Information Gathering Report

Target: testphp.vulnweb.com

Performed on Kali Linux

December 2025

1 Introduction

This report documents the passive and active legal information gathering performed on the target **testphp.vulnweb.com**, a publicly accessible and intentionally vulnerable web application hosted by Acunetix for cybersecurity testing and research. No intrusive or unauthorized exploitation was attempted.

2 Objective

The objectives of this assignment were:

- Gather publicly available information about the target.
- Enumerate DNS records, hosting provider, subdomains, technologies, directories, and ports.
- Document results with screenshots.
- Follow ethical hacking rules and avoid intrusive techniques.

3 Target Details

Target Subdomain: `testphp.vulnweb.com`
Parent Domain: `vulnweb.com`

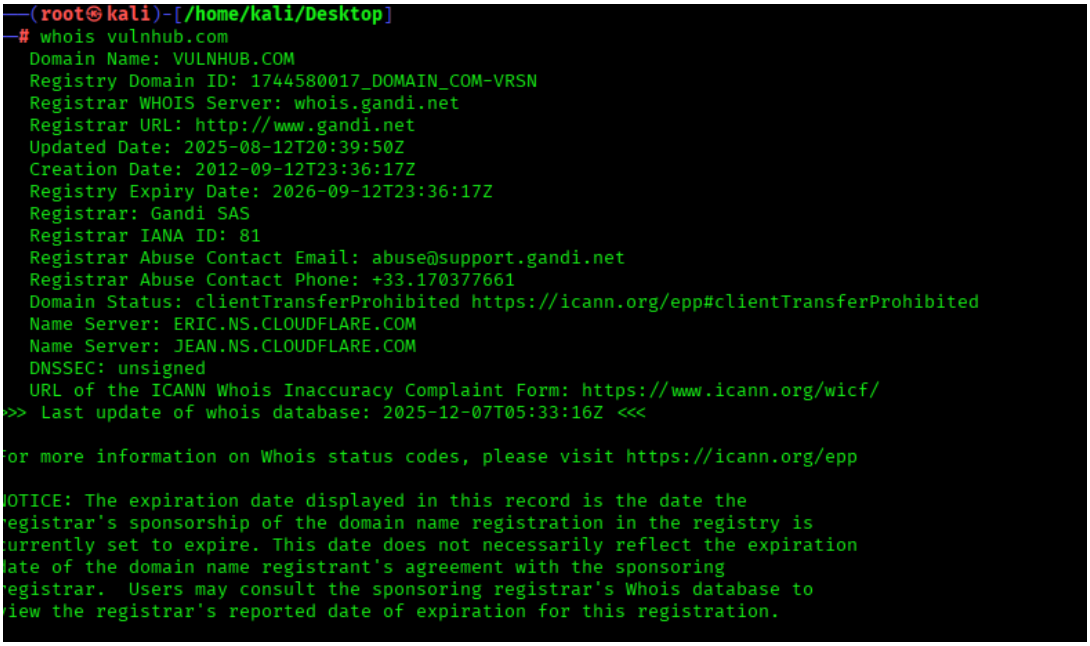
4 Basic Information Gathering

4.1 WHOIS Lookup

WHOIS entries apply only to the root domain. Command used:

```
whois vulnweb.com
```

Screenshot:



4.2 DNS Enumeration

Commands executed:

```
dig vulnweb.com
dig ANY vulnweb.com
dig MX vulnweb.com
dig NS vulnweb.com
nslookup vulnweb.com
```

Screenshots:

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# dig testphp.vulnhub.com ANY

; <<>> DiG 9.20.11-4+b1-Debian <<>> testphp.vulnhub.com ANY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33647
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;testphp.vulnhub.com.           IN      ANY

;; ANSWER SECTION:
testphp.vulnhub.com.    3600    IN      HINFO   "RFC8482" ""
testphp.vulnhub.com.    3600    IN      RRSIG   HINFO 13 3 3600 20251208065640 20251206045640 34505 vulnhub.com. rAV
Q39zTIz1Rh8oWzSL29hVYA0/gksXGUvOWTLDFeSiSPkcAKqSBl5NJ pNbLz9LVz3DPj0VXANW3lMSc5/5gAg==

;; Query time: 551 msec
;; SERVER: 10.139.49.25#53(10.139.49.25) (TCP)
;; WHEN: Sun Dec 07 11:27:30 UTC 2025
;; MSG SIZE  rcvd: 176
```

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# dig NS vulnhub.com

; <<>> DiG 9.20.11-4+b1-Debian <<>> NS vulnhub.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53139
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;vulnhub.com.                   IN      NS

;; ANSWER SECTION:
vulnhub.com.            86400   IN      NS      eric.ns.cloudflare.com.
vulnhub.com.            86400   IN      NS      jean.ns.cloudflare.com.

;; Query time: 155 msec
;; SERVER: 10.139.49.25#53(10.139.49.25) (UDP)
;; WHEN: Sun Dec 07 11:30:55 UTC 2025
;; MSG SIZE  rcvd: 92
```

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nslookup testphp.vulnhub.com
Server:         10.139.49.25
Address:        10.139.49.25#53

Non-authoritative answer:
*** Can't find testphp.vulnhub.com: No answer
```

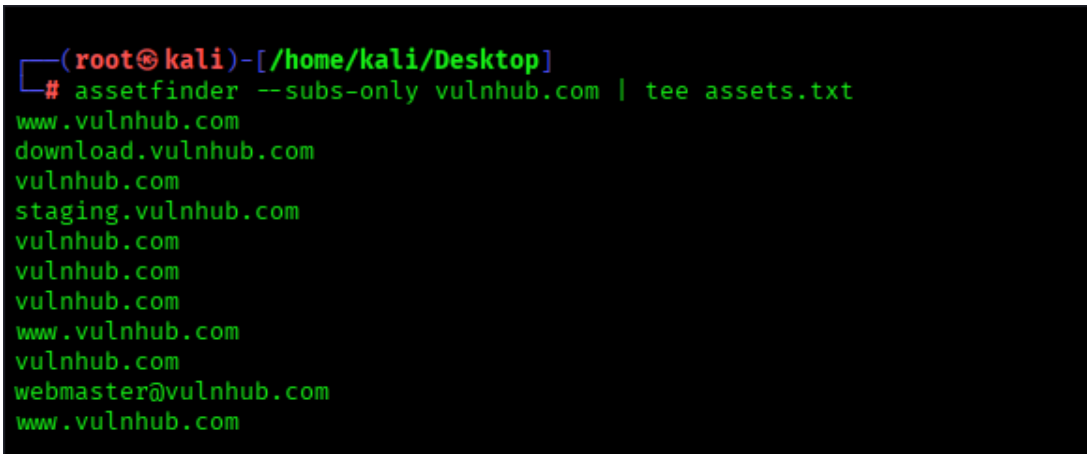
5 Subdomain Enumeration

Tools used: `assetfinder`, `amass`

5.1 assetfinder

```
assetfinder --subs-only vulnweb.com
```

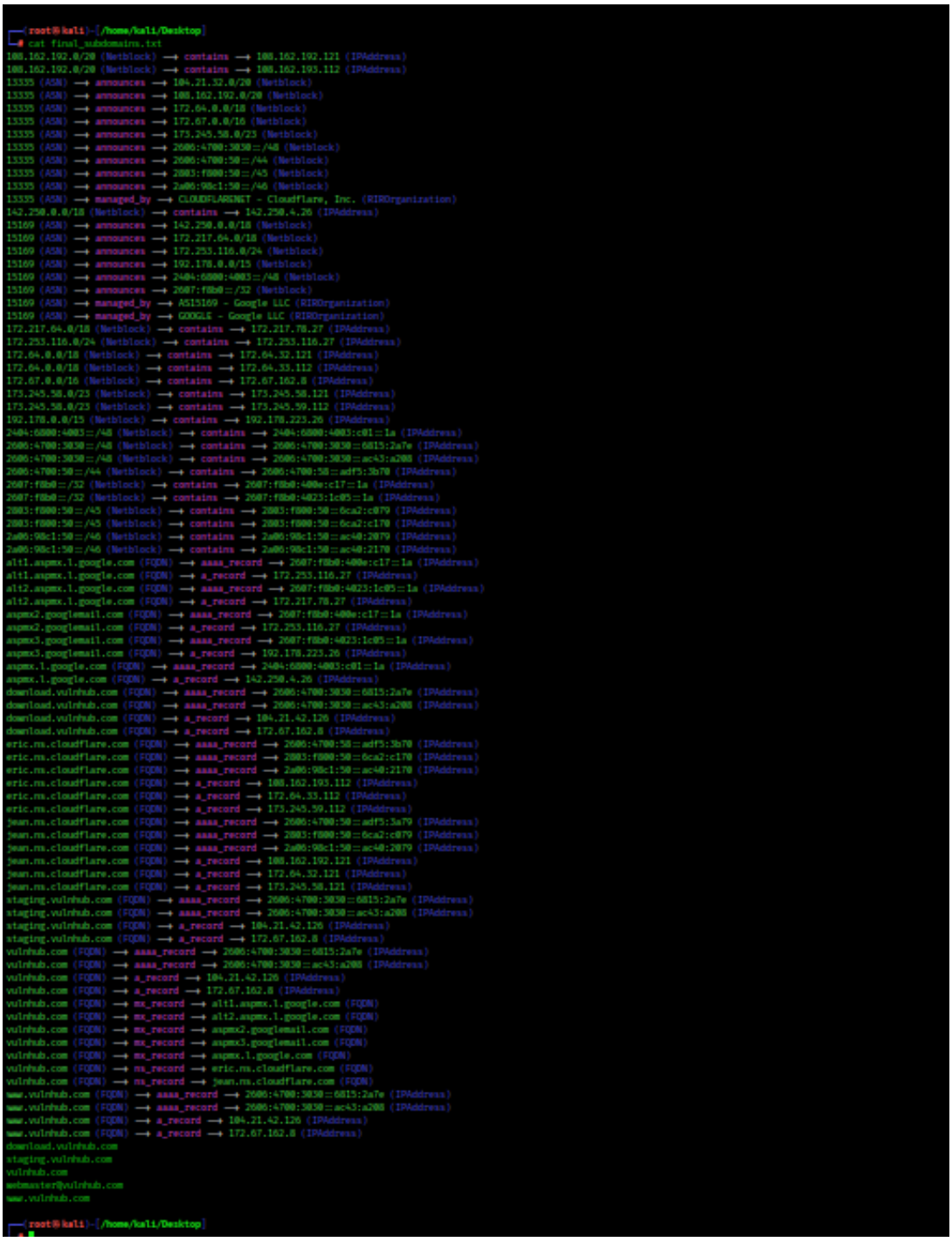
Screenshot:



5.2 amass

```
amass enum -passive -d vulnweb.com
```

Screenshot:

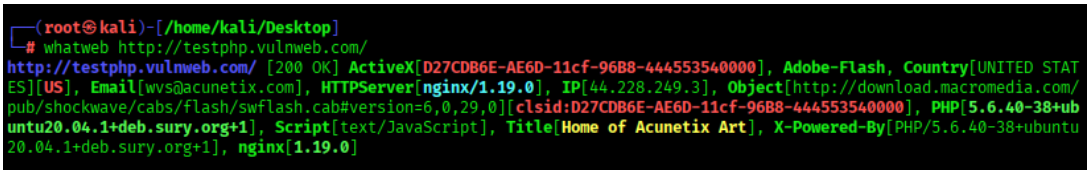


6 Technology Fingerprinting

6.1 WhatWeb

`whatweb http://testphp.vulnweb.com`

Screenshot:

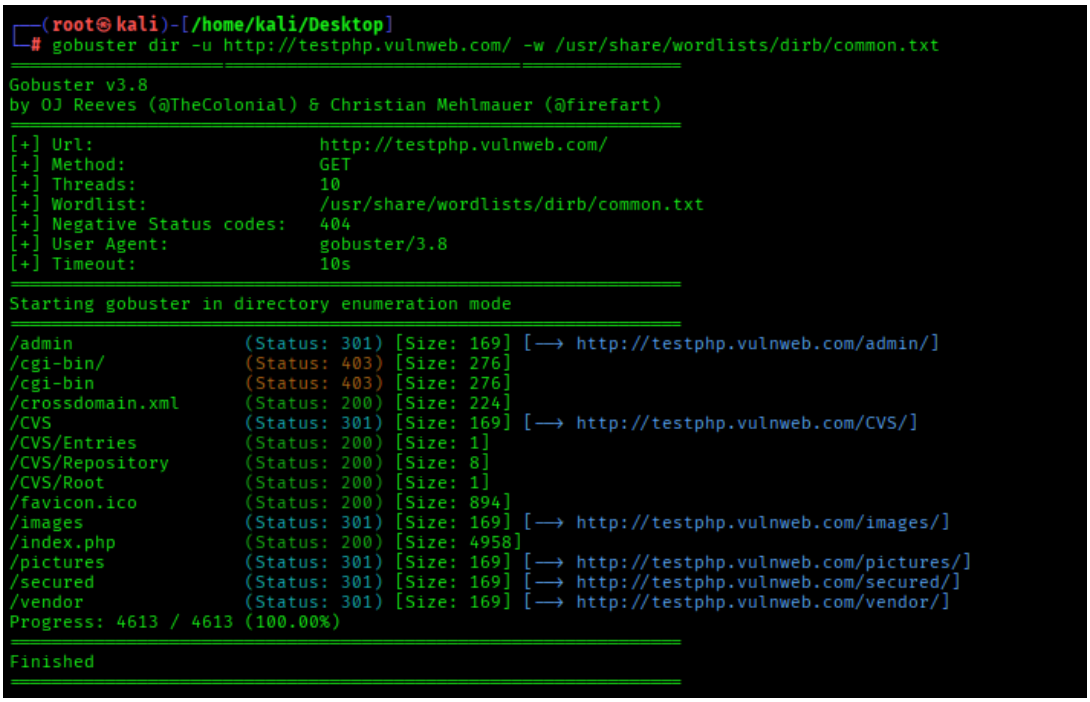


7 Directory and File Discovery

7.1 Gobuster

```
gobuster dir -u http://testphp.vulnweb.com \
-w /usr/share/wordlists/dirb/common.txt
```

Screenshot:



7.2 Dirb

`dirb http://testphp.vulnweb.com`

Screenshot:

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# dirb http://testphp.vulnweb.com/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Dec  7 11:41:10 2025
URL_BASE: http://testphp.vulnweb.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://testphp.vulnweb.com/ ----
==> DIRECTORY: http://testphp.vulnweb.com/admin/
--> Testing: http://testphp.vulnweb.com/bl
+ http://testphp.vulnweb.com/cgi-bin (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/crossdomain.xml (CODE:200|SIZE:224)
==> DIRECTORY: http://testphp.vulnweb.com/CVS/
+ http://testphp.vulnweb.com/CVS/Entries (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/CVS/Repository (CODE:200|SIZE:8)
+ http://testphp.vulnweb.com/CVS/Root (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/favicon.ico (CODE:200|SIZE:894)
==> DIRECTORY: http://testphp.vulnweb.com/images/
+ http://testphp.vulnweb.com/index.php (CODE:200|SIZE:4958)

(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT CONNECT)

-----------------
END_TIME: Sun Dec  7 12:03:17 2025
DOWNLOADED: 2488 - FOUND: 8
```

8 Open Ports and Service Enumeration

8.1 Nmap Scan

`nmap -sV -sC testphp.vulnweb.com`

Screenshot:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -sC testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 11:59 UTC
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.059s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.co
m
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.19.0
|_http-title: Home of Acunetix Art

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.84 seconds
```

9 Public OSINT Information

Manual Google queries:

```
site:vulnweb.com contact
vulnweb.com security
"vulnweb" linkedin
```

Findings:

- Vulnweb belongs to Acunetix (Invicti Security).
- Public documentation indicates intentionally vulnerable labs.
- No sensitive leaks or unauthorized information found.

10 Summary of Findings

- WHOIS: Valid root domain information for vulnweb.com
- DNS: Standard MX, NS, A records, no zone transfer allowed
- Subdomains: Several discovered, no sensitive ones
- Ports: Only port 80 open running Apache/PHP
- Directories: PHP info, admin pages, test pages discovered
- Technologies: PHP, Apache (from WhatWeb)
- Emails: Limited emails harvested

11 Challenges Faced

- Subdomain WHOIS lookup failed (expected)
- AXFR zone transfer blocked
- Rate limiting slowed directory enumeration

12 Conclusion

The target **testphp.vulnweb.com** behaves as an intentionally vulnerable environment for cybersecurity testing. Information-gathering results align with standard testbed configurations. No exploitation or unauthorized access was performed. Results may be used for academic and security research purposes under ethical guidelines.