

REPORT



Title: Information Gathering Report for testphp.vulnweb.com

Date: 28th October, 2023

Prepared by: Ssozi Malik

Position: Cybersecurity Intern

Objective:

The objective of this report is to present the findings of the information gathering and reconnaissance activities conducted on senselearner.com in a legal and ethical manner. The information collected is intended for security assessment and risk analysis.

Table of Contents

Executive Summary

Introduction

Domain Information

DNS Footprinting

Web Footprinting

Network and WHOIS Enumeration

Vulnerabilities and Security Concerns

Recommendations

Conclusion

EXECUTIVE SUMMARY

Provide a brief overview of the key findings and highlights of my information gathering efforts.

INTRODUCTION

This report outlines the results of my ethical and lawful information gathering and reconnaissance activities on testphp.vulnweb.com. My aim is to provide security insights and risk analysis during my internship. My efforts are geared towards helping testphp.vulnweb.com enhance its security, protect sensitive data and maintain user trust. All my actions adhered to legal and ethical guidelines, respecting the platform's integrity. This report details my methods, findings and recommendations for a safer digital environment.

DOMAIN INFORMATION

Domain Name: testphp.vulnweb.com

IP Address: 44.228.249.3

Domain Dossier

Investigate domains and IP addresses

domain or IP address

☒ domain whois record ☒ DNS records ☐ traceroute

☒ network whois record ☐ service scan

user: anonymous [102.222.234.17]
balance: 48 units
[log in](#) | [account info](#)

CentralOps.net

Do you see Whois records that are missing contact information?
[Read about reduced Whois data due to the GDPR.](#)

Address lookup

canonical name
aliases
addresses

Registrar:

```
Registry Registrant ID:  
Registrant Name: Acunetix Acunetix  
Registrant Organization: Acunetix Ltd  
Registrant Street: 3rd Floor,, J&C Building,, Road Town  
Registrant City: Tortola  
Registrant State/Province:  
Registrant Postal Code: VG1110  
Registrant Country: VG  
Registrant Phone: +1.23456789  
Registrant Fax:  
Registrant Email: administrator@acunetix.com  
Registry Admin ID:  
Admin Name: Acunetix Acunetix  
Admin Organization: Acunetix Ltd  
Admin Street: 3rd Floor,, J&C Building,, Road Town  
Admin City: Tortola  
Admin State/Province:  
Admin Postal Code: VG1110  
Admin Country: VG  
Admin Phone: +1.23456789  
Admin Fax:  
Admin Email: administrator@acunetix.com  
Registry Tech ID:  
Tech Name: Acunetix Acunetix  
Tech Organization: Acunetix Ltd  
Tech Street: 3rd Floor,, J&C Building,, Road Town  
Tech City: Tortola  
Tech State/Province:  
Tech Postal Code: VG1110  
Tech Country: VG  
Tech Phone: +1.23456789  
Tech Fax:  
Tech Email: administrator@acunetix.com
```

Creation, registration and updated Dates:

Domain Whois record

Queried whois.internic.net with "dom vulnweb.com"...

```
Domain Name: VULNWEB.COM  
Registry Domain ID: 1602006391_DOMAIN_COM-VRSN  
Registrar WHOIS Server: whois.eurodns.com  
Registrar URL: http://www.EuroDNS.com  
Updated Date: 2023-05-26T07:56:15Z  
Creation Date: 2010-06-14T07:50:29Z  
Registry Expiry Date: 2025-06-14T07:50:29Z  
Registrar: EuroDNS S.A.  
Registrar IANA ID: 1052  
Registrar Abuse Contact Email: legal.services@eurodns.com  
Registrar Abuse Contact Phone: +352.27220150  
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited  
Name Server: NS1.EURODNS.COM  
Name Server: NS2.EURODNS.COM  
Name Server: NS3.EURODNS.COM  
Name Server: NS4.EURODNS.COM  
DNSSEC: unsigned  
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/  
>>> Last update of whois database: 2023-10-27T08:49:42Z <<<
```

Status: Active

who.is

Search for domains or IP addresses

Premium Domains

Transfer

Features

Log Out

testphp.vulnweb.com

diagnostic tools

Whois

DNS Records

Diagnostics

Ping

PING testphp.vulnweb.com (44.228.249.3) 56(84) bytes of data.
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=1 ttl=42 time=60.2 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=2 ttl=42 time=60.2 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=3 ttl=42 time=60.2 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=4 ttl=42 time=60.2 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=5 ttl=42 time=60.2 ms

--- testphp.vulnweb.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 60.241/60.253/60.275/0.011 ms

DNS FOOTPRINTING

Name Servers:

```
Tech Email: administrator@acunetix.com
Name Server: ns1.eurodns.com
Name Server: ns2.eurodns.com
Name Server: ns3.eurodns.com
Name Server: ns4.eurodns.com
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2023-10-27T08:49:55Z <<<
```

| Where these Name Servers come from | | | | |
|------------------------------------|----|----|-----------------|---------------------|
| vulnweb.com | IN | NS | ns2.eurodns.com | 86400s (1.00:00:00) |
| vulnweb.com | IN | NS | ns3.eurodns.com | 86400s (1.00:00:00) |
| vulnweb.com | IN | NS | ns4.eurodns.com | 86400s (1.00:00:00) |
| vulnweb.com | IN | NS | ns1.eurodns.com | 86400s (1.00:00:00) |

DNS Records:

A records

| | | | |
|---------------------|---|------|--------------|
| testphp.vulnweb.com | A | 2286 | 44.228.249.3 |
|---------------------|---|------|--------------|

SOA records

| DNS Records for testphp.vulnweb.com | | | | |
|-------------------------------------|------|------|----------|---|
| Hostname | Type | TTL | Priority | Content |
| testphp.vulnweb.com | SOA | 1017 | | ns1.eurodns.com hostmaster@eurodns.com 2021110100 86400 7200 604800 86400 |

PTR records

3.249.228.44.in-addr.arpa IN PTR ec2-44-228-249-3.us-west-2.compute.amazonaws.com 300s (00:05:00)

TXT records

| TXT Records | | ** Find more hosts in Sender Policy Framework (SPF) configurations |
|-------------|--|--|
| | | "google-site-verification:toEctYsulNIxgraKk7H3z58PCyz2IOcc36pIupEPmYQ" |

Subdomains:

```
(kali@kali)-[~/Desktop]
$ sudo subfinder -d testphp.vulnweb.com
[INF] Detected old /root/.config/subfinder/config.yaml config file, trying to migrate p
roviders to /root/.config/subfinder/provider-config.yaml
[INF] Migration successful from /root/.config/subfinder/config.yaml to /root/.config/su
bfinder/provider-config.yaml.

projectdiscovery.io

[INF] Current subfinder version v2.6.0
[INF] Loading provider config from /root/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for testphp.vulnweb.com
www.testphp.vulnweb.com
[INF] Found 1 subdomains for testphp.vulnweb.com in 2 seconds 699 milliseconds
```

WEB FOOTPRINTING

Web Server Information:

Web Servers

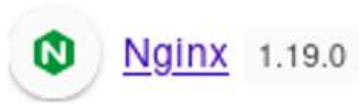
nginx

[nginx Usage Statistics](#) · [Download List of All Websites using nginx](#)

nginx [engine x] is a HTTP server and mail proxy server written by Igor Sysoev.

Web Server Version:

Web servers



Document Encoding:

Document Encoding

[View Global Trends](#)

W ISO/IEC 8859

[ISO/IEC 8859 Usage Statistics](#)

ISO 8859, more formally ISO/IEC 8859, is a joint ISO and IEC standard for 8-bit character encodings for use by computers. The standard is divided into numbered, separately published parts, such as ISO/IEC 8859-1, ISO/IEC 8859-2, etc., each of which may be informally referred to as a standard in itself. There are currently 15 parts as of 2006 excluding the abandoned ISO/IEC 8859-12 standard.

Document Standards:

Document Standards

[View Global Trends](#)

W3 HTML 4.01 Transitional DTD

[HTML 4.01 Transitional DTD Usage Statistics](#)

Claims HTML 4.01 Transitional DTD, which includes presentation attributes and elements that W3C expects to phase out as support for style sheets matures.

W Cascading Style Sheets

[Cascading Style Sheets Usage Statistics](#)

Cascading Style Sheets (CSS) is a stylesheet language used to describe the presentation of a document written in a markup language. Its most common application is to style web pages written in HTML.

W Javascript

[Javascript Usage Statistics](#)

JavaScript is a scripting language most often used for client-side web development.

Operating system:

Operating Systems and Servers

[View Global Trends](#)



[Ubuntu Usage Statistics](#) · [Download List of All Websites using Ubuntu](#)

Ubuntu is a free, Debian derived Linux-based operating system, available with both community and professional support.

Operating system version:

```
(kali@kali)-[/opt]
$ whatweb http://testphp.vulnweb.com
http://testphp.vulnweb.com [200 OK] ActiveX[027CDB6E-AE6D-11cf-9688-444553540000], Adobe-Flash, Country[UNITED STATES][US], Email[wvs@acunetix.com], HTTPServer[nginx/1.19.0], IP[44.228.249.3], Object[http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0][clsid:027CDB6E-AE6D-11cf-9688-444553540000], PHP[5.6.40-38+ubuntu20.04.1+deb.sury.org+1], Script[text/JavaScript], Title[Home of Acunetix Art], X-Powered-By[PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1], nginx[1.19.0]
```

Hidden Directories and File Structure:

```
(kali@kali)-[~/Desktop]
$ sudo gobuster dir -u http://testphp.vulnweb.com -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[sudo] password for kali:

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://testphp.vulnweb.com
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/images (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/images/]
/cgi-bin (Status: 403) [Size: 276]
/admin (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/admin/]
/pictures (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/pictures/]
/vendor (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/vendor/]
/Templates (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/Templates/]
/Flash (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/Flash/]
/CVS (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/CVS/]
/AJAX (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/AJAX/]
/secured (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/secured/]
```

Technologies in Use:

Frameworks:

Frameworks

[View Global Trends](#)

Shockwave Flash Embed

[Shockwave Flash Embed Usage Statistics](#) · [Download List of All Websites using Shockwave Flash Embed](#)

Adobe Flash Macromedia shockwave content. End of life product retiring in 2020.

PHP

[PHP Usage Statistics](#) · [Download List of All Websites using PHP](#)

PHP is a widely used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML.

Framework version:

Programming languages



Editor:

Editor



Reverse Proxies:

Reverse proxies



Scripting Languages:

```
(kali@kali)-[/opt]
$ whatweb http://testphp.vulnweb.com
http://testphp.vulnweb.com [200 OK] ActiveX[027CDB6E-AE6D-11cf-9688-444553540000], Adobe-Flash, Country[UNITED STATES][US], Email[wvs@acunetix.com], HTTPServer[nginx/1.19.0], IP[44.228.249.3], Object[http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0][c1sid:027CDB6E-AE6D-11cf-9688-444553540000], PHP[5.6.40-38+ubuntu20.04.1+deb.sury.org+1], Script[text/JavaScript], Title[Home of Acunetix Art], X-Powered-By[PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1], nginx[1.19.0]
```


NETWORK AND WHOIS ENUMERATION

Network Scans:

```
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.34s latency).
Not shown: 65533 filtered tcp ports (no-response), 1 filtered tcp ports (host-unreach)
PORT      STATE SERVICE VERSION
80/tcp    open  http      nginx 1.19.0

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 43796.97 seconds

(kali@kali)-[/opt]
```

ASN Information:

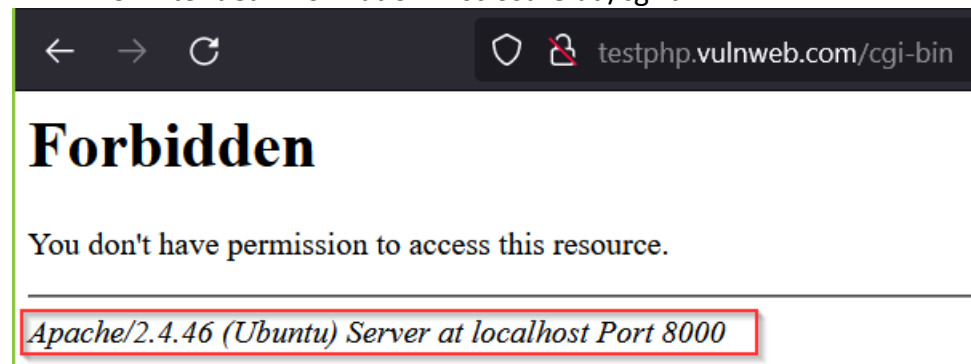
AS Number

AS16509

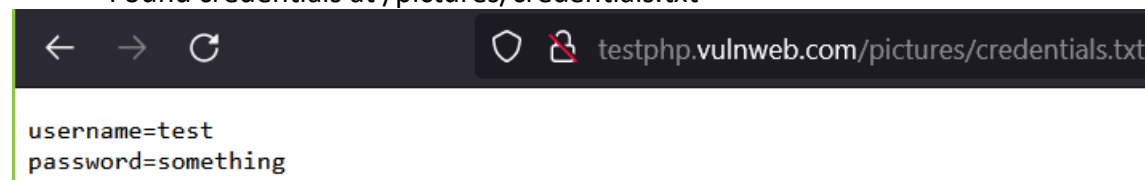
VULNERABILITIES AND SECURITY CONCERNS

Identify any vulnerabilities or security concerns based on the gathered information. This could include outdated software, exposed directories, or other potential issues that may pose a security risk.

While browsing the found hidden directories, I discovered the following;
Unintended Information Disclosure at /cgi-bin



Found credentials at /pictures/credentials.txt



HTML Transitional DTD used has a vulnerability

CVE-2016-10033 → PHPMailer Remote Code Execution

More details about this vulnerability can be found here: <https://www.fortinet.com/blog/threat-research/analysis-of-phpmailer-remote-code-execution-vulnerability-cve-2016-10033>

The screenshot shows the NIST National Vulnerability Database (NVD) detail page for CVE-2016-10033. The browser address bar shows the URL: <https://nvd.nist.gov/vuln/detail/CVE-2016-10033>. A green button labeled "VULNERABILITIES" is visible. The main heading is "CVE-2016-10033 Detail". Below it is the "Description" section, which states: "The mailSend function in the isMail transport in PHPMailer before 5.2.18 might allow remote attackers to pass extra parameters to the mail command and consequently execute arbitrary code via a \" (backslash double quote) in a crafted Sender property." Below the description is a "Severity" section with tabs for "CVSS Version 3.x" and "CVSS Version 2.0". Under "CVSS 3.x Severity and Metrics:", there is a "NIST: NVD" icon, a "Base Score: 9.8 CRITICAL" badge, and a "Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H". A note at the bottom states: "NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA. Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List."

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score: 9.8 CRITICAL** **Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H**

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

PHP v5.6.40 used on the website has several critical vulnerabilities like

- CVE-2022-4900 → Local Buffer overflow in PHP
- CVE-2021-21703 → Privilege Escalation in PHP
- CVE-2014-3538 → Input Validation Error in PHP
- CVE-2013-7345 → Permissions, Privileges & Access Controls in PHP

More details about these vulnerabilities can be found via: https://www.cybersecurity-help.cz/vdb/php_group/php/5.6.40/



Home / Vulnerability Database / PHP Group / PHP / 5.6.40

Search vulnerability database

☐ With exploit

☐ With patch

Vulnerabilities in PHP 5.6.40

Local buffer overflow in PHP 30 Mar, 2020

Low [Patched](#)

Input validation error in PHP 09 Jul, 2014

Medium [Not Patched](#)

Privilege escalation in PHP 26 Oct, 2008

Low [Patched](#)

Permissions, Privileges, and Access Controls in PHP 24 Mar, 2014

Medium [Patched](#)



CVE-2019-9021

For more details: <https://www.rapid7.com/db/vulnerabilities/php-cve-2019-9021/>

PHP Vulnerability: CVE-2019-9021

| Severity | CVSS | Published | Created | Added | Modified |
|----------|----------------------|------------|------------|------------|------------|
| 8 | (AV:N/AC:L /Au:N/C:P | 02/22/2019 | 03/19/2019 | 02/27/2019 | 07/21/2021 |

And CSRF (Change Admin Email)

Further details about this vulnerability: <https://www.exploit-db.com/exploits/48494>

forma.lms 5.6.40 - Cross-Site Request Forgery (Change Admin Email)

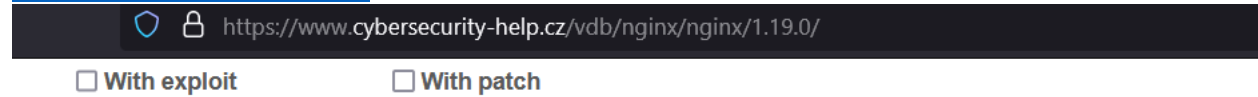
| | | | | | |
|---|--------------------|--------------------------------|-------------------------|-------------------------|----------------------------|
| EDB-ID: 48494 | CVE: N/A | Author: DANIEL ORTIZ | Type: WEBAPPS | Platform: PHP | Date: 2020-05-21 |
| EDB Verified: ✗ | | Exploit: / | | Vulnerable App: | |

Nginx for web services also has several vulnerabilities like

- CVE-2022-41741
- CVE-2022-41742

- CVE-2021-3618 → Security Restrict Bypass in Nginx
- CVE-2021-23017 → Remote Code Execution

More details about these vulnerabilities are at: <https://www.cybersecurity-help.cz/vdb/SB2022101941>



Vulnerabilities in nginx 1.19.0

Multiple vulnerabilities in nginx 19 Oct, 2022

Medium ✓ Patched

Security restrictions bypass in nginx 09 Jan, 2022

Medium ✓ Patched

Remote code execution in nginx 25 May, 2021

High ✓ Patched

Apache Web Server version also has several vulnerabilities

- CVE-2006-20001, CVE-2021-39275 and CVE-2021-44790 → Buffer overflow
- CVE-2020-35452 → Stack-based Buffer overflow
- CVE-2022-36760, CVE-2022-22720, CVE-2022-26377 and CVE-2021-33193 → Inconsistent interpretation of HTTP requests
- CVE-2022-37436 → HTTP response splitting
- CVE-2022-23943 → Out-of-bounds write
- CVE-2022-22721 → Integer overflow
- CVE-2022-22719, CVE-2021-30641 and CVE-2022-29404 → Input validation error
- CVE-2021-34798, CVE-2021-31618, CVE-2021-26691, CVE-2021-26690 and CVE-2020-13950 → NULL pointer dereference
- CVE-2021-36160, CVE-2022-28330, CVE-2022-28614, CVE-2022-28615, CVE-2022-30556 and CVE-2023-31122 → Out-of-bounds read
- CVE-2021-40438 and CVE-2021-44224 → Server-Side Request Forgery (SSRF)
- CVE-2020-13938 → Improper Privilege Management

- CVE-2019-17567 → Security restrictions bypass
- CVE-2023-25690 and CVE-2023-27522 → HTTP response splitting
- CVE-2022-30522 → Resource exhaustion
- CVE-2022-31813 → Improper Authentication
- CVE-2023-45802 and CVE-2023-43622 → Resource management error

More details are at: https://www.cybersecurity-help.cz/vdb/apache_foundation/apache_http_server/2.4.46/

With exploit With patch

Vulnerabilities in Apache HTTP Server 2.4.46

| Vulnerability Title | Severity | Status | Date |
|---|----------|---------|--------------|
| Multiple vulnerabilities in Apache HTTP Server | Medium | Patched | Oct, 2023 |
| HTTP response splitting vulnerabilities in Apache HTTP Server | Medium | Patched | 07 Mar, 2023 |
| Multiple vulnerabilities in Apache HTTP Server | Medium | Patched | Jan, 2023 |
| Multiple vulnerabilities in Apache HTTP Server | Medium | Patched | Jun, 2022 |
| Multiple vulnerabilities in Apache HTTP Server | High | Patched | Mar, 2022 |
| Multiple vulnerabilities in Apache HTTP Server | Critical | Patched | Dec, 2021 |
| Multiple vulnerabilities in Apache HTTP Server | High | Patched | Sep, 2021 |
| HTTP request smuggling in Apache HTTP Server | Medium | Patched | 13 Sep, 2021 |
| Multiple vulnerabilities in Apache HTTP Server | Medium | Patched | Jun, 2021 |

RECOMMENDATIONS

- Updating PHP to the latest version.
- Updating Apache and Nginx Web services to the latest version
- Updating Ubuntu OS to the latest version
- Enhancing server security configurations.
- Securing sensitive information.
- Implementing best practices for online privacy.

CONCLUSION

Thank you for the learning opportunity.

REFERENCES

The following are the tools used during the information gathering process.

Domain Footprinting

- who.is

- dnsdumpster.com

- Domain dossier <https://centralops.net/co/DomainDossier.aspx>

- Hurricane Electric Internet Services (he.net)

Web footprinting

- Wappalyzer

- BuiltWith

- WhatWeb

Sub-domain Finding

- Sub-finder

Network Scanning

- Nmap

Hidden Directories

- Gobuster

END