

Esercizio S3/L2 di Giorgio Ciaschini del 06/02/2024

Di seguito gli screenshot della configurazione di mysql e dell'utilizzo di BurpSuite dove abbiamo intercettato i pacchetti inviati dal client ai server.

```
GNU nano 7.2      config.inc.php
<?php

# If you are having problems connecting to the>
# try changing the 'db_server' variable from l>
# 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_d>
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use>
# See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ] = getenv( 'DB_SERVER' ) >
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'dvwa';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';
$_DVWA[ 'db_port' ] = '3306';

# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module
# You'll need to generate your own keys at: >
[ Read 56 lines (Converted from DOS format) ]
^G Help      ^O Write Ou^W Where Is^K Cut
^X Exit      ^R Read Fil^_ Replace ^U Paste
```

```
(root@kali)-[/var/www/html/DVWA/config]
```

```
(root@kali)-[/var/www/html/DVWA/config]
```

```
# service mysql start
```

```
(root@kali)-[/var/www/html/DVWA/config]
```

```
# mysql -u root -p
```

Enter password:

Welcome to the MariaDB monitor. Commands end with ; or \g.

Your MariaDB connection id is 31

Server version: 10.11.5-MariaDB-3 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 (0.017 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali';

Query OK, 0 rows affected (0.014 sec)

MariaDB [(none)]> exit


Bye

```
(root@kali)-[/var/www/html/DVWA/config]
```

```
#
```

127.0.0.1/DVWA/security.php

Kali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec



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

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

BurpProjectIntruderRepeaterViewHelp

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderCompar

ExtensionsLearn

3 x4 x+

SendCancel<>Follow redirection

Request

Raw

1 POST /DVWA/login.php HTTP/1.1

2 Host: 127.0.0.1

3 Content-Length: 87

4 Cache-Control: max-age=0

5 sec-ch-ua: "Chromium";v="119",

6 "Not?A_Brand";v="24"

7 sec-ch-ua-mobile: ?0

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

9 Upgrade-Insecure-Requests: 1

10 Origin: http://127.0.0.1

11 Content-Type: application/x-www-form-urlencoded

12 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

13 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

14 Sec-Fetch-Site: same-origin

15 Sec-Fetch-Mode: navigate

16 Sec-Fetch-User: ?1

17 Sec-Fetch-Dest: document

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

19 Accept-Encoding: gzip, deflate, br

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

21 Cookie: security=low; PHPSESSID=ejem8e9c3uk7cs7r3fkhvhu3tl4

22 Connection: close

23 username=errore&password=errore&Login=Login&user_token=bfb815daf9325c4f9071eab396bbbc71

Response

Raw

1 HTTP/1.1 302 Found

2 Date: Tue, 06 Feb 2024 16:49:52 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=f0rqn462ted82nl50s24do4h2k; expires=Wed, 07 Feb 2024 16:49:52 GMT; Max-Age=86400; path=/

8 Location: login.php

9 Content-Length: 0

10 Connection: close

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

12

13

0 highlights

0 highlights