W8D1 - Pratica

- Traccia:

Dopo aver avviato il repo DVWA e avviato mysql.

Lanciamo Burpsuite, scegliamo un progetto temporaneo ed apriamo un browser, inserendo l'indirizzo della nostra DVWAß 1270.0.1/DVWA e inseriamo nei campi login e password i valori «admin» e «password» rispettivamente. Intercettiamo la richiesta con burp e vediamo come possiamo modificarla. Guardate i parametri di login, possiamo modificarli a nostro piacimento prima di inviare la richiesta all'app.

Proviamo a modificare i campi, ed inviare la richiesta inserendo delle credenziali sicuramente errate. Prima di inviare la richiesta, clicchiamo con il tasto destro e selezioniamo «send to repeater» Clicchiamo su send per inviare la richiesta di login ed e poi su follow redirection.

Facoltativo: Ripetere tutti i passi visti, con livello di sicurezza "Medium" e "High". Cosa cambia?

- Svolgimento:

Dopo aver avviato DVWA con apache e avviato mysql, ho creato un user e gli ho assegnato tutti i privilegi sul database dvwa.

Successivamente dopo aver avviato Burpsuite e da li il suo browser per fare una richiesta su localhost/DVWA/config.php per configurare l'ambiente.

Mi sono recato sulla pagina di login su http://localhost/DVWA/login.php e ho messo in ascolto Burpsuite tramite funzione proxy.

Ho intercettato le credenziali e l'id della sessione, le ho modificate e inviate a repeater, chiaramente non sono riuscito a fare l'accesso perché ho sostituito le credenziali corrette con credenziali inesistenti, ho avuto modo di analizzare la risposta del server con tutti i livelli di difficoltà che oltre all'id della sessione, non cambia nulla.

Al contrario potevo inserire credenziali errate e inserire tramite repeater le creadenziali corrette, oppure prendere una sessione e sostituirla non una che ha l'accesso per accedere al website del caso.....

In allegato le prove effettuate:

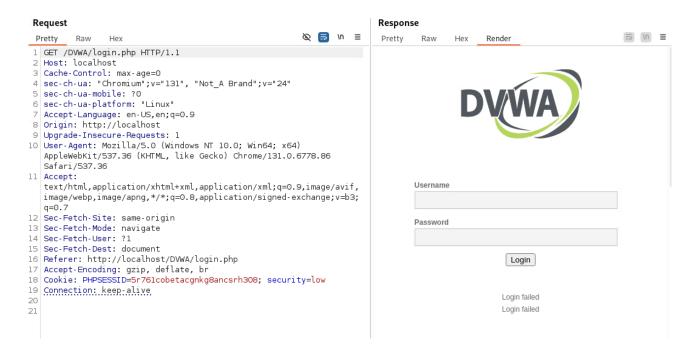
mysql attivo

apache2 attivo

- Low Difficult:

Richiesta POST intercettata

```
1 POST /DVWA/Login.php HTTP/1.1
2 Host: localhost
3 Content-Length: 88
4 Cache-Control: max-age=0
5 sec.ch-ua: "Chromium";v="131", "Not_A Brand";v="24"
6 sec.ch-ua-bobile: 70
7 sec.ch-ua-platform: "Linux"
8 Accept-Language: en-US,en;q=0.9
9 Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Wins4; x64)
AppleWebkit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86
Safari/S37.36
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-Dest: documen
17 Sec.-Fetch-Dest: documen
18 Referer: http://localhost/DVWA/login.php
19 Accept-Encoding: gzip, deflate, br
10 Coohie: PHPSESSID=5761cobetacgnkg8ancsrh308; security=low
11 Connection: keep.alive
12 username=Francesco6password=test_Login=Login&user_token=
a771ad3327ab66ae1dc48847d955e480
```



Medium Difficult:

Richiesta POST intercettata

```
1 POST /DVWA/login.php HTTP/1.1
2 Host: localhost
3 Content-Length: 88
4 Cache-Control: max-age=0
5 sec-ch-ua-mobile: 70
7 sec-ch-ua-mobile: 70
7 sec-ch-ua-mobile: 70
9 origin: http://localhost
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/131.0.6778.86
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-ex change;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Node: navigate
16 Sec-Fetch-Dest: document
17 Sec-Fetch-Dest: document
18 Referer: http://localhost/DVWA/login.php
18 Accept-Encoding: gzip, deflate, br
19 Cookie: PHPSESSID=vb5gqfc7jdjdbOtnekgltenpi; security=medium
20 Connection: keep-alive
21 username=Francesco&password=medium&Login=Login&user_token=7054f4b46636e88dfdedadd80e09689d
```

```
POST /DVWA/login.php HTTP/l.1

Host: localhost

Content-Length: 88

Cache-Control: max-age=0

sec-ch-ua: "Chromium"; v="131", "Not_A Brand"; v="24"

sec-ch-ua-mobile: 70

sec-ch-ua-platform: "Linux"

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

Origin: http://localhost

Content-Type: application/x-www-form-urlencoded

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86

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-Mode: navigate

Sec-Fetch-Mode: navigate

Sec-Fetch-Dest: document

Referer: http://localhost/DVWA/login.php

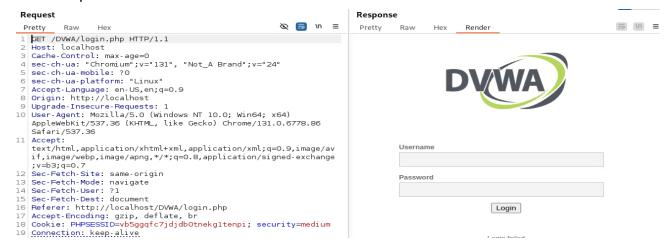
Accept-Encoding: gzip, deflate, br

Cookie: PHPSESSID=vbSggqfc7jdjdbOtnekgltenpi; security=medium

Connection: ksep:alixe

username=Francesco&password=medium&Login=Login&user_token=

7054f4b46636e88dfdedadd80e09689d
```

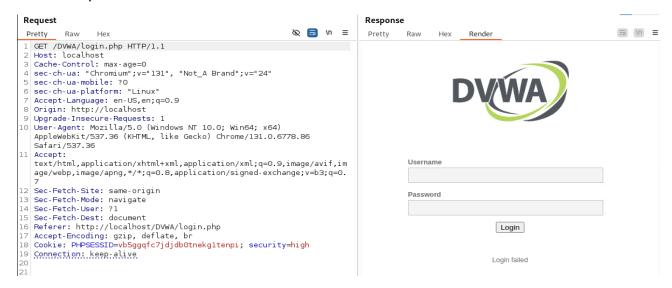


High Difficult:

Richiesta POST intercettata

```
1 POST /DVWA/login.php HTTP/1.1
2 Host: localhost
3 Content-Length: 88
4 Cache-Control: max-age=0
5 sec-ch-ua- mobile: 70
7 sec-ch-ua-nobile: 70
7 sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
9 Origin: http://localhost
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/131.0.6778.86
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-ex change;v=b3;q=0.7
4 Sec-Fetch-Site: same-origin
5 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-Dese: 71
18 Referer: http://localhost/DWWA/login.php
19 Accept-Encoding: gzip, deflate, br
10 Cooke: PHPSESSID=vb5gqfc7jdjdbOtnekgltenpi; security=high
10 Connection: keep-alive
12 username=admin&password=password&Login=Login&user_token=f92c762013df9ffabb7df73ebbd7fafb
```

```
1 POST /DWA/login.php HTTP/1.1
2 Host: localhost
3 Content-Length: 88
4 Cache-Control: max-age=0
5 sec.-ch-ua: "Chromium";v="131", "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://localhost
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/S.0 (Windows NT 10.0; Win64; x64)
AppleWekKit/S37.36 (KHFML, like Gecko) Chrome/131.0.6778.86
Safari/S37.36
13 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/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-Dest: document
17 Sec-Fetch-Dest: document
18 Referer: http://localhost/DWWA/login.php
19 Accept-Encoding: gzip, deflate, br
10 Coonte: PHPSESSID=vb5ggqfc7jdjdbOtnekgltenpi; security=high
11 Connection: keep:alive
12 username=Francesco&password=high&Login=Login&user_token=
f92c762013df9ffabb7df73ebbd7fafb
```



Impossible Difficult:

Richiesta POST intercettata

```
1 POST /DVMA/login.php HTTP/1.1
2 Host: localhost
3 Content-Length: 88
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="131", "Not_A Brand";v="24"
6 sec-ch-ua-platform: "Linux"
8 Accept-Language: en-US,en;q=0.9
9 Origin: http://localhost
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/131.0.6778.86
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-Stie: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-Mode: navigate
18 Referer: http://localhost/DVWA/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: security-impossible; PHPSESSID=0ihvn8lqhul3mj9k0i2dg78ts9
21 Connection: keep-alive
```

```
POST /DVWA/login.php HTTP/1.1

Host: localhost

Content-Length: 88

Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="131", "Not_A Brand";v="24"
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86
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=b
3;q=0.7

Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Cookie: security=impossible; PHPSESSID=
S8mg32im69jad7rmqmslh5p7g0
Connection: keep:alive

username=Francesco&password=Impossible&Login=Login&user_token=
65b033ebb795deac81964413ee469107
```

