

# DVWA Installation and Vulnerability Discovery

## Step 1 — Installation & Setup

Update & install DVWA

Command-sudo apt update

sudo apt install dvwa

```
(marie@math)-[~]
$ sudo apt install dvwa
[sudo] password for marie:
The following packages were automatically installed and are no longer required:
amass-common libgeos3.14.0 libobjc-14-dev libwireshark18 python3-kismetcapturefreaklabszigbee samba-ad-dc
docker-buildx libgirepository-1.0-1 libplacebo349 libwiretap15 python3-kismetcapturertl433 samba-ad-provision
girl1.2-girepository-2.0 libgpgmepp6t64 libportmidi0 libwsutil16 python3-kismetcapturertladsb samba-dsdb-modules
libarmadillo14 libinstpatch-1.0-2 librav1e0.7 libx264-164 python3-kismetcapturertlamr
libbluray2 libjs-jquery-ui libsqlcipher1 python3-bluepy python3-pysmi
libbson-1.0-0t64 libjs-underscore libtheoraec1 python3-click-plugins python3-xlutils
libdisplay-info2 libmongoc-1.0-0t64 libtheoraenc1 python3-gpg python3-xlwt
libgdal37 libnet1 libudfread0 python3-kismetcapturebtgeiger python3-zombie-imp

Use 'sudo apt autoremove' to remove them.

Installing:
dvwa

Installing dependencies:
php8.4-fpm php8.4-gd

Suggested packages:
php-pear

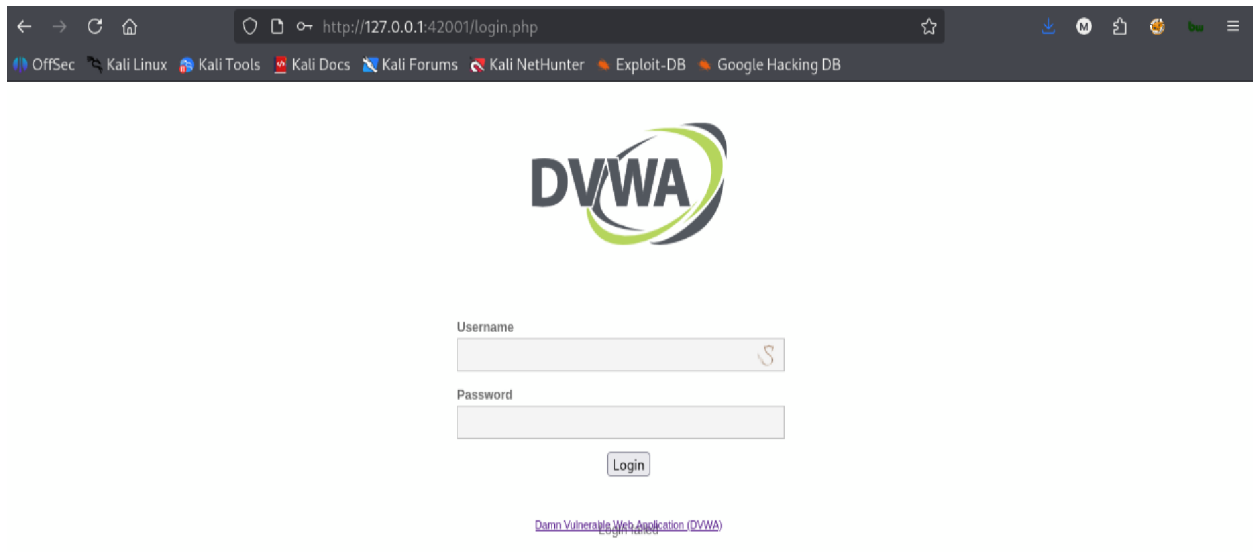
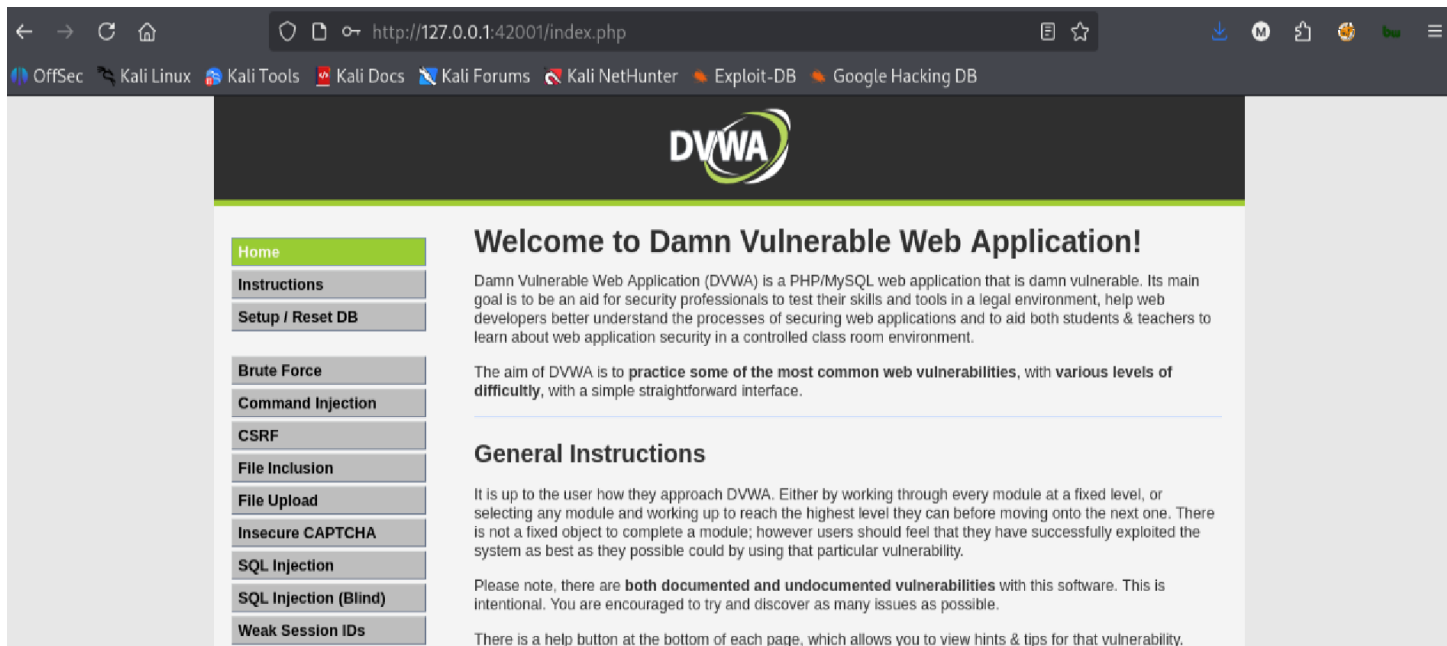
Summary:
Upgrading: 0, Installing: 3, Removing: 0, Not Upgrading: 77
Download size: 2,689 kB
Space needed: 7,975 kB / 2,417 MB available

Continue? [Y/n] y
Get:1 https://http.kali.org/kali kali-rolling/main amd64 php8.4-fpm amd64 8.4.11-1+b1 [1,860 kB]
```

```
Unpacking php8.4-fpm (8.4.11-1+b1) ...
Selecting previously unselected package php8.4-gd.
Preparing to unpack .../php8.4-gd_8.4.11-1+b1_amd64.deb ...
Unpacking php8.4-gd (8.4.11-1+b1) ...
Selecting previously unselected package dvwa.
Preparing to unpack .../dvwa_2.4-0kali1_all.deb ...
Unpacking dvwa (2.4-0kali1) ...
Setting up php8.4-gd (8.4.11-1+b1) ...
Creating config file /etc/php/8.4/mods-available/gd.ini with new version
Setting up php8.4-fpm (8.4.11-1+b1) ...
Creating config file /etc/php/8.4/fpm/php.ini with new version
NOTICE: Not enabling PHP 8.4 FPM by default.
NOTICE: To enable PHP 8.4 FPM in Apache2 do:
NOTICE: a2enmod proxy_fcgi setenvif
NOTICE: a2enconf php8.4-fpm
NOTICE: You are seeing this message because you have apache2 package installed.
update-rc.d: We have no instructions for the php8.4-fpm init script.
update-rc.d: It looks like a network service, we disable it.
Setting up dvwa (2.4-0kali1) ...
dvwa.service is a disabled or a static unit, not starting it.
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for libapache2-mod-php8.4 (8.4.11-1+b1) ...
Processing triggers for kali-menu (2025.4.2) ...
Processing triggers for php8.4-cli (8.4.11-1+b1) ...
Processing triggers for php8.4-fpm (8.4.11-1+b1) ...
NOTICE: Not enabling PHP 8.4 FPM by default.
NOTICE: To enable PHP 8.4 FPM in Apache2 do:
NOTICE: a2enmod proxy_fcgi setenvif
NOTICE: a2enconf php8.4-fpm
NOTICE: You are seeing this message because you have apache2 package installed.
```

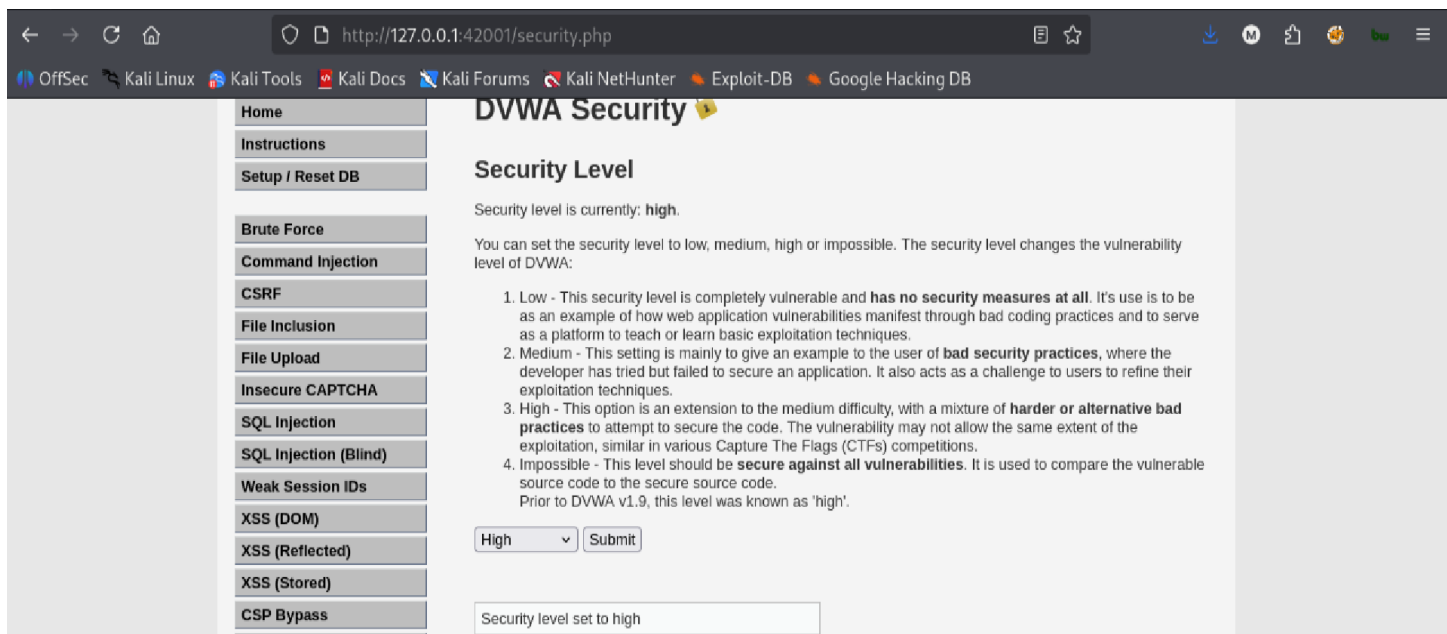
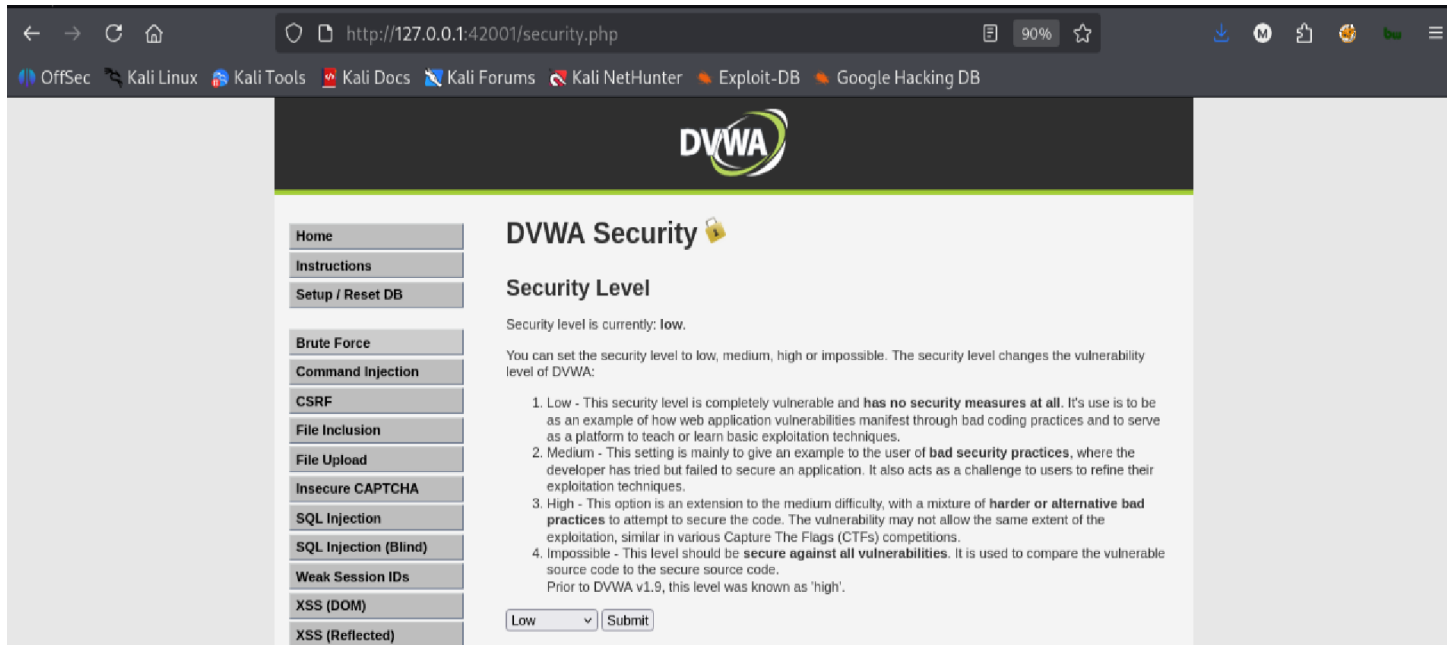
## 2.Run the Dvwa with the command

`sudo dvwa-start`



## Step 2: DVWA Security Levels

In DVWA set Security to Low first , Run tests , then set to medium and high & Rerun the tests



## Step 3: Vulnerability Exercises

### Sql Injection



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Authorization Bypass

### 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 Information

- [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)
- <https://www.netparker.com/blog/web-security/sql-injection-cheat-sheet/>

`http://127.0.0.1:42001/instructions.php`

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Authorization Bypass

Open HTTP Redirect

Cryptography

DVWA Security

PHP Info

About

Logout

### Vulnerability: SQL Injection

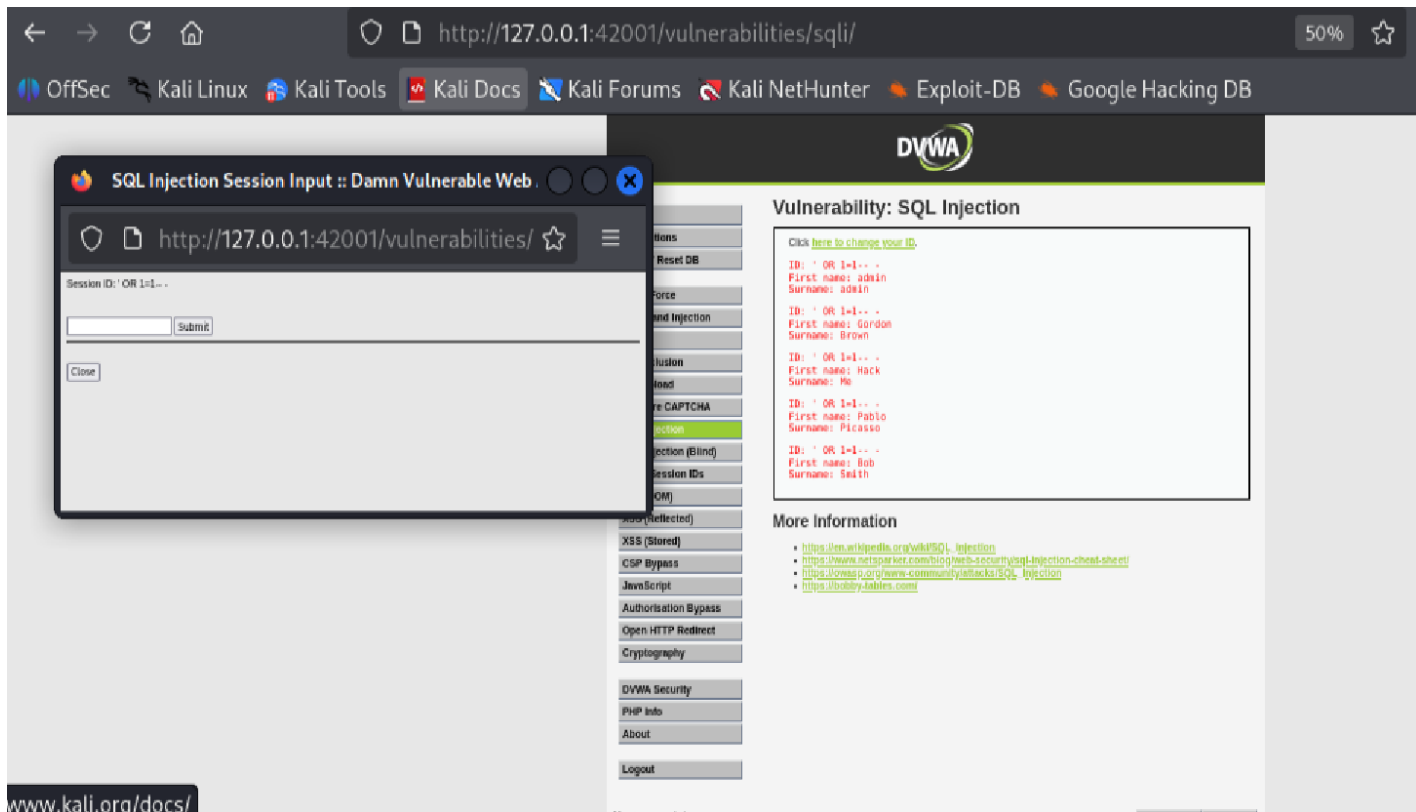
User ID:

ID: 1  
First name: admin  
Surname: admin

#### More Information

- [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)
- <https://www.netparker.com/blog/web-security/sql-injection-cheat-sheet/>
- <https://www.exploit-db.com/exploits/10131/sql-injection/>
- <https://www.exploit-db.com/exploits/10131/sql-injection/>

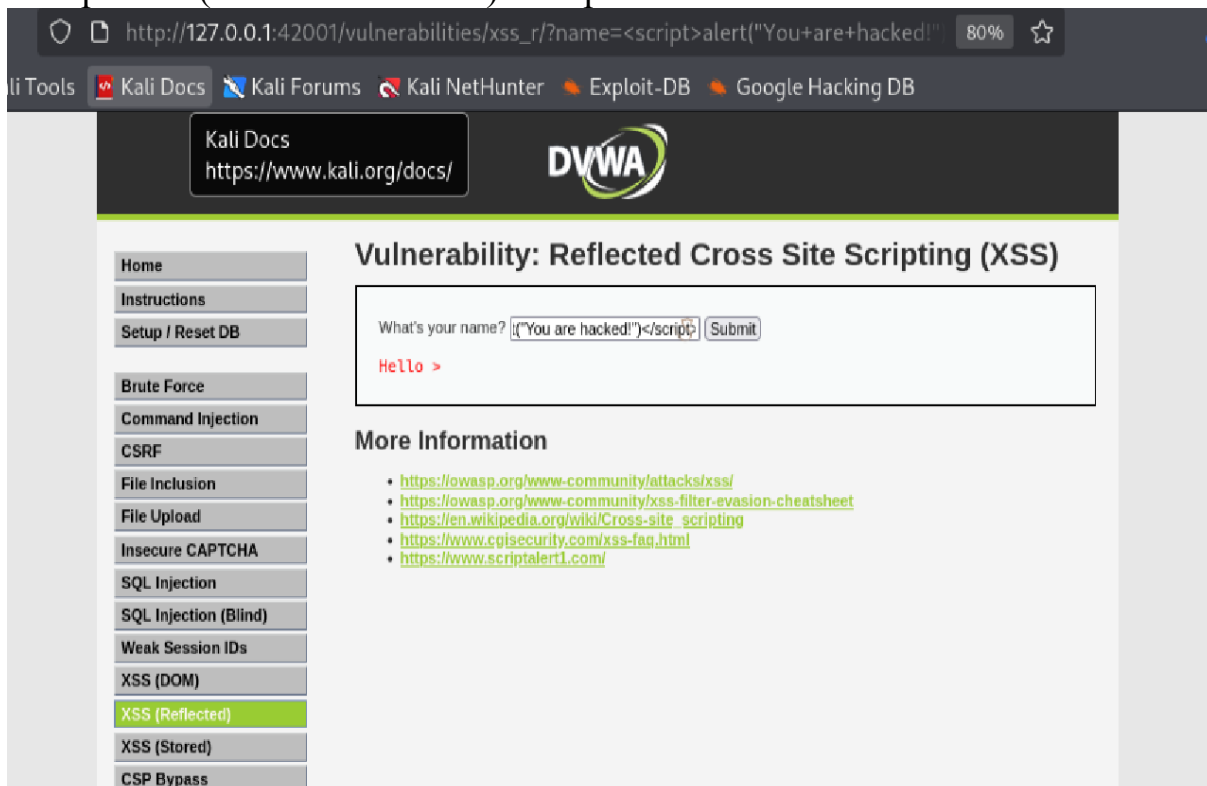
Username: admin  
Security Level: medium  
Locale: en  
SQL DB: mysql



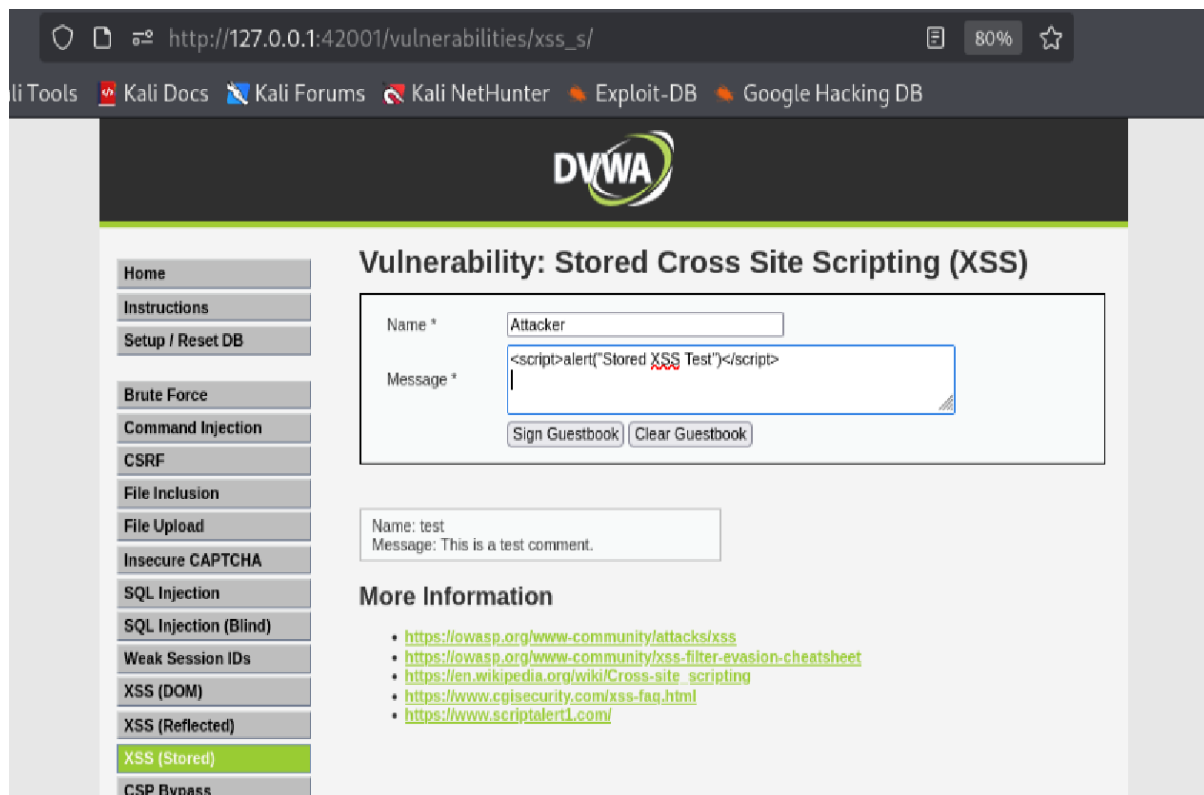
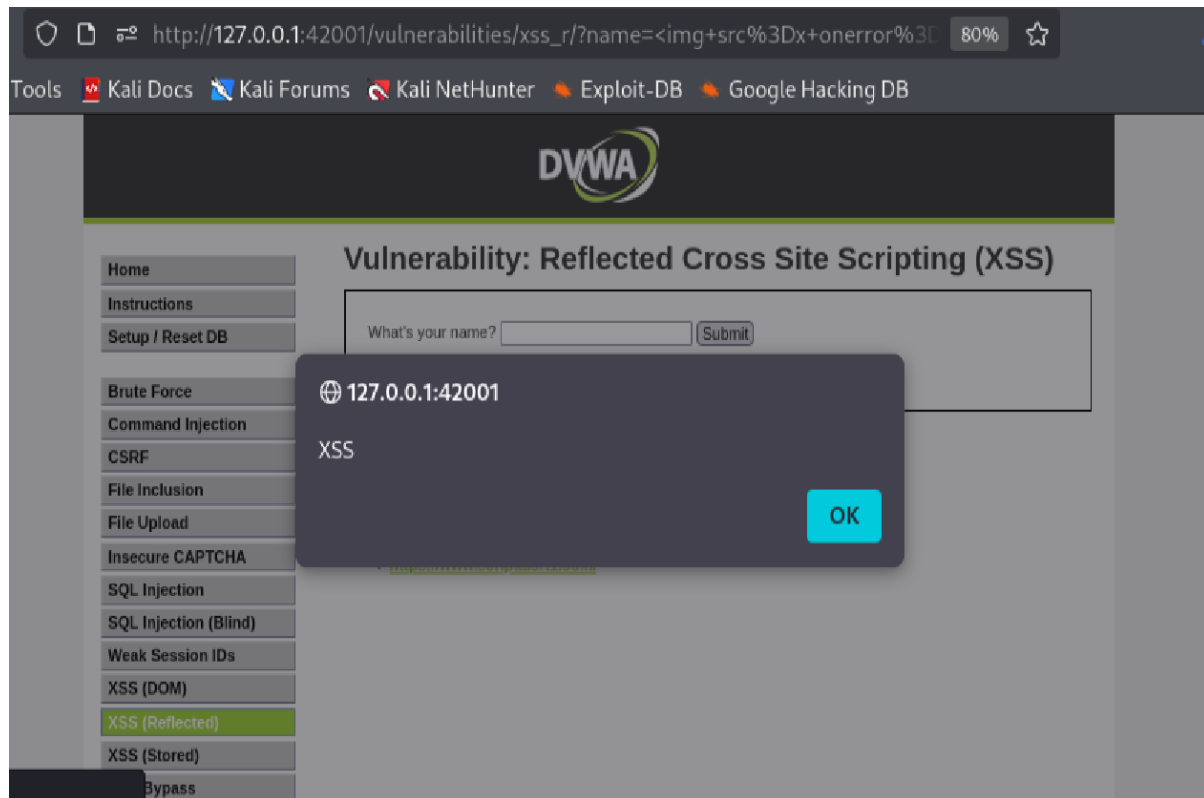
## Cross Site Scripting-

When the following payload is entered

```
<script>alert("You are hacked!")</script>
```



<img src=x onerror=alert(“XSS”)>



Script is saved in the database

http://127.0.0.1:42001/vulnerabilities/xss\_s/ 80%

Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

**DVWA**

Home  
Instructions  
Setup / Reset DB  
Brute Force  
Command Injection  
CSRF  
File Inclusion  
File Upload  
Insecure CAPTCHA  
SQL Injection  
SQL Injection (Blind)  
Weak Session IDs  
XSS (DOM)  
XSS (Reflected)  
**XSS (Stored)**  
CSP Bypass

### Vulnerability: Stored Cross Site Scripting (XSS)

Name \*   
Message \*

Name: test  
Message: This is a test comment.

Name: Attacker  
Message: alert("Stored XSS Test")

#### More Information

- <https://owasp.org/www-community/attacks/xss>
- <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>
- [https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)
- <https://www.cisecurity.com/xss-faq.html>
- <https://www.scriptalert1.com/>

## Command Injection

http://127.0.0.1:42001/vulnerabilities/exec/# 80%

li Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

**DVWA**

Home  
Instructions  
Setup / Reset DB  
Brute Force  
**Command Injection**  
CSRF  
File Inclusion  
File Upload  
Insecure CAPTCHA  
SQL Injection  
SQL Injection (Blind)  
Weak Session IDs  
XSS (DOM)  
XSS (Reflected)  
XSS (Stored)  
CSP Bypass

### Vulnerability: Command Injection

Ping a device

Enter an IP address: 127.0.0.1; whoami

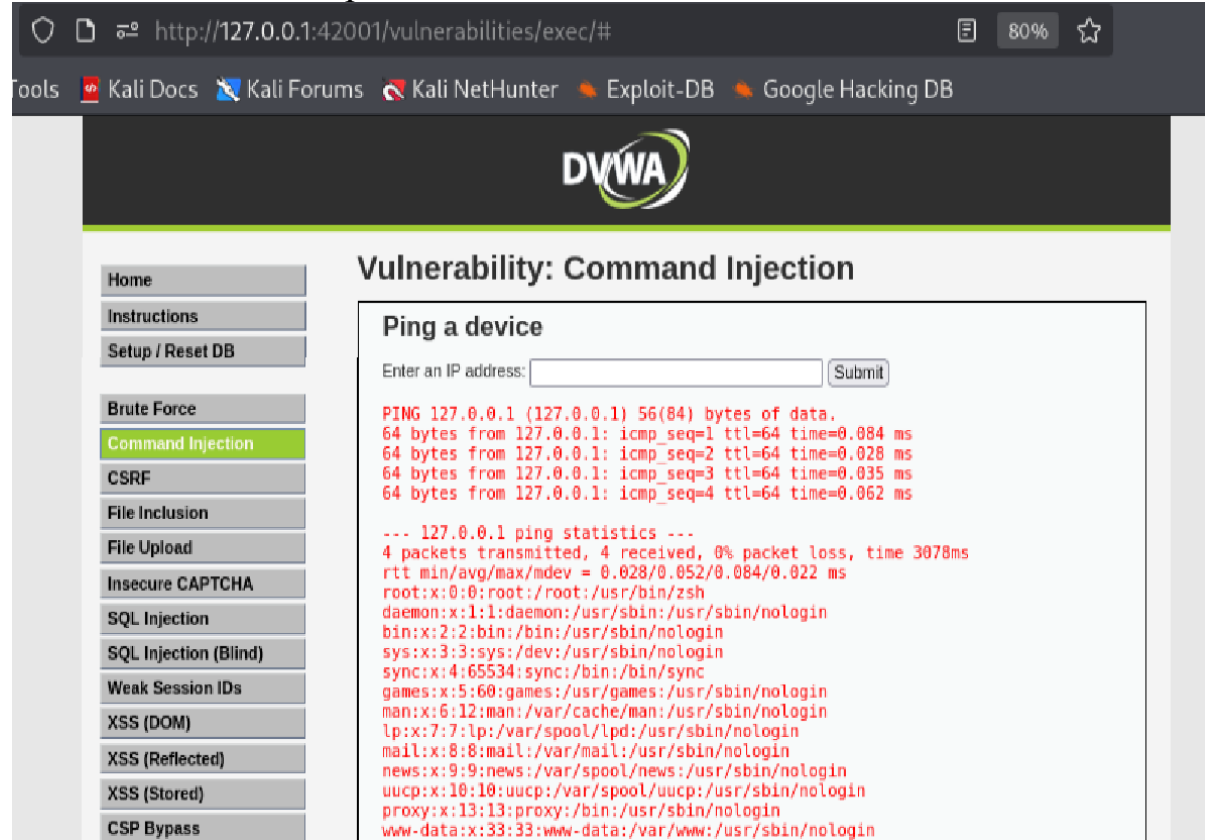
```
PING 127.0.0.1: 127.0.0.1: whoami
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.605 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.037 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.032 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.038 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3025ms
rtt min/avg/max/mdev = 0.032/0.178/0.605/0.246 ms
_dvwa
```

#### More Information

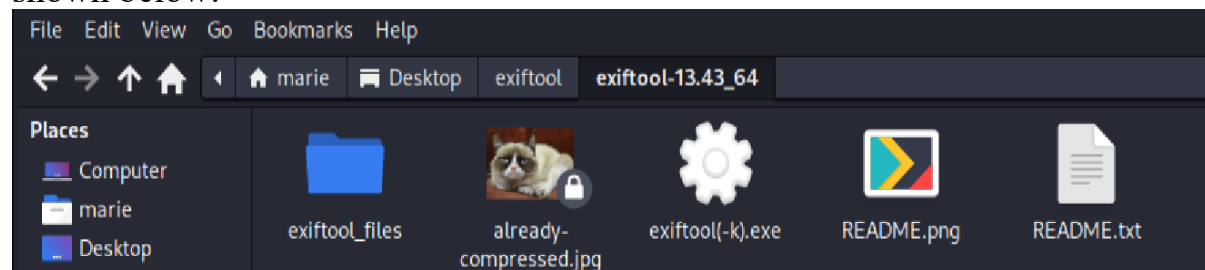
- <https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/ht/>
- [https://owasp.org/www-community/attacks/Command\\_injection](https://owasp.org/www-community/attacks/Command_injection)

127.0.0.1 && cat /etc/passwd



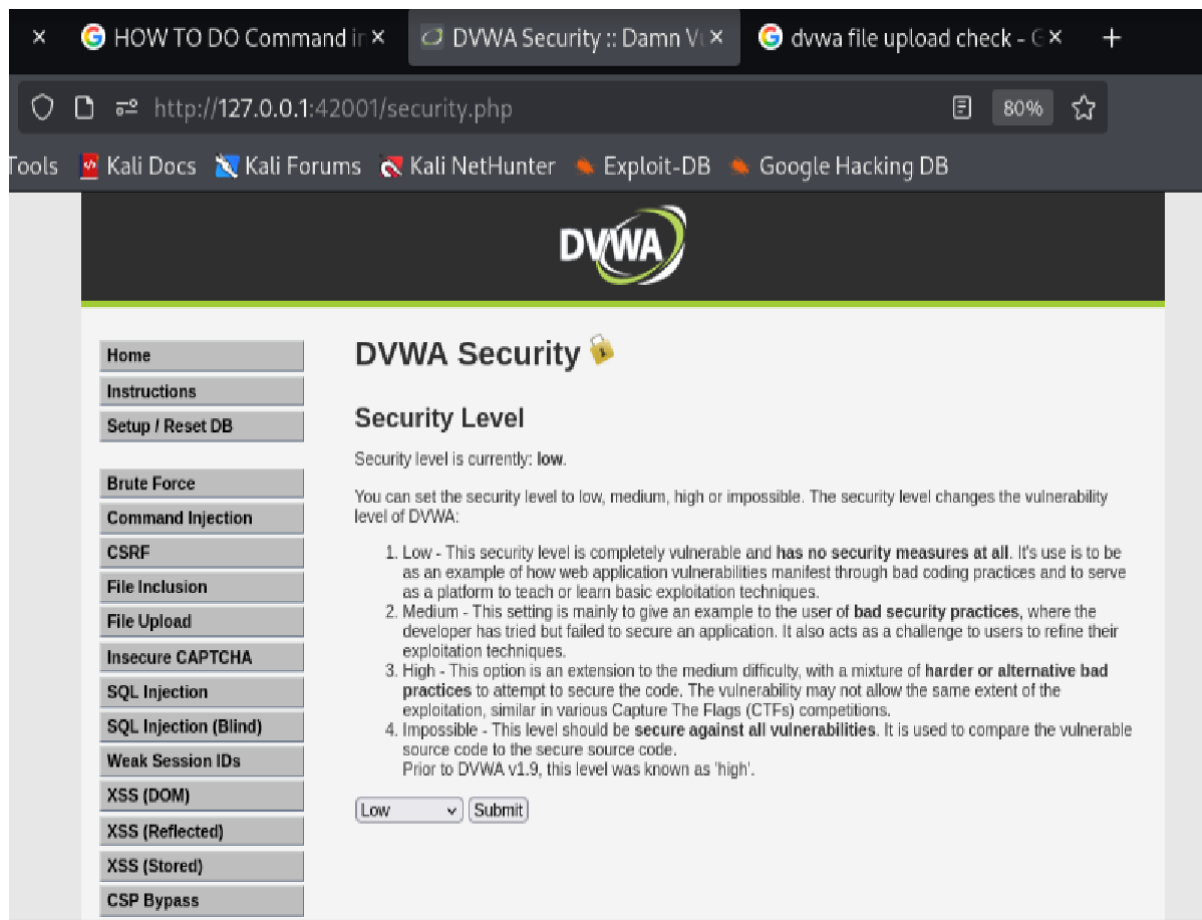
## File Upload / Unrestricted File Upload

Trying to upload a “Readme.txt” file with the extension changed to “.png” as shown below:

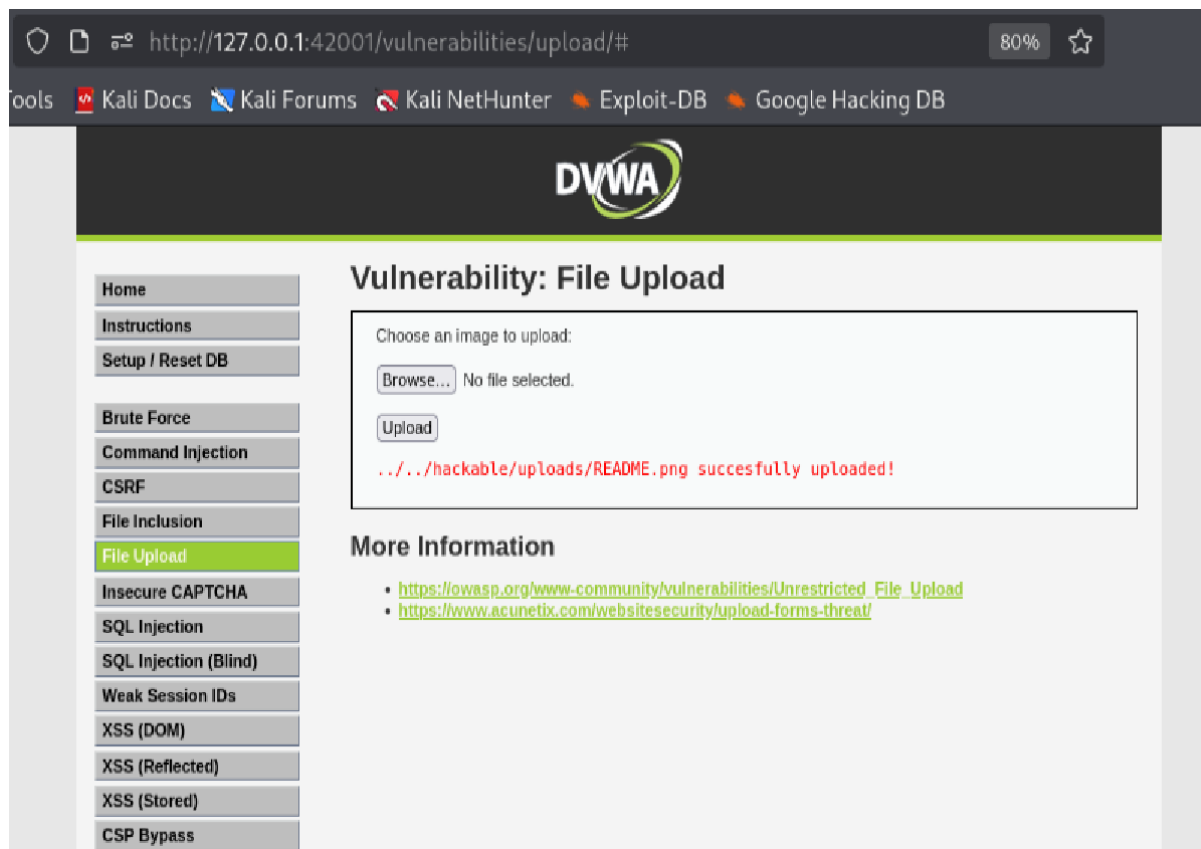


Setting the security level to “Low”





The file is accepted and uploaded as shown below though it is not originally a .png file:



The same observation is made for “Medium” level too. Setting the security level above “Medium” i.e, to “Impossible” or “High” to check if the vulnerability will be detected or not for the falsely created “Readme.png” file:

🔒

📄

🌐

http://127.0.0.1:42001/security.php

📄

80%

☆

🔧 tools


Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

## DVWA Security

### Security Level

Security level is currently: **low**.

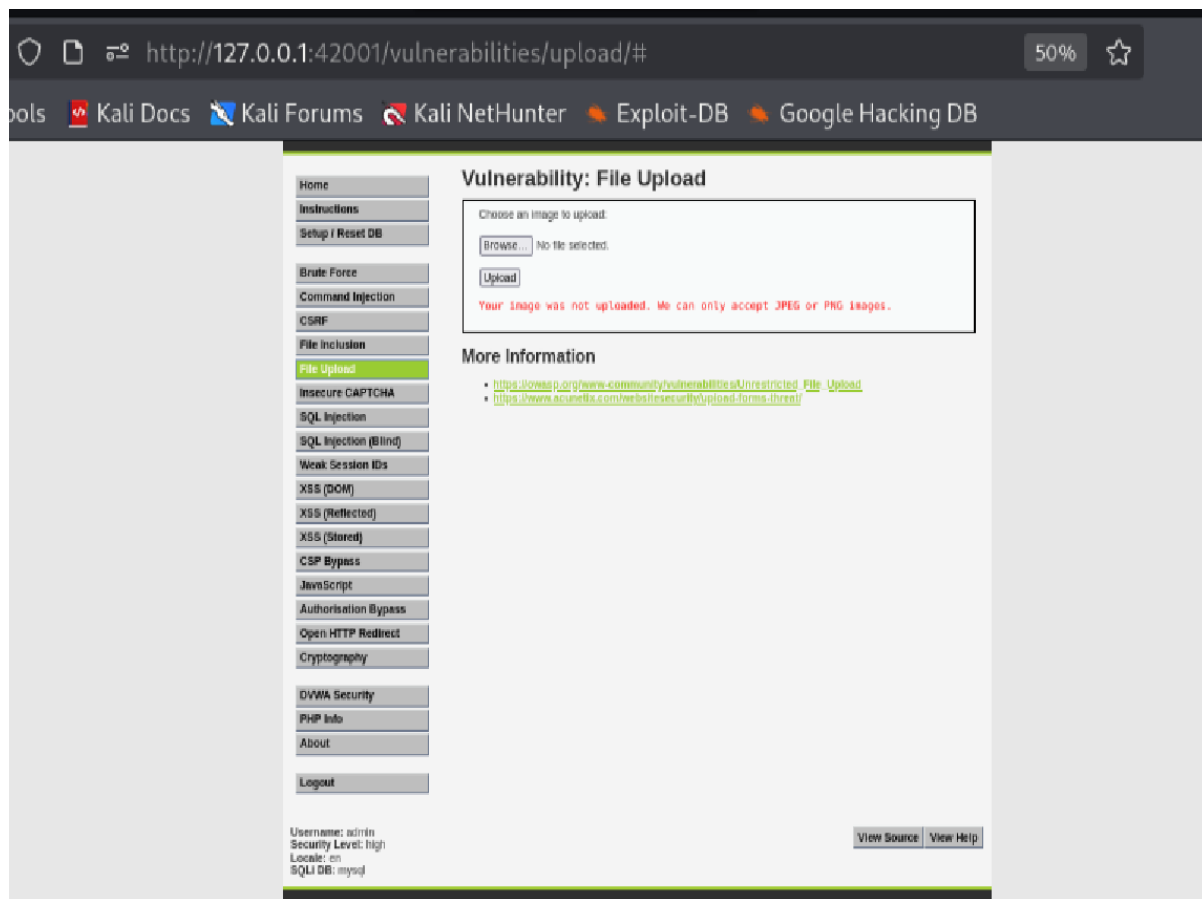
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.  
Prior to DVWA v1.9, this level was known as 'high'.

Medium

▼

Submit



## Security Misconfigurations / Insecure headers

```
(marie@math)-[/home/marie]
PS> curl -I http://127.0.0.1:42001/
HTTP/1.1 302 Found
Server: nginx/1.28.0
Date: Sat, 20 Dec 2025 22:36:16 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Set-Cookie: security=impossible; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=5b9f6546e1e7993e399fe361b3fbd4dc; expires=Sun, 21 Dec 2025 22:36:16 GMT; Max-Age=86400; path=/; domain=127.0.0.1; HttpOnly; SameSite=Strict
Location: login.php
```

## Step 4: Light automation

### Run Nikto for quick server Misconfigurations

```
(marie@math)-[/home/marie]
PS> nikto -h http://127.0.0.1:42001/
- Nikto v2.5.0

+ Target IP:      127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port:    42001
+ Start Time:     2025-12-20 17:39:24 (GMT-5)

+ Server: nginx/1.28.0
+ /: 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/
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /login.php: Admin login page/section found.
+ 8074 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:      2025-12-20 17:39:34 (GMT-5) (10 seconds)

+ 1 host(s) tested
```

### Run whatweb for Fingerprinting

```
(marie@math)-[/home/marie]
PS> whatweb http://127.0.0.1:42001/
http://127.0.0.1:42001/ [302 Found] Cookies[PHPSESSID,security], Country[RESERVED][22], HTTPServer[nginx/1.28.0], HttpOnly[PHPSESSID,security], IP[127.0.0.1], RedirectLocation[login.php], nginx[1.28.0]
http://127.0.0.1:42001/login.php [200 OK] Country[RESERVED][22], DVWA, HTML5, HTTPServer[nginx/1.28.0], IP[127.0.0.1], PHP, PasswordField[password], Title[Login]
ogin :: Damn Vulnerable Web Application (DVWA)], nginx[1.28.0]
```

### Run Dirb or any other Content Discovery tool

```
(marie@math)-[/home/marie]
PS> dirb http://127.0.0.1:42001/

DIRB v2.22
By The Dark Raver

START_TIME: Sat Dec 20 17:42:45 2025
URL_BASE: http://127.0.0.1:42001/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

— Scanning URL: http://127.0.0.1:42001/ —
=> DIRECTORY: http://127.0.0.1:42001/config/
=> DIRECTORY: http://127.0.0.1:42001/database/
=> DIRECTORY: http://127.0.0.1:42001/docs/
=> DIRECTORY: http://127.0.0.1:42001/external/
+ http://127.0.0.1:42001/favicon.ico (CODE:200|SIZE:1406)
+ http://127.0.0.1:42001/index.php (CODE:302|SIZE:0)
+ http://127.0.0.1:42001/php.ini (CODE:200|SIZE:154)
+ http://127.0.0.1:42001/phpinfo.php (CODE:302|SIZE:0)
+ http://127.0.0.1:42001/robots.txt (CODE:200|SIZE:25)

— Entering directory: http://127.0.0.1:42001/config/ ---
— Entering directory: http://127.0.0.1:42001/database/ —
```

```
— Entering directory: http://127.0.0.1:42001/docs/ —  
+ http://127.0.0.1:42001/docs/copyright (CODE:200|SIZE:1085)  
⇒ DIRECTORY: http://127.0.0.1:42001/docs/graphics/  
  
— Entering directory: http://127.0.0.1:42001/external/ —  
  
— Entering directory: http://127.0.0.1:42001/docs/graphics/ —  
  
END_TIME: Sat Dec 20 17:42:50 2025  
DOWNLOADED: 27672 - FOUND: 6
```

## Run nuclei

```
(marie@math)-[/home/marie]  
PS> nuclei -u http://127.0.0.1:42001/  
  
nuclei v3.4.10  
projectdiscovery.io  
  
[WRN] Found 1 templates with syntax error (use -validate flag for further examination)  
[INF] Current nuclei version: v3.4.10 (outdated)  
[INF] Current nuclei-templates version: v10.3.5 (latest)  
[INF] New templates added in latest release: 57  
[INF] Templates loaded for current scan: 8910  
[INF] Executing 8908 signed templates from projectdiscovery/nuclei-templates  
[WRN] Loading 2 unsigned templates for scan. Use with caution.  
[INF] Targets loaded for current scan: 1  
[INF] Templates clustered: 1862 (Reduced 1749 Requests)  
[dvwa-default-login] [http] [critical] http://127.0.0.1:42001/index.php [password="password",username="admin"]  
[cookies-without-secure] [javascript] [info] 127.0.0.1:42001 ["security","PHPSESSID"]  
[waf-detect:nginxgeneric] [http] [info] http://127.0.0.1:42001/  
[INF] Scan completed in 1m. 3 matches found.
```