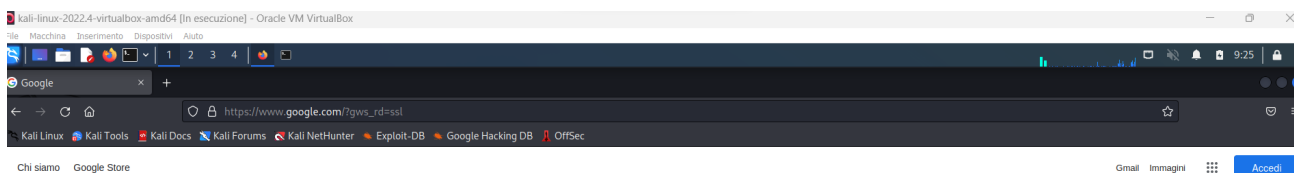


Configurazione DVWA in Kali Linux

Dopo aver modificato le impostazioni della scheda di rete (da internal a Bridged) e dopo aver selezionato da terminale "sudo nano /etc/network/interfaces", per modificare l'indirizzo statico con quello dinamico, la macchina Kali Linux ha accesso a internet.



Dopo aver inserito su terminale le istruzioni forniteci nell'esercizio nell'editor di testo, modifico user e password inserendo "kali" in entrambi gli sheet.

```
GNU nano 6.4
?php
If you are having problems connecting to the MySQL database and all of the variables below are con
try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
Thanks to @digininja for the fix.

Database management system to use
DBMS = 'MySQL';
$DBMS = 'PGSQL'; // Currently disabled

Database variables
WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
Please use a database dedicated to DVWA.

If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
See README.md for more information on this.
_DVWA = array();
_DVWA[ 'db_server' ] = '127.0.0.1';
_DVWA[ 'db_database' ] = 'dvwa';
_DVWA[ 'db_user' ] = 'kali';
_DVWA[ 'db_password' ] = 'kali';
_DVWA[ 'db_port' ] = '3306';

ReCAPTCHA settings
Used for the 'Insecure CAPTCHA' module
You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
_DVWA[ 'recaptcha_public_key' ] = '';
_DVWA[ 'recaptcha_private_key' ] = '';

Default security level
Default value for the security level with each session.
The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or impos
_DVWA[ 'default_security_level' ] = 'impossible';

Default PHPIDS status
PHPIDS status with each session.
The default is 'disabled'. You can set this to be either 'enabled' or 'disabled'.
_DVWA[ 'default_phpids_level' ] = 'disabled';

Verbose PHPIDS messages
Enabling this will show why the WAF blocked the request on the blocked request.
The default is 'disabled'. You can set this to be either 'true' or 'false'.
_DVWA[ 'default_phpids_verbose' ] = 'false';
```

Creare un'utenza sul DB e assegnare i privilegi all'utente kali, usando mysql, nel modo seguente:

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

(root@kali)-[~]
# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.6.10-MariaDB-1+b1 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create user 'kali'@'127.0.0.1' identified by 'kali' ;
Query OK, 0 rows affected (0.023 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ;
Query OK, 0 rows affected (0.005 sec)

MariaDB [(none)]> exit
Bye
```

A questo punto, procedo a configurare apache. Dopo essermi accertato che la versione presente su kali sia 8.1 apro la cartella php.ini su nano e configuro "allow_url_include" su ON.

```
(root@kali)-[/etc/php/8.1/apache2]
# cd /etc/php/

(root@kali)-[/etc/php]
# ls
8.1

(root@kali)-[/etc/php]
# nano php.ini

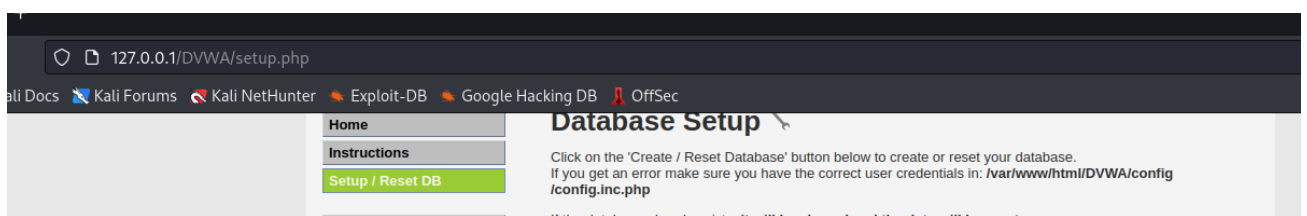
(root@kali)-[/etc/php]
# cd /etc/php/8.1/apache2

(root@kali)-[/etc/php/8.1/apache2]
# nano php.ini

(root@kali)-[/etc/php/8.1/apache2]
# service apache2 start

(root@kali)-[/etc/php/8.1/apache2]
#
```

Andando sul browser ed inserendo "127.0.0.1/DVWA/setup.php" nella barra degli indirizzi, mi si aprirà una schermata, da cui potrò creare/resettare un database.



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

DVWA Security

PHP Info

About

Logout

You can also use this to reset the administrator credentials ("admin // password") at any stage.

Setup Check

Web Server SERVER_NAME: 127.0.0.1

Operating system: *nix

PHP version: 8.1.12

PHP function display_errors: Disabled

PHP function safe_mode: Disabled

PHP function allow_url_include: Disabled

PHP function allow_url_fopen: Enabled

PHP function magic_quotes_gpc: Disabled

PHP module gd: Missing - Only an issue if you want to play with captchas

PHP module mysql: Installed

PHP module pdo_mysql: Installed

Backend database: MySQL/MariaDB

Database username: kali

Database password: *****

Database database: dvwa

Database host: 127.0.0.1

Database port: 3306

reCAPTCHA key: Missing

[User: root] Writable folder /var/www/html/DVWA/hackable/uploads/: Yes

[User: root] Writable file /var/www/html/DVWA/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt: Yes

[User: root] Writable folder /var/www/html/DVWA/config: Yes

Status in red, indicate there will be an issue when trying to complete some modules.

If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.

allow_url_fopen = On

allow_url_include = On

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Create / Reset Database

Seleziono DVWA Security dove posso impostare il livello di sicurezza

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

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 level of DVWA:

1. Low - This security level is completely vulnerable and has no security measures at all. as an example of how web application vulnerabilities manifest through bad coding practices 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 practice: developer has tried but failed to secure an application. It also acts as a challenge to user exploitation techniques.

3. High - This option is an extension to the medium difficulty, with a mixture of harder or all practices to attempt to secure the code. The vulnerability may not allow the same extent exploitation, similar in various Capture The Flags (CTFs) competitions.

4. Impossible - This level should be secure against all vulnerabilities. It is used to compare source code to the secure source code.

Prior to DVWA v1.9, this level was known as 'high'.

Impossible

Submit

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: disabled. [\[Enable PHPIDS\]](#)

Lancio Burpsuite e provo a cambiare le credenziali (che non ci sono)

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerLoggerExtenderProject optionsUser options

InterceptHTTP historyWebSockets historyOptions

Request to http://127.0.0.1:80

ForwardDropIntercept is onActionOpen Browser

PrettyRawHex

1 GET /DVWA HTTP/1.1

2 Host: 127.0.0.1

3 sec-ch-ua: "Chromium";v="107", "Not=A?Brand";v="24"

4 sec-ch-ua-mobile: ?0

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

6 Upgrade-Insecure-Requests: 1

7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36

8 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=0.9

9 Sec-Fetch-Site: none

10 Sec-Fetch-Mode: navigate

11 Sec-Fetch-User: ?1

12 Sec-Fetch-Dest: document

13 Accept-Encoding: gzip, deflate

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

15 Connection: close

16

17 username=ciao&password=ciao&Login=Login&user_token=b9a2cb60b22830f3abf0336e768eb

Clicco su Send

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerLoggerExtenderProject optionsUser optionsLearn

1 x2 x3 x+

SendCancelFollow redirection

Target

Request

PrettyRawHex

1 GET /DVWA HTTP/1.1

2 Host: 127.0.0.1

3 sec-ch-ua: "Chromium";v="107", "Not=A?Brand";v="24"

4 sec-ch-ua-mobile: ?0

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

6 Upgrade-Insecure-Requests: 1

7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36

8 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=0.9

9 Sec-Fetch-Site: none

10 Sec-Fetch-Mode: navigate

11 Sec-Fetch-User: ?1

12 Sec-Fetch-Dest: document

13 Accept-Encoding: gzip, deflate

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

15 Connection: close

16 Content-Length: 80

17

18 username=ciao&password=ciao&Login=Login&user_token=b9a2cb60b22830f3abf0336e768eb

Response

PrettyRawHexRender

1 HTTP/1.1 301 Moved Permanently

2 Date: Wed, 08 Feb 2023 15:57:58 GMT

3 Server: Apache/2.4.54 (Debian)

4 Location: http://127.0.0.1/DVWA/

5 Content-Length: 305

6 Connection: close

7 Content-Type: text/html; charset=iso-8859-1

8

9 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">

10 <html>

11 <head>

12 <title>

13 301 Moved Permanently

14 </title>

15 </head>

16 <body>

17 <h1>

18 Moved Permanently

19 </h1>

20 <p>

21 The document has moved <http://127.0.0.1/DVWA/>

22 here

23

24 </p>

25 <hr>

26 <address>

27 Apache/2.4.54 (Debian) Server at 127.0.0.1 Port 80

28 </address>

29 </body>

30 </html>

E poi su Follow Redirection

Response		Inspect
f,i ;q=	<div>PrettyRawHexRender</div> <div>1 HTTP/1.1 200 OK 2 Date: Wed, 08 Feb 2023 15:58:13 GMT 3 Server: Apache/2.4.54 (Debian) 4 Set-Cookie: security=impossible; path=/; HttpOnly 5 Set-Cookie: PHPSESSID=10c10gfm4s8levhjqlu6q9od3t; expires=Thu, 09-Feb-2023 15:58:13 GMT; Max-Age=86400; path=/; domain=127.0.0.1; HttpOnly; SameSite=1 6 Expires: Tue, 23 Jun 2009 12:00:00 GMT 7 Cache-Control: no-cache, must-revalidate 8 Pragma: no-cache 9 Vary: Accept-Encoding 10 Content-Length: 6331 11 Connection: close 12 Content-Type: text/html; charset=utf-8 13 14 <!DOCTYPE html> 15 16 <html lang="en-GB"> 17 18 <head> 19 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /> 20 21 <title> 22 Welcome :: Damn Vulnerable Web Application (DVWA) v1.10 23 *Development* 24 </title> 25 26 <link rel="stylesheet" type="text/css" href="dvwa/css/main.css" /> 27 28 <link rel="icon" type="image/ico" href="favicon.ico" /> 29 30 <script type="text/javascript" src="dvwa/js/dvwaPage.js"> 31 </script> 32 33 </head> 34 35 <body class="home"> 36 <div id="container"> 37 38 <div id="header"> 39 40 41 42 </div> 43 44 </div> 45 46 </body> 47 </html></div>	Request Request Request Request Request Response

Riesco ad entrare perchè non ho impostato alcun login.