

# Credenziali

ApplicationsPlacesFirefox ESR

Dec 6 04:02

🏠🔊🔒

DVWA Security :: Damn V × +

🔍📄🔖🌟📧📁☰

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

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

JavaScript

Authorisation Bypass

Open HTTP Redirect

DVWA Security

PHP Info

About

Logout

DVWA Security🔒

Security Level

Security level is currently: impossible.

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'.

Low

Submit

Username: admin

🔍📄🔖🌟📧📁☰


CTRL (DESTRA)

backdoor1.py

backdoor2.py

Login :: Damn Vulnerable

127.0.0.1/DVWA/login.php



Username

admin

Password

\*\*\*\*\*

Login

You have logged out

[Damn Vulnerable Web Application \(DVWA\)](#)

Dec 6 04:15

## Burp Suite Community Edition v2023.9.1 - Temporary Project

Intercept HTTPHistory WebSockets history Proxy settings

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action Open browser

Comment this item HTTP/1

Pretty Raw Hex

```
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 88
4 Cache-Control: max-age=0
5 sec-ch-ua:
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: ""
8 Upgrade-Insecure-Requests: 1
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 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
12 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
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://127.0.0.1/DVWA/login.php
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=7vvu076dcj6qfqf36a0a12c2f1; security=impossible
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=f131c534277dd109d7016bf5a54eef7b
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 4

Request cookies 2

Request headers 20

Search... 0 highlights

# Inserisco credenziali errate

Burp Suite Community Edition v2023.9.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Organizer Settings

1 x 2 x +

Send Cancel < >

Target: http://127.0.0.1 HTTP/1

**Request**

Pretty Raw Hex

```
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 88
4 Cache-Control: max-age=0
5 sec-ch-ua:
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: ""
8 Upgrade-Insecure-Requests: 1
9 Origin: http://127.0.0.1
10 Content-Type:
  application/x-www-form-urlencoded
11 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
12 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
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://127.0.0.1/DVWA/login.php
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=7vvu076dcj6qfqf36a0a12c2f1
  ; security-impossible
21 Connection: close
22
23 username=kali&password=kali&login=Login&
  user_token=adb1babb8b7fe9e524f83f8e419553c1
```

**Response**

Pretty Raw Hex Render

**Inspector**

Request attributes 2

Request query parameters 0

Request body parameters 4

Request cookies 2

Request headers 20

Search... 0 highlights

Ready

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings

Extensions Learn

1 x 2 x +

🔍 ?

Send Cancel &lt; &gt;

Target: http://127.0.0.1 HTTP/1 ?

## Request

Pretty Raw Hex

🔍 ln ≡

```
1 GET /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Cache-Control: max-age=0
4 sec-ch-ua:
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: ""
7 Upgrade-Insecure-Requests: 1
8 Origin: http://127.0.0.1
9 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
10 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
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: http://127.0.0.1/DVWA/login.php
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: PHPSESSID=7vvu076dcj6qfqf36a0a12c2f1
; security=impossible
19 Connection: close
20
21
```

## Response

Pretty Raw Hex Render

🔍 ln ≡

```

50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
size="20" name="password">
<br />
<br />
<p class="submit">
  <input type="submit" value="
  Login" name="Login">
</p>
</fieldset>
<input type="hidden" name="
user_token" value="
e628697b46c98a5c654e83507c483dcb"
/>
</form>
<br />
<div class="message">
  Login failed
</div>
<br />
<br />
<br />
<br />
<br />
<br />
<br />
</div>
<!--<div id="content">-->
<div id="footer">
```

## Inspector

🔍 ≡ ⚙️ ✕

Request attributes 2 ▾

Request query parameters 0 ▾

Request body parameters 0 ▾

Request cookies 2 ▾

Request headers 18 ▾

Response headers 9 ▾

🔍 ⚙️ ⬅️ ➡️ Search... 0 highlights

🔍 ⚙️ ⬅️ ➡️ Search... 0 highlights