

# Report di Test sulla Vulnerabilità DVWA tramite Burp Suite

## Obiettivo del Test

L'obiettivo di questo test era eseguire una verifica base di vulnerabilità su una DVWA (Damn Vulnerable Web Application), impostata su un livello di sicurezza **basso**, al fine di comprendere le funzionalità principali dello strumento **Burp Suite** e simulare un attacco di tipo brute force o di manipolazione delle credenziali.

## Strumenti Utilizzati

- **Burp Suite** (edizione Community)
- **DVWA** configurata in ambiente di test
- Browser integrato in Burp Suite

## Descrizione del Test

Il test si è concentrato sull'intercettazione e la manipolazione delle richieste HTTP di login. Di seguito sono riportati i passaggi eseguiti:

1. **Avvio di Burp Suite** e accesso alla scheda **Proxy**, con il comando **"Intercept On"** attivo.
2. Utilizzo del **browser integrato** per accedere alla pagina di login della DVWA.
3. Inserimento di credenziali arbitrarie (username e password) nella pagina di login.

4. Intercettazione della richiesta HTTP contenente le credenziali tramite la scheda **Proxy**.
5. Inoltro della richiesta alla scheda **Repeater**, che consente di analizzare e modificare manualmente i parametri.
6. Test con credenziali corrette e credenziali errate:
  - Con **credenziali corrette**, la simulazione prosegue correttamente con accesso alla pagina successiva.
  - Con **credenziali errate**, viene restituito il messaggio **“Login Failed”**.

### **Difficoltà Riscontrate**

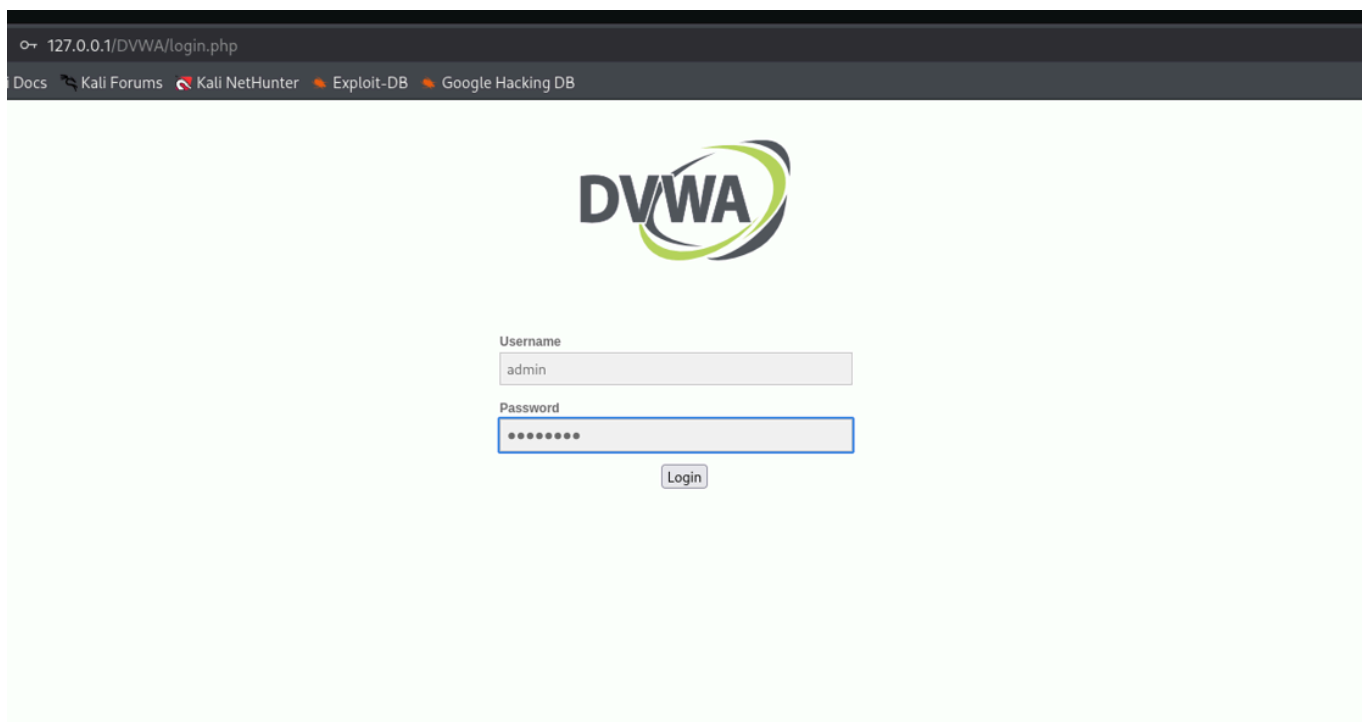
Durante il test sono emerse alcune difficoltà legate alla **limitata familiarità con Burp Suite**. L'interfaccia e le numerose funzionalità richiedono una curva di apprendimento non banale. È evidente la necessità di ulteriore pratica per acquisire una piena padronanza dello strumento e per sfruttarne al meglio tutte le potenzialità, in particolare nelle fasi di analisi, manipolazione e automazione delle richieste.

### **Considerazioni Finali**

Nonostante le difficoltà iniziali, il test ha fornito una prima comprensione del funzionamento di Burp Suite e delle dinamiche di comunicazione tra client e server in una web app vulnerabile. Questo esercizio rappresenta un primo passo concreto verso l'apprendimento dell'attività di penetration testing in ambienti controllati.

*(In allegato: immagini a supporto del test eseguito)*

## PAGINA PRINCIPALE BROWSER (da dove tentiamo l'accesso)



127.0.0.1/DVWA/login.php

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

**DVWA**

Username  
admin

Password  
••••••••••

Login

## SCHEDA PROXY CON PAGINA TRADOTTA IN TESTO (CON USERNAME E PASSWORD)

Request

Pretty Raw Hex

```
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="137", "Not/A) Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Accept-Language: en-US,en;q=0.9
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 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 Cookie: security=impossible; PHPSESSID=ce0c4506261edd22218a19136247b269
21 Connection: keep-alive
22
23 username=admin+&password=password&Login=Login&user_token=93cdacae024d93479c8b5f710628a830
```

Search

## SCHEDA MANDATA AL REPEATER CON CREDENZIALI CORRETTE

```
Request
Pretty Raw Hex
1 POST /DWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 89
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Accept-Language: en-US,en;q=0.9
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
13 Chrome/137.0.0.0 Safari/537.36
14 Accept:
15 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
16 */*;q=0.8,application/signed-exchange;v=b3;q=0.7
17 Sec-Fetch-Site: same-origin
18 Sec-Fetch-Mode: navigate
19 Sec-Fetch-User: ?1
20 Sec-Fetch-Dest: document
21 Referer: http://127.0.0.1/DWA/login.php
22 Accept-Encoding: gzip, deflate, br
23 Cookie: security=impossible; PHPSESSID=ce0c4506261edd22218a19136247b269
24 Connection: keep-alive
25
26 username=admin&password=password&Login=Login&user_token=
27 93cdacae024d93479c8b5f710628a830
```

## DIMOSTRAZIONE NEL REPEATER CONNESSIONE RIUSCITA

Request

Pretty Raw Hex

1 GET /DWA/index.php HTTP/1.1  
2 Host: 127.0.0.1  
3 Cache-Control: max-age=0  
4 sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"  
5 sec-ch-ua-mobile: ?0  
6 sec-ch-ua-platform: "Linux"  
7 Accept-Language: en-US,en;q=0.9  
8 Origin: http://127.0.0.1  
9 Upgrade-Insecure-Requests: 1  
10 User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko)  
11 Chrome/137.0.0.0 Safari/537.36  
12 Accept:  
13 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/DWA/login.php  
19 Accept-Encoding: gzip, deflate, br  
20 Cookie: security=low; PHPSESSID=3465f855279a8a0209c9cab071ff43e0  
21 Connection: keep-alive

Response

Pretty Raw Hex Render

DVWA

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

Welcome to Damn Vulnerabl

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL goal is to be an aid for security professionals to test their skill developers better understand the processes of securing web learn about web application security in a controlled class roo

The aim of DVWA is to **practice some of the most common difficulties**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by work selecting any module and working up to reach the highest level is not a fixed object to complete a module; however users should learn about web application security in a controlled class room

Please note, there are **both documented and undocumented** intentional. You are encouraged to try and discover as many

There is a help button at the bottom of each page, which allows. There are also additional links for further background reading

WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not** folder or any Internet facing servers, as they will be compromised (such as **VirtualBox** or **VMware**), which is set to NAT network download and install **XAMPP** for the web server and database

Disclaimer

We do not take responsibility for the way in which any one u

## SCHEDA CON CREDENZIALI MANDATE AL REPEATER SBAGLIATE

```
Request
Pretty Raw Hex
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 89
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Accept-Language: en-US,en;q=0.9
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/137.0.0.0 Safari/537.36
13 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;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 Cookie: security=impossible; PHPSESSID=ce0c4506261edd22218a19136247b269
21 Connection: keep-alive
22
23 username=pippo+&password=mio&Login=Login&user_token=93cdacae024d93479c8b5f710628a830
```

## DIMOSTRAZIONE SUL REPEATER DEL LOGIN NON EFFETTUATO


Request

Pretty Raw Hex

1 GET /DVWA/login.php HTTP/1.1  
2 Host: 127.0.0.1  
3 Cache-Control: max-age=0  
4 sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"  
5 sec-ch-ua-mobile: ?0  
6 sec-ch-ua-platform: "Linux"  
7 Accept-Language: en-US,en;q=0.9  
8 Origin: http://127.0.0.1  
9 Upgrade-Insecure-Requests: 1  
10 User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/137.0.0.0 Safari/537.36  
11 Accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap  
ng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
12 Sec-Fetch-Site: same-origin  
13 Sec-Fetch-Mode: navigate  
14 Sec-Fetch-User: ?1  
15 Sec-Fetch-Dest: document  
16 Referer: http://127.0.0.1/DVWA/login.php  
17 Accept-Encoding: gzip, deflate, br  
18 Cookie: security=low; PHPSESSID=3465f855279a8a0209c9cab071ff43e0  
19 Connection: keep-alive  
20  
21

Response

Pretty Raw Hex Render



Username

Password

Login

Login failed