

Esercizio S3/L2

```
(root@kali)-[/home/kali]
# history
1  s
2  sudo -a
3  exit
4  apt-get update
5  apt install gettext man-db procps nano tree bsdmainutils x11-apps wget
6  wget https://github.com/phyver/GameShell/releases/download/latest/gameshell.sh
7  bash gameshell.sh
8  sudo -a
9  sudo -s
10 kill
11 cd /var/www/html
12 git clone https://github.com/digininja/DVWA
13 chmod -R 777 DVWA/
14 chmod -R 777 DVWA
15 cd DVWA/config
16 cp config.inc.php.dist config.inc.php
17 nano config.inc.php
18 service mysql start
19 mysql -u root -p
20 mysql -u root -p
21 cd /etc/php
22 ls
23 cd /etc/php/8.2/apache2
24 nano php.ini
25 service apache2 start

(root@kali)-[/home/kali]
#
```

Kali-Linux [in esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Auto

DVWA Security :: Damn V X

127.0.0.1/DVWA/security.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec DVWA Security :: Dam...

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'.

Impossible

Submit

Username: admin

Security Level: impossible

https://www.kali.org

CTRL (DESTRA)

Burp Project Intruder Repeater View Help

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

 Intercept HTTP history WebSockets history Proxy settings

 Request to http://127.0.0.1:80

 Forward Drop Intercept is on Action Open browser

 Pretty Raw Hex

 1 POST /DWA/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: "Chromium";v="119", "Not?A_Brand";v="24"

 6 sec-ch-ua-mobile: 0

 7 sec-ch-ua-platform: "Linux"

 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/119.0.6045.159 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/DWA/login.php

 18 Accept-Encoding: gzip, deflate, br

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

 20 Cookie: security=impossible; PHPSESSID=ogcb0iqik6coe9q49f5bcs8rg

 21 Connection: close

 22

 23 username=credenzial&password=sbagliate&Login=Login&user_token=34c28db753cb5acc0c2a91778d001da4

 Inspector

 Request attributes 2

 Request query parameters 0

 Request body parameters 4

 Request cookies 2

 Request headers 20

Burp Project Intruder Repeater View Help

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

 10 x +

 Send Cancel < > Follow redirection

 Target: http://127.0.0.1 HTTP/1

 Request

 Pretty Raw Hex

 1 POST /DWA/login.php HTTP/1.1

 2 Host: 127.0.0.1

 3 Content-Length: 95

 4 Cache-Control: max-age=0

 5 sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"

 6 sec-ch-ua-mobile: 0

 7 sec-ch-ua-platform: "Linux"

 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/119.0.6045.159 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/DWA/login.php

 18 Accept-Encoding: gzip, deflate, br

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

 20 Cookie: security=impossible; PHPSESSID=ogcb0iqik6coe9q49f5bcs8rg

 21 Connection: close

 22

 23 username=credenzial&password=sbagliate&Login=Login&user_token=34c28db753cb5acc0c2a91778d001da4

 Response

 Pretty Raw Hex Render

 1 HTTP/1.1 302 Found

 2 Date: Tue, 06 Feb 2024 15:53:36 GMT

 3 Server: Apache/2.4.58 (Debian)

 4 Expires: Thu, 19 Nov 1981 08:52:00 GMT

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

 6 Pragma: no-cache

 7 Set-Cookie: PHPSESSID=a754a74073cecbjne35oe21ge; expires=Wed, 07 Feb 2024 15:53:36 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict

 8 Location: login.php

 9 Content-Length: 0

 10 Connection: close

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

 12

 13

 Inspector

 Request attributes 2

 Request query parameters 0

 Request body parameters 4

 Request cookies 2

 Request headers 20

 Response headers 10

Burp Project Intruder Repeater View Help

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

 10 x +

 Send Cancel < >

 Target: http://127.0.0.1 HTTP/1

 Request

 Pretty Raw Hex

 1 GET /DWA/login.php HTTP/1.1

 2 Host: 127.0.0.1

 3 Cache-Control: max-age=0

 4 sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"

 5 sec-ch-ua-mobile: 0

 6 sec-ch-ua-platform: "Linux"

 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/119.0.6045.159 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/DWA/login.php

 16 Accept-Encoding: gzip, deflate, br

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

 18 Cookie: security=impossible; PHPSESSID=ogcb0iqik6coe9q49f5bcs8rg

 19 Connection: close

 20

 21

 Response

 Pretty Raw Hex Render

 1 HTTP/1.1 200 OK

 2 Date: Tue, 06 Feb 2024 15:55:07 GMT

 3 Server: Apache/2.4.58 (Debian)

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

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

 6 Pragma: no-cache

 7 Vary: Accept-Encoding

 8 Content-Length: 1342

 9 Connection: close

 10 Content-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>

 21 Login :: Damn Vulnerable Web Application (DVWA)

 22 </title>

 23

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

 25

 26 </head>

 27

 28 <body>

 29

 30 <div id="wrapper">

 31

 32 <div id="header">

 33

 34

 35

 36

 37

 38 </div>

 39 <!--div id="header"-->

 40

 41 <div id="content">

 42

 43 <form action="login.php" method="post">

Done

 1,633 bytes | 36 millis

Come si può notare dalle immagini, sul nostro sistema Kali, siamo riusciti ad installare una DVWA (Damn Vulnerable Web App). Fatto ciò abbiamo utilizzato Burp come server proxy per poter andare ad analizzare il pacchetto e modificarlo inviandolo tramite la sezione Repeater con le credenziali sbagliate.