

Esercizio Epicode 09.10.2023

Web Application - preparazione ambiente

```
(kali@kali)-[~]
└─$ sudo su
[sudo] password di kali:
(root@kali)-[/home/kali]
└─# cd /var/www/html

(root@kali)-[/var/www/html]
└─# git clone https://github.com/digininja/DVWA
Clone in 'DVWA' in corso ...
remote: Enumerating objects: 4112, done.
remote: Counting objects: 100% (126/126), done.
remote: Compressing objects: 100% (71/71), done.
remote: Total 4112 (delta 62), reused 114 (delta 54), pack-reused 3986
Ricezione degli oggetti: 100% (4112/4112), 1.85 MiB | 6.20 MiB/s, fatto.
Risoluzione dei delta: 100% (1929/1929), fatto.
```

```
(root@kali)-[/var/www/html]
└─# chmod -R 777 DVWA/

(root@kali)-[/var/www/html]
└─# cd DVWA/config

(root@kali)-[/var/www/html/DVWA/config]
└─# cp config.inc.php.dist config.inc.php

(root@kali)-[/var/www/html/DVWA/config]
└─# nano config.inc.php

(root@kali)-[/var/www/html/DVWA/config]
└─# service mysql start

(root@kali)-[/var/www/html/DVWA/config]
└─# mysql -u root -p

(root@kali)-[/var/www/html/DVWA/config]
└─# service apache2 start

(root@kali)-[/var/www/html/DVWA/config]
└─# cd /etc/php

(root@kali)-[/etc/php]
└─# ls
8.1 8.2

(root@kali)-[/etc/php]
└─# cd /etc/php/8.2/apache2

(root@kali)-[/etc/php/8.2/apache2]
└─# nano php.ini

(root@kali)-[/etc/php/8.2/apache2]
└─# sudo nano php.ini

(root@kali)-[/etc/php/8.2/apache2]
└─# service apache2 start

(root@kali)-[/etc/php/8.2/apache2]
└─#
```

Web Server SERVER_NAME: 127.0.0.1

Operating system: *nix

PHP version: 8.1.2

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


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'.

Low  Submit

BurpProjectIntruderRepeaterWindowHelp

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerLoggerExtens

InterceptHTTPHistoryWebSockets historyOptions

 Request to http://127.0.0.1:80

ForwardDropIntercept is onActionOpen Browser


PrettyRawHex

```
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 88
9 Origin: http://127.0.0.1
10 Connection: close
11 Referer: http://127.0.0.1/DVWA/login.php
12 Cookie: PHPSESSID=h9ock3ql2qdutenl37bsutd8jv; security=low
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 username=mariano&password=mariano&Login=Login&user_token=a5d8b4c9740682622b6cd677bbf5b959
```

Burp
 Project
 Intruder
 Repeater
 Window
 Help

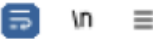
Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder
-----------	--------	-------	----------	----------	-----------	---------

1 ×
 2 ×
 3 ×
 4 ×
 +

Send
 
 Cancel
 < | v
 > | v

Request

Pretty
 Raw
 Hex



```

1 POST /DWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:102.0)
  Gecko/20100101 Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 88
9 Origin: http://127.0.0.1
10 Connection: close
11 Referer: http://127.0.0.1/DWA/login.php
12 Cookie: PHPSESSID=h9ock3ql2qduten137bsutd8jv; security=low
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 username=mariano&password=mariano&Login=Login&user_token=
  a5d8b4c9740682622b6cd677bbf5b959
    
```