

# 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 DVWA 127.0.0.1/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 lì 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 credenziali 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

```
(root@kali)~# service mysql status
● mariadb.service - MariaDB 11.4.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
   Active: active (running) since Tue 2025-01-07 18:50:11 EST; 3min 51s ago
     Invocation: 745254737fe648468387a8fa2a693616
       Docs: man:mariadb(8)
            https://mariadb.com/kb/en/library/systemd/
   Process: 8047 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, status=0/SUCCESS)
   Process: 8057 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
   Process: 8060 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || VAR="/usr/bin/galera_recovery"; [ $?
   Process: 8165 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
   Process: 8167 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
  Main PID: 8119 (mariabdd)
    Status: "Taking your SQL requests now..."
     Tasks: 10 (limit: 61963)
  Memory: 241.9M (peak: 246.5M)
       CPU: 9.263s
   CGroup: /system.slice/mariadb.service
           └─8119 /usr/sbin/mariabdd

Jan 07 18:50:07 kali mariabdd[8119]: 2025-01-07 18:50:07 0 [Note] Plugin 'FEEDBACK' is disabled.
Jan 07 18:50:07 kali mariabdd[8119]: 2025-01-07 18:50:07 0 [Note] Plugin 'wsrep-provider' is disabled.
Jan 07 18:50:07 kali mariabdd[8119]: 2025-01-07 18:50:07 0 [Note] InnoDB: Buffer pool(s) load completed at 250107 18:50:07
Jan 07 18:50:10 kali mariabdd[8119]: 2025-01-07 18:50:10 0 [Note] Server socket created on IP: '127.0.0.1'.
Jan 07 18:50:11 kali mariabdd[8119]: 2025-01-07 18:50:11 0 [Note] mariabdd: Event Scheduler: Loaded 0 events
Jan 07 18:50:11 kali mariabdd[8119]: 2025-01-07 18:50:11 0 [Note] /usr/sbin/mariabdd: ready for connections.
Jan 07 18:50:11 kali mariabdd[8119]: Version: '11.4.3-MariaDB-1' socket: '/run/mysqld/mysqld.sock' port: 3306 Debian n/a
Jan 07 18:50:11 kali systemd[1]: Started mariadb.service - MariaDB 11.4.3 database server.
Jan 07 18:50:11 kali /etc/mysql/debian-start[8170]: Upgrading MariaDB tables if necessary.
Jan 07 18:50:11 kali /etc/mysql/debian-start[8190]: Checking for insecure root accounts.
lines 1-29/29 (END)
```

## apache2 attivo

```
(root@kali)-[/var/www/html/DVWA/config]
# service apache2 start

(root@kali)-[/var/www/html/DVWA/config]
# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Tue 2025-01-07 19:19:13 EST; 4s ago
 Invocation: 6cbe3a7aa0844b70971df1611c5884d5
    Docs: https://httpd.apache.org/docs/2.4/
   Process: 22189 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 22213 (apache2)
     Tasks: 6 (limit: 9388)
    Memory: 20.3M (peak: 20.7M)
       CPU: 329ms
    CGroup: /system.slice/apache2.service
            └─22213 /usr/sbin/apache2 -k start
              22216 /usr/sbin/apache2 -k start
              22217 /usr/sbin/apache2 -k start
              22218 /usr/sbin/apache2 -k start
              22219 /usr/sbin/apache2 -k start
              22220 /usr/sbin/apache2 -k start

Jan 07 19:19:13 kali systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Jan 07 19:19:13 kali apachectl[22204]: AH00558: apache2: Could not reliably determine the
Jan 07 19:19:13 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-21/21 (END)
```

## - 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-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/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-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://localhost/DVWA/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: PHPSESSID=5r761cobetacgkng8ancsrh308; security=low
21 Connection: keep-alive
22
23 username=admin&password=password&Login=Login&user_token=a771ad3327ab66ae1dc48847d955e480
```

### Invio al Repeater


```
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-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/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-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://localhost/DVWA/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: PHPSESSID=5r761cobetacgkng8ancsrh308; security=low
21 Connection: keep-alive
22
23 username=Francesco&password=test&Login=Login&user_token=a771ad3327ab66ae1dc48847d955e480
```

## Risposta del server

**Request**  
Pretty Raw Hex

```
1 GET /DVWA/login.php HTTP/1.1
2 Host: localhost
3 Cache-Control: max-age=0
4 sec-ch-ua: "Chromium";v="131", "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://localhost
9 Upgrade-Insecure-Requests: 1
10 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
11 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
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Referer: http://localhost/DVWA/login.php
17 Accept-Encoding: gzip, deflate, br
18 Cookie: PHPSESSID=5r761cobetacgnkg8ancsrh308; security=low
19 Connection: keep-alive
20
21
```

**Response**  
Pretty Raw Hex Render

Username

Password

Login

Login failed  
Login failed

## 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: "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/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-ex
    change;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://localhost/DVWA/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: PHPSESSID=5r761cobetacgnkg8ancsrh308; security=low
21 Connection: keep-alive
22
23 username=Francesco&password=medium&Login=Login&user_token=7054f4b46636e88dfdedadd80e09689d
```

### Invio al Repeater


```
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-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/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/av
    if,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://localhost/DVWA/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: PHPSESSID=5r761cobetacgnkg8ancsrh308; security=low
21 Connection: keep-alive
22
23 username=Francesco&password=medium&Login=Login&user_token=
    7054f4b46636e88dfdedadd80e09689d
```

## Risposta del server

**Request**  
Pretty Raw Hex

```
1 GET /DVWA/login.php HTTP/1.1
2 Host: localhost
3 Cache-Control: max-age=0
4 sec-ch-ua: "Chromium";v="131", "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://localhost
9 Upgrade-Insecure-Requests: 1
10 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
11 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
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Referer: http://localhost/DVWA/login.php
17 Accept-Encoding: gzip, deflate, br
18 Cookie: PHPSESSID=vb5ggqfc7jdjdb0tnekg1tenpi; security=medium
19 Connection: keep-alive
```

**Response**  
Pretty Raw Hex Render

Username

Password

Login

Login failed

## 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: "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/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-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://localhost/DVWA/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: PHPSESSID=vb5ggqfc7jdjdb0tnekg1tenpi; security=high
21 Connection: keep-alive
22
23 username=admin&password=password&Login=Login&user_token=f92c762013df9ffabb7df73ebbd7fafb
```

### Invio al Repeater


```
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-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/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-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://localhost/DVWA/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: PHPSESSID=vb5ggqfc7jdjdb0tnekg1tenpi; security=high
21 Connection: keep-alive
22
23 username=Francesco&password=high&Login=Login&user_token=f92c762013df9ffabb7df73ebbd7fafb
```

## Risposta del server

**Request**  
Pretty Raw Hex

```
1 GET /DVWA/login.php HTTP/1.1
2 Host: localhost
3 Cache-Control: max-age=0
4 sec-ch-ua: "Chromium";v="131", "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://localhost
9 Upgrade-Insecure-Requests: 1
10 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
11 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
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Referer: http://localhost/DVWA/login.php
17 Accept-Encoding: gzip, deflate, br
18 Cookie: PHPSESSID=vb5ggqfc7jdjdb0tnekg1tenpi; security=high
19 Connection: keep-alive
20
21
```

**Response**  
Pretty Raw Hex Render

Username

Password

Login

Login failed

## Impossible 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-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/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-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://localhost/DVWA/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: security=impossible; PHPSESSID=0ihvn81qhu13mj9k0i2dg78ts9
21 Connection: keep-alive
22
23 username=admin&password=password&Login=Login&user_token=Sf106f7094c34a3ab3fbf7598c634826
```

### Invio al Repeater

```
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-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/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=b
    3;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://localhost/DVWA/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: security=impossible; PHPSESSID=
    58mg32im69jad7rmqms1h5p7g0
21 Connection: keep-alive
22
23 username=Francesco&password=Impossible&Login=Login&user_token=
    65b033ebb795deac81964c13ee469107
```


## Risposta del server

### Request

```
1 GET /DVWA/login.php HTTP/1.1
2 Host: localhost
3 Cache-Control: max-age=0
4 sec-ch-ua: "Chromium";v="131", "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://localhost
9 Upgrade-Insecure-Requests: 1
10 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
11 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
    ge/webp,image/apng,*/*;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://localhost/DVWA/login.php
17 Accept-Encoding: gzip, deflate, br
18 Cookie: PHPSESSID=5r761cobetacgnkg8ancsrh308; security=low
19 Connection: keep-alive
20
21
```

### Response

Pretty Raw Hex **Render**



Username

Password

Login

Login failed  
Login failed

Francesco Rinaldi