

# Report S3/L3

Matteo Congiu

Traccia: Nella lezione pratica di oggi vedremo come configurare una DVWA – ovvero damn vulnerable web application in Kali Linux. La DVWA ci sarà molto utile per i nostri test.

## Svolgimento

Per iniziare sono andato sul terminale di kali e sono entrato nella modalità root con il comando `-sudo su`, poi ho seguito i seguenti comandi:

- `cd /var/www/html`
- `git clone https://github.com/digininja/DVWA`
- `chmod -R 777 DVWA/`
- `cd DVWA/config`
- `cp config.inc.php.dist config.inc.php`
- `nano config.inc.php`

```
File Actions Edit View Help
(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: 4954, done.
remote: Counting objects: 100% (114/114), done.
remote: Compressing objects: 100% (45/45), done.
remote: Total 4954 (delta 68), reused 102 (delta 61), pack-reused 4840 (from 1)
Receiving objects: 100% (4954/4954), 2.45 MiB | 2.23 MiB/s, done.
Resolving deltas: 100% (2405/2405), done.
(kali@kali)-[/var/www/html]
└─# chmod -R 777 DVWA/
chmod: invalid mode: '\211R'
Try 'chmod --help' for more information.
(kali@kali)-[/var/www/html]
└─# cd DVWA/config
(kali@kali)-[/var/www/html/DVWA/config]
└─# cp config.inc.php.dist config.inc.php
(kali@kali)-[/var/www/html/DVWA/config]
└─# nano config.inc.php
(kali@kali)-[/var/www/html/DVWA/config]
└─# nano config.inc.php
```

```
#!/usr/bin/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 = getenv('DBMS') ? : 'MySQL';
$dbms = 'PGSQL'; // 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';
$_DVWA['db_database'] = getenv('DB_DATABASE') ? : 'dvwa';
$_DVWA['db_user'] = getenv('DB_USER') ? : 'kali';
$_DVWA['db_password'] = getenv('DB_PASSWORD') ? : 'kali';
$_DVWA['db_port'] = getenv('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'] = getenv('RECAPTCHA_PUBLIC_KEY') ? : '';
$_DVWA['recaptcha_private_key'] = getenv('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'] = getenv('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'] = getenv('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'] = getenv('DISABLE_AUTHENTICATION') ? : false;

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

# SQLite DB Backend
```

Nel file `file config.inc.php` ho cambiato le credenziali user e passord come richiesto e ho salvato con `ctrl+o`.

Successivamente ho fatto partire il servizio mysql con il comando: `service mysql start`

Poi mi son connesso al db utilizzando le credenziali precedentemente cambiate. Il comando usato è: **mysql -u root -p**

```
(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: 10.11.7-MariaDB-4 Debian n/a

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

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Ho creato un'utenza sul db con: **create user 'kali'@'127.0.0.1' identified by 'kali' ;**

e gli ho assegnato i privilegi di root: **grant all privileges on dvwa.\* to 'kali'@'127.0.0.1' identified by 'kali' ;**

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ;
Query OK, 0 rows affected (0.009 sec)
```

```
MariaDB [(none)]> exit
Bye
```

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

Dopo aver terminato la configurazione ho lanciato il comando per il servizio apache: **service apache2 start**

Mi son spostato nella cartella apache2 con: **cd /etc/php/8.2/apache2**

Nel file **php.ini** modificato le voci **allow\_url\_fopen** e **allow\_url\_include** configurandole su ON.

```
(root@kali)-[/var/www/html/DVWA/config]
# service apache2 start
Home
(root@kali)-[/var/www/html/DVWA/config]
# cd /etc/php/8.1/apache2
cd: no such file or directory: /etc/php/8.1/apache2

(root@kali)-[/var/www/html/DVWA/config]
# cd /etc/php
Current
(root@kali)-[/etc/php]
# ls
8.2

(root@kali)-[/etc/php]
# cd /etc/php/8.2/apache2
Escaped
(root@kali)-[/etc/php/8.2/apache2]
# ls
conf.d  php.ini

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

Ho eseguito nuovamente il comando **service apache2 start**.

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

Successivamente con il browser firefox ho aperto la pagina **127.0.0.1/DVWA/setup.php** e ho cliccato su «**Create / Reset Database**» e in seguito ho fatto l'accesso con le credenziali di default **Username: admin - Password: password**.

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: **8.2.18**  
 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**

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Create / Reset Database

Una volta eseguito l'accesso ho cliccato sulla scheda **DVWA Security** e ho scelto il livello di sicurezza dell'APP. Più basso sarà il livello di sicurezza impostato, meno sarà complicato sfruttare le vulnerabilità.

DVWA

DVWA Security

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

Cryptography

DVWA Security

PHP Info

About

Logout

## DVWA Security

### Security Level

Security level is currently: **impossible**.

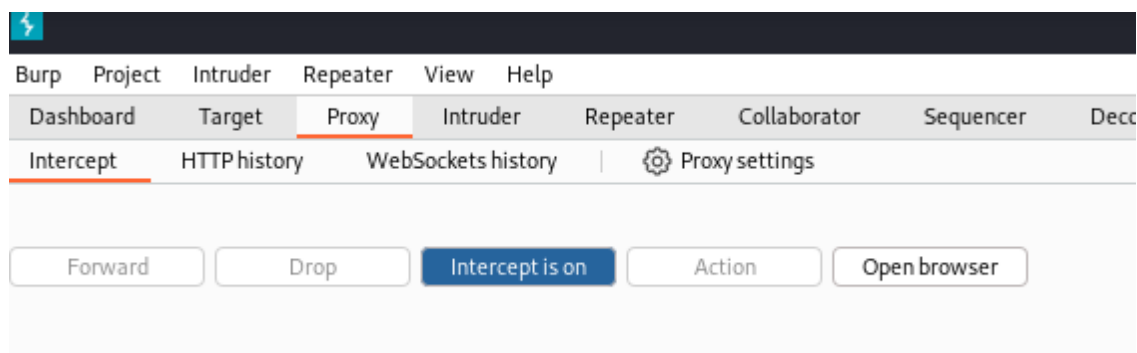
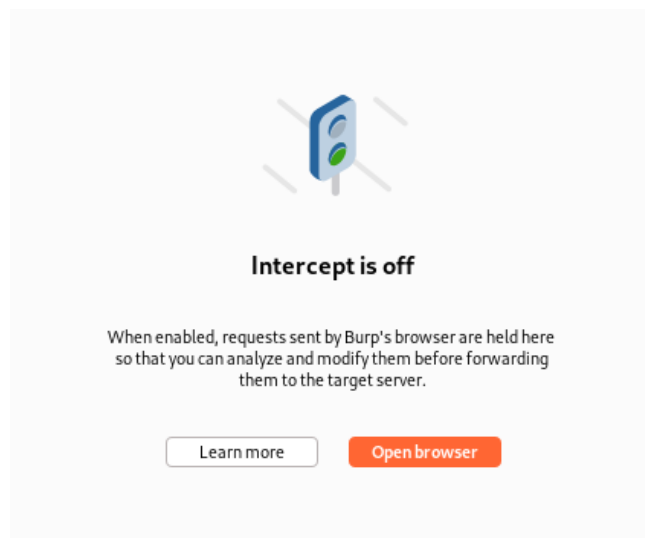
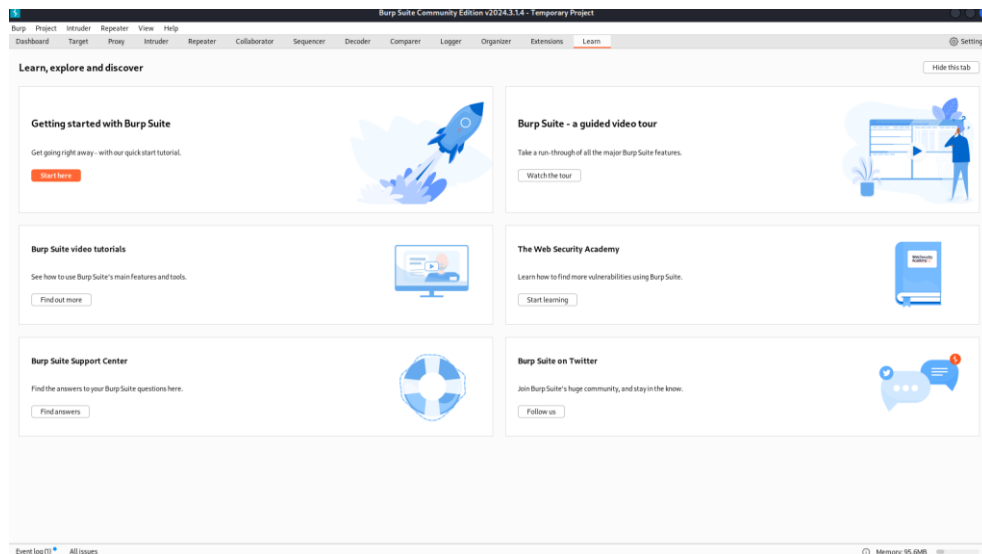
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

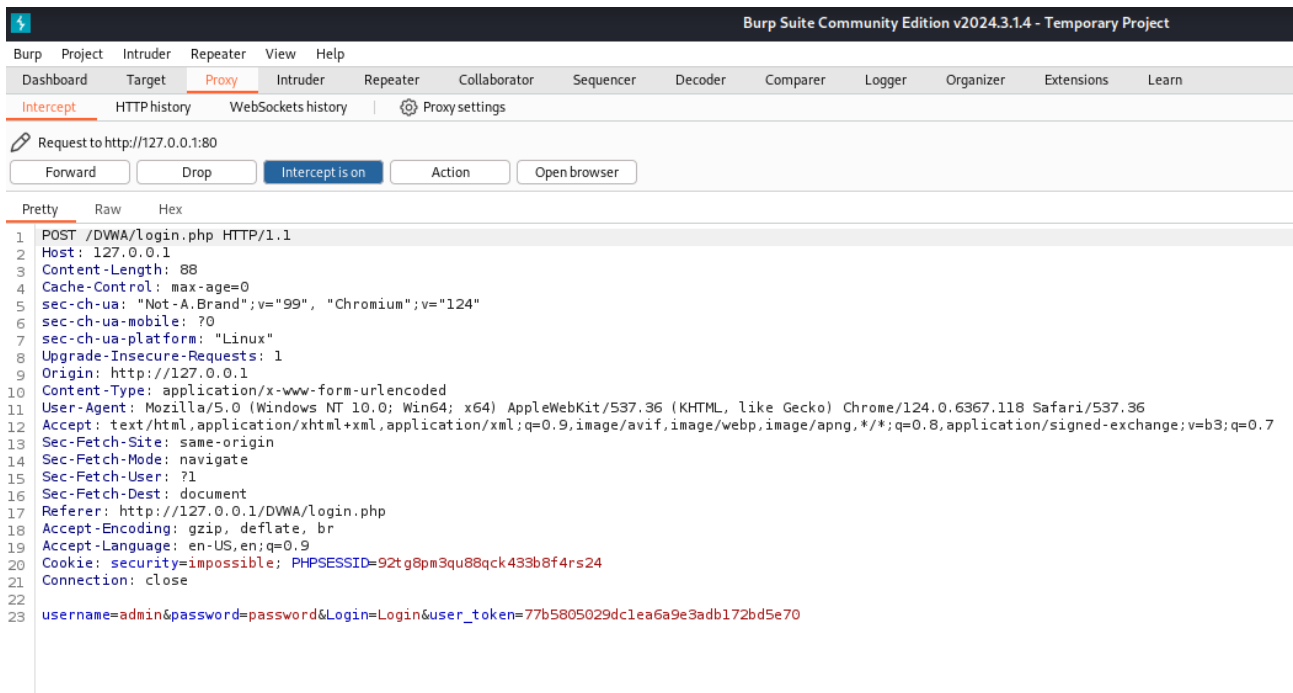
1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting 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

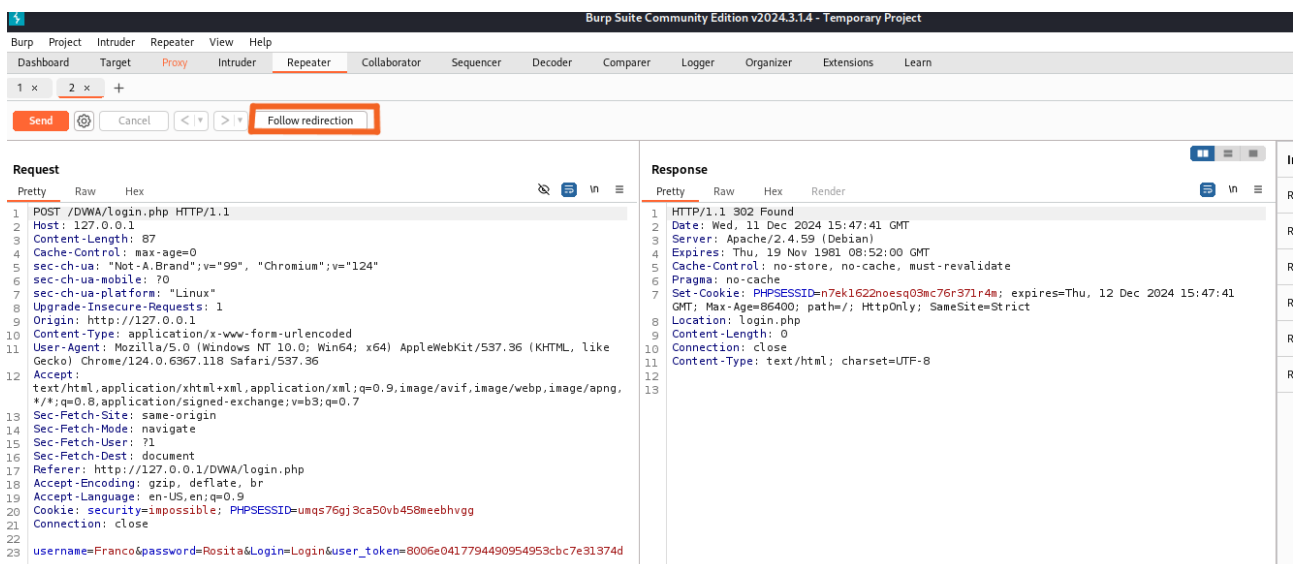
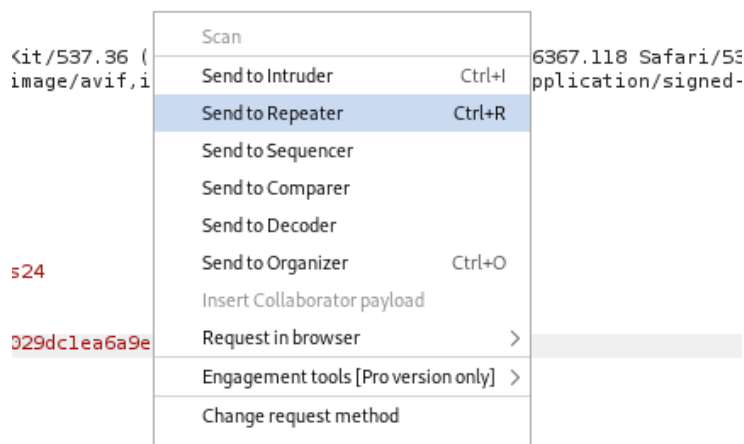
Submit

Ho avviato **Burpsuite** e sul suo browser ho cercato: **127.0.0.1/DVWA**, sul software ho cliccato su **intercept is off** per metterlo in **modalità on**, ho inserito le credenziali sulla pagina web e ho fatto l'accesso. Subito **Burpsuite** ha intercettato l'accesso comunicandomi il seguente messaggio:





Ho provato a modificare i campi, ed inviare la richiesta inserendo delle credenziali **sbagliate**, user **Franco** e password **Rosita**. Prima di inviare la richiesta ho cliccato con il **tasto destro** e ho selezionato **send to repeater**. Mi son spostato sulla sezione **Repeater** e ho cliccato su **send** per inviare la richiesta di login ed e poi su **follow redirection**.



Response

Pretty

Raw

Hex

Render

ln

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

</fieldset>

<input type='hidden' name='user\_token' value='76d2e89ca372ef437765a9cc17f3355e' />

</form>

<br />

<div class="message">

Login failed

</div>

<br />

<br />

<br />

<br />

<br />

<br />

<br />

</div>

<!--<div id="content">-->

<div id="footer">

<p>

<a href="https://github.com/digininja/DVWA/" target="\_blank">

Damn Vulnerable Web Application (DVWA)

</a>

</p>

</div>

<!--<div id="footer"> -->

</div>

<!--<div id="wrapper"> -->

</body>

</html>

ights

?

⚙

⬅

➡

Search

0 highlights

Insp

Requ

Requ

Requ

Requ

Requ

Resp