

DVWA

Dopo aver seguito i passaggi per la configurazione faccio l'accesso a DVWA

The screenshot shows the DVWA Security page. The security level is currently set to 'low'. The DVWA logo is at the top. On the left, there's a sidebar with various attack types: 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 Attacks, Authorisation Bypass, Open HTTP Redirect, Cryptography, and API. Below the sidebar, the DVWA Security menu is highlighted. The main content area has a heading 'DVWA Security' with a lock icon. It says 'Security level is currently: low.' and provides a description of what each security level means. A dropdown menu shows 'Low' is selected, with a 'Submit' button next to it. Below this, there's a link to 'View Broken Access Control Logs'. At the bottom, it shows the current session details: Username: admin, Security Level: Security Level: low, Locale: en, and SQLI DB: mysql.

Lanciamo Burpsuite, scegliamo un progetto temporaneo ed apriamo un browser, inserendo l'indirizzo della nostra DVWA 1270.0.1/DVWA e inseriamo nei campi login e password i valori «admin» e «password». Lanciamo Burpsuite, scegliamo un progetto temporaneo ed apriamo un browser, inserendo l'indirizzo della nostra DVWA. Intercettiamo la richiesta con burp.

Possiamo notare nell'ultima riga le informazioni inserite

S Burp Project Intruder Repeater View Help

Burp Suite Community Edition v2025.7.4 - Temporary Project

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

Intercept HTTP history WebSockets history Match and replace Proxy settings

Request to http://127.0.0.1:80 Open browser

Time Type Direction Method URL Status code Length

17:58:32 13 nov ... HTTP → Request POST http://127.0.0.1/DVWA/login.php

Request

Pretty Raw Hex

```

4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="139", "Not;A=Brand";v="99"
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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 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-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://127.0.0.1/DVWA/login.php
18 Accept-Encoding: gzip, deflate, br
20 Cookie: PHPSESSID=470c399e0fe01f6b7eb33a3bf7019ba7; security=low
21 Connection: keep-alive
22
23 username=admin&password=password&Login=Login&user_token=db994ccb7120cbfa3c08397909485034

```

Event log All issues

Inspector Notes

Memory: 114,6MB Disabled

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.

20 Cookie: PHPSESSID=470c399e0fe01f6b7eb33a3bf7019ba7; security=low
21 Connection: keep-alive
22
23 username=pinco&password=pallino&Login=Login&user_token=dc8c1cad6e3c77f163947b6912b82e48

Event log All issues

Memory: 114,6MB Disabled

Burp Suite Community Edition v2025.7.4 - Temporary Project

Target: http://127.0.0.1 [HTTP]

Repeater

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="139", "Not=ABrand";v="99"
5 sec-ch-u-a-mobile: 70
6 sec-ch-u-a-platform: "Linux"
7 Accept-Language: en-US,en;q=0.9
8 Origin: http://127.0.0.1
9 Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/139.0.0.0 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: ?3
15 Sec-Fetch-Dest: document
16 Referer: http://127.0.0.1/DVWA/login.php
17 Content-Encoding: gzip, deflate, br
18 Cookie: PHPSESSID=479c399e0fe01f6b7eb33a3bf7019ba7; security=low
    Connection:keep-alive
19 Content-Type:application/x-www-form-urlencoded
20 Content-Length: 1388
21
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Thu, 19 Nov 2025 17:05:28 GMT
3 Server: Apache/2.4.65 (Debian)
4 Last-Modified: Tue, 28 Nov 2009 12:00:00 GMT
5 Cache-Control: no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Encoding: gzip
9 Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: text/html;charset=utf-8
12
13 <!DOCTYPE html>
14 <html lang="en-GB">
15   <head>
16     <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
17   </head>
18   <body>
19     <div id="wrapper">
20       <div id="header">
21         <br />
22         <p>
23           
24         </p>
25         <br />
26       </div>
27     </div>
28   </body>
29 </html>
30
31
32
33
34
35
36
37
38
39
```

Inspector

Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Response headers

Done Event log All issues

1.709 bytes | 1.008 millis

Memory: 114.6MB Disabled

Damn Vulnerable Web Application (DVWA)

Burp Suite Community Edition v2025.7.4 - Temporary Project

Target: http://127.0.0.1 [HTTP]

Repeater

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="139", "Not=ABrand";v="99"
5 sec-ch-u-a-mobile: 70
6 sec-ch-u-a-platform: "Linux"
7 Accept-Language: en-US,en;q=0.9
8 Origin: http://127.0.0.1
9 Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/139.0.0.0 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: ?3
15 Sec-Fetch-Dest: document
16 Referer: http://127.0.0.1/DVWA/login.php
17 Content-Encoding: gzip, deflate, br
18 Cookie: PHPSESSID=479c399e0fe01f6b7eb33a3bf7019ba7; security=low
    Connection:keep-alive
19 Content-Type:application/x-www-form-urlencoded
20 Content-Length: 1388
21
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Thu, 19 Nov 2025 17:05:28 GMT
3 Server: Apache/2.4.65 (Debian)
4 Last-Modified: Tue, 28 Nov 2009 12:00:00 GMT
5 Cache-Control: no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Encoding: gzip
9 Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: text/html;charset=utf-8
12
13 <!DOCTYPE html>
14 <html lang="en-GB">
15   <head>
16     <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
17   </head>
18   <body>
19     <div id="wrapper">
20       <div id="header">
21         <br />
22         <p>
23           
24         </p>
25         <br />
26       </div>
27     </div>
28   </body>
29 </html>
30
31
32
33
34
35
36
37
38
39
```

Inspector

Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Response headers

Done Event log All issues

1.709 bytes | 1.008 millis

Memory: 114.6MB Disabled

Damn Vulnerable Web Application (DVWA)