



File Actions Edit View

```
(root@kali)-[~]  
# service mysql start
```

```
(root@kali)-[~]  
# service apache2 start
```

```
(root@kali)-[~]  
#
```



Search...



root@kali: ~



Filter

High

Medium

Low

Info

Certain

Firm

Tentative

In Scope



Help

Issue type

Host

Path

ⓘ Suspicious input transformation (reflected)	http://insecure-bank.com	/url-shorten
🔴 SMTP header injection	http://insecure-website.c...	/contact-us
🔴 Serialized object in HTTP message	http://insecure-bank.com	/blog
🔴 Cross-site scripting (DOM-based)	https://insecure-bank.com	/
🔴 XML external entity injection	https://vulnerable-websit...	/product/stock
🔴 External service interaction (HTTP)	https://insecure-website....	/product
🔴 Web cache poisoning	http://insecure-bank.com	/contact-us
🔴 Server-side template injection	http://insecure-bank.com	/user-homepage
🔴 SQL injection	https://vulnerable-websit...	/
🔴 OS command injection	https://insecure-website....	/feedback/submit

Advisory

[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](#)[Authorisation Bypass](#)[Open HTTP Redirect](#)[DVWA Security](#)[PHP Info](#)[About](#)[Logout](#)

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'.



Security level set to low

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExtensionsLearn

InterceptHTTP historyWebSockets historyProxy settings

Request to http://127.0.0.1:80

ForwardDropIntercept is onActionOpen browser

PrettyRawHex

1 POST /DVWA/ HTTP/1.1

2 Host: 127.0.0.1

3 Upgrade-Insecure-Requests: 1

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

6 Sec-Fetch-Site: none

7 Sec-Fetch-Mode: navigate

8 Sec-Fetch-User: ?1

9 Sec-Fetch-Dest: document

10 sec-ch-ua:

11 sec-ch-ua-mobile: ?0

12 sec-ch-ua-platform: ""

13 Accept-Encoding: gzip, deflate

14 Accept-Language: en-US,en;q=0.9

15 Cookie: PHPSESSID=tmq7edp0q2tqh1mgmbadmsku

16 Connection: close

17

18

1 x +

Send

Cancel

< ▾

> ▾

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExtensionsLearn

Request

PrettyRawHex

In

1 POST /DVWA/ HTTP/1.1

2 Host: 127.0.0.1

3 Upgrade-Insecure-Requests: 1

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

6 Sec-Fetch-Site: none

7 Sec-Fetch-Mode: navigate

8 Sec-Fetch-User: ?1

9 Sec-Fetch-Dest: document

10 sec-ch-ua:

11 sec-ch-ua-mobile: ?0

12 sec-ch-ua-platform: ""

13 Accept-Encoding: gzip, deflate

14 Accept-Language: en-US,en;q=0.9

15 Cookie: PHPSESSID=tmq7edp0q2tqh1mgmbadmsku

16 Connection: close

17

18

Response

PrettyRawHexRender

In

1 HTTP/1.1 200 OK

2 Date: Thu, 12 Oct 2023 07:48:48 GMT

3 Server: Apache/2.4.57 (Debian)

4 Set-Cookie: security=impossible; path=/; HttpOnly

5 Expires: Tue, 23 Jun 2009 12:00:00 GMT

6 Cache-Control: no-cache, must-revalidate

7 Pragma: no-cache

8 Vary: Accept-Encoding

9 Content-Length: 6016

10 Connection: close

11 Content-Type: text/html; charset=utf-8

12

13 <!DOCTYPE html>

14

15 <html lang="en-GB">

16

17 <head>

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

19

20 <title>

21 Welcome :: Damn Vulnerable Web Application (DVWA)

22 </title>

23

24 <link rel="stylesheet" type="text/css" href="dvwa/css/main.css" />

25

26 <script type="text/javascript" src="dvwa/js/dvwaPage.js">

27 </script>

28

29 </head>

30 <body class="home">

31 <div id="container">

32

33 <div id="header">

34

35

36

37 </div>

38

39

40