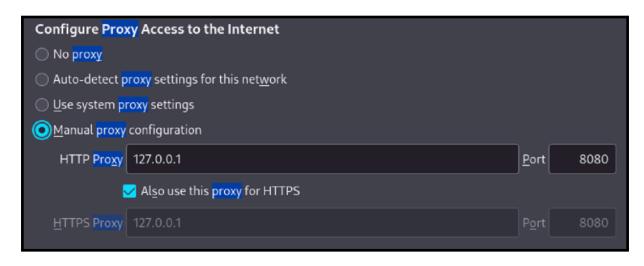
M2 W8D3

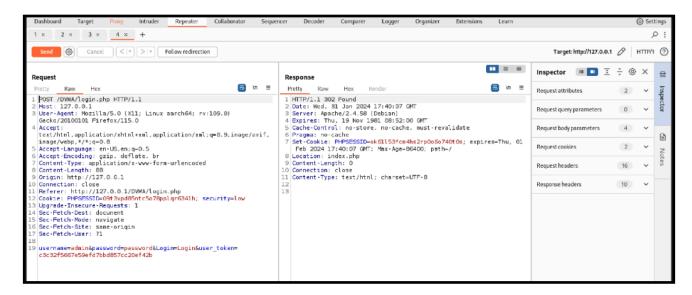
Avviare Burp Suite e configurare il browser per utilizzare il proxy di Burp.



Utilizzare la funzione di "Intruder" di Burp per effettuare attacchi mirati sui possibili punti vulnerabili.



Utilizzare la funzione di "Repeater" di Burp per modificare e ripetere le richieste specifiche all'applicazione web.



```
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 security=medium&seclev_submit=Submit&user_token=
00b50f0llb64eabl2d02a8l02df09620
```

17 Sec-Fetch-User: ?1
18
19 security=low&seclev_submit=Submit&user_token=
1b85257eb5d1alc0212fb16e09a80366

Modifica del livello di sicurezza da "medium" a "low"

Response "200 OK"
Richiesta HTTP completata con successo.

```
Response
Pretty
       Raw
                                                                  In ≡
                  Hex
 1 HTTP/1.1 200 OK
 2 Date: Wed, 31 Jan 2024 18:49:12 GMT
   Server: Apache/2.4.58 (Debian)
4 Expires: Tue, 23 Jun 2009 12:00:00 GMT 5 Cache-Control: no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 4652
9 Connection: close
10 Content-Type: text/html;charset=utf-8
12 <!DOCTYPE html>
14 <html lang="en-GB">
16
        <meta http-equiv="Content-Type" content="text/html;</pre>
       charset=UTF-8" />
18
         DVWA Security :: Damn Vulnerable Web Application (DVWA)
       </title>
20
       <link rel="stylesheet" type="text/css" href="
dvwa/css/main.css" />
21
22
        <link rel="icon" type="\image/ico" href="favicon.ico" />
23
       <script type="text/javascript" src="dvwa/js/dvwaPage.js">
25
```