

## ESERCIZIO S3L2

Nell'esercizio di oggi si vedrà come configurare una DVWA (damn vulnerable web application).

Inizialmente si è installato la web application DVWA, un progetto software che include intenzionalmente vulnerabilità di sicurezza, esso ci servirà per proseguire con l'esercizio richiesto. Successivamente si è cambiato nome utente e password nel file "config.inc.php" entrando con il comando "sudo nano config.inc.php" ed inserendo per entrambi 'kali'

```
File Actions Edit View Help
GNU nano 7.2 config.inc.php
<?php

# If you are having problems connecting to the MySQL database and all of
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixe
# 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 DE
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create
# See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ] = getenv('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/recap
$_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'
$_DVWA[ 'default_security_level' ] = 'impossible';
```

Dopo aver configurato le nostre credenziali abbiamo avviato il servizio web **Apache2** e il servizio database **mysql**, utilizzando i permessi di amministratore tramite il comando 'sudo'. **mysql** si è avviato tramite il database MariaDB ed abbiamo creato un'utenza (kali) assegnandogli i privilegi da amministratore:

```
kali@kali: /etc/php/8.2/apache2
File Actions Edit View Help
(kali@kali)-[/var/www/html/DVWA/config]
$ mysql -u root -p
Enter password:
ERROR 1698 (28000): Access denied for user 'root'@'localhost'

(kali@kali)-[/var/www/html/DVWA/config]
$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 10.11.6-MariaDB-2 Debian n/a

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

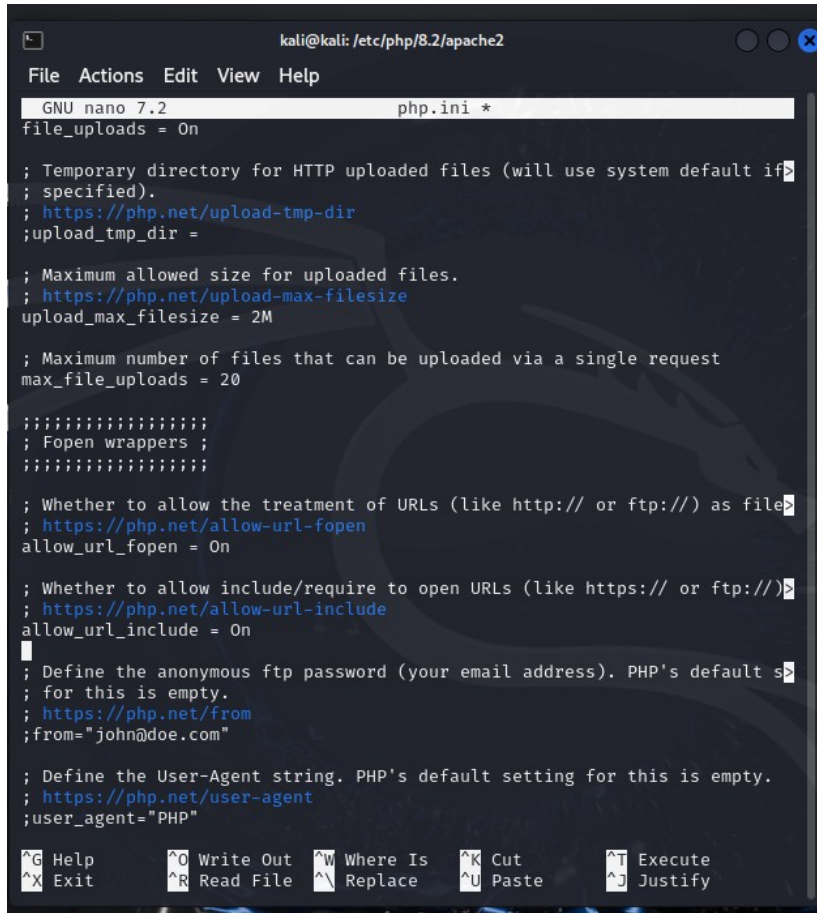
Type 'help;' or '\h' for help. Type '\c' to clear the current input statem
ent.

MariaDB [(none)]> create user 'kali'@'127.0.0.1' identified by 'kali' ;
Query OK, 0 rows affected (0.014 sec)
```

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ;
Query OK, 0 rows affected (0.013 sec)

MariaDB [(none)]> exit
```

Si è effettuata anche la configurazione per il servizio web **apache2**, in particolare si è modificato il file 'php.ini' per consentire la richiesta di aprire gli URLs.

A screenshot of a terminal window on a Kali Linux system. The window title is 'kali@kali: /etc/php/8.2/apache2'. The terminal shows the nano text editor editing the 'php.ini' file. The editor's menu bar includes 'File', 'Actions', 'Edit', 'View', and 'Help'. The status bar at the bottom shows various keyboard shortcuts like '^G Help', '^X Exit', '^O Write Out', '^R Read File', '^W Where Is', '^N Replace', '^K Cut', '^U Paste', '^T Execute', and '^J Justify'. The visible code in the file includes settings for file uploads, temporary directories, maximum file size (2M), maximum number of files (20), and URL handling options like 'allow\_url\_fopen' and 'allow\_url\_include', all currently set to 'On'. There are also comments about the anonymous ftp password and the User-Agent string.

```
kali@kali: /etc/php/8.2/apache2
File Actions Edit View Help
GNU nano 7.2 php.ini *
file_uploads = On

; Temporary directory for HTTP uploaded files (will use system default if
; specified).
; https://php.net/upload-tmp-dir
;upload_tmp_dir =

; Maximum allowed size for uploaded files.
; https://php.net/upload-max-filesize
upload_max_filesize = 2M

; Maximum number of files that can be uploaded via a single request
max_file_uploads = 20

;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;

; Whether to allow the treatment of URLs (like http:// or ftp://) as file
; https://php.net/allow-url-fopen
allow_url_fopen = On

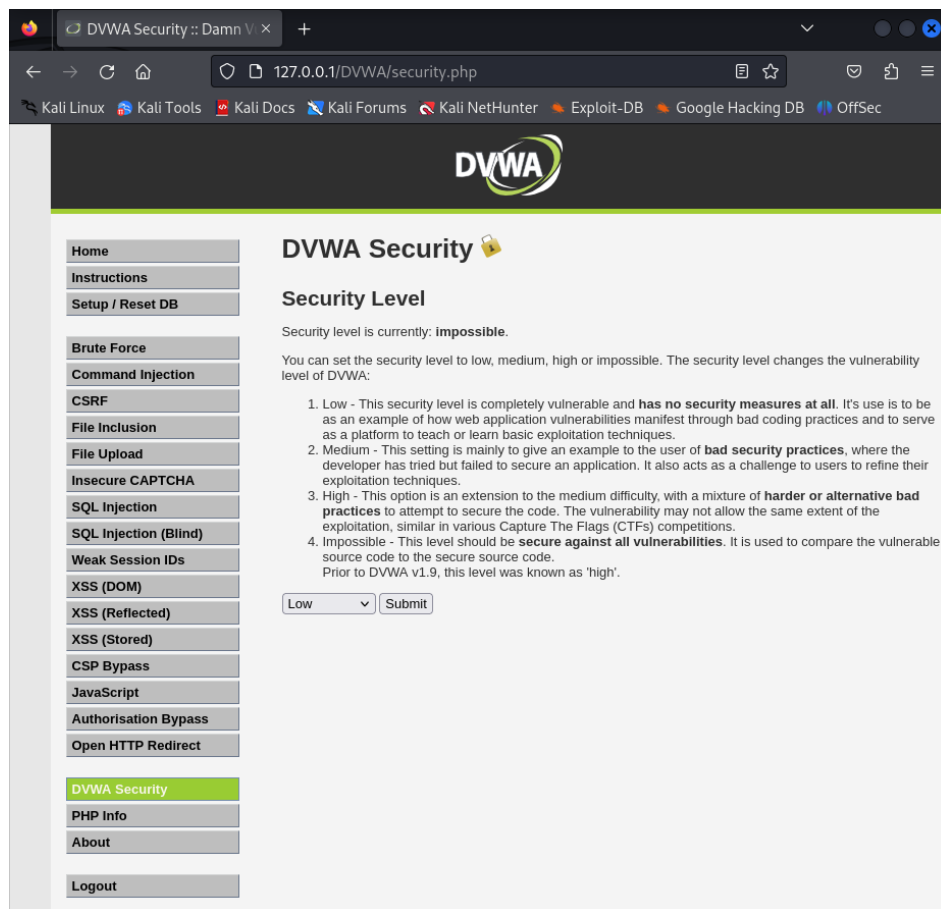
; Whether to allow include/require to open URLs (like https:// or ftp://)
; https://php.net/allow-url-include
allow_url_include = On

; Define the anonymous ftp password (your email address). PHP's default s
; for this is empty.
; https://php.net/from
;from="john@doe.com"

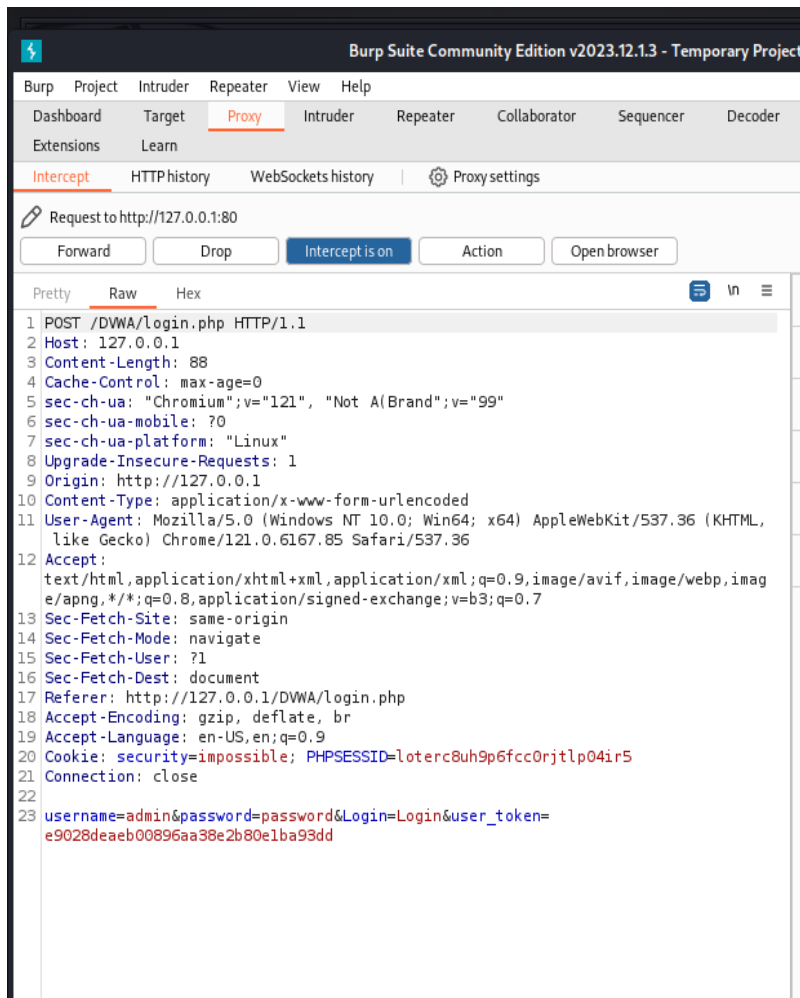
; Define the User-Agent string. PHP's default setting for this is empty.
; https://php.net/user-agent
user_agent="PHP"

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute
^X Exit      ^R Read File ^N Replace   ^U Paste     ^J Justify
```

Successivamente si è creato un database su DVWA, si è effettuato l'accesso con username(**admin**) e password(**password**) e si è scelto il livello di sicurezza della web app settandolo al minimo (Low). Più basso sarà il livello di sicurezza impostato, meno sarà complicato sfruttare le vulnerabilità.



A questo punto si è fatto uso dell'applicazione **Burp Suite**, e si è scelto un progetto temporaneo. Attivando l'intercettazione della richiesta di login su Burp, si è poi effettuato l'accesso tramite browser all'indirizzo '127.0.0.1/DVWA'. Così facendo si è provato ad intercettare la nostra stessa richiesta di login fatta tramite browser.



Per verificarlo sono state cambiate username e password iniziali con delle credenziali sbagliate, proprio per verificare che fallisse il login.

```
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=loterc8uh9p6fcc0rjtlp04ir5
21 Connection: close
22
23 username=ciao&password=ciao&Login=Login&user_token=
    e9028deaeb00896aa38e2b80e1ba93dd
```

Come ci si aspettava, con le credenziali errate non si è riuscito ad effettuare il login. Se ne ha evidenza nel body della http response dove si legge «Login failed» a riga 63.

The screenshot displays the Burp Suite interface with the 'Repeater' tab selected. The target is set to 'http://127.0.0.1'. The 'Request' pane on the left shows an HTTP GET request to '/DWA/login.php'. The 'Response' pane on the right shows the corresponding HTML response. The response body contains the text 'Login failed' at line 63, indicating an unsuccessful login attempt. The 'Inspector' pane on the right shows the request and response details.

```
Request
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="121", "Not
  A(Brand";v="99"
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/121.0.6167.85 Safari/537.36
10 Accept:
  text/html,application/xhtml+xml,applica
  tion/xml;q=0.9,image/avif,image/webp,im
  age/apng,*/*;q=0.8,application/signed-e
  xchange;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=
  aqr2htf60k6dudovaud5e3vrck
19 Connection: close
20
21

Response
54 <input type="submit" value
55   ="Login" name="Login">
56 </p>
57 </fieldset>
58 <input type='hidden' name='
59   user_token' value='
60   9782cdcaa753773115b8b5caf4e20c
61   65' />
62 </form>
63 <div class="message">
64   Login failed
65 </div>
66 <br />
67 <br />
68 <br />
69 <br />
70 <br />
71 <br />
72 <br />
73 </div>
74 <!--div id="content"-->
75 <div id="footer">
76 <p>
77   <a href="
78     https://github.com/digininja/D
79     WWA/" target="_blank">
80     Damn Vulnerable Web
81     Application (DWA)
82   </a>
83 </p>
84 </div>
```

Team 4

Roberta - Andrea (db)- Mario (rt) – Antonio – Giammarco