

Pratica S3/L4

-In questo esercizio utilizzeremo l'applicazione di DVWA e Burpsuit. L'obbiettivo è l'intercettazione e la modifica di un login.

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

Entriamo nel sito e ci dirigiamo su DVWA security dove posso modificare la vulnerabilità del sito, ad esempio in questo caso è stato impostato su Low, ora apriremo Burpsuit e cominceremo ad intercettare il login della pagina.

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action Open browser

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: "Not-A.Brand";v="99", "Chromium";v="124"
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/124.0.6367.118 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/DVWA/login.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security=impossible; PHPSESSID=s28psg96p7bg4he1hg1ntbq393
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=f4f7bc6c389d41092ce346ee2b648d79
```

Ora che abbiamo intercettato la nostra pagina di login, andremo a modificare la nostra password utilizzando send repeater con il tasto destro, spostandosi nella pagina repeater potremo fare la nostra modifica, come si può notare dall'immagine e con il tasto send poi follow, andremo ad apportare le nostre modifiche, compromettendo il nostro login e completando l'esercizio.

The screenshot displays the 'Request' tab of a web browser's developer tools. The request is a POST to `/DVWA/login.php` with the following details:

- Method:** POST
- URL:** `/DVWA/login.php`
- Host:** `127.0.0.1`
- Content-Length:** 88
- Cache-Control:** `max-age=0`
- sec-ch-ua:** `"Not-A.Brand"; v="99", "Chromium"; v="124"`
- sec-ch-ua-mobile:** `?0`
- sec-ch-ua-platform:** `"Linux"`
- Upgrade-Insecure-Requests:** 1
- Origin:** `http://127.0.0.1`
- Content-Type:** `application/x-www-form-urlencoded`
- 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`
- 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`
- Sec-Fetch-Site:** `same-origin`
- Sec-Fetch-Mode:** `navigate`
- Sec-Fetch-User:** `?1`
- Sec-Fetch-Dest:** `document`
- Referer:** `http://127.0.0.1/DVWA/login.php`
- Accept-Encoding:** `gzip, deflate, br`
- Accept-Language:** `en-US,en;q=0.9`
- Cookie:** `security=impossible; PHPSESSID=s28psg96p7bg4helhg1ntbq393`
- Connection:** `close`

The request body is `username=admin&password=ciao&Login=Login&user_token=f4f7bc6c389d41092ce346ee2b648d79`. The interface also shows a 'Response' tab on the right, which is currently empty. The status bar at the bottom indicates 'Ready'.