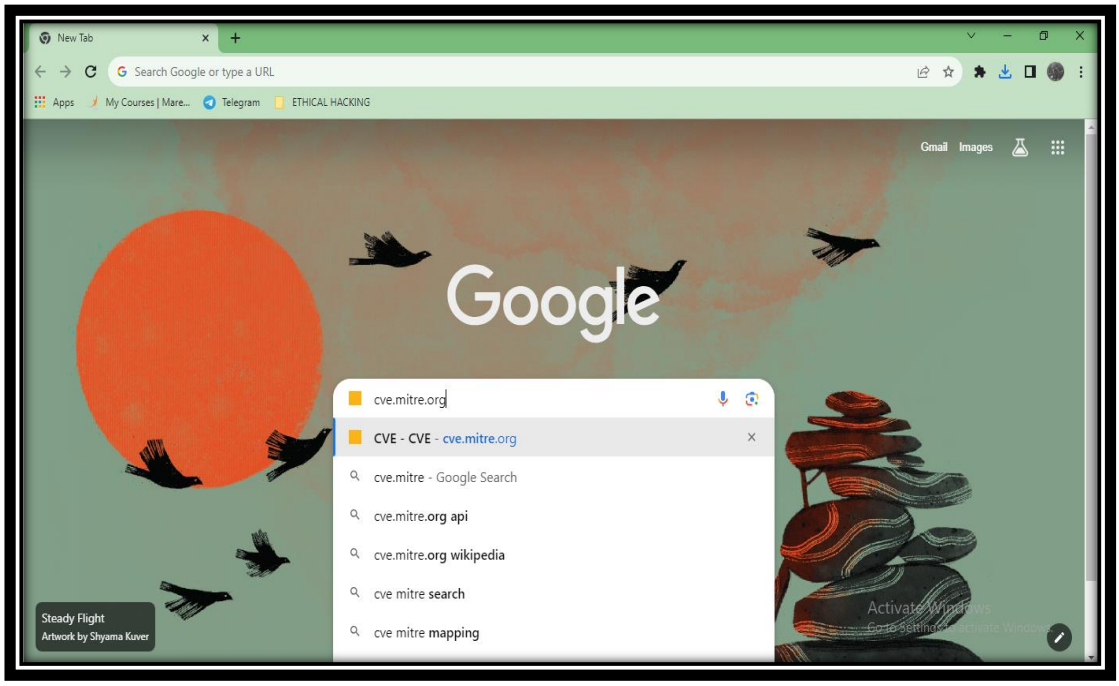
- Specifically, I selected the "SQL Injection" vulnerability, which led me to a dedicated page containing various options related to this specific vulnerability. Among these options, I chose to download the details of the vulnerability in text format, which included essential information such as the exploit title, author, date, description, path, parameters, and other pertinent data for comprehensive understanding.

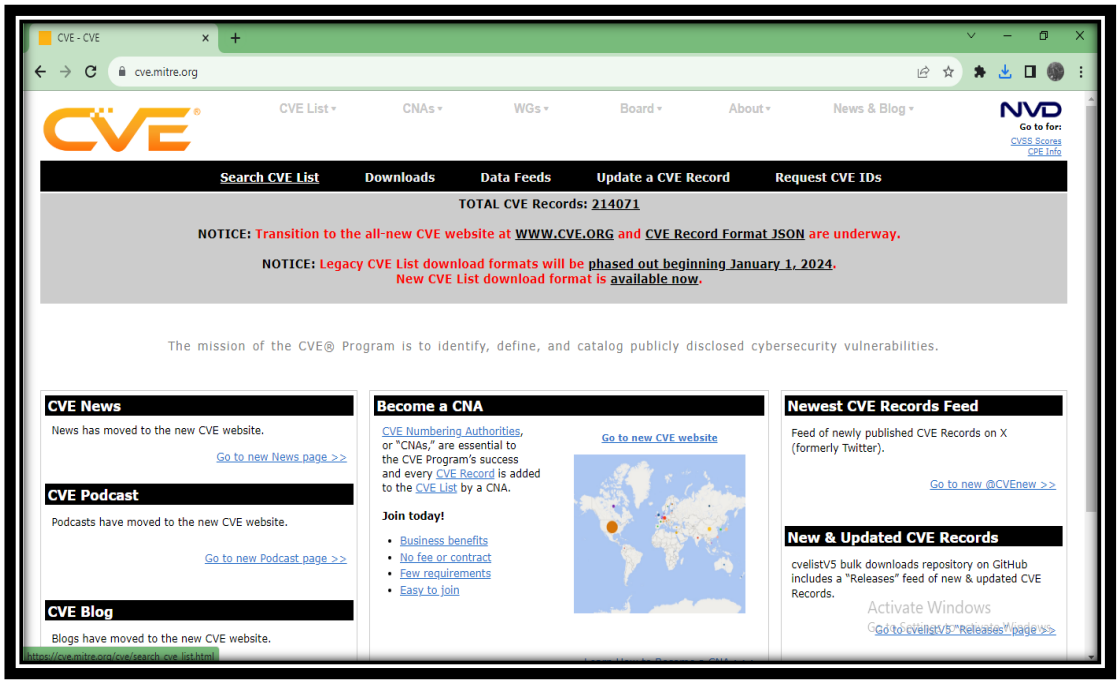


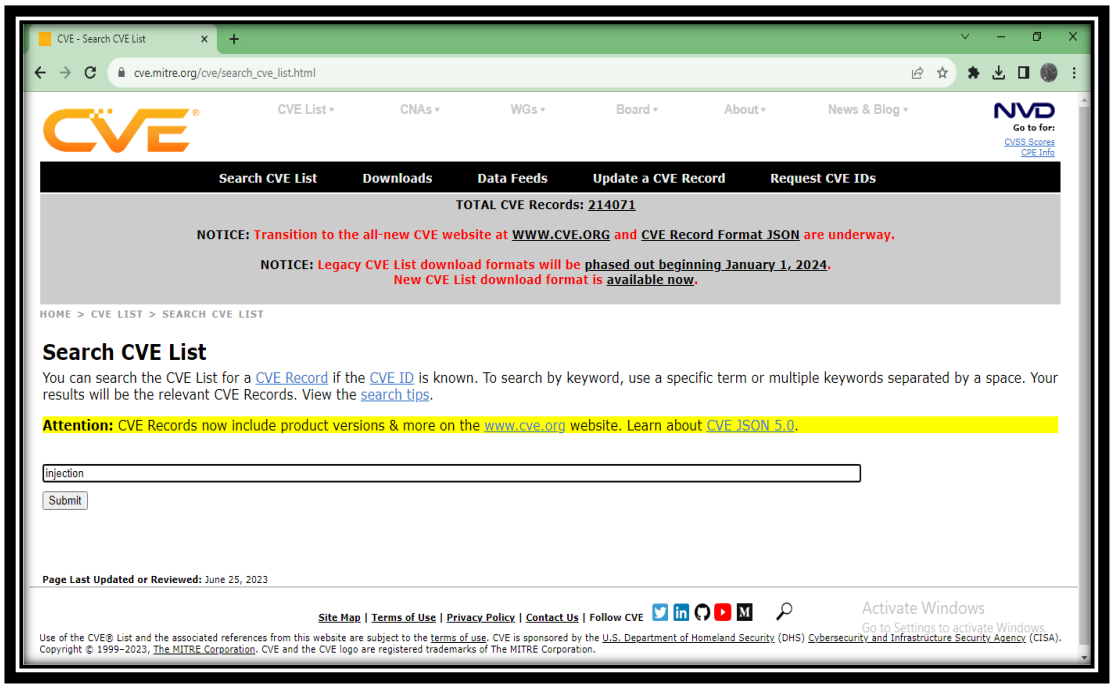




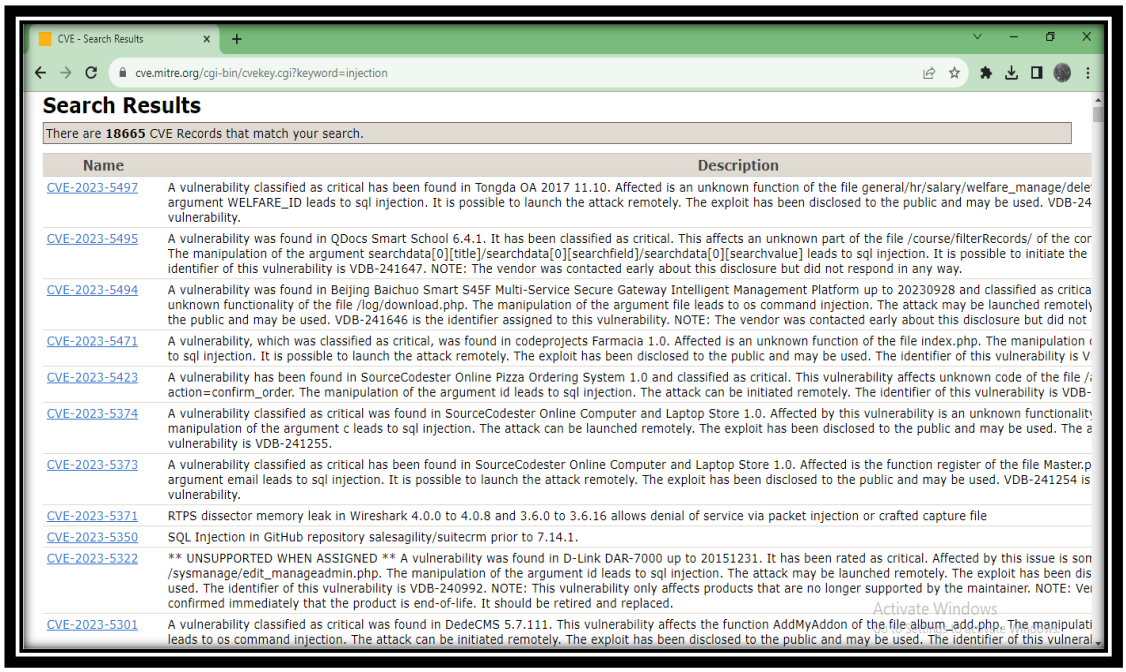
- Subsequently, I explored another exploit database, cve.mitre.org, and upon entering this site, I observed an option located at the top-left corner labelled 'Search CVE List.' Upon clicking this option, a search bar appeared, and I once again conducted a search for injection vulnerabilities by typing "injection" and submitting the query.

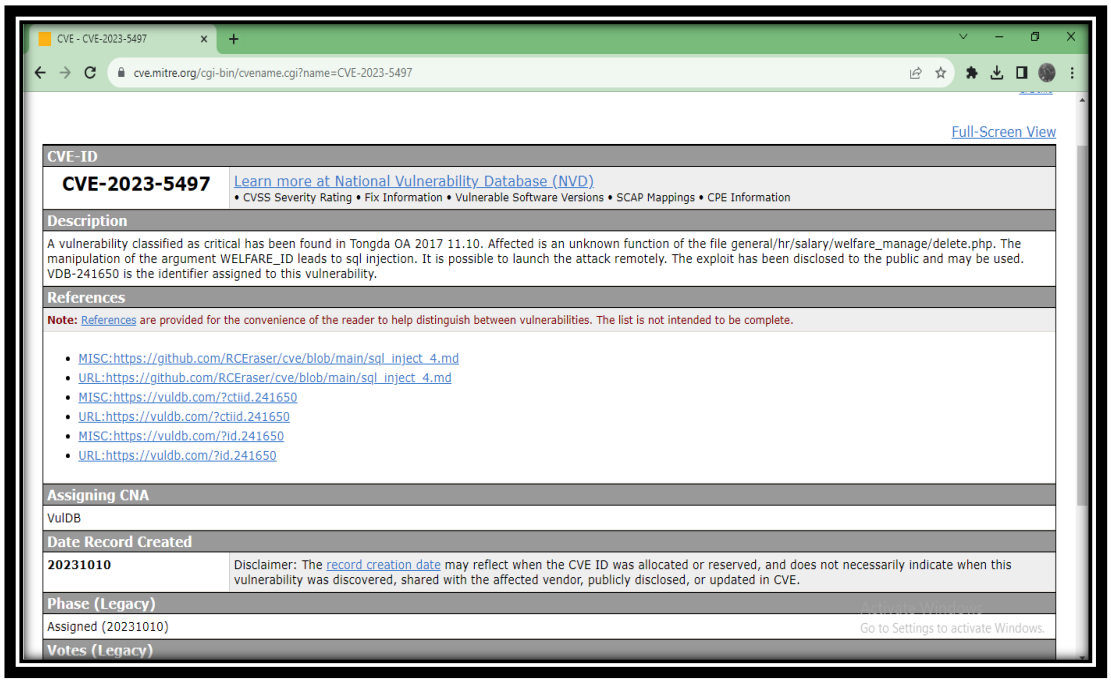

New Tab
Search Google or type a URL
Apps
My Courses | Mare...
Telegram
ETHICAL HACKING
Gmail
Images
Google
cve.mitre.org
CVE - CVE - cve.mitre.org
cve.mitre - Google Search
cve.mitre.org api
cve.mitre.org wikipedia
cve mitre search
cve mitre mapping
Steady Flight
Artwork by Shyama Kuver
Activate Windows


CVE - CVE
cve.mitre.org
CVE List
CNAs
WGs
Board
About
News & Blog
NVD
Go to for:
CVSS Scores
CPE Info
Search CVE List
Downloads
Data Feeds
Update a CVE Record
Request CVE IDs
TOTAL CVE Records: 214071
NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.
NOTICE: Legacy CVE List download formats will be phased out beginning January 1, 2024.
New CVE List download format is available now.
The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.
CVE News
News has moved to the new CVE website.
Go to new News page >>
CVE Podcast
Podcasts have moved to the new CVE website.
Go to new Podcast page >>
CVE Blog
Blogs have moved to the new CVE website.
Become a CNA
CVE Numbering Authorities, or "CNAs," are essential to the CVE Program's success and every CVE Record is added to the CVE List by a CNA.
Go to new CVE website
Join today!
Business benefits
No fee or contract
Few requirements
Easy to join
Newest CVE Records Feed
Feed of newly published CVE Records on X (formerly Twitter).
Go to new @CVEnew >>
New & Updated CVE Records
cvelistV5 bulk downloads repository on GitHub includes a "Releases" feed of new & updated CVE Records.
Go to cvelistV5 "Releases" page >>
Activate Windows



- The search results displayed a list of injection vulnerabilities denoted by numbers and accompanied by brief descriptions. By selecting one of these numbered vulnerabilities, I accessed a detailed page that provided additional information about the specific vulnerability, including extended descriptions, reference URLs, and other relevant details.



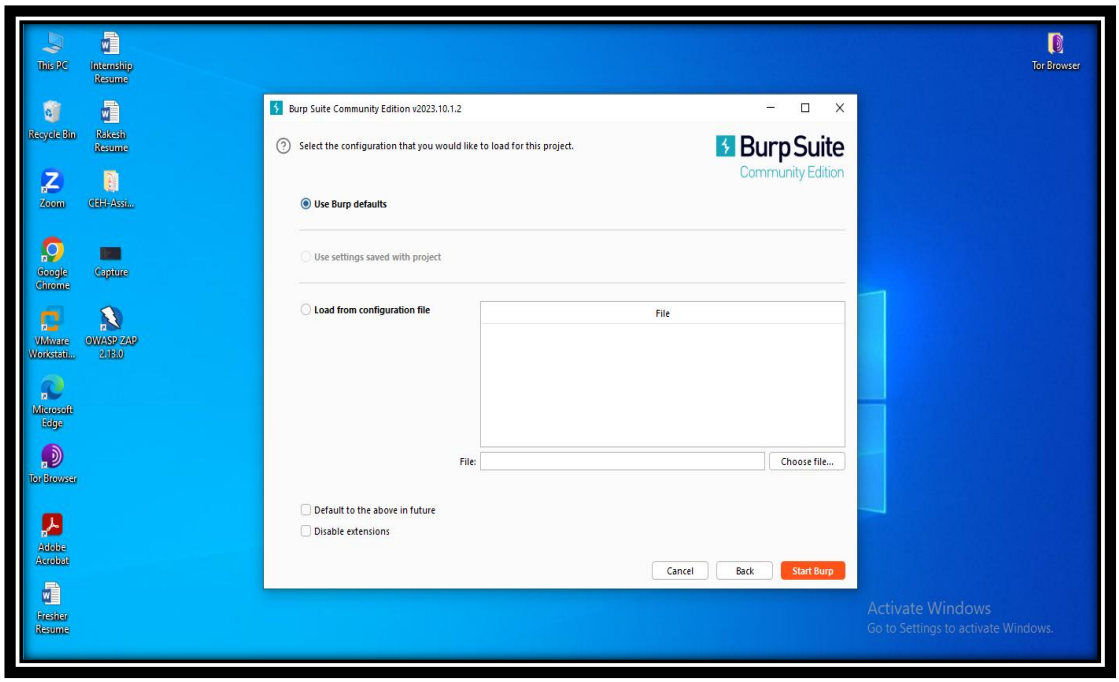


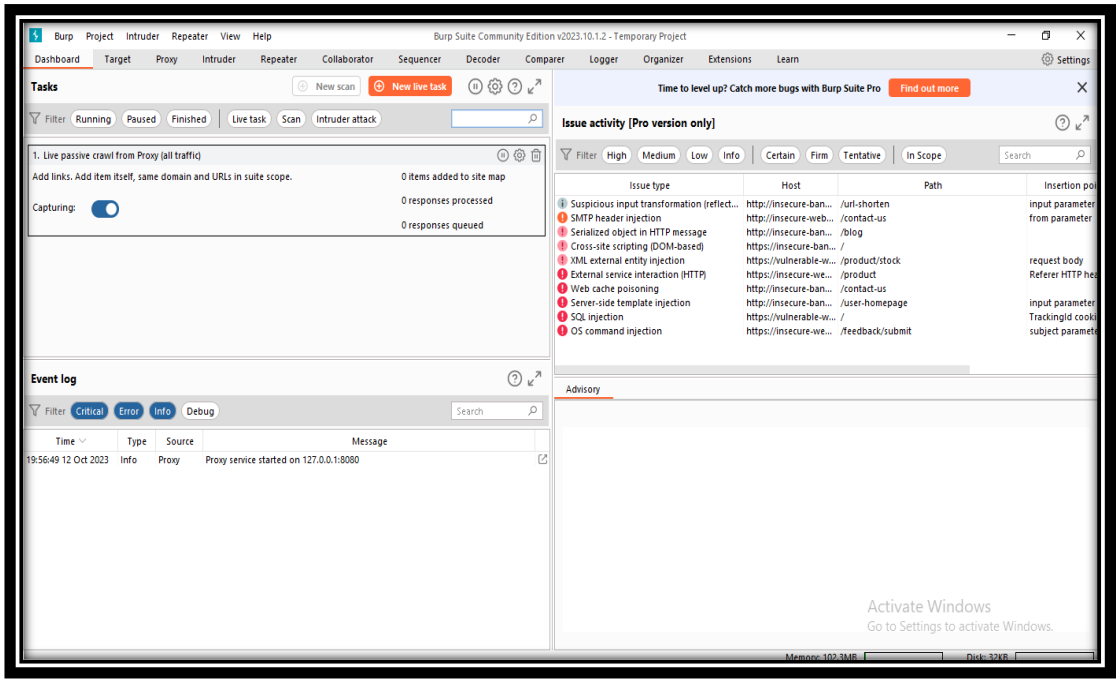
- This assignment allowed me to gain insights into vulnerabilities and their documentation through these two valuable exploit databases.

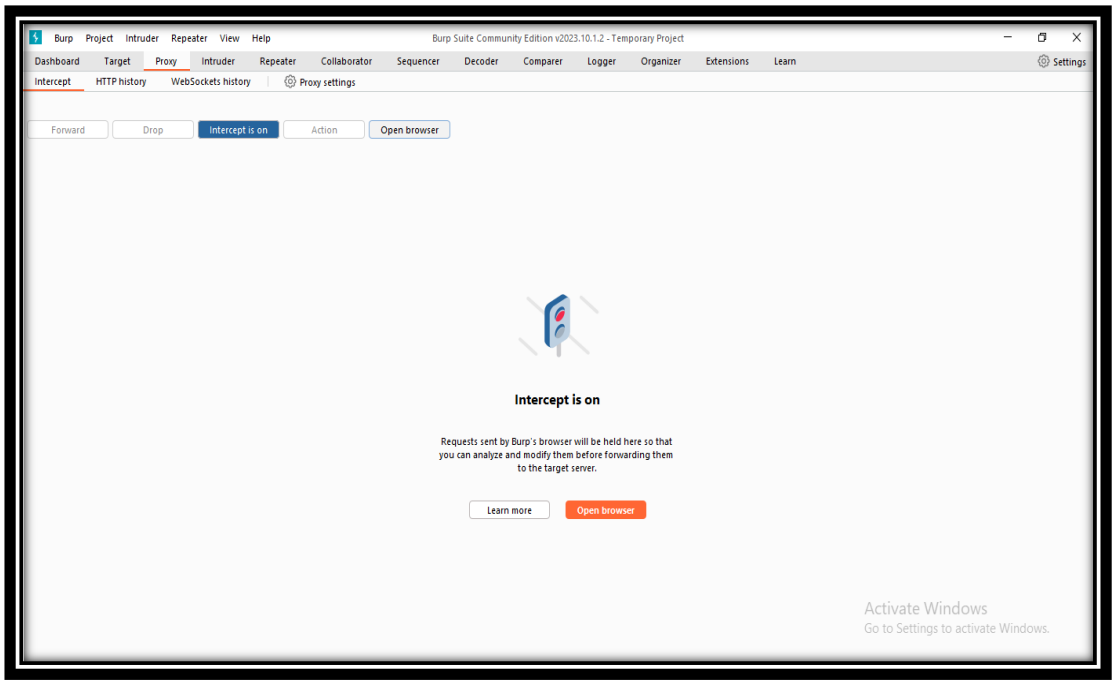
Objective: 02

Intercept traffic using Burp suite software

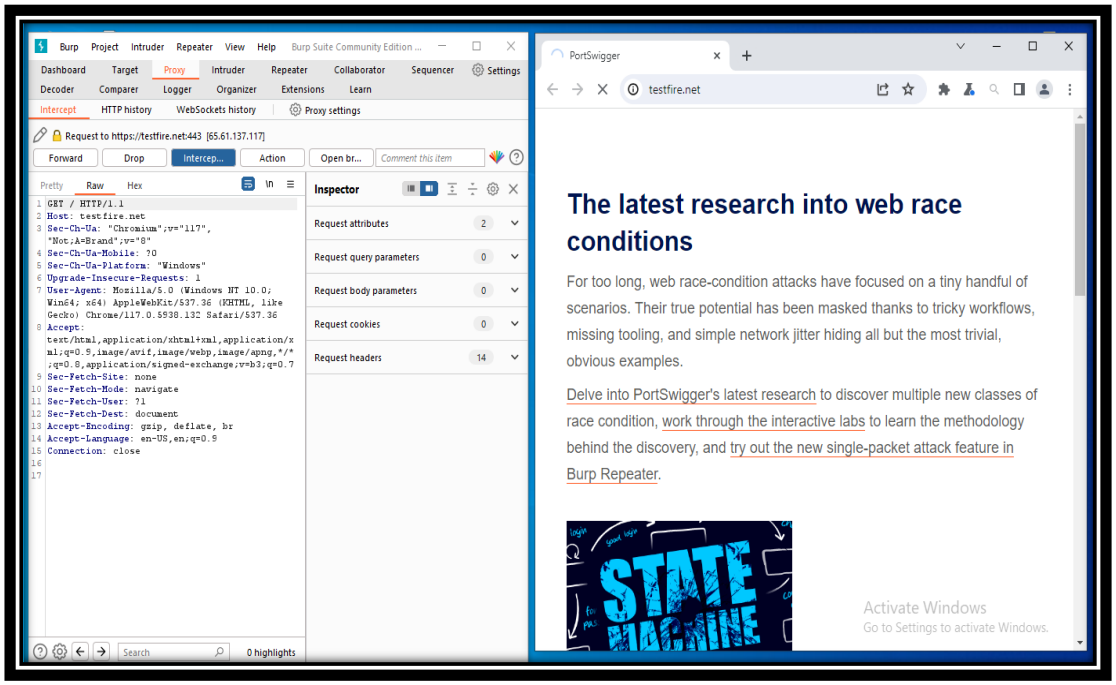
- In the dynamic field of cybersecurity, the ability to intercept and scrutinize network traffic is a pivotal skill for security professionals and ethical hackers. Understanding the flow of data within a network and being capable of intercepting this data is essential for identifying vulnerabilities, maintaining data integrity, and safeguarding against potential threats. This lab assignment is dedicated to the fundamental task of intercepting network traffic using an indispensable tool: Burp Suite.
- To start, I downloaded Burp Suite and launched it on my base machine, selecting a temporary project. Upon opening Burp Suite, I accessed the dashboard. In the dashboard, I navigated to the "Proxy" option, which presented several sub-options, including "Intercept" and "Proxy Settings." Within the "Proxy" section, I activated the "Intercept" option and then clicked on the "Browser" option.

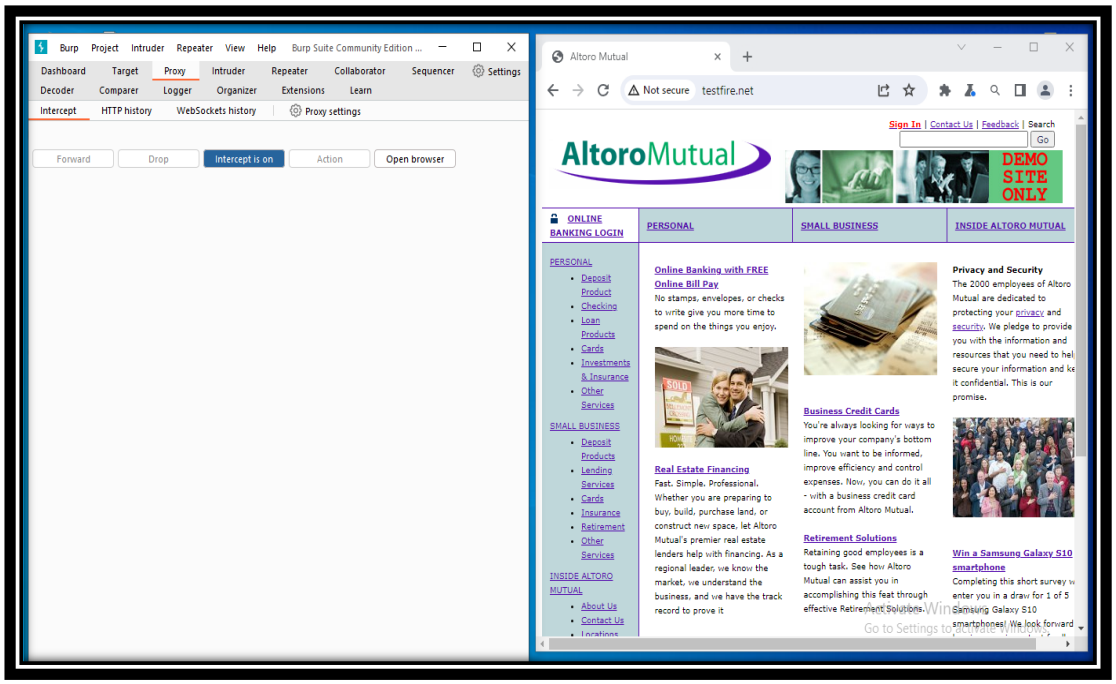

This PC
Internship Resume
Recycle Bin
Rakesh Resume
Zoom
CEH-Assi...
Google Chrome
Capture
VMware Workstati...
OWASP ZAP 2.13.0
Microsoft Edge
Tor Browser
Adobe Acrobat
Fresher Resume
Tor Browser
Burp Suite Community Edition v2023.10.1.2
Select the configuration that you would like to load for this project.
Burp Suite
Community Edition
Use Burp defaults
Use settings saved with project
Load from configuration file
File
File:
Choose file...
Default to the above in future
Disable extensions
Cancel
Back
Start Burp
Activate Windows
Go to Settings to activate Windows.

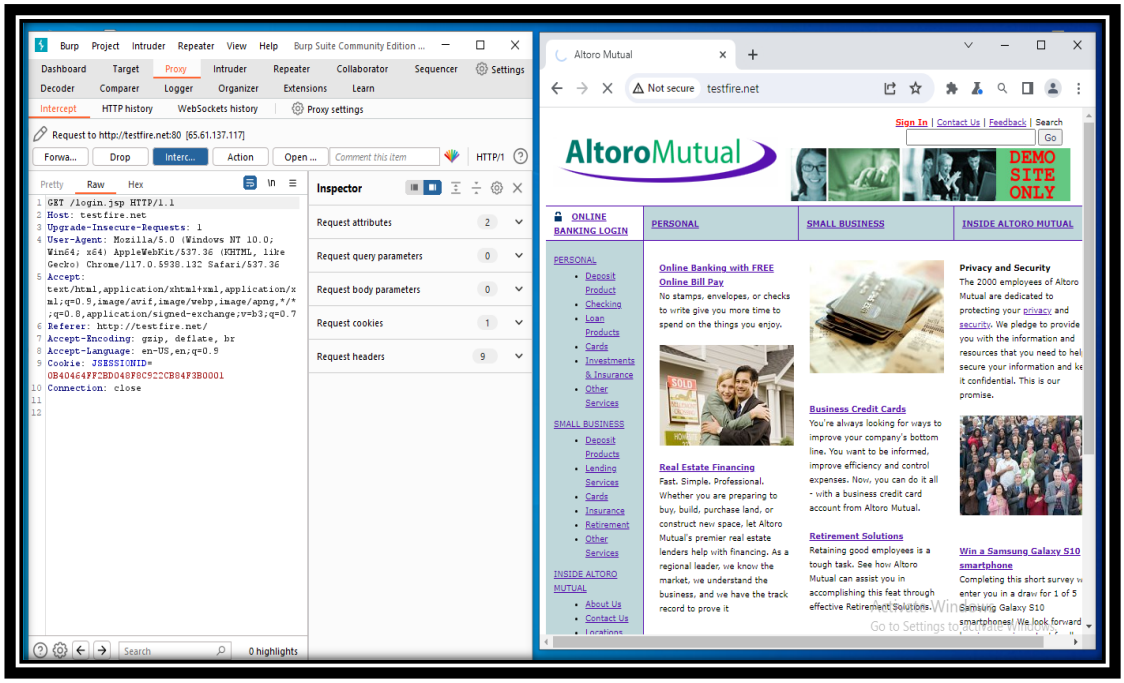

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.10.1.2 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Tasks
New scan
New live task
Filter Running Paused Finished Live task Scan Intruder attack
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing:
0 items added to site map
0 responses processed
0 responses queued
Time to level up? Catch more bugs with Burp Suite Pro
Find out more
Issue activity [Pro version only]
Filter High Medium Low Info Certain Firm Tentative In Scope
Search
Issue type
Host
Path
Suspicious input transformation (reflect...
http://insecure-ban...
/url-shorten
SMTP header injection
http://insecure-web...
/contact-us
Serialized object in HTTP message
http://insecure-ban...
/blog
Cross-site scripting (DOM-based)
https://insecure-ban...
/
XML external entity injection
https://vulnerable-w...
/product/stock
External service interaction (HTTP)
https://insecure-we...
/product
Web cache poisoning
http://insecure-ban...
/contact-us
Server-side template injection
http://insecure-ban...
/user-homepage
SQL injection
https://vulnerable-w...
/
OS command injection
https://insecure-we...
/feedback/submit
Event log
Filter Critical Error Info Debug
Search
Time
Type
Source
Message
19:56:49 12 Oct 2023
Info
Proxy
Proxy service started on 127.0.0.1:8080
Advisory
Activate Windows
Go to Settings to activate Windows.
Memory: 102.3MB
Disk: 32KB



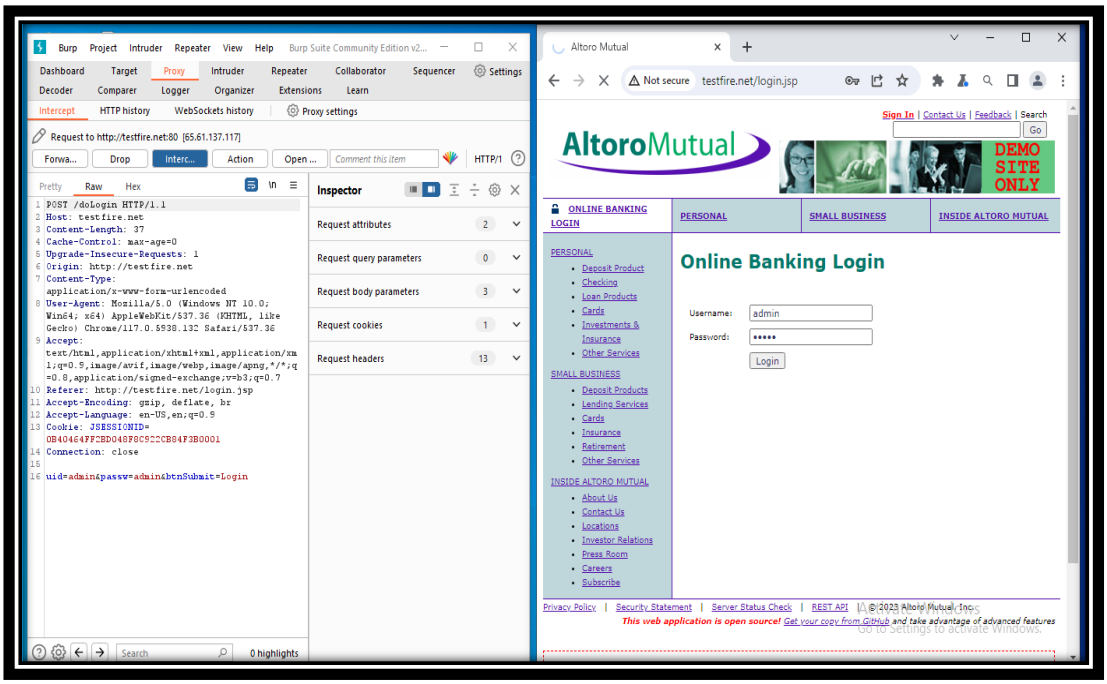
- With the browser interface open, I entered the target web application's URL, testfire.net "Altoro Mutual Banking web application." Returning to Burp Suite, I observed that it had intercepted the web traffic, capturing various pieces of information. I clicked "Forward" in Burp Suite and then returned to the browsers. As a result, the target web application, Altoro Mutual Banking, opened in the browser.

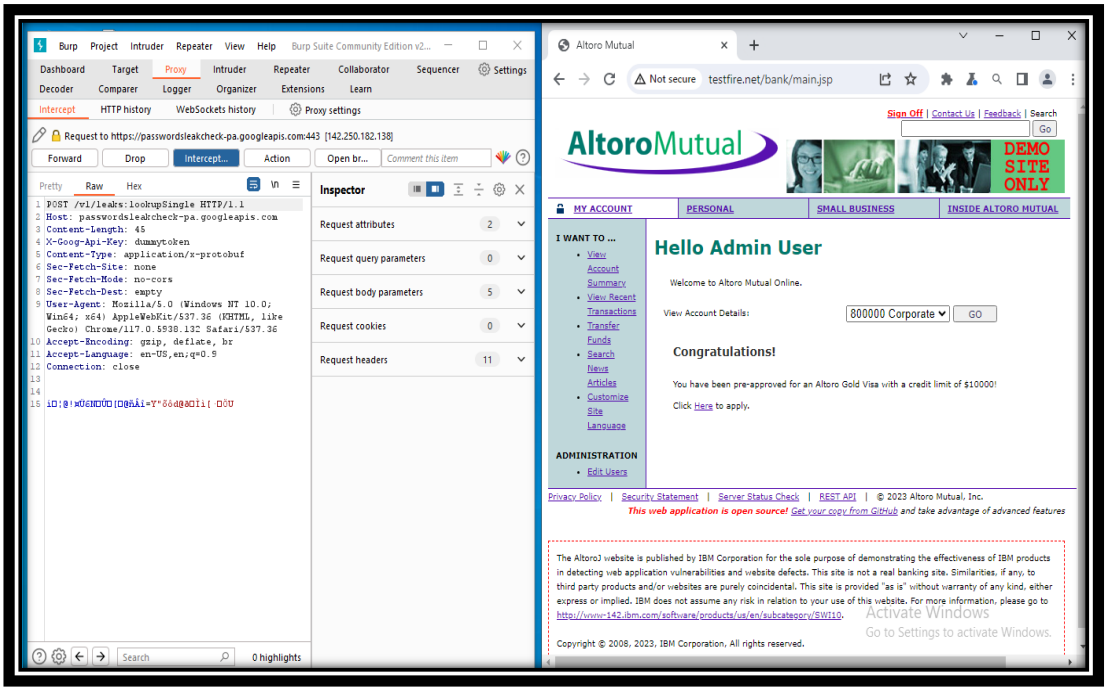






- Proceeding with the assignment, I clicked on the "Sign In" option within the target web application. Returning to Burp Suite, it continued to capture all traffic. Clicking "Forward" in Burp Suite once again, I returned to the browser interface, where I could access the login portal. Here, I entered my login credentials and clicked the "Login" button.



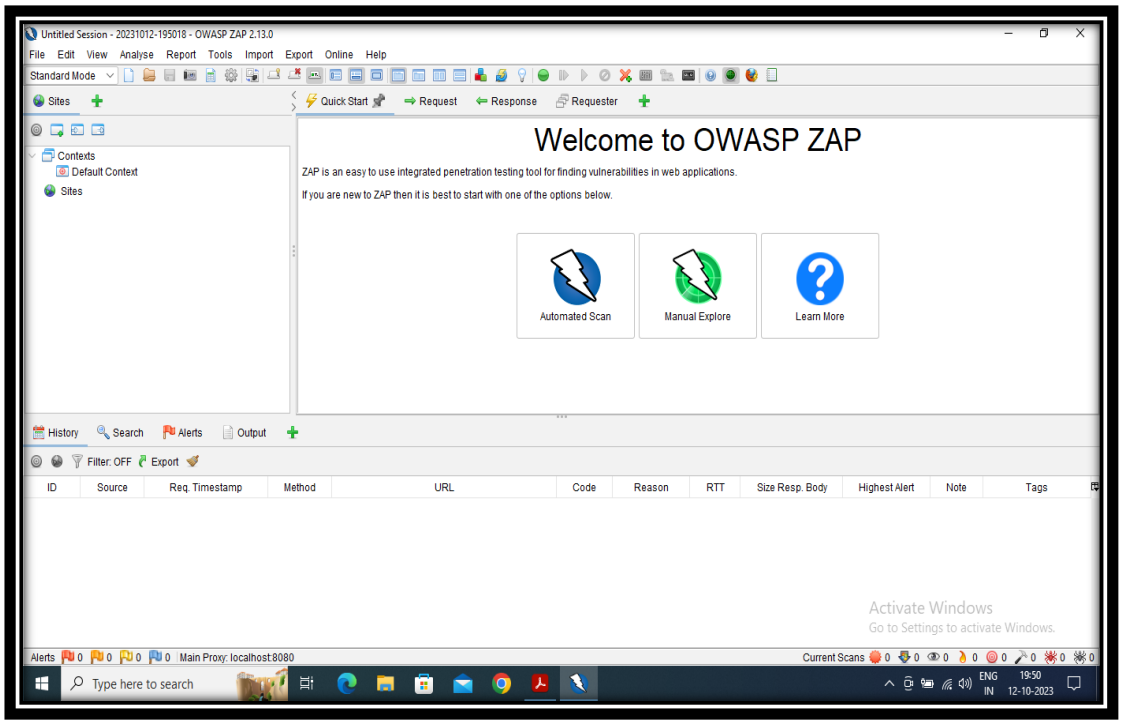


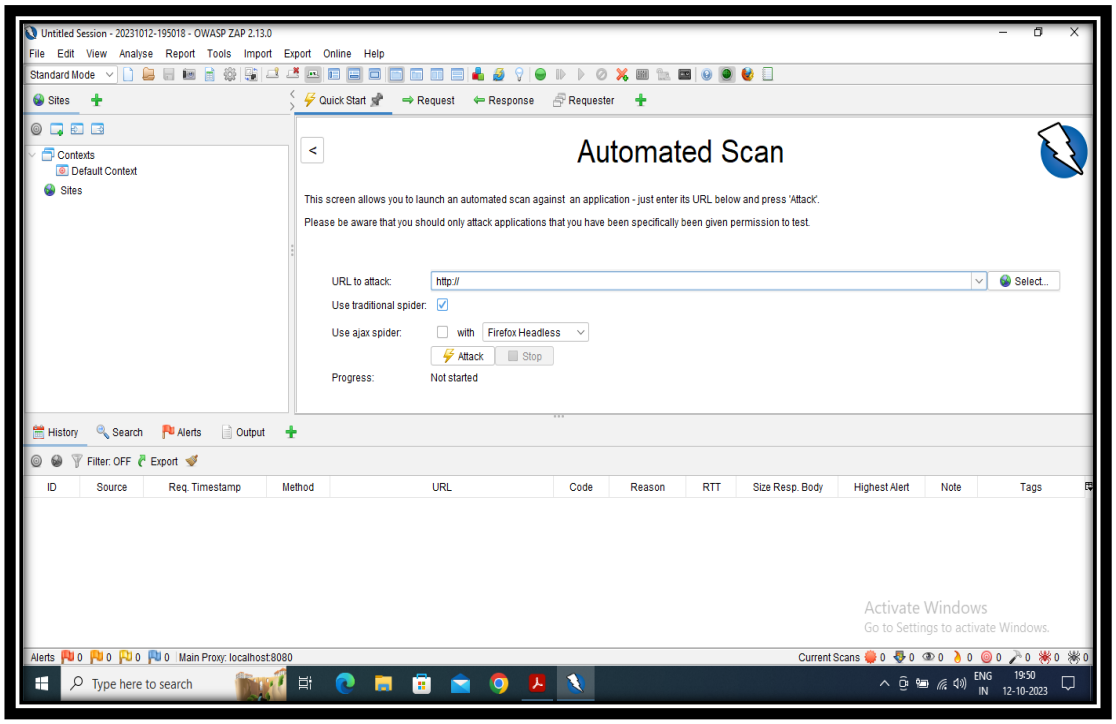
- Back in Burp Suite, I could see the entire web traffic, including my login credentials. This assignment demonstrated how Burp Suite is a valuable tool for capturing and analysing web traffic, offering insights into its functionality for security and testing purposes.

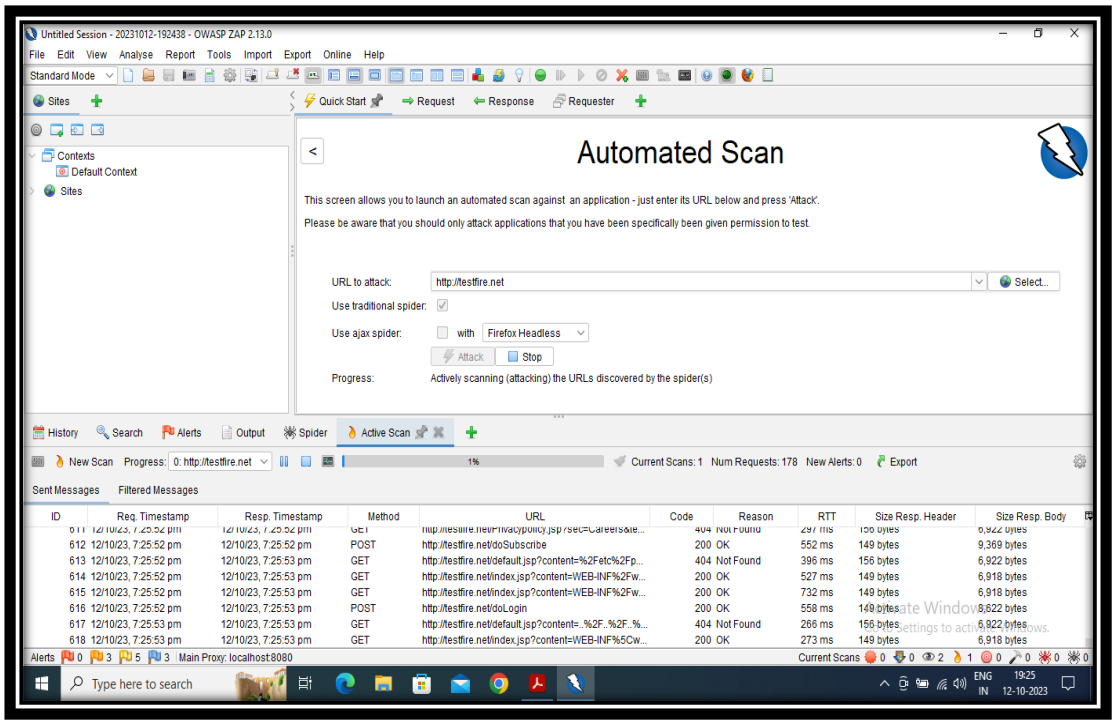
Objective: 03

Perform vulnerability research using ZAP

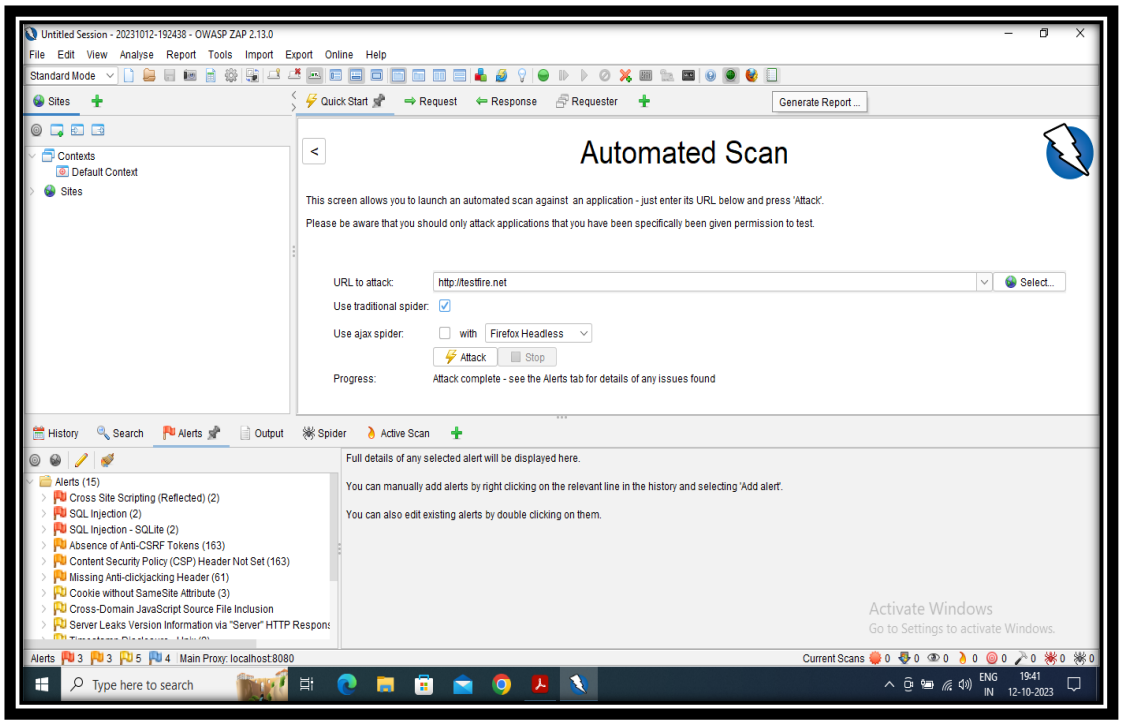
- In the ever-evolving landscape of cybersecurity, staying one step ahead of potential threats is paramount. Vulnerability research is the cornerstone of this proactive approach, enabling us to unearth and address vulnerabilities in software, systems, and applications before malicious actors can exploit them. This lab assignment is dedicated to the essential task of conducting vulnerability research using the formidable ZAP, also known as the Zed Attack Proxy.
- The goal of this assignment was to perform vulnerability research using the ZAP (Zed Attack Proxy) tool and understand its capabilities in identifying and reporting vulnerabilities.
- To begin, I downloaded the ZAP tool and launched it. Upon opening ZAP, I was greeted with a dashboard containing several options. I navigated to the "Automated Scan" option and proceeded to enter my target URL for testing, which was "testfire.net." After inputting the target URL, I initiated the scanning process by clicking the "Attack" button. The scanning process began, and I patiently waited for it to complete.

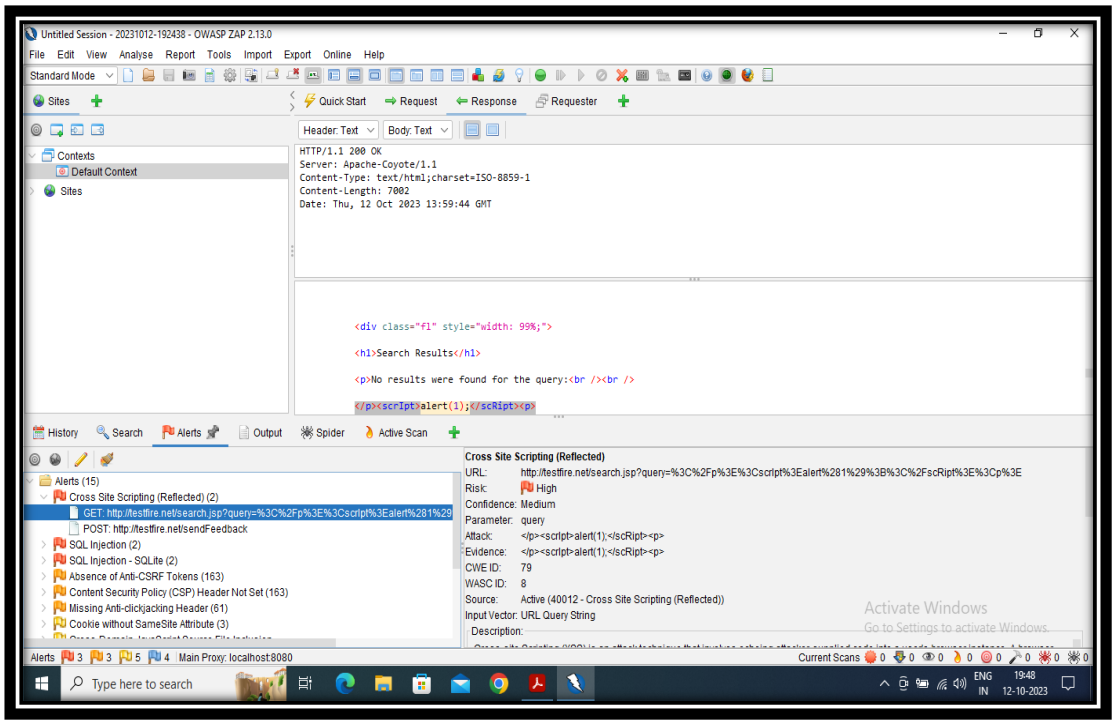

Untitled Session - 20231012-195018 - OWASP ZAP 2.13.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Welcome to OWASP ZAP
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
If you are new to ZAP then it is best to start with one of the options below.
Automated Scan
Manual Explore
Learn More
History
Search
Alerts
Output
Filter: OFF
Export
ID
Source
Req. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Body
Highest Alert
Note
Tags
Activate Windows
Go to Settings to activate Windows.
Alerts
Main Proxy: localhost:8080
Current Scans
Type here to search
ENG
IN
19:50
12-10-2023


Untitled Session - 20231012-195018 - OWASP ZAP 2.13.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
http://
Select...
Use traditional spider:
Use ajax spider:
with
Firefox Headless
Attack
Stop
Progress:
Not started
History
Search
Alerts
Output
Filter: OFF
Export
ID
Source
Req. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Body
Highest Alert
Note
Tags
Activate Windows
Go to Settings to activate Windows.
Alerts
Main Proxy: localhost:8080
Current Scans
Type here to search
ENG
IN
19:50
12-10-2023

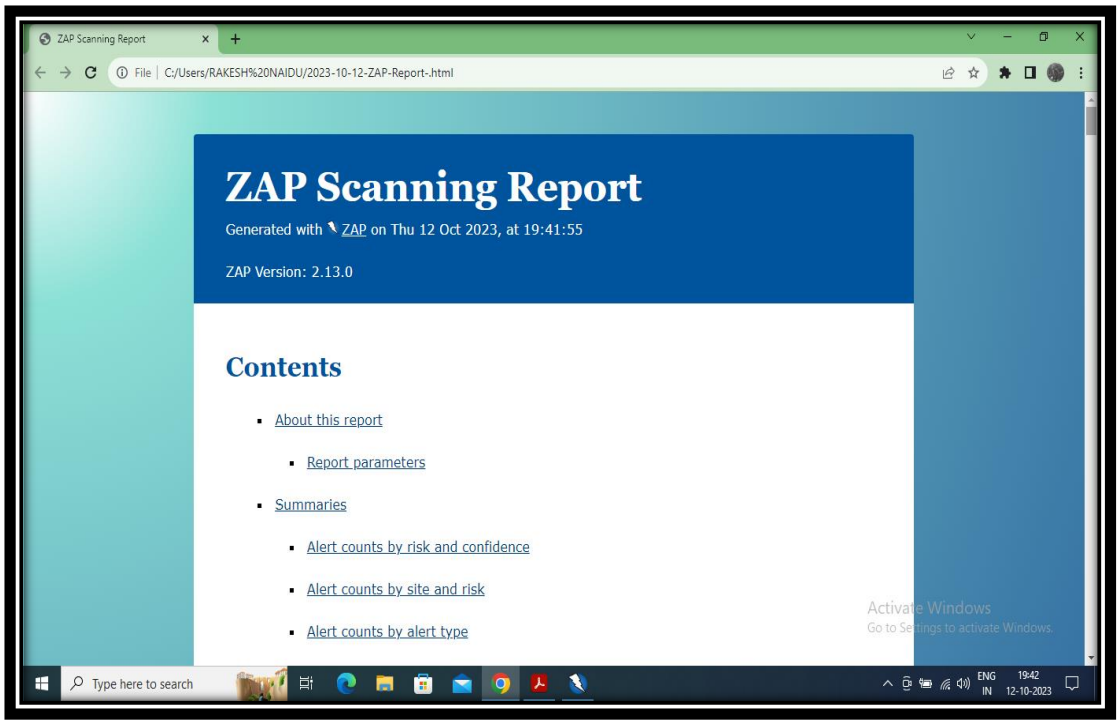


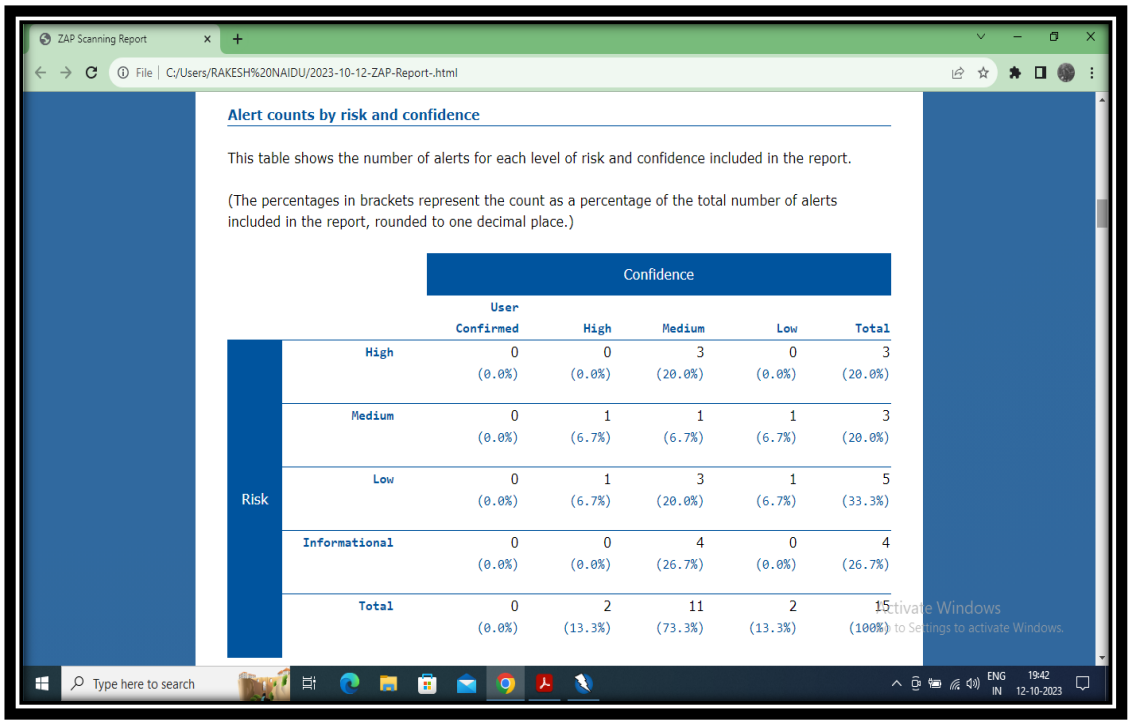
- Upon the completion of the scan, I discovered a multitude of vulnerabilities within my target web application. To access detailed information about these vulnerabilities, I checked the "Alerts" option, which provided a comprehensive list of each vulnerability along with its description.

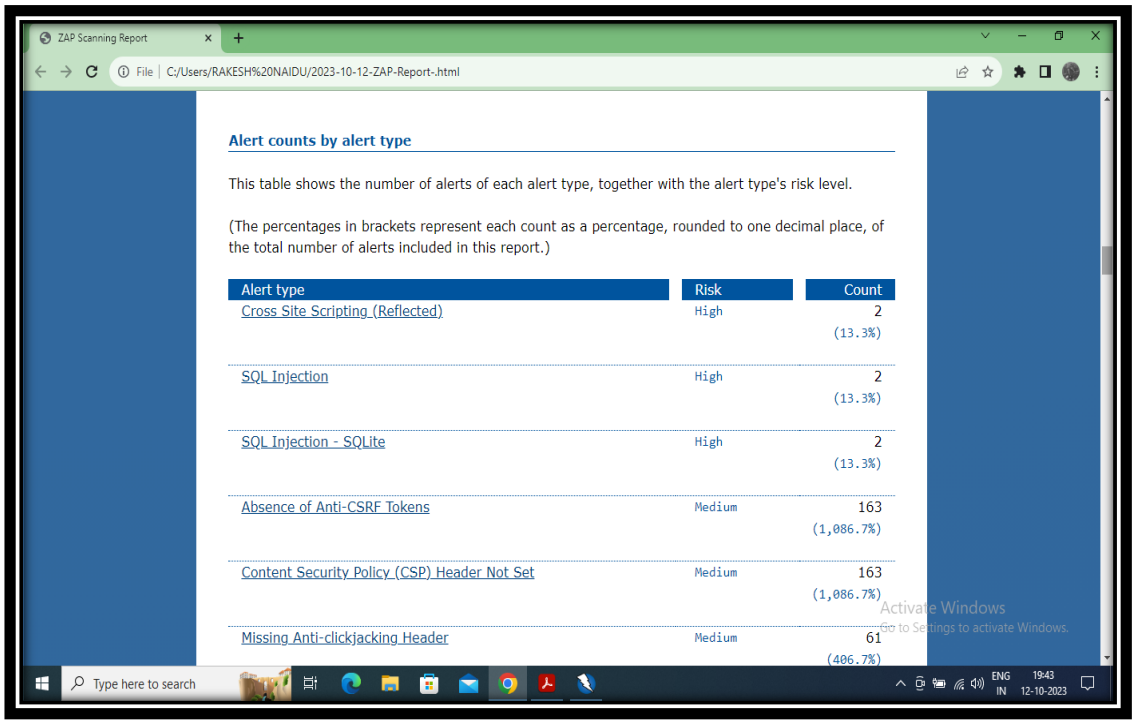


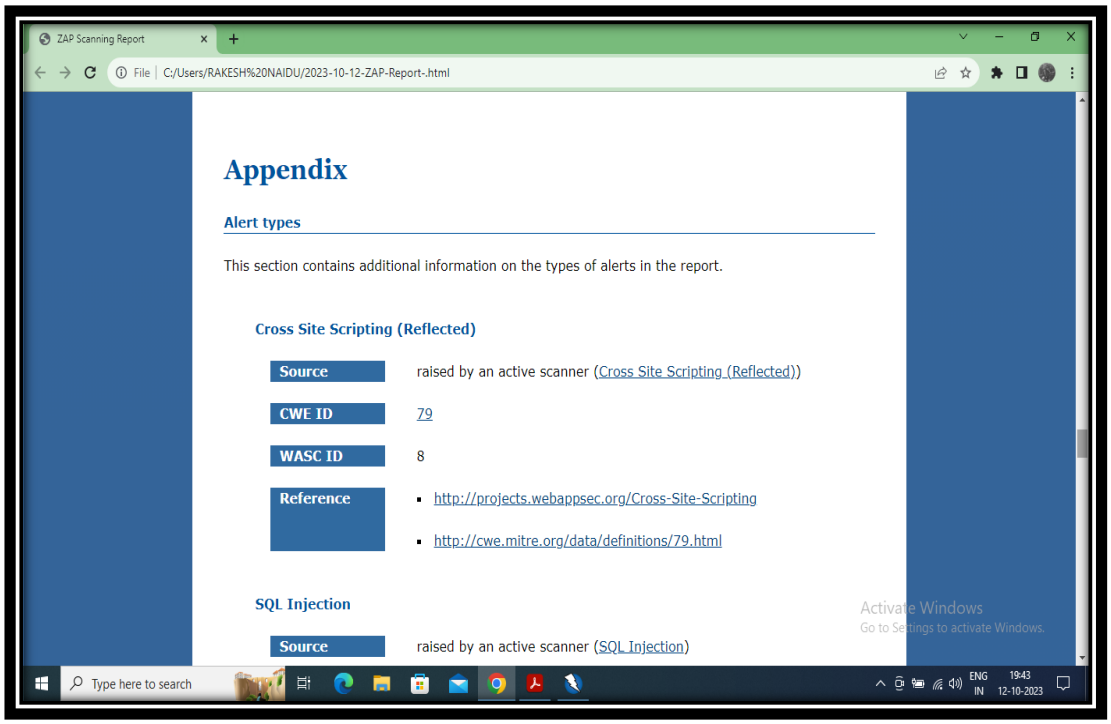


- A notable feature of ZAP was the "Generate Report" option, which I utilized. Clicking this option generated a comprehensive scanning report for the entire session. This report was presented in a well-understood format, including risk percentages, various alerts, different types of vulnerabilities, and their respective risk factors.




ZAP Scanning Report
File | C:/Users/RAKESH%20NAIDU/2023-10-12-ZAP-Report-.html
Alert counts by risk and confidence
This table shows the number of alerts for each level of risk and confidence included in the report.
(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)
Confidence
User Confirmed
High
Medium
Low
Total
Risk
High 0 (0.0%) 0 (0.0%) 3 (20.0%) 0 (0.0%) 3 (20.0%)
Medium 0 (0.0%) 1 (6.7%) 1 (6.7%) 1 (6.7%) 3 (20.0%)
Low 0 (0.0%) 1 (6.7%) 3 (20.0%) 1 (6.7%) 5 (33.3%)
Informational 0 (0.0%) 0 (0.0%) 4 (26.7%) 0 (0.0%) 4 (26.7%)
Total 0 (0.0%) 2 (13.3%) 11 (73.3%) 2 (13.3%) 15 (100%)
Activate Windows
Type here to search
ENG IN 19:42 12-10-2023


ZAP Scanning Report
File | C:/Users/RAKESH%20NAIDU/2023-10-12-ZAP-Report-.html
Alert counts by alert type
This table shows the number of alerts of each alert type, together with the alert type's risk level.
(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)
Alert type Risk Count
Cross Site Scripting (Reflected) High 2 (13.3%)
SQL Injection High 2 (13.3%)
SQL Injection - SQLite High 2 (13.3%)
Absence of Anti-CSRF Tokens Medium 163 (1,086.7%)
Content Security Policy (CSP) Header Not Set Medium 163 (1,086.7%)
Missing Anti-clickjacking Header Medium 61 (406.7%)
Activate Windows
Type here to search
ENG IN 19:43 12-10-2023



- This assignment demonstrated how ZAP is an effective tool for conducting vulnerability research, offering in-depth insights into the security posture of a web application and providing clear and informative reports.

Submitted By

Marepalli Rakesh

(Marepalli.rakesh@gmail.com)