CEH Module 6: System Hacking
Assignment - 03
(Sairaj Mothukuri)

Given Lab Scenario

For a professional ethical hacker or pen tester, the first step in system hacking is to analyze 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

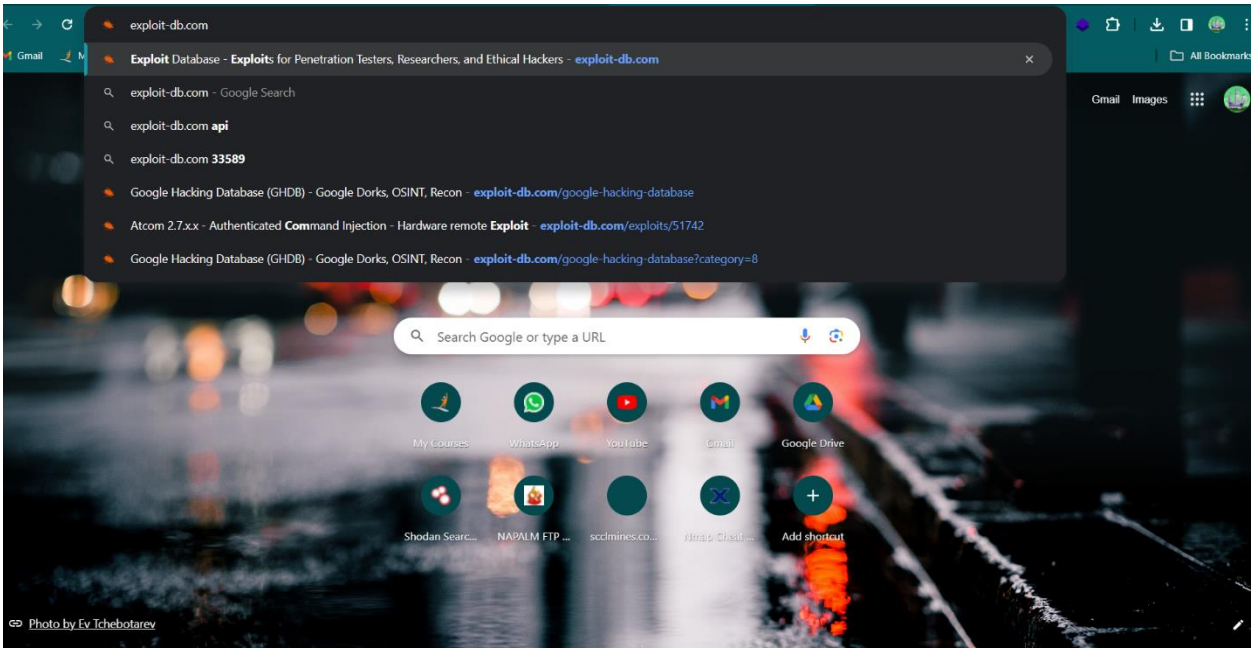
Given Lab Objectives:

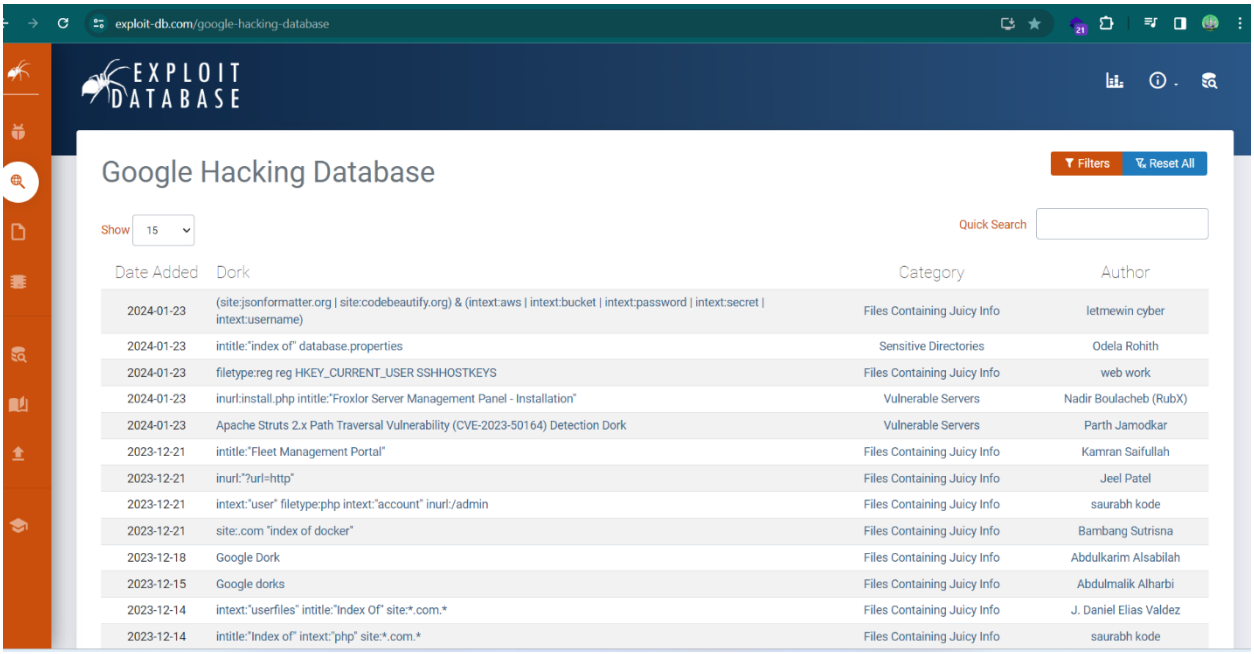
- Find vulnerabilities on exploit sites
- Intercept traffic using Burp suite software
- Perform vulnerability research using ZAP

Objective: 01

Find vulnerabilities on exploit sites

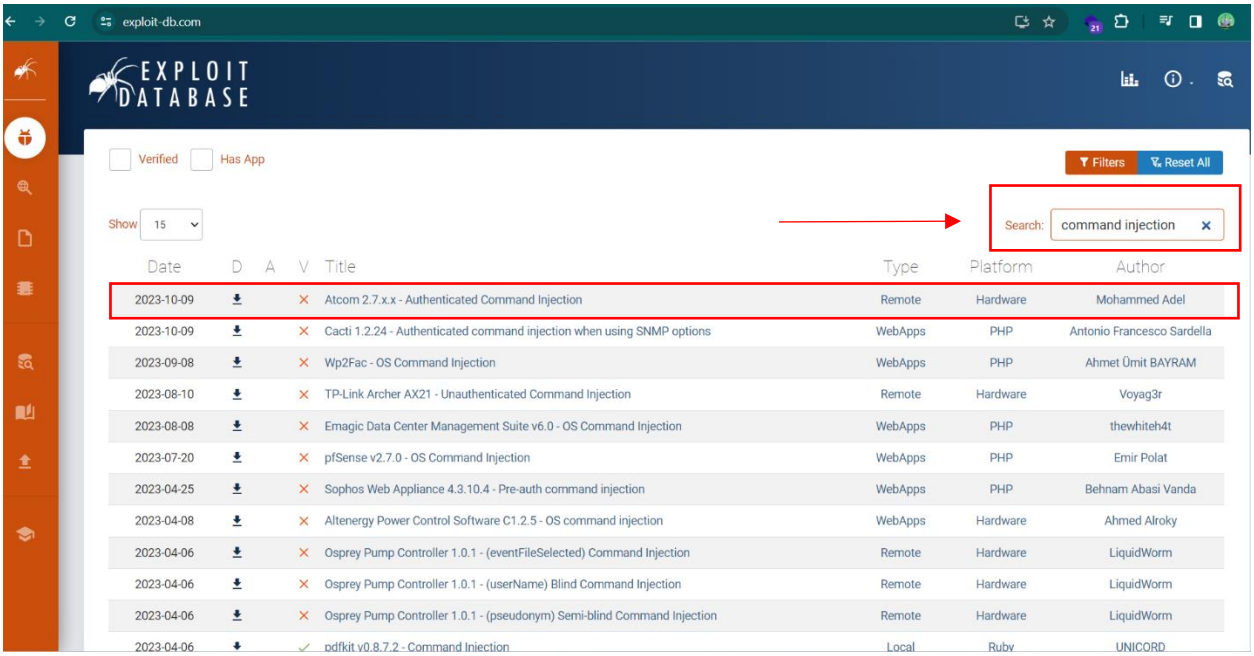
- Vulnerability exploitation involves the execution of multiple complexes, interrelated steps to gain access to remote system
- Vulnerabilities are found every day, and they don't discriminate from one operating system to another.
- They're present on all operating systems used on electronic devices, from mobile phones to smart TVs, from the IoT to computers
- The objective of the assignment was to explore vulnerabilities by using of online exploit database.
- To perform the lab scenario, I am using Exploit Data Base and Vulners exploit sites
- To perform the assignment, I opened a web browser and search for the "Exploit Data Base".

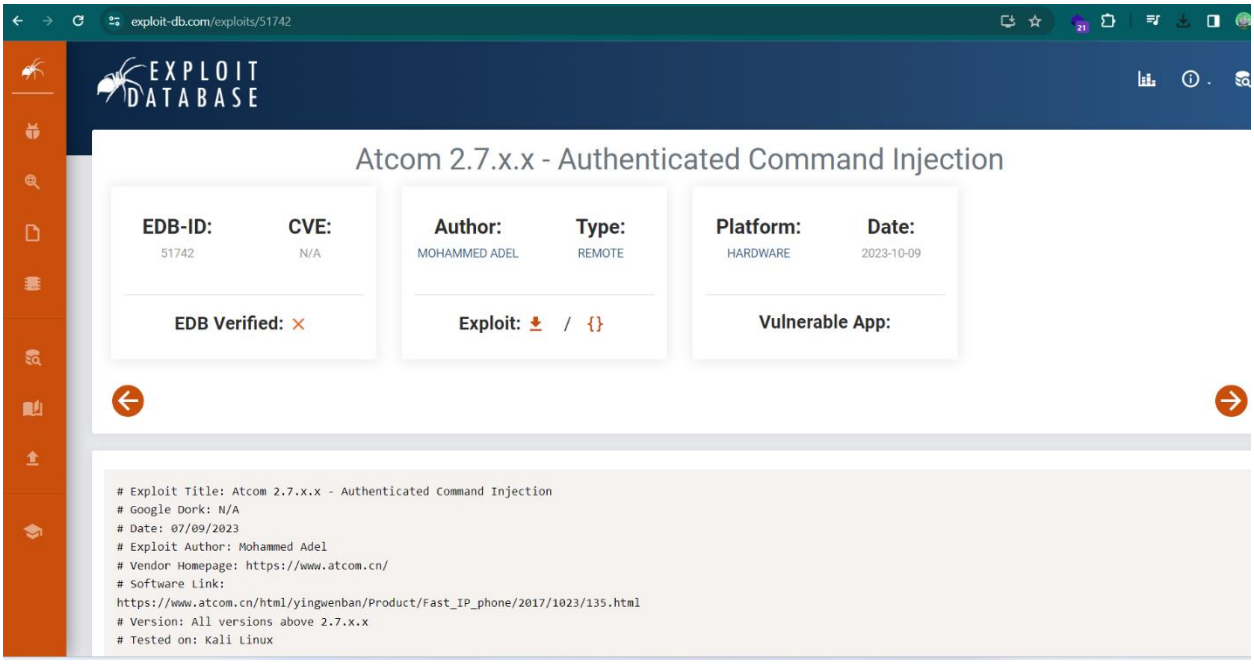


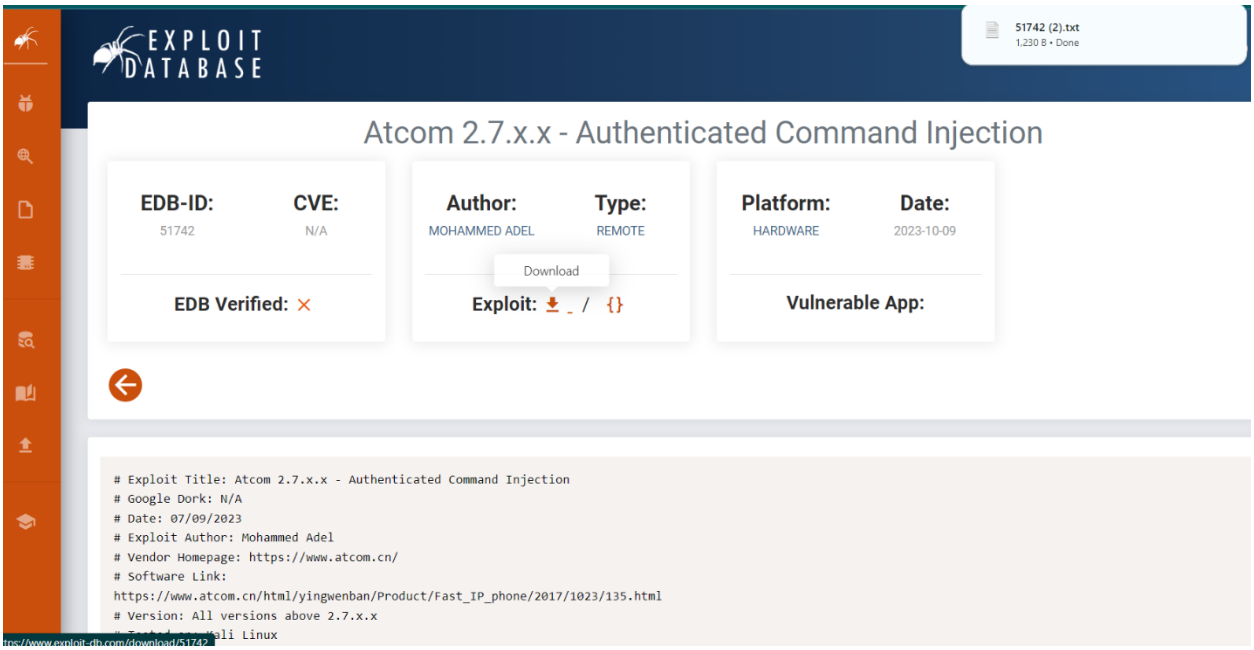


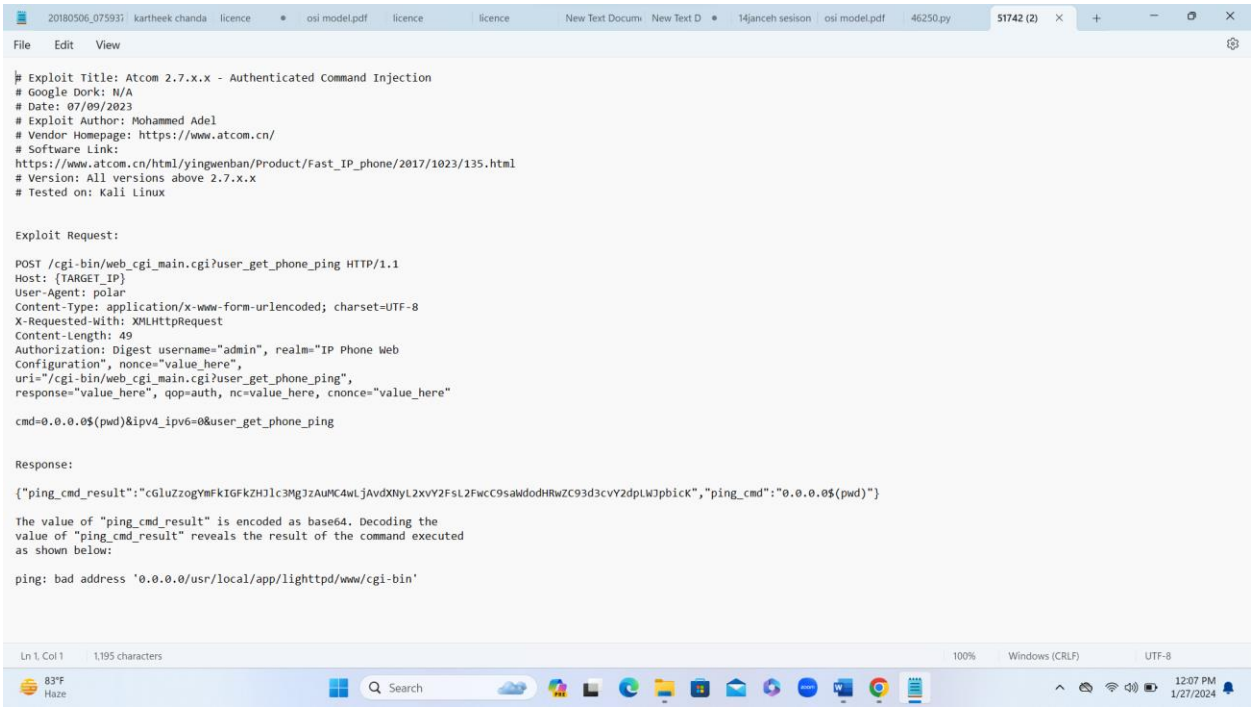
- After opening the exploit site at the left of the site I have searched the command injection.
- And I chosen the Authenticated command injection and download the details of the vulnerability in text format, which include essential information such as the exploit title, author, date,

description, path, parameter and other pertinent data for comprehensive understanding.



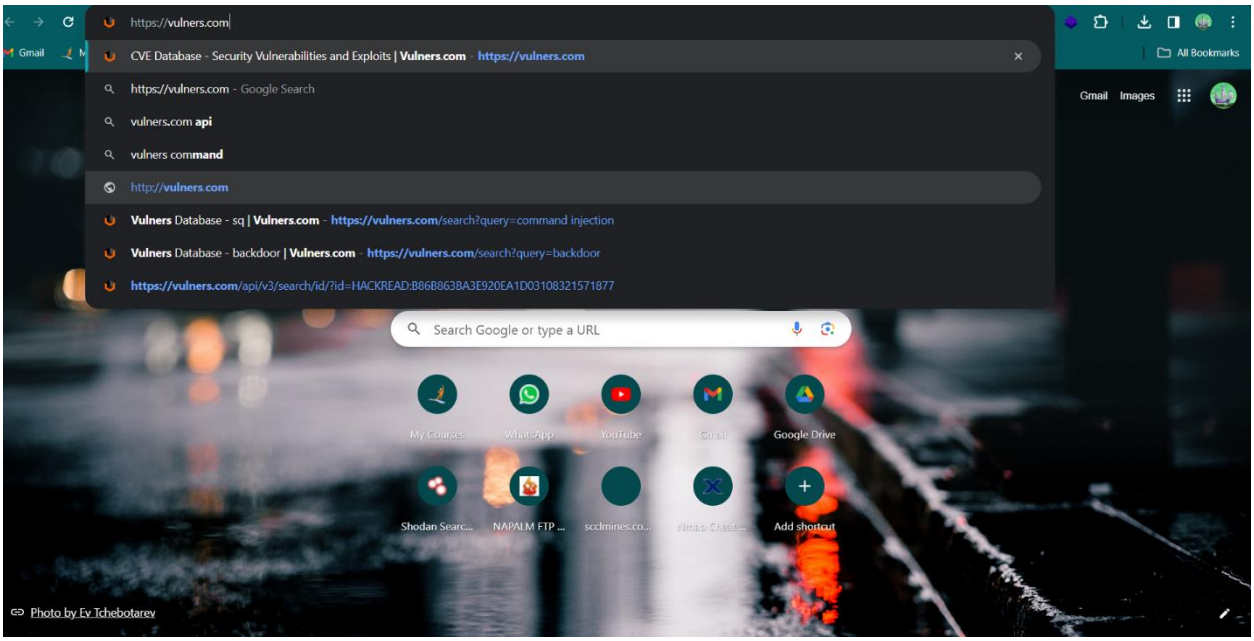


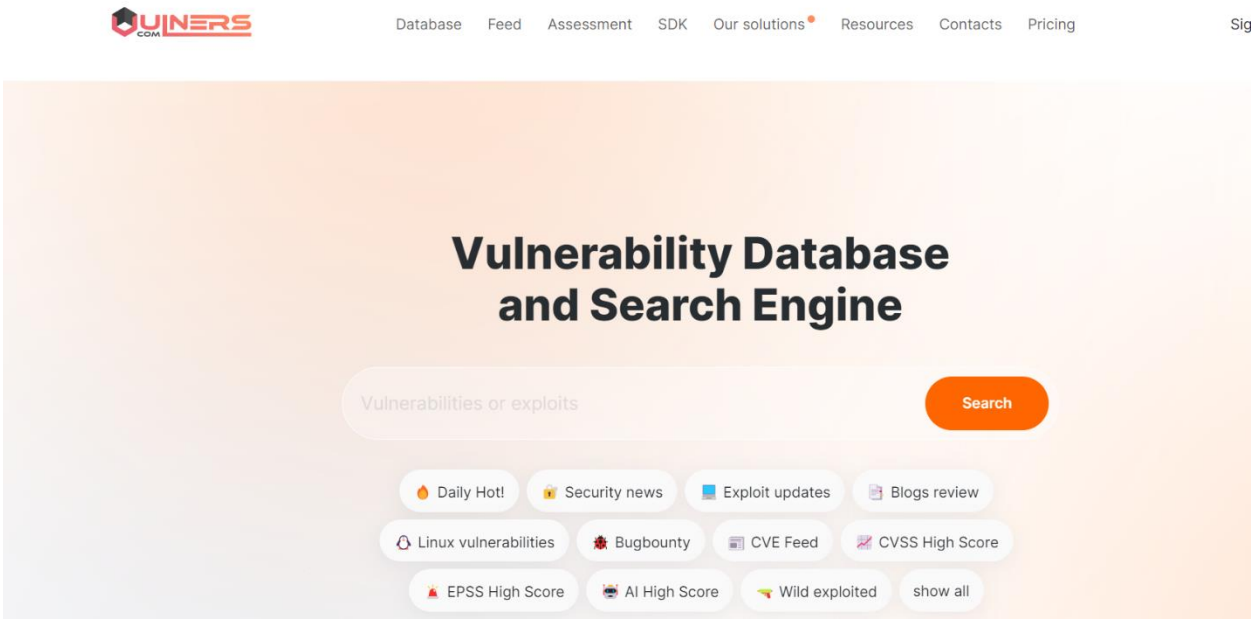


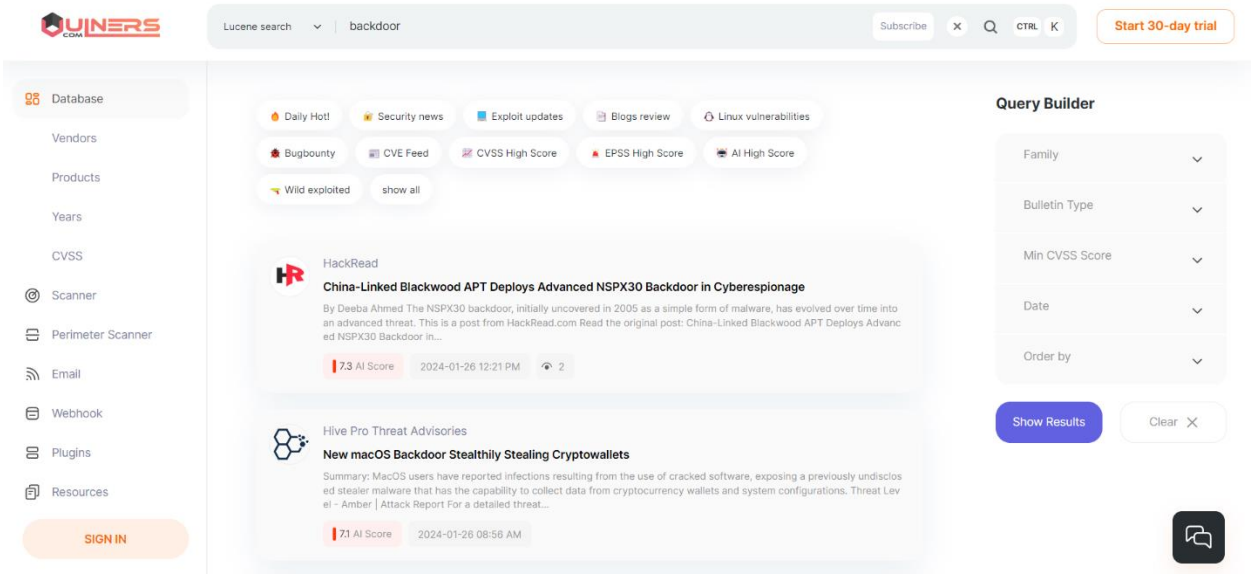


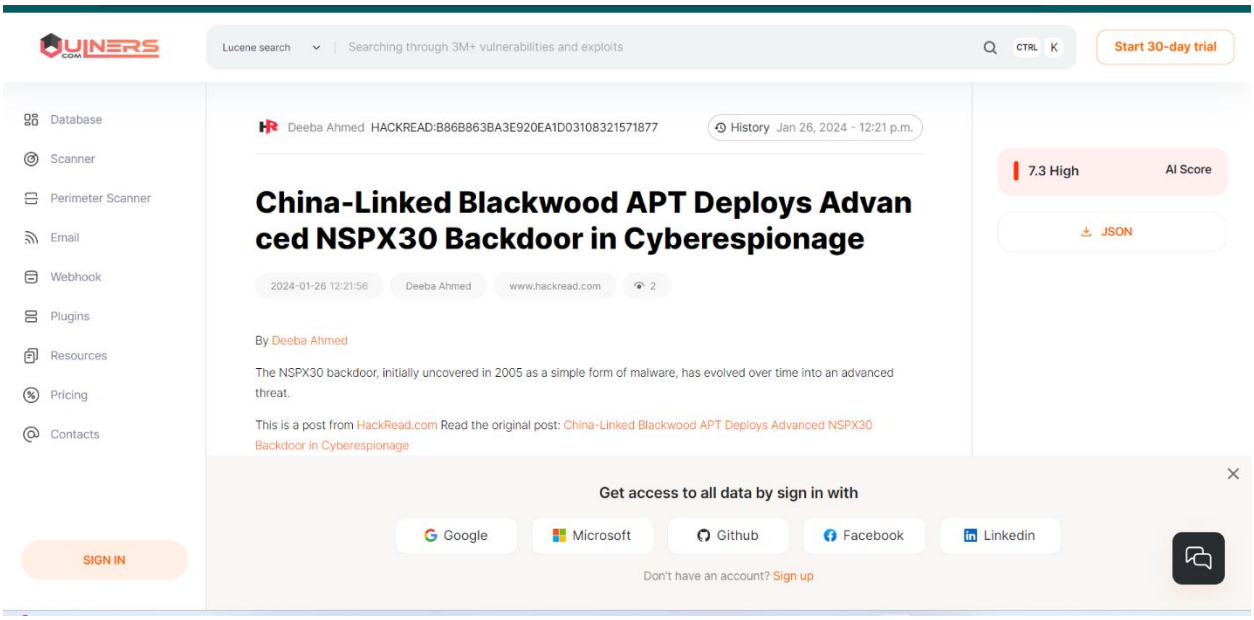
- Subsequently, I explored another exploit database, vulner.com and upon entering this site, I observed an option located at the middle of the page labelled 'Vulnerability Database and Search

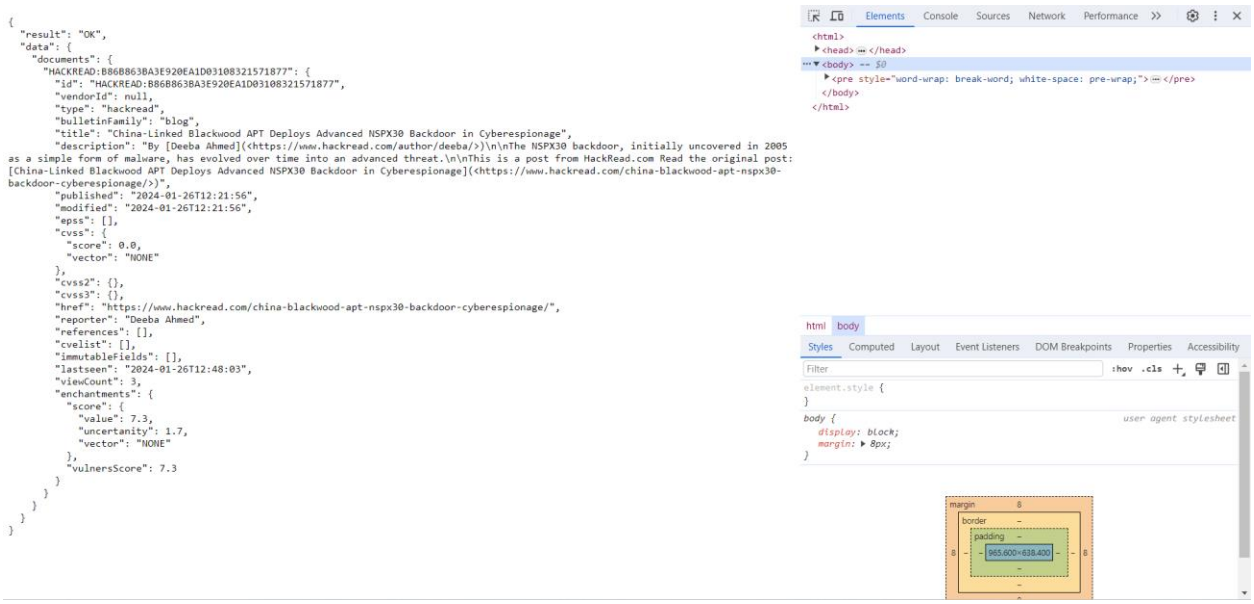
Engine ' Upon clicking this option, a search bar appeared, and I once again conducted a search for in back door vulnerabilities by typing "backdoor" and submitting the query.




Database
Feed
Assessment
SDK
Our solutions
Resources
Contacts
Pricing
Sig
Vulnerability Database and Search Engine
Vulnerabilities or exploits
Search
Daily Hot!
Security news
Exploit updates
Blogs review
Linux vulnerabilities
Bugbounty
CVE Feed
CVSS High Score
EPSS High Score
AI High Score
Wild exploited
show all


Lucene search
backdoor
Subscribe
CTRL
K
Start 30-day trial
Database
Vendors
Products
Years
CVSS
Scanner
Perimeter Scanner
Email
Webhook
Plugins
Resources
SIGN IN
Daily Hot!
Security news
Exploit updates
Blogs review
Linux vulnerabilities
Bugbounty
CVE Feed
CVSS High Score
EPSS High Score
AI High Score
Wild exploited
show all
HackRead
China-Linked Blackwood APT Deploys Advanced NSPX30 Backdoor in Cyberespionage
By Deeba Ahmed The NSPX30 backdoor, initially uncovered in 2005 as a simple form of malware, has evolved over time into an advanced threat. This is a post from HackRead.com Read the original post: China-Linked Blackwood APT Deploys Advanced NSPX30 Backdoor in...
7.3 AI Score
2024-01-26 12:21 PM
2
Hive Pro Threat Advisories
New macOS Backdoor Stealthily Stealing Cryptowallets
Summary: MacOS users have reported infections resulting from the use of cracked software, exposing a previously undisclosed stealer malware that has the capability to collect data from cryptocurrency wallets and system configurations. Threat Level - Amber | Attack Report For a detailed threat...
7.1 AI Score
2024-01-26 08:56 AM
Query Builder
Family
Bulletin Type
Min CVSS Score
Date
Order by
Show Results
Clear





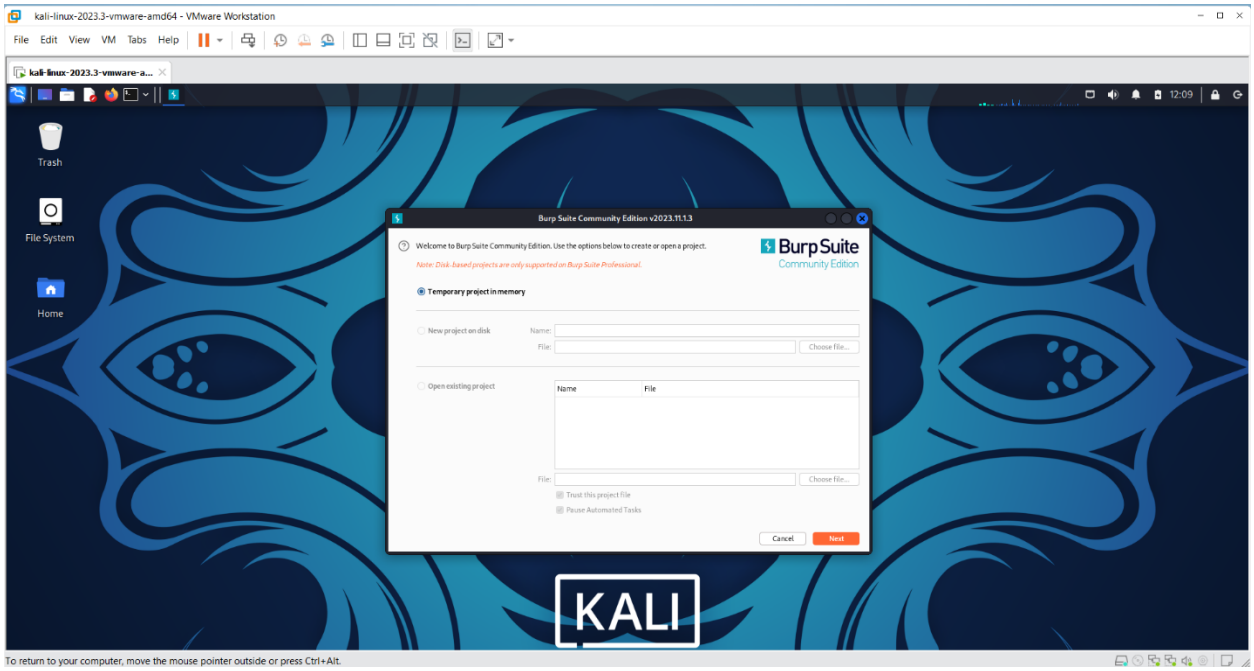
- This assignment allowed me to gain insights into vulnerabilities and their documentation through these two valuable exploit databases.

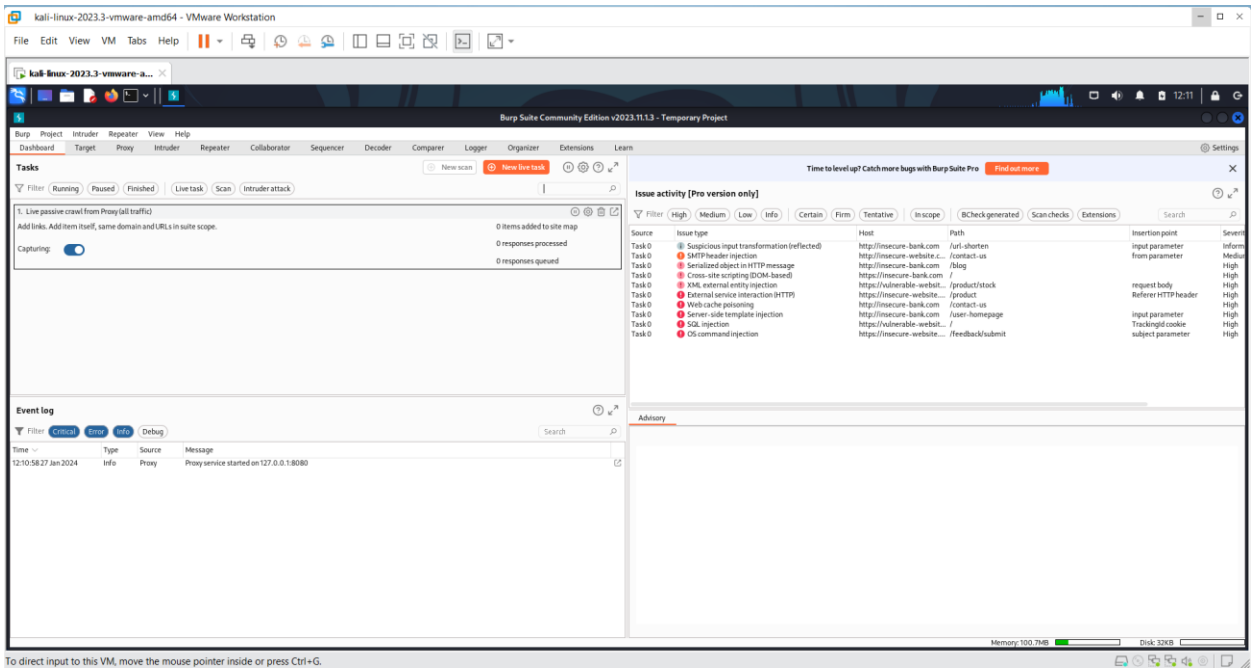
Objective: 02

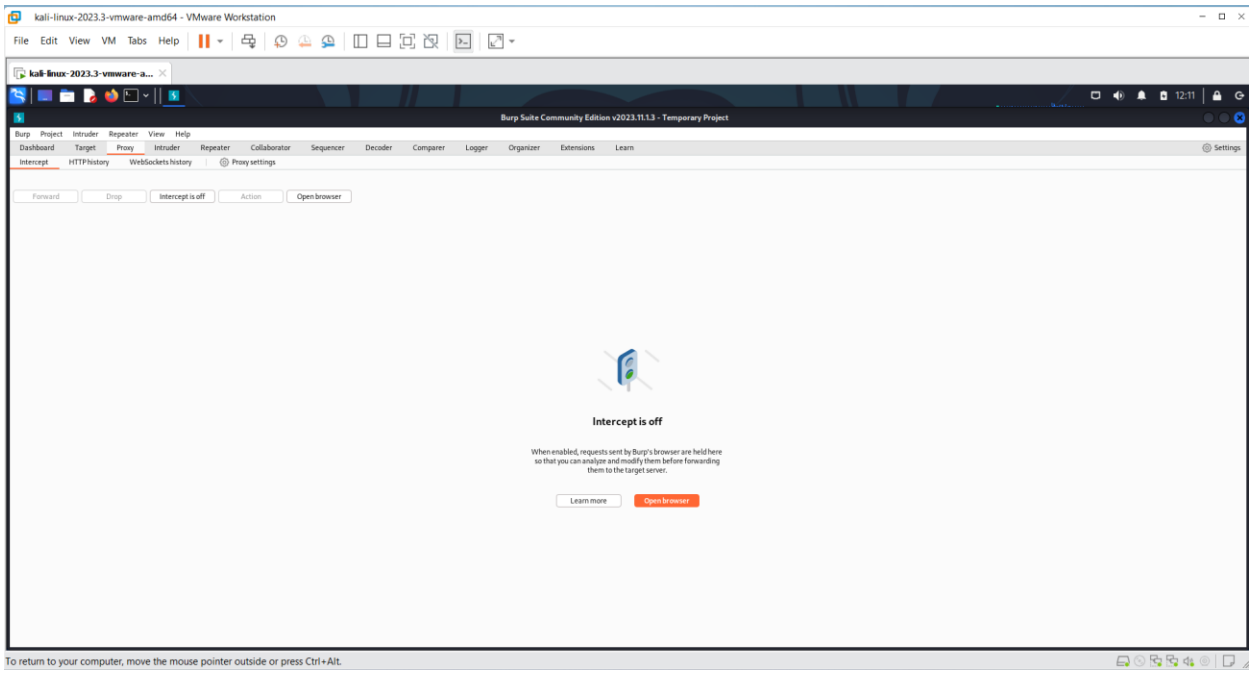
Intercept traffic using Burp suite software

- ✓ Burp suite software capture request and response which are given to the browser to server and server to browser.
- ✓ Burp suit will act like mediator between browser and server.
- ✓ Burp suit can do all web application attack
- ✓ The major thing is we can capture the request tampering and forward in to server
- ✓ We can also capture respond from the server and tamper it and send to clint

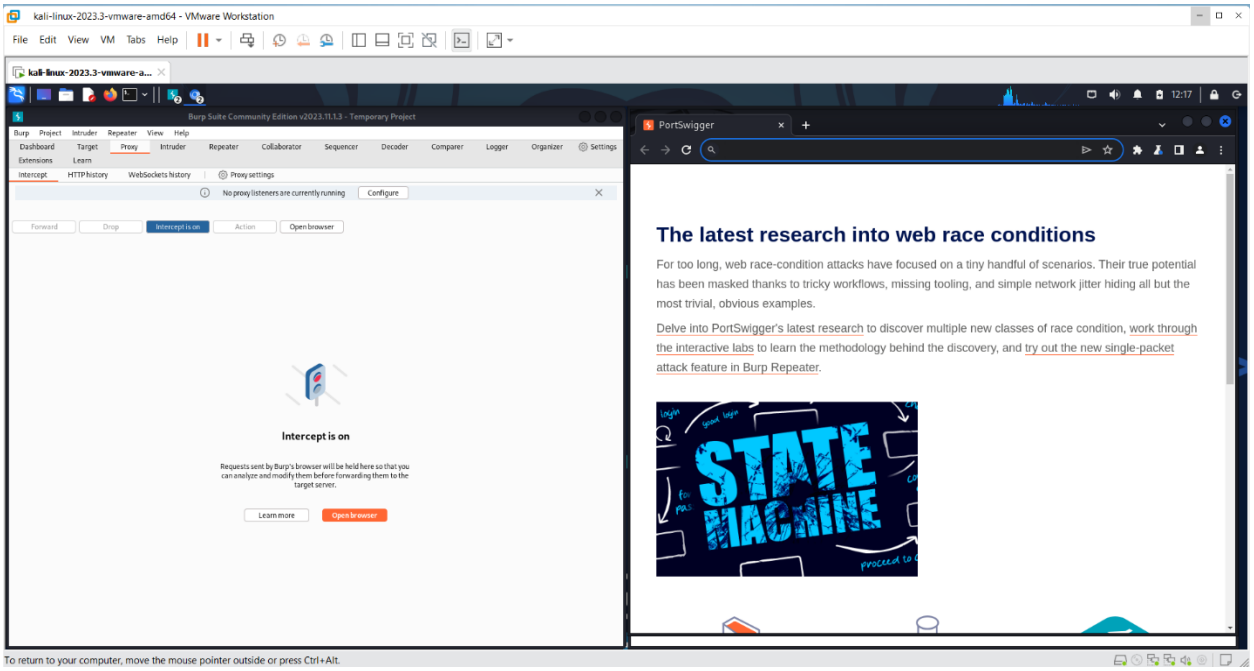
- ➢ To start, I opened the kali, the Burp suit is already pre-installed tool and Upon opening Burp Suite, I accessed the dashboard. In the dashboard, I navigated to the "Proxy" option, which presented several sub-options, including "Intercept" and "Proxy Settings." Within the "Proxy" section, I activated the "Intercept" option and then clicked on the "Browser" option.

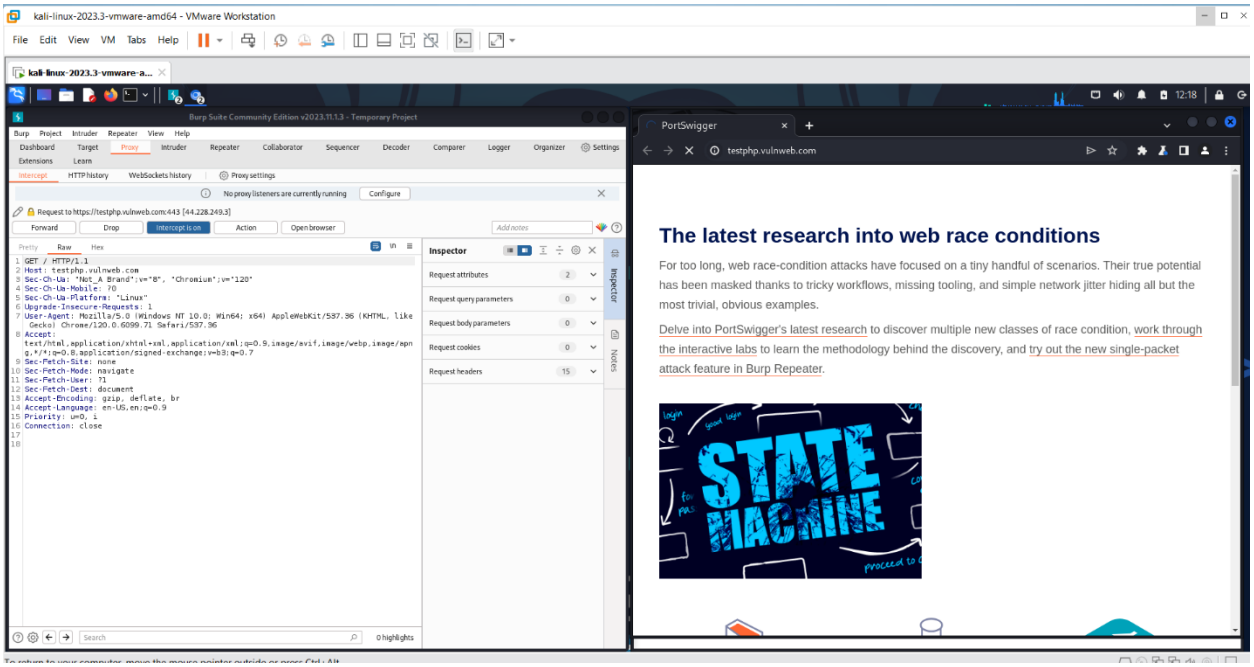

kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2023.3-vmware-a...
Trash
File System
Home
Burp Suite Community Edition v2023.11.1.3
Welcome to Burp Suite Community Edition. Use the options below to create or open a project.
Note: Disk-based projects are only supported on Burp Suite Professional.
Burp Suite
Community Edition
Temporary project in memory
New project on disk
Name:
File:
Choose file...
Open existing project
Name
File
Trust this project file
Pause Automated Tasks
Cancel
Next
KALI
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

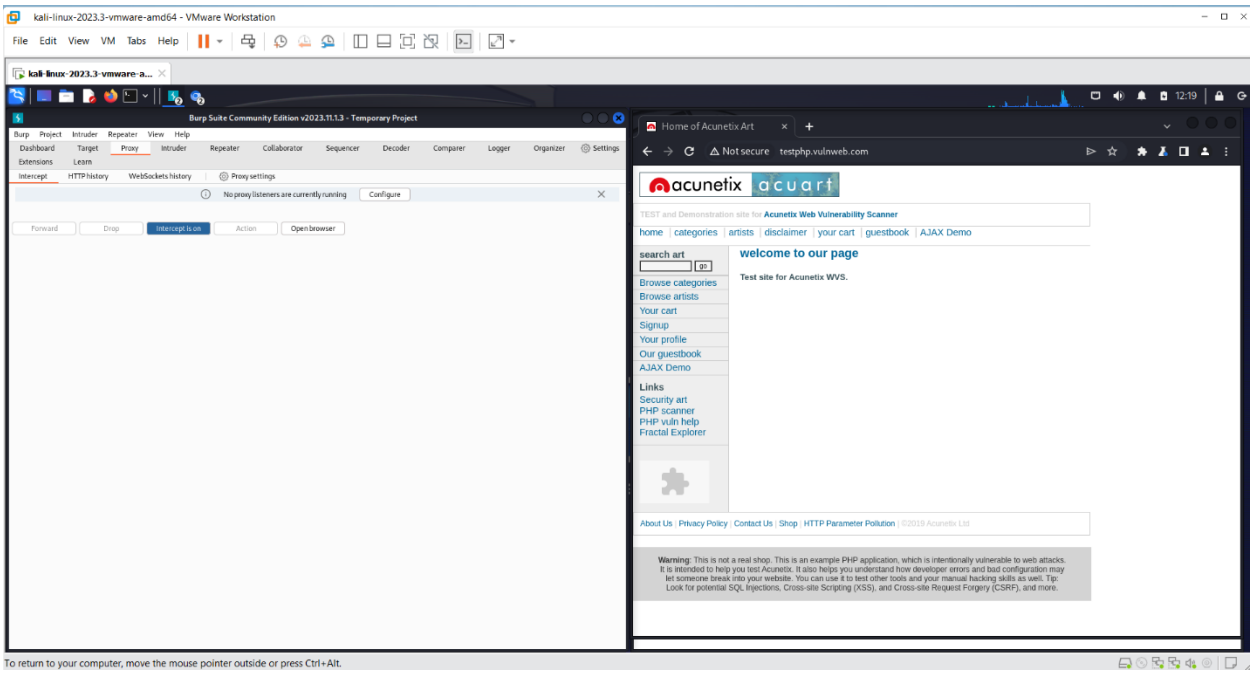

kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2023.3-vmware-a...
Burp Suite Community Edition v2023.11.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Tasks
New scan
New live task
Time to level up? Catch more bugs with Burp Suite Pro
Find out more
Issue activity [Pro version only]
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
Event log
Advisory
Memory: 100.7MB
Disk: 32KB
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

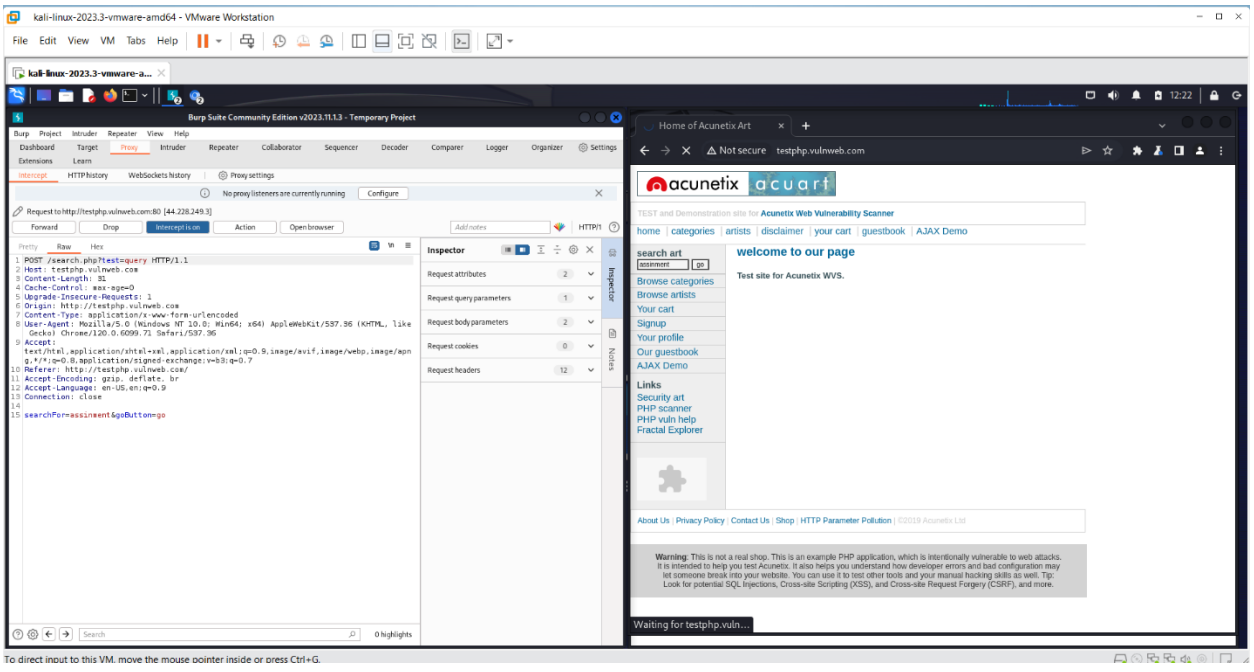


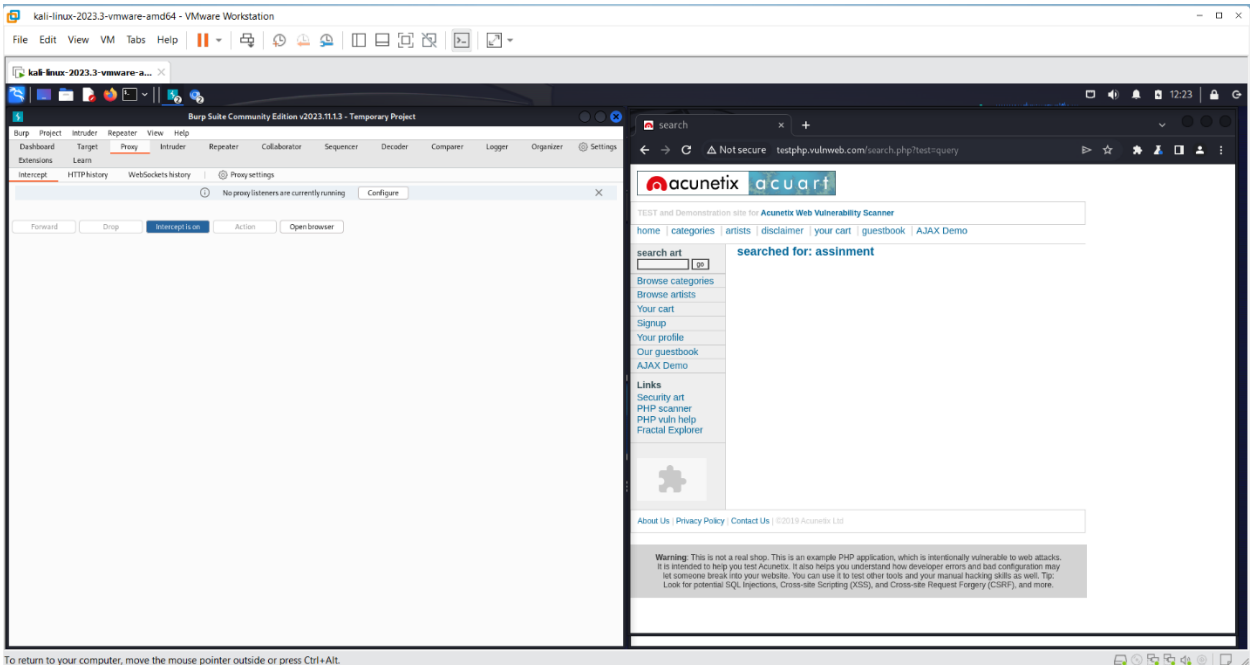
- With the browser interface open, I entered the target web application's URL, testphp.com "vulnweb application." Returning to Burp Suite, I observed that it had intercepted the web traffic, capturing various pieces of information. I clicked "Forward" in Burp Suite and then returned to the browsers.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


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Burp Suite Community Edition v2023.11.1.3 - Temporary Project
Intercept is on
Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.
Learn more
Open browser
PortSwigger
The latest research into web race conditions
For too long, web race-condition attacks have focused on a tiny handful of scenarios. Their true potential has been masked thanks to tricky workflows, missing tooling, and simple network jitter hiding all but the most trivial, obvious examples.
Delve into PortSwigger's latest research to discover multiple new classes of race condition, work through the interactive labs to learn the methodology behind the discovery, and try out the new single-packet attack feature in Burp Repeater.
STATE MACHINE
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

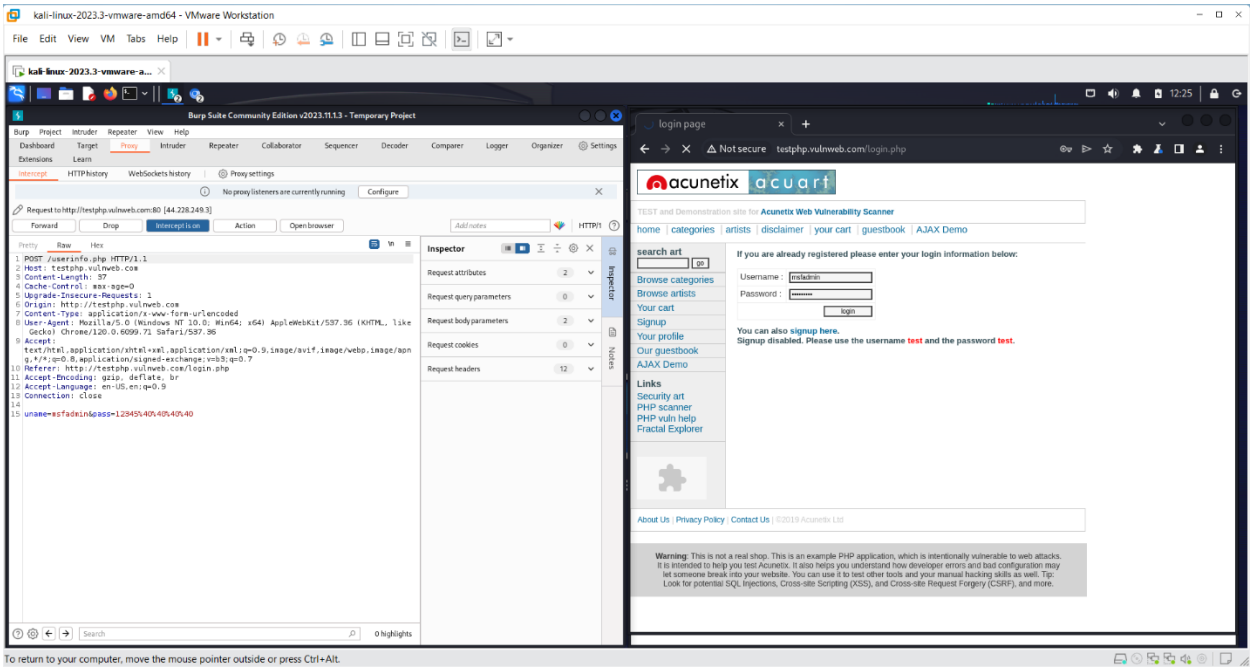

kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Burp Suite Community Edition v2023.11.1.3 - Temporary Project
Request to https://testphp.vulnweb.com:443 [44.228.249.3]
Inspector
PortSwigger
testphp.vulnweb.com
The latest research into web race conditions
For too long, web race-condition attacks have focused on a tiny handful of scenarios. Their true potential has been masked thanks to tricky workflows, missing tooling, and simple network jitter hiding all but the most trivial, obvious examples.
Delve into PortSwigger's latest research to discover multiple new classes of race condition, work through the interactive labs to learn the methodology behind the discovery, and try out the new single-packet attack feature in Burp Repeater.
STATE MACHINE


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Burp Suite Community Edition v2023.11.1.3 - Temporary Project
Home of Acunetix Art
Not secure testphp.vulnweb.com
acunetix acuart
welcome to our page
Test site for Acunetix WVS.
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Burp Suite Community Edition v2023.11.1.3 - Temporary Project
POST /search.php?test=query HTTP/1.1
searchFor=assinment&goButton=go
Home of Acunetix Art
Not secure testphp.vulnweb.com
acunetix acuart
welcome to our page
Test site for Acunetix WVS.
Waiting for testphp.vuln...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



- 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"

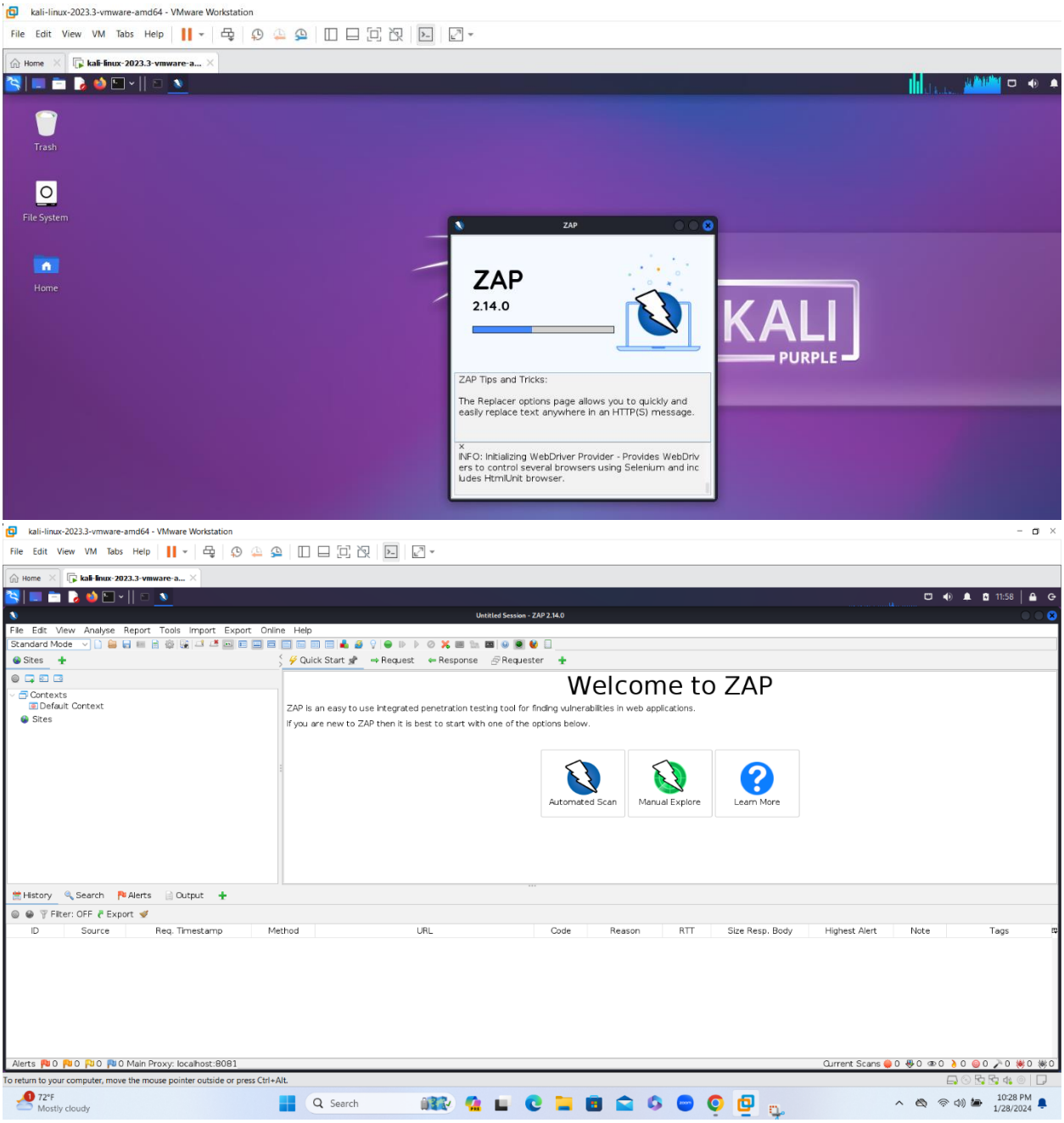


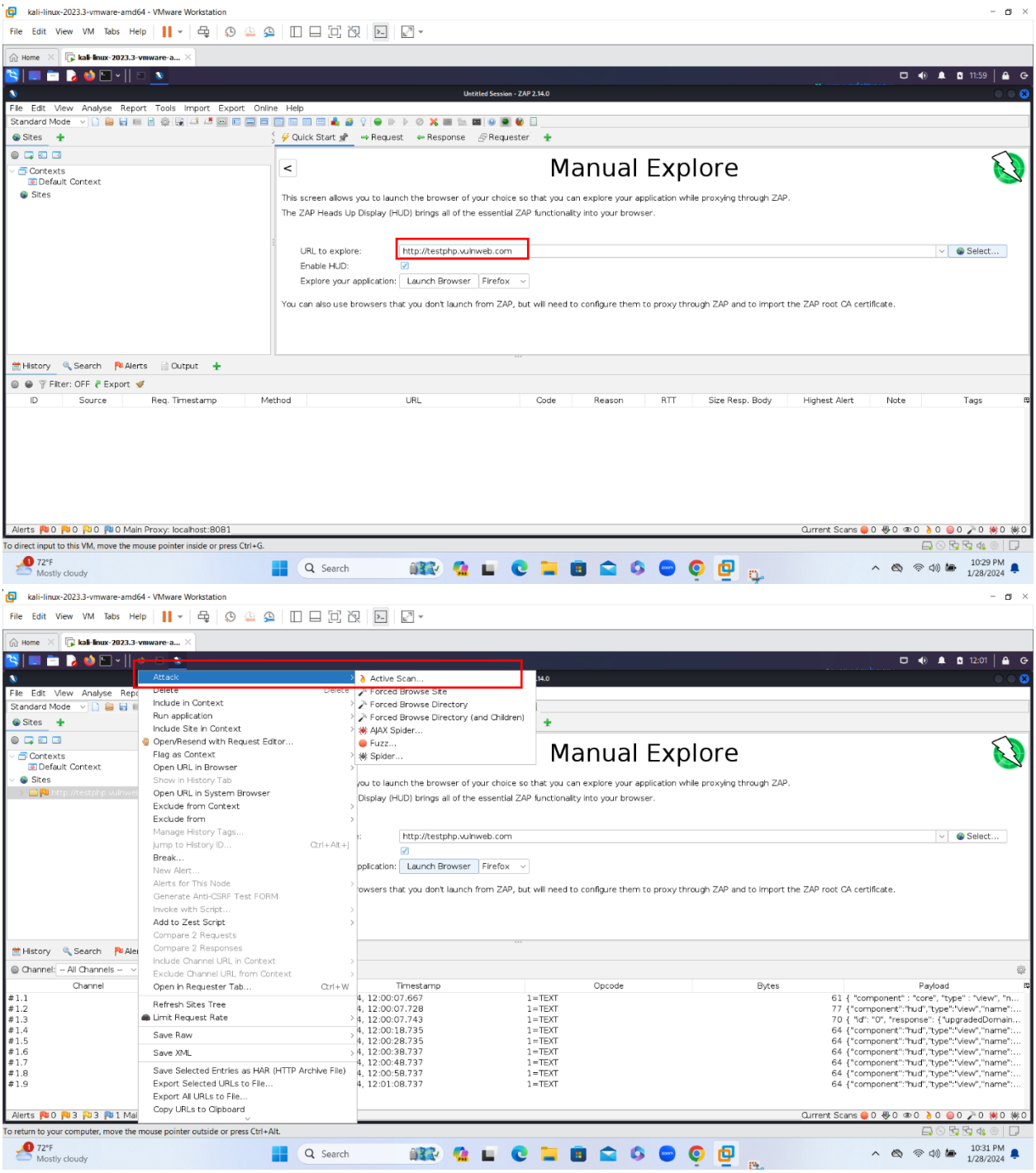
- Back in Burp Suite, I could see the entire web traffic, including my login credentials. This assignment demonstrated how Burp Suite is a valuable tool for capturing and analyzing web traffic, offering insights into its functionality for security and testing purposes.

Objective: 03

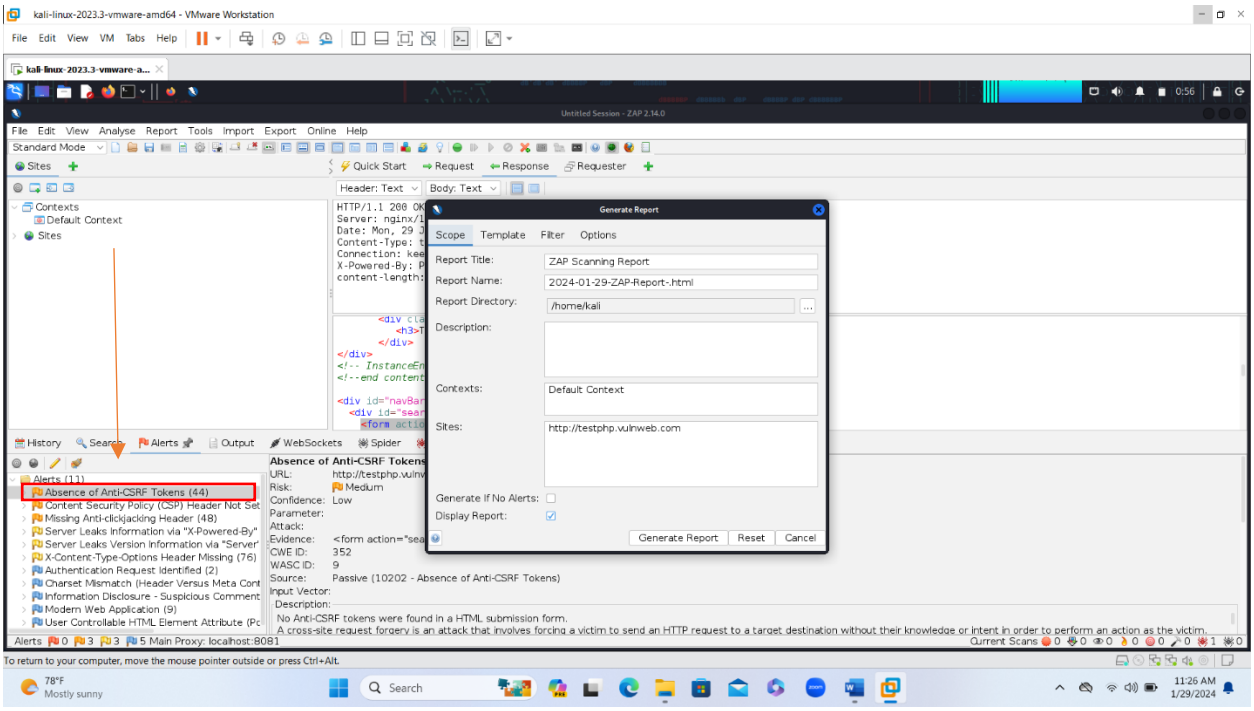
Perform vulnerability research using ZAP

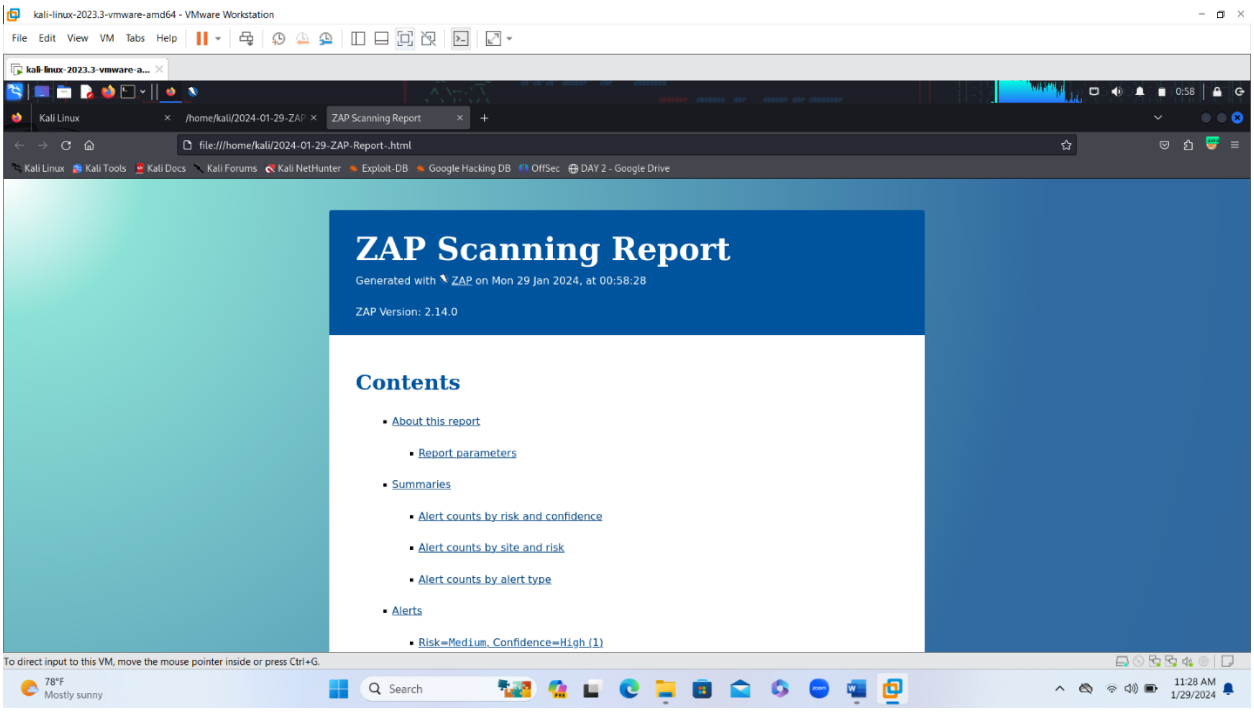
- OWASP ZAP is a penetration testing tool that help developers and security professionals detect and find vulnerabilities in web application. OWASP ZAP performs multiple security functions including: Passively scanning web requests. Using dictionary lists to search for files and folders on web servers.
- It is designed to be used by people with a wide range of security experience and as such is ideal for developers and functional testers who are new to penetration testing.
- OWASP ZAP is a valuable resource for organizations looking to enhance the security of their web applications by identifying and addressing potential vulnerabilities before they can be exploited by malicious actors.
- I installed ZAP in kali-linux. And performed vulnerability research using ZAP
- For vulnerability research I have used " testphp.vulnweb.com"

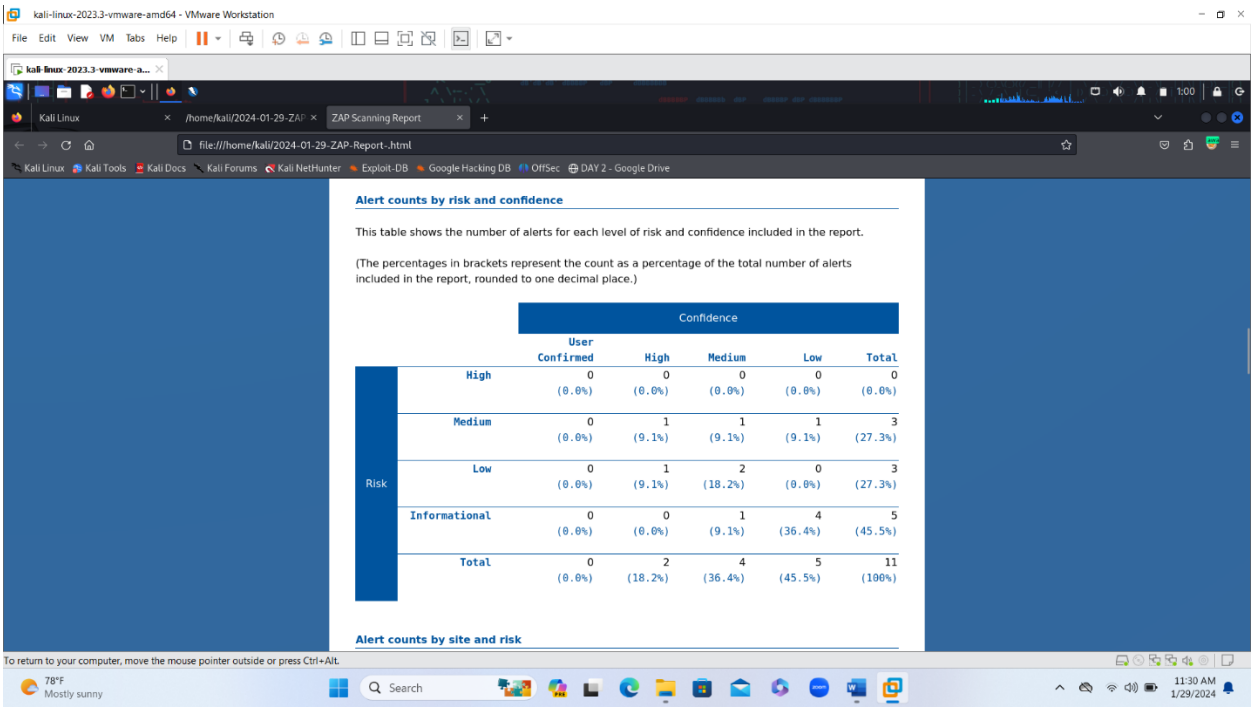

kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.3-vmware-a...
Trash
File System
Home
ZAP
ZAP
2.14.0
KALI
PURPLE
ZAP Tips and Tricks:
The Replacer options page allows you to quickly and easily replace text anywhere in an HTTP(S) message.
INFO: Initializing WebDriver Provider - Provides WebDrivers to control several browsers using Selenium and includes HtmlUnit browser.
kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.3-vmware-a...
Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Welcome to 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
Alerts 0 0 0 0 Main Proxy: localhost:8081
Current Scans 0 0 0 0 0 0 0 0 0
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
72°F
Mostly cloudy
Search
10:28 PM
1/28/2024



- 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.


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Generate Report
Scope Template Filter Options
Report Title: ZAP Scanning Report
Report Name: 2024-01-29-ZAP-Report-.html
Report Directory: /home/kali
Description:
Contexts: Default Context
Sites: http://testphp.vulnweb.com
Generate If No Alerts:
Display Report:
Generate Report Reset Cancel
Alerts (11)
Absence of Anti-CSRF Tokens (44)
Content Security Policy (CSP) Header Not Set
Missing Anti-clickjacking Header (48)
Server Leaks Information via "X-Powered-By"
Server Leaks Version Information via "Server"
X-Content-Type-Options Header Missing (76)
Authentication Request Identified (2)
Charset Mismatch (Header Versus Meta Cont
Information Disclosure - Suspicious Comment
Modern Web Application (9)
User Controllable HTML Element Attribute (Pc
Absence of Anti-CSRF Tokens
URL: http://testphp.vulnv
Risk: Medium
Confidence: Low
Parameter:
Attack:
Evidence: <form action="sea
CWE ID: 352
WASC ID: 9
Source: Passive (10202 - Absence of Anti-CSRF Tokens)
Input Vector:
Description:
No Anti-CSRF tokens were found in a HTML submission form.
A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim.
Alerts 0 3 3 5 Main Proxy: localhost:8081
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
78°F Mostly sunny
Search
11:26 AM 1/29/2024


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Kali Linux
/home/kali/2024-01-29-ZAP
ZAP Scanning Report
file:///home/kali/2024-01-29-ZAP-Report-.html
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec DAY 2 - Google Drive
ZAP Scanning Report
Generated with ZAP on Mon 29 Jan 2024, at 00:58:28
ZAP Version: 2.14.0
Contents
About this report
Report parameters
Summaries
Alert counts by risk and confidence
Alert counts by site and risk
Alert counts by alert type
Alerts
Risk=Medium, Confidence=High (1)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
78°F Mostly sunny
Search
11:28 AM 1/29/2024



- 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

Sairaj mothukuri

[sairajmothukuri28@gmail.com]