

Lavoro Corsi Night ride - playlist by Alex01 Accesso come utente "root" grant all privileges on dvwa.\* to 'root' x

https://open.spotify.com/playlist/6oPegNCaXSp4KLOJIT0uww?si=RARtjcSIQO2eLo6hqvWL6q&utm\_source=whatsapp&nd=1

kali-linux-2013.3-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Auto

DVWA Security :: Damn Vulnerable Web Application

127.0.0.1/DVWA/security.php

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

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

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'.

Low Submit

Security level set to low

Installa app

ride

Aggiunto il giorno

MS 1 giorno fa 1:49

23°C Parzial. sereno 15:49 11/10/2023

kali-linux-2023.3-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto



Burp Suite Community Edition v2023.9.1 - Temporary Project

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

Intercept HTTP history 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: ?
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: security-impossible; PHPSESSID=gttgfga7bh1uh1sq9614125uv
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=ceeb710b430c758abd9fa3f21fbc3d3b
```

Inspector

- Request attributes 2
- Request query parameters 0
- Request body parameters 4
- Request cookies 2
- Request headers ...

Oracle VM VirtualBox Guest Tools

File Macchina Aiuto

23°C Soleggiato 16:16 11/10/2023

127.0.0.1

2

+

SendCancel<>

Target: http://127.0.0.1HTTP/1.1

Request

Raw

Hex

VI

1GET /DVWA/login.php HTTP/1.1

2Host: 127.0.0.1

3Cache-Control: max-age=0

4sec-ch-ua:

5sec-ch-ua-mobile: ?0

6sec-ch-ua-platform: ""

7Upgrade-Insecure-Requests: 1

8Origin: http://127.0.0.1

9User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36

10Accept: 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

11Sec-Fetch-Site: same-origin

12Sec-Fetch-Mode: navigate

13Sec-Fetch-User: ?1

14Sec-Fetch-Dest: document

15Referer: http://127.0.0.1/DVWA/login.php

16Accept-Encoding: gzip, deflate

17Accept-Language: en-US,en;q=0.9

18Cookie: security-impossible; PHPSESSID=h545z8pprup1298jjmbelt1e2p

19Connection: close

20

21

Response

Raw

Hex

Render

VI

4Expires: Tue, 23 Jun 2020 12:00:00 GMT

5Cache-Control: no-cache, must-revalidate

6Pragma: no-cache

7Vary: Accept-Encoding

8Content-Length: 1434

9Connection: close

10Content-Type: text/html; charset=utf-8

11

12<!DOCTYPE html>

13

14<html lang="en-GB">

15

16<head>

17

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

19

20<title>Login :: Damn Vulnerable Web Application (DVWA)</title>

21

22<link rel="stylesheet" type="text/css" href="dvwa/css/login.css" />

23

24</head>

25

26<body>

27

28<div id="wrapper">

29

30<div id="header">

31

32<br />

33

Request attributes2

Request query parameters0

Request body parameters0

Request cookies2

Request headers18

Response headers9

0 highlights

0 highlights

Work environment showing a Kali Linux virtual machine running Burp Suite Community Edition v2023.9.1. The interface displays a request to http://127.0.0.1:80, with the 'Intercept' tab selected. The request details are visible in the 'Inspector' panel, showing headers and body parameters. The body parameters include 'username=admin&password=password&Login=Login&user\_token=74387a70e3953642e77d566f189ab4e'. The 'Forward' button is highlighted.

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action Open browser Comment this item HTTP/1.1

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 4

Request cookies 2

Request headers 20

0 highlights

Work environment showing a web application interface. The page title is 'Esercizio Web App'. The page content is partially visible, showing a 'password standard' field. The page number '6' is visible at the bottom right.

Esercizio Web App

password standard

6

Workstation interface showing a Kali Linux virtual machine running Burp Suite Community Edition v2023.9.1. The interface displays a network request and response for the target `http://127.0.0.1`.

**Request:**

```
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;
10 AppleWebKit/537.36 (KHTML, like Gecko)
11 Chrome/115.0.5790.171 Safari/537.36
12 Accept:
13 text/html,application/xhtml+xml,application/xml;q=0
14 .9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
15 cation/signed-exchange;v=0.3;q=0.7
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: navigate
18 Sec-Fetch-User: ?1
19 Sec-Fetch-Dest: document
20 Referer: http://127.0.0.1/DVWA/login.php
```

**Response:**

```
19 <head>
20
21 <meta http-equiv="Content-Type" content="
22 text/html, charset=UTF-8" />
23
24 <title>
25 Login :: Damn Vulnerable Web Application
26 (DVWA)
27 </title>
28
29 <link rel="stylesheet" type="text/css" href="
30 dvwa/css/login.css" />
31
32 </head>
33
34 <body>
35
36 <div id="wrapper">
37
38 <div id="header">
```

**Inspector:**

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 2
- Request headers: 18
- Response headers: 9

Done 1,764 bytes | 0 millis

Web application interface titled "Esercizio Web App". The page displays the text "password standard".

2023-10-11 (3).png

22°C Soleggiato

16:41 11/10/2023



