

Installazione e configurazione di una Damn Vulnerable Web Application

```
root@kali: /var/www/html/DVWA/config
File Azioni Modifica Visualizza Aiuto
(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: 3986, done.
remote: Total 3986 (delta 0), reused 0 (delta 0), pack-reused 3986
Ricezione degli oggetti: 100% (3986/3986), 1.77 MiB | 3.97 MiB /s, fatto.
Risoluzione dei delta: 100% (1867/1867), fatto.

(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
File Azioni Modifica Visualizza Aiuto
GNU nano 6.3 config.inc.php *
1 <?php
2
3 # If you are having problems connecting to the MySQL database
4 # try changing the 'db_server' variable from localhost to 1
5 # Thanks to @digininja for the fix.
6
7 # Database management system to use
8 $DBMS = 'MySQL';
9 # $DBMS = 'PGSQL'; // Currently disabled
10
11 # Database variables
12 # WARNING: The database specified under db_database WILL
13 # Please use a database dedicated to DVWA.
14 #
15 # If you are using MariaDB then you cannot use root, you mu
16 # See README.md for more information on this.
17 $_DVWA = array();
18 $_DVWA[ 'db_server' ] = '127.0.0.1';
19 $_DVWA[ 'db_database' ] = 'dvwa';
20 $_DVWA[ 'db_user' ] = 'kali';
21 $_DVWA[ 'db_password' ] = 'kali';
22 $_DVWA[ 'db_port' ] = '3306';
23
24 # ReCAPTCHA settings
25 # Used for the 'Insecure CAPTCHA' module
26 # You'll need to generate your own keys at: https://www.g
27 $_DVWA[ 'recaptcha_public_key' ] = '';
28 $_DVWA[ 'recaptcha_private_key' ] = '';
29
30 # Default security level
31 # Default value for the security level with each session.

^G Help ^O Salva ^W Cerca ^K Cut ^T Execute
^X Esci ^R Inserisci ^\ Sostituisci ^U Paste ^J Giustifica
```

Configurazione DVWA

Attraverso i comandi della prima immagine, si abilita la DVWA, mentre, nella seconda, si modificano la credenziali per MySQL, alla Riga 20 e 21 dal file *config.ini.php*.

```
root@kali: /
File Azioni Modifica Visualizza Aiuto

(root@kali)-[/]
# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 33
Server version: 10.6.8-MariaDB-1 Debian buildd-unstable

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 (0.004 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ;
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> exit
Bye


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

```
root@kali: /etc/php/8.1/apache2
File Azioni Modifica Visualizza Aiuto

GNU nano 6.3 php.ini *
846 ;upload_tmp_dir =
847
848 ; Maximum allowed size for uploaded files.
849 ; https://php.net/upload-max-filesize
850 upload_max_filesize = 2M
851
852 ; Maximum number of files that can be uploaded via a single request
853 max_file_uploads = 20
854
855 ;;;;;;;;;;;;;;;;;;;;;;;;;
856 ; Fopen wrappers ;
857 ;;;;;;;;;;;;;;;;;;;;;;;;;
858
859 ; Whether to allow the treatment of URLs (like http:// or https://) as
860 ; https://php.net/allow-url-fopen
861 allow_url_fopen = On
862
863 ; Whether to allow include/require to open URLs (like http:// or https://)
864 ; https://php.net/allow-url-include
865 allow_url_include = On
866
867 ; Define the anonymous ftp password (your email address).
868 ; for this is empty.
869 ; https://php.net/from
870 ;from="john@doe.com"
871
872 ; Define the User-Agent string. PHP's default setting for
873 ; https://php.net/user-agent
874 ;user_agent="PHP"
875
876 ; Default timeout for socket based streams (seconds)
```

Configurazione MySQL e configurazione file php.ini

Attraverso i comandi della prima immagine, si crea un utente per MySQL con tutti i privilegi, mentre, nella seconda, si abilitano, attraverso *On*, alle Righe 861 e 865, i loro parametri.



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: **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'.

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. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and 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**. [\[Enable PHPIDS\]](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Security level set to low

Username: admin

Configurazione MySQL e configurazione file php.ini

Dal browser, nella sezione *DVWA Security*, si imposta il livello di sicurezza della DVWA, preimpostato a *Impossible*.



Username

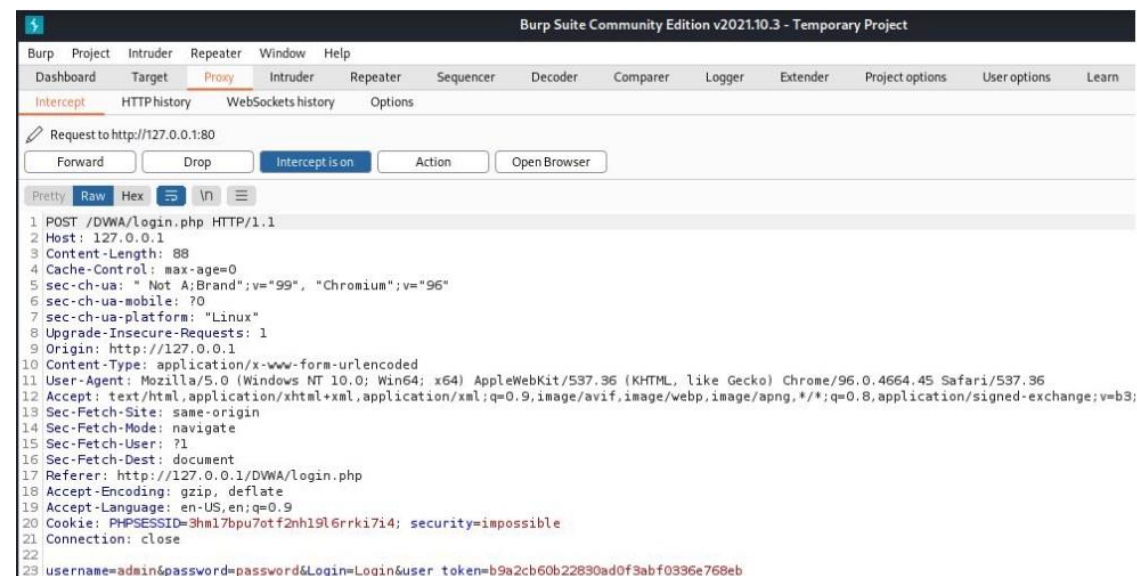
admin

Password

password

Login

[Damn Vulnerable Web Application \(DVWA\)](#)



Intercettazioni richieste attraverso Burp Suite




Sul browser, inseriamo l'indirizzo: 127.0.0.1/DVWA e, nei campi login e password, inseriamo *admin* e *password* rispettivamente. Attraverso Burp Suite, nella sezione proxy, si intercetta la richiesta nella Riga 17.

Dashboard Target Proxy Intruder **Repeater** Sequencer Decoder Comparer Logger Extender Project options User options

1 x ...

Send Cancel < > Follow redirection

Request




Pretty Raw Hex   

```

1 POST /DWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 83
4 Cache-Control: max-age=0
5 sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="96"
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/96.0.4664.45
  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=0.9
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
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=9hn17bpu7otf2nh19l6rrki7i4; security=
  impossible
21 Connection: close
22
23 username=ciao&password=ciao&Login=Login&user_token=
  b9a2cb60b22890ad0f3abf0396e768eb

```

Response




Pretty Raw Hex Render   

```

1 HTTP/1.1 302 Found
2 Date: Fri, 03 Jun 2022 11:57:01 GMT
3 Server: Apache/2.4.52 (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 Location: login.php
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12

```

Response

Pretty Raw Hex Render   

```

48
49     <label for="pass">
      Password
    </label>
    <input type="password" class="loginInput"
      AUTOCOMPLETE="off" size="20" name="password">
    <br />
50
51    <br />
52
53    <p class="submit">
      <input type="submit" value="Login" name="Login">
    </p>
54
55    </fieldset>
56
57    <input type='hidden' name='user_token' value='
      9d0e117fd3c0a1be8c82dd6e4971d7d4' />
58
59  </form>
60
61  <br />
62
63  <div class="message">
    Login failed
  </div>
64
65  <br />
66  <br />
67

```

Modifica credenziali

Si possono modificare i campi ed inviare la richiesta inserendo delle credenziali sbagliate, cliccando, prima con il tasto destro: *send to repeater* e, successivamente su *send*, ma, senza la possibilità di entrare, come evidenziato nel body della http, dalla Riga 63 alla Riga 64.