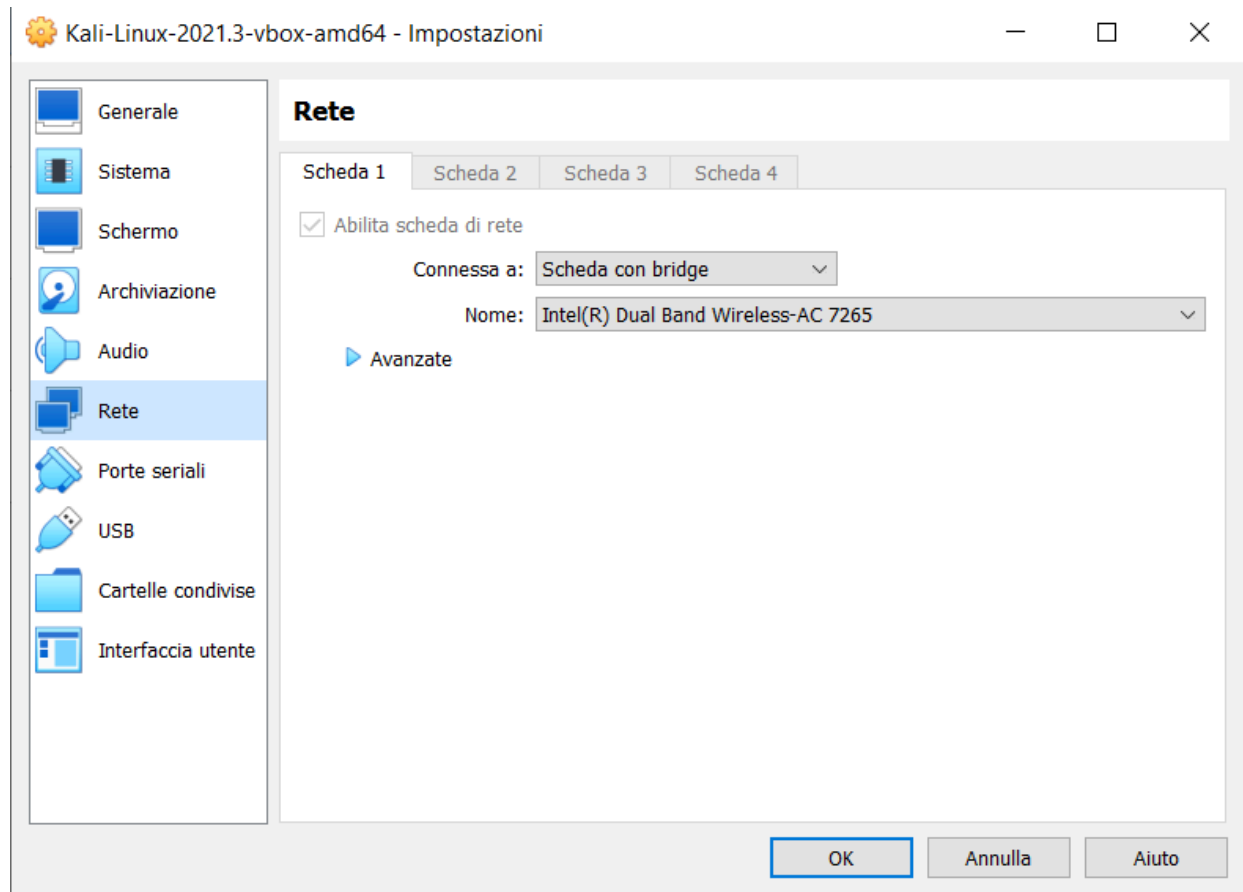
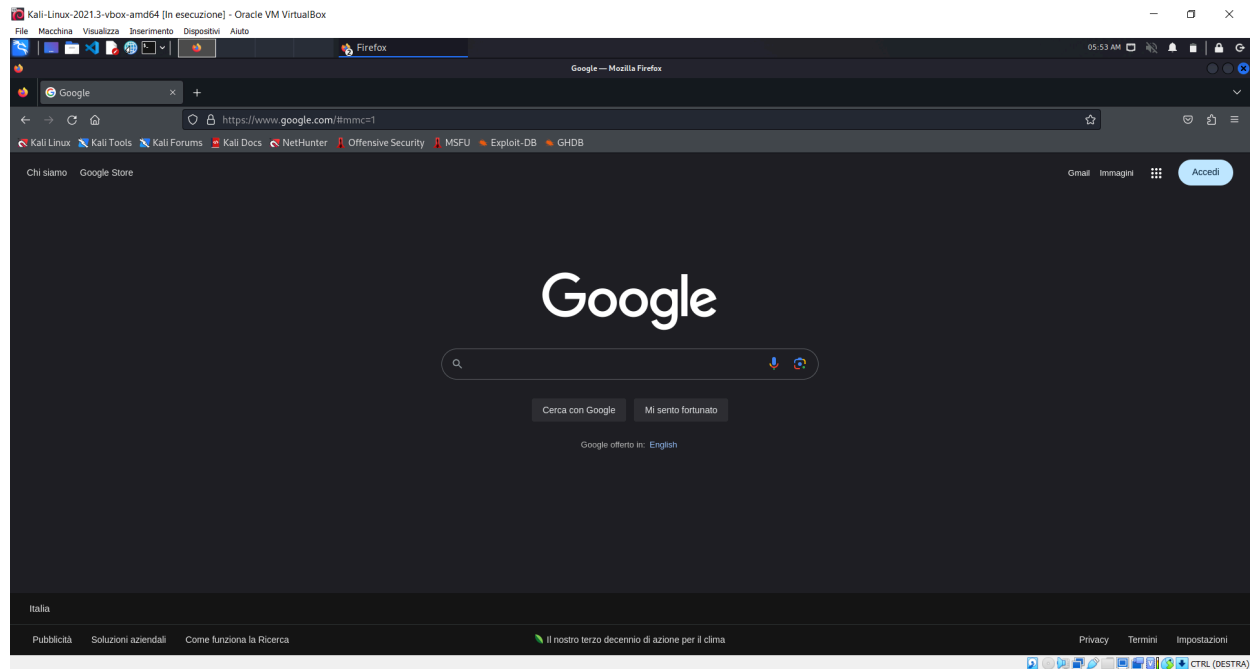


Verifica scheda di rete macchina Kali



Verifica accesso internet



Installazione DVWA

```

(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(kali㉿kali)-[/home/kali]
# cd /var/www/html

(kali㉿kali)-[/var/www/html]
# git clone https://github.com/digininja/DVWA
Cloning into 'DVWA' ...
remote: Enumerating objects: 4590, done.
remote: Counting objects: 100% (140/140), done.
remote: Compressing objects: 100% (103/103), done.
remote: Total 4590 (delta 58), reused 101 (delta 36), pack-reused 4450
Receiving objects: 100% (4590/4590), 2.34 MiB | 6.09 MiB/s, done.
Resolving deltas: 100% (2153/2153), done.

(kali㉿kali)-[/var/www/html]
# chmod -R 777 DVWA/
chmod: invalid mode: '-R'
Try 'chmod --help' for more information.

(kali㉿kali)-[/var/www/html]
# chmod -r 777 DVWA/
chmod: invalid mode: '-r'
Try 'chmod --help' for more information.

(kali㉿kali)-[/var/www/html]
# chmod --help
Usage: chmod [OPTION]... MODE[,MODE]... FILE ...
or:  chmod [OPTION]... OCTAL-MODE FILE ...
or:  chmod [OPTION]... --reference=RFILE FILE ...
Change the mode of each FILE to MODE.
With --reference, change the mode of each FILE to that of RFILE.

  -c, --changes          like verbose but report only when a change is made
  -f, --silent, --quiet  suppress most error messages
  -v, --verbose          output a diagnostic for every file processed
                        --no-preserve-root  do not treat '/' specially (the default)
                        --preserve-root    fail to operate recursively on '/'
                        --reference=RFILE  use RFILE's mode instead of specifying MODE values.
                                           RFILE is always dereferenced if a symbolic link.
  -R, --recursive       change files and directories recursively
  --help                display this help and exit
  --version              output version information and exit

Each MODE is of the form '[ugoa]*([-+=]([rwxXst]*|[ugo]))+|[-+=][0-7]+'

GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Full documentation <https://www.gnu.org/software/coreutils/chmod>
or available locally via: info '(coreutils) chmod invocation'

```

```

(kali㉿kali)-[/var/www/html]
# chmod 777 DVWA/ -R

```

```
(root@kali)-[/var/www/html]
# ls -alt
total 28
drwxrwxrwx 12 root root 4096 Jun 25 05:54 DVWA
drwxr-xr-x 3 root root 4096 Jun 25 05:54 .
-rw-r--r-- 1 root root 10701 Sep 8 2021 index.html
-rw-r--r-- 1 root root 612 Sep 8 2021 index.nginx-debian.html
drwxr-xr-x 3 root root 4096 Sep 8 2021 ..
```

```
(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
```

Modifica file config.inc.php. User: kali, password: kali

```
GNU nano 8.0 config.inc.php
<?php
# If you are having problems connecting to the MySQL database and all of the variables below are correct
# 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 = 'PdoSql'; // 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' ] = getenv('DB_SERVER') ? '127.0.0.1' : 'localhost';
$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 impossible'.
$DVWA[ 'default_security_level' ] = 'impossible';

# Default locale
# Default locale for the help page shown with each session.
# The default is 'en'. You may wish to set this to either 'en' or 'zh'.
$DVWA[ 'default_locale' ] = 'en';

# Disable authentication
# Some tools don't like working with authentication and passing cookies around
# so this setting lets you turn off authentication.
$DVWA[ 'disable_authentication' ] = false;

define( 'MYSQL', 'mysql' );
define( 'SQLITE', 'sqlite' );

# SQLite DB Backend
# Use this to switch the backend database used in the SQLite and Blind SQLite labs.
```

```

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

(root@kali)-[/var/www/html/DVWA/config]
# mysql -u root -p
mysql Ver 15.1 Distrib 10.5.12-MariaDB, for debian-linux-gnu (x86_64) using Editline wrapper
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Usage: mysql [OPTIONS] [database]

Default options are read from the following files in the given order:
/etc/my.cnf /etc/mysql/my.cnf ~/.my.cnf
The following groups are read: mysql mariadb-client client-server client-mariadb
The following options may be given as the first argument:
--print-defaults          Print the program argument list and exit.
--no-defaults             Don't read default options from any option file.
The following specify which files/extra groups are read (specified before remaining options):
--defaults-file=#         Only read default options from the given file #.
--defaults-extra-file=#   Read this file after the global files are read.
--defaults-group-suffix=# Additionally read default groups with # appended as a suffix.

-?, --help                Display this help and exit.
-I, --help                Synonym for -?
--abort-source-on-error   Abort 'source filename' operations in case of errors
--auto-rehash             Enable automatic rehashing. One doesn't need to use
                          'refresh' to get table and field completion, but startup
                          Pubblia - Soluzioni

```

Partenza servizio db - comando: `systemctl start mariadb`

Creazione utenza e assegnazione privilegi all'utente kali

```

(root@kali)-[~]
# mysql -u root -p

Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 34
Server version: 10.5.12-MariaDB-1 Debian 11

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 (0.014 sec)

```

```

MariaDB [(none)]> GRANT ALL PRIVILEGES ON dvwa.* TO 'kali'@'127.0.0.1' IDENTIFIED BY 'kali';
Query OK, 0 rows affected (0.007 sec)

MariaDB [(none)]> SHOW GRANTS FOR 'kali'@'127.0.0.1';
+-----+-----+
| Grants for kali@127.0.0.1 |
+-----+-----+
| GRANT USAGE ON *.* TO `kali`@`127.0.0.1` IDENTIFIED BY PASSWORD '*D64F6611CF18EA567ED1E8E74F2243AC1EDF54C4' |
| GRANT ALL PRIVILEGES ON `dvwa`.* TO `kali`@`127.0.0.1` |
+-----+-----+
2 rows in set (0.000 sec)

MariaDB [(none)]> exit
Bye

```

Partenza servizio apache e modifica voci *allow_url_fopen* e *allow_url_include* su file `php.ini`

```
(root@kali)~# service apache2 start

(root@kali)~# cd /etc/php/8.1/apache2
cd: no such file or directory: /etc/php/8.1/apache2

(root@kali)~# cd /etc/php

(root@kali)/etc/php# ls
7.4  8.2

(root@kali)/etc/php# cd /etc/php/8.2/apache2

(root@kali)/etc/php/8.2/apache2# nano php.ini
```

```
GNU nano 8.0 php.ini *
;cgi.rfc2616_headers = 0

;cgi.check_shebang_line controls whether CGI PHP checks for line starting with #!
; (shebang) at the top of the running script. This line might be needed if the
; script support running both as stand-alone script and via PHP CGI<. PHP in CGI
; mode skips this line and ignores its content if this directive is turned on.
; https://php.net/cgi.check-shebang-line
;cgi.check_shebang_line=1

;
; File Uploads
;
; Whether to allow HTTP file uploads.
; https://php.net/file-uploads
file_uploads = On

; Temporary directory for HTTP uploaded files (will use system default if not
; 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 files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

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

; Define the anonymous ftp password (your email address). PHP's default setting
; 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"
```

Partenza servizio apache e sessione browser su 127.0.0.1/DVWA/setup.php

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

Setup :: Damn Vulnerable

127.0.0.1/DVWA/setup.php

Kali LinuxKali ToolsKali ForumsKali DocsNetHunterOffensive SecurityMSFUExploit-DBGHDB

Setup DVWA

Instructions

About

Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: `/var/www/html/DVWA/config/config.inc.php`

If the database already exists, **it will be cleared and the data will be reset.**
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: **7.4.21**
PHP function display_errors: **Disabled**
PHP function display_startup_errors: **Disabled**
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: **Enabled**
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**

Writable folder `/var/www/html/DVWA/hackable/uploads/`: **Yes**
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
```

Creazione database

Create / Reset Database

Database has been created.

'users' table was created.

Data inserted into 'users' table.

'guestbook' table was created.

Data inserted into 'guestbook' table.

Backup file /config/config.inc.php.bak automatically created

Setup successful!

Please [login](#).

Login

Username: admin

password: password



Username

admin

Password

••••••••

Login

Impostazione livello di sicurezza su “low”



- 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
- Logout

DVWA Security

Security Level

Security level is currently: **low**.

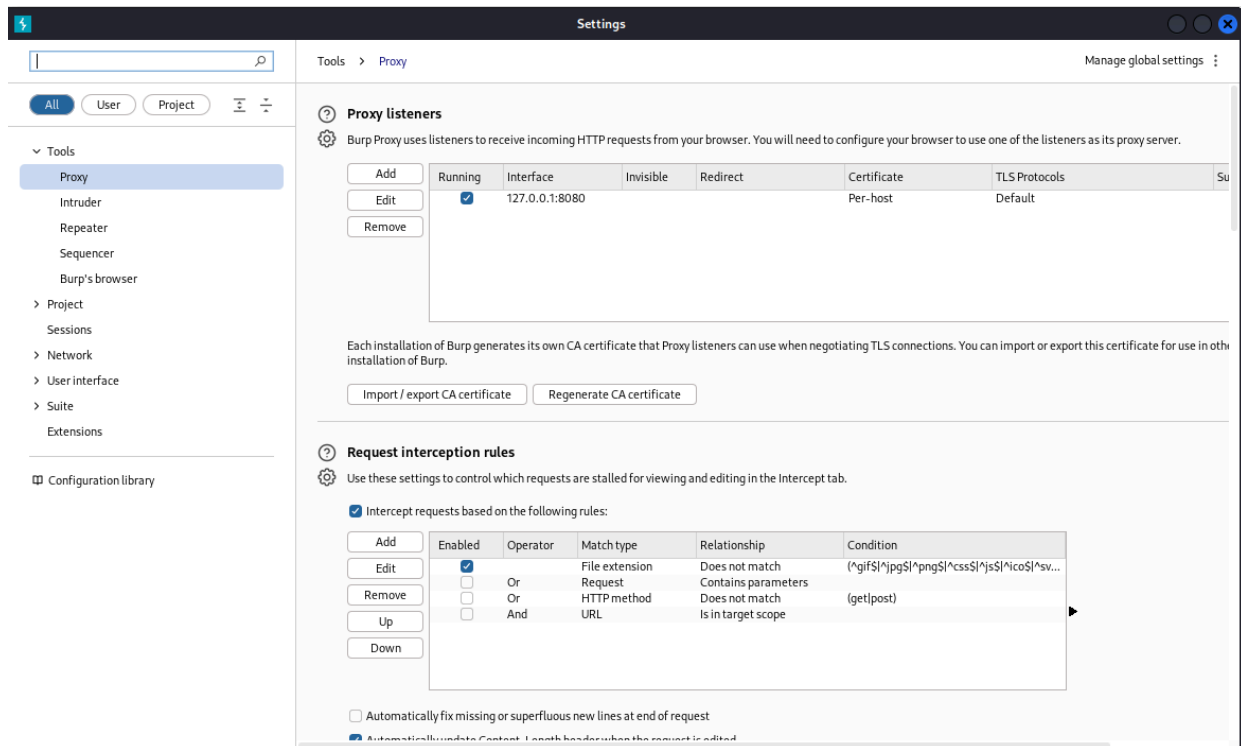
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

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'.

Low

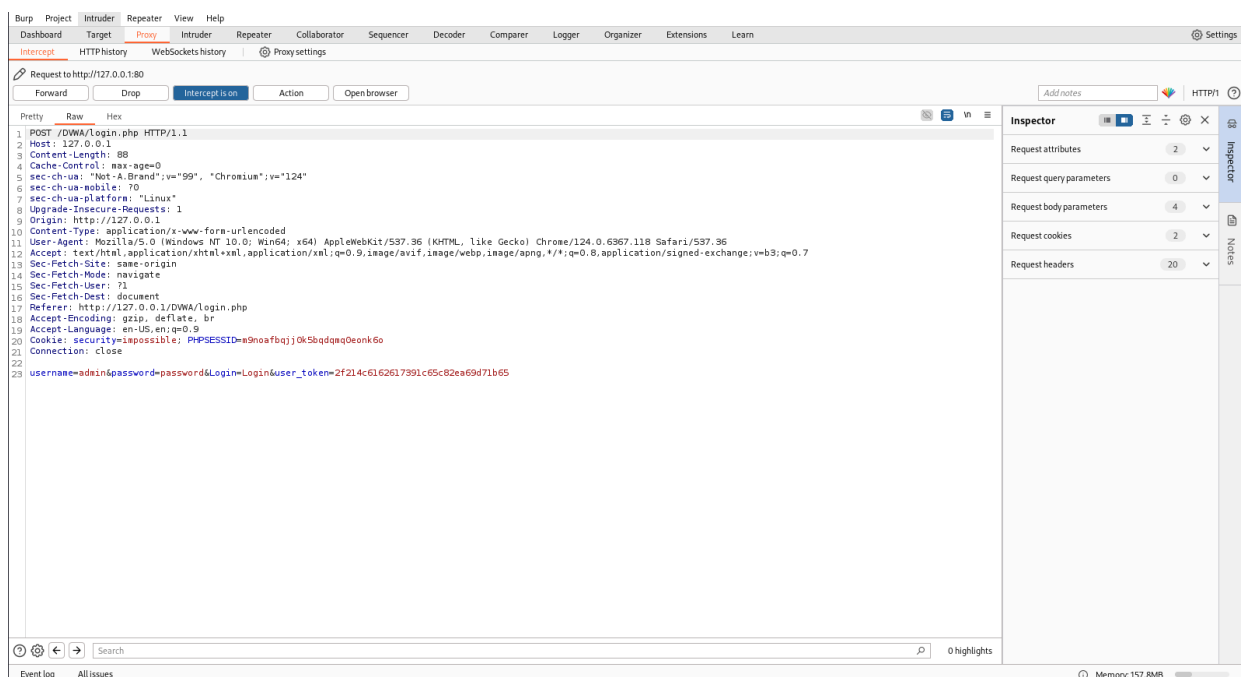
Security level set to low

Verifica configurazione servizio proxy su Burpsuite

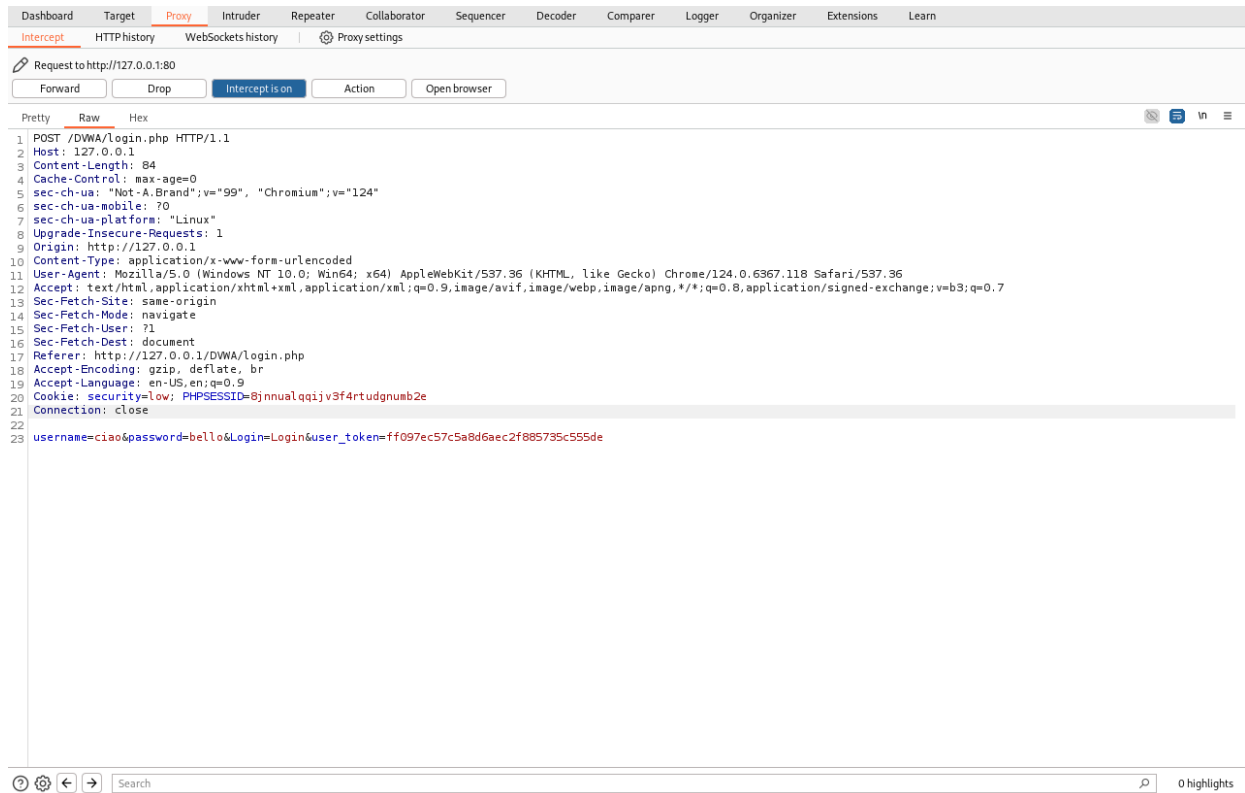


Utilizzo Burpsuite

Dopo aver inserito l'indirizzo 1270.0.1/DVWA nel browser di Burpsuite, essere arrivati alla schermata di login e aver inserito nome utente e password, facciamo click su forward per passare dalla richiesta GET alla richiesta POST:



Proviamo a modificare i campi, ed inviare la richiesta inserendo delle credenziali sicuramente errate.



Prima di inviare la richiesta, clicchiamo con il tasto destro e selezioniamo «send to repeater»
Clicchiamo su send per inviare la richiesta di login e poi su follow redirection. Livello sicurezza impostato: **Low**

Send Cancel < >

Request
Pretty Raw Hex
1 POST /DWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 84
4 Cache-Control: max-age=0
5 sec-ch-ua: "Not-A.Brand";v="99", "Chromium";v="124"
6 sec-ch-ua-mobile: 70
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/124.0.6967.118 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=0.7
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, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security=low; PHPSESSID=Bjnnualqqjv3f4rtudgnumb2e
21 Connection: close
22
23 username=ciao&password=bello&Login=Login&user_token=ff097ec57c5a8d6aec2f885735c555de

Response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Date: Tue, 25 Jun 2024 12:30:55 GMT
3 Server: Apache/2.4.58 (Debian)
4 Set-Cookie: PHPSESSID=Bjnnualqqjv3f4rtudgnumb2e; expires=Wed, 26-Jun-2024 12:30:55 GMT; Max-Age=86400; path=/
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Location: login.php
9 Content-Length: 0
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12
13

Search 0 highlights Search 0 highlights

Con le credenziali errate non si riesce a effettuare il login. Nel body della http response leggiamo «Login failed»

Send Cancel < >

Request
Pretty Raw Hex
1 GET /DWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Cache-Control: max-age=0
4 sec-ch-ua: "Not-A.Brand";v="99", "Chromium";v="124"
5 sec-ch-ua-mobile: 70
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/124.0.6967.118 Safari/537.36
10 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
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=low; PHPSESSID=Bjnnualqqjv3f4rtudgnumb2e
19 Connection: close
20
21

Response
Pretty Raw Hex Render
54
55 </fieldset>
56
57 <input type='hidden' name='user_token' value='
9979b55d4e1c23c3f234453622e7d418' />
58
59 </form>
60
61

62
63 <div class="message">
Login failed
</div>
64
65

66

67

68

69

70

71

72

73
74 </div>
75 <!--div id="content"-->
76
77 <div id="footer">
78
79
Damn Vulnerable Web Application (DWAA)

80
81 </div>
82 <!--div id="footer"-->
83
84 </div>
85 <!--div id="wrapper"-->
86 </body>
</html>

Search 0 highlights Search 0 highlights

The screenshot shows a web browser's developer tools with the 'Network' tab selected. A request to `/DWA/login.php` is highlighted. The 'Request' pane shows the raw HTTP request, and the 'Response' pane shows the raw HTML response. A red box highlights the 'Cookie' header in the request, which contains a CSRF token. Another red box highlights the 'message' div in the response, which contains the text 'CSRF token is incorrect'.

```
Request
Pretty Raw Hex
1 GET /DWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Cache-Control: max-age=0
4 sec-ch-ua: "Not-A.Brand";v="99", "Chromium";v="124"
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/124.0.6367.118 Safari/537.36
10 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
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=medium; PHPSESSID=ooqus87a86va2613ml3mh67c6f
19 Connection: close
20
21

Response
Pretty Raw Hex Render
50
51 <br />
52
53 <p class="submit">
54 <input type="submit" value="Login" name="Login">
55 </p>
56 </fieldset>
57 <input type="hidden" name='user_token' value='
58 711709b6c3da609247006d8ff4027199' />
59 </form>
60
61 <br />
62 <div class="message">
63 CSRF token is incorrect
64 </div>
65 <br />
66 <br />
67 <br />
68 <br />
69 <br />
70 <br />
71 <br />
72 <br />
73
74 </div>
75 <!--div id="content"-->
76 <div id="footer">
77 <p>
78 <a href="https://github.com/digininja/DWA/" target="_blank">
79 Damn Vulnerable Web Application (DWVA)
80 </a>
81 </p>
82 </div>
83 <!--div id="footer"-->
```

Per implementare un livello di sicurezza contro i brute force attacks nelle web app, spesso vengono incorporati nelle applicazioni dei token CSRF (Cross-Site Request Forgery) che sono sequenze random e difficili da indovinare. Le web app con un livello di sicurezza più elevato necessitano di un token CSRF che sia unico per ogni richiesta, di modo da ovviare a molteplici tentativi di indovinare le credenziali corrette per effettuare il login. Quindi se proviamo a cambiare le credenziali nella stessa sessione, riceveremo un messaggio relativo al CSRF scorretto.