




# CONSEGNA S3/L3

*di Giuseppe Lupoi*



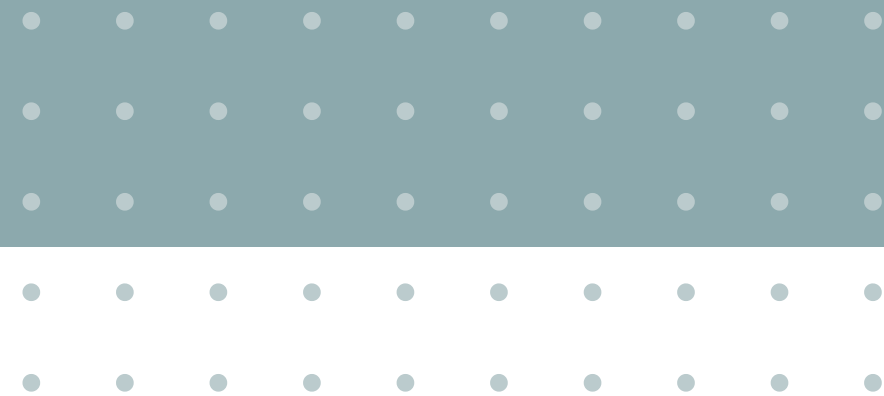


*Come richiesto quest'oggi dalla traccia  
andremo a vedere da Kali Linux con Burp Suite  
le varie "request" e "response"  
quando proviamo  
a collegarci ad una pagina web*



# 01.

Come vedremo nella slide  
successiva, se proviamo a collegarci a  
**127.0.0.1/DVWA** con  
username e password corretti  
riusciamo, ovviamente, a raggiungere il sito



Burp Suite Community Edition v2023.10.3.7 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Collaborator Settings  
Sequencer Decoder Comparer Logger Organizer Extensions  
Learn

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Met...	URL	Status code	Length	MIM
1	http://127.0.0.1	GET	/DVWA/	200	6358	HTML
3	http://127.0.0.1	GET	/DVWA/dvwa/js/add_event_listeners.js	200	875	script
5	http://127.0.0.1	GET	/DVWA/dvwa/js/dvwaPage.js	200	1313	script
6	http://127.0.0.1	GET	/DVWA/security.php			HTML

**Request**

Pretty Raw Hex

```
1 GET /DVWA/dvwa/js/dvwaPage.js
2 HTTP/1.1
3 Host: 127.0.0.1
4 sec-ch-ua: "Chromium";v="119",
  "Not?A_Brand";v="24"
5 sec-ch-ua-mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows
  NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/119.0.6045.199
  Safari/537.36
7 sec-ch-ua-platform: "Linux"
8 Accept: */*
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Dest: script
12 Referer: http://127.0.0.1/DVWA/
```

**Response**

Pretty Raw Hex

```
1 HTTP/1.1 200 OK
2 Date: Wed, 06 Dec 2023 14:37:07
  GMT
3 Server: Apache/2.4.57 (Debian)
4 Last-Modified: Wed, 06 Dec 2023
  13:22:30 GMT
5 ETag: "406-60bd73e419d4e-gzip"
6 Accept-Ranges: bytes
7 Vary: Accept-Encoding
8 Content-Length: 1030
9 Connection: close
10 Content-Type: text/javascript
11
12 /* Help popup */
13
14 function popUp(URL) {
15   day = new Date();
```

Welcome :: Damn Vulnerable x

127.0.0.1/DVWA/

**DVWA**

## Welcome to Damn Vulnerable W

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

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

### General Instructions

It is up to the user how they approach DVWA. Either by working thro selecting any module and working up to reach the highest level they is not a fixed object to complete a module; however users should fee system as best as they possible could by using that particular vulner

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

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

### WARNING!

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

### Disclaimer

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

- 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

# 02.

Noteremo ora come andando a cambiare  
username e password da Burp Suite  
provando a raggiungere il sito con  
credenziali  
volutamente errate ci verrà restituito un  
errore





⚡

Burp Suite Community Edition v2023.10.3.7 - Temporary Project

Burp

Project

Intruder

Repeater

View

Help

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Settings

Decoder

Comparer

Logger

Organizer

Extensions

Learn

Intercept

HTTP history

WebSockets history

Proxy settings

✎

Request to http://127.0.0.1:80

Forwa...

Drop

Inter...

Action

Open...

Add notes

HTTP/1

?

Pretty

Raw

Hex

1

POST /DVWA/login.php HTTP/1.1

2

Host: 127.0.0.1

3

Content-Length: 88

4

Cache-Control: max-age=0

5

sec-ch-ua: "Chromium";v="119", "Not?A\_Brand";v="24"

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/119.0.6045.199 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/DVWA/login.php

18

Accept-Encoding: gzip, deflate, br

19

Accept-Language: en-US,en;q=0.9

20

Cookie: security=impossible; PHPSESSID=917fjdk9ga13egmv036d10toim

21

Connection: close

22

username=hola&password=hola&login=Login&user\_token=759a81ec4b8b6bfa9dd2236030bf40f7

Inspector

Notes

?

⚙

⬅

➡

Search

0 highlights

Login :: Damn Vulnerable

+

⬅

➡

✕

📄

127.0.0.1/DVWA/login.php

▶


☆

⚙

🔍

👤

⋮



Username

admin

Password

\*\*\*\*\*

Login

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

Burp Suite Community Edition v2023.10.3.7 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x 2 x 3 x 4 x 5 x +

Send Cancel < >

### 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="119", "Not?A_Brand";v="24"
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/119.0.6045.199 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
```

0 highlights

### Response

Pretty Raw Hex Render

```
59 </form>
60
61 <br />
62
63 <div class="message">
64   CSRF token is incorrect
65 </div>
66
67 <br />
68 <br />
69 <br />
```

0 highlights

Done