

# S3E4

## Traccia

L'esercizio di oggi comprende dopo la creazione di una DVWA, di fare pratica con burpsuite, mostrando come possiamo cambiare le credenziali di accesso e notare che tramite il protocollo http, avremo tutte le informazioni in chiaro.

## Esercizio


Dopo aver creato la DVWA, andiamo su burpsuite e accediamo alla pagina tramite il suo browser. Appena entrati nella pagina del login e aver inserito username e password noteremo alcuni particolari.

```
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="129", "Not=A?Brand";v="8"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Accept-Language: it-IT,it;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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
    Gecko) Chrome/129.0.6668.71 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=mfjccj3emu7n46ueb26p3m2atp
21 Connection: keep-alive
22
23 username=admin&password=password&Login=Login&user_token=00b9311b434949b7c87ca23d6e1de5f2
```

Da questa immagine si può notare come si possono ottenere una serie di informazioni come ad esempio browser che si sta utilizzando o il tipo di richiesta in cui siamo (in questo caso post). In basso si possono anche vedere username e password dell'utente che in questo caso noi possiamo andare a modificare.

```
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="129", "Not=A?Brand";v="8"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Accept-Language: it-IT,it;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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
    Gecko) Chrome/129.0.6668.71 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=mfjccj3emu7n46ueb26p3m2atp
21 Connection: keep-alive
22
23 username=admin&password=pallino&Login=Login&user_token=00b9311b434949b7c87ca23d6e1de5f2
```

Andiamo a modificare in questo caso la password ma lasciamo lo stesso nome utente, facciamo tutto da burpsuite senza toccare il browser, e continuiamo a mandare la richiesta come faremmo normalmente.

Username

Password

Login

Login failed

Come mostra in questo caso la schermata, noi avevamo non solo la possibilità di vedere la password, ma anche eventualmente di cambiarla. E continuando con la richiesta ci arriverà il messaggio di login fallito.

