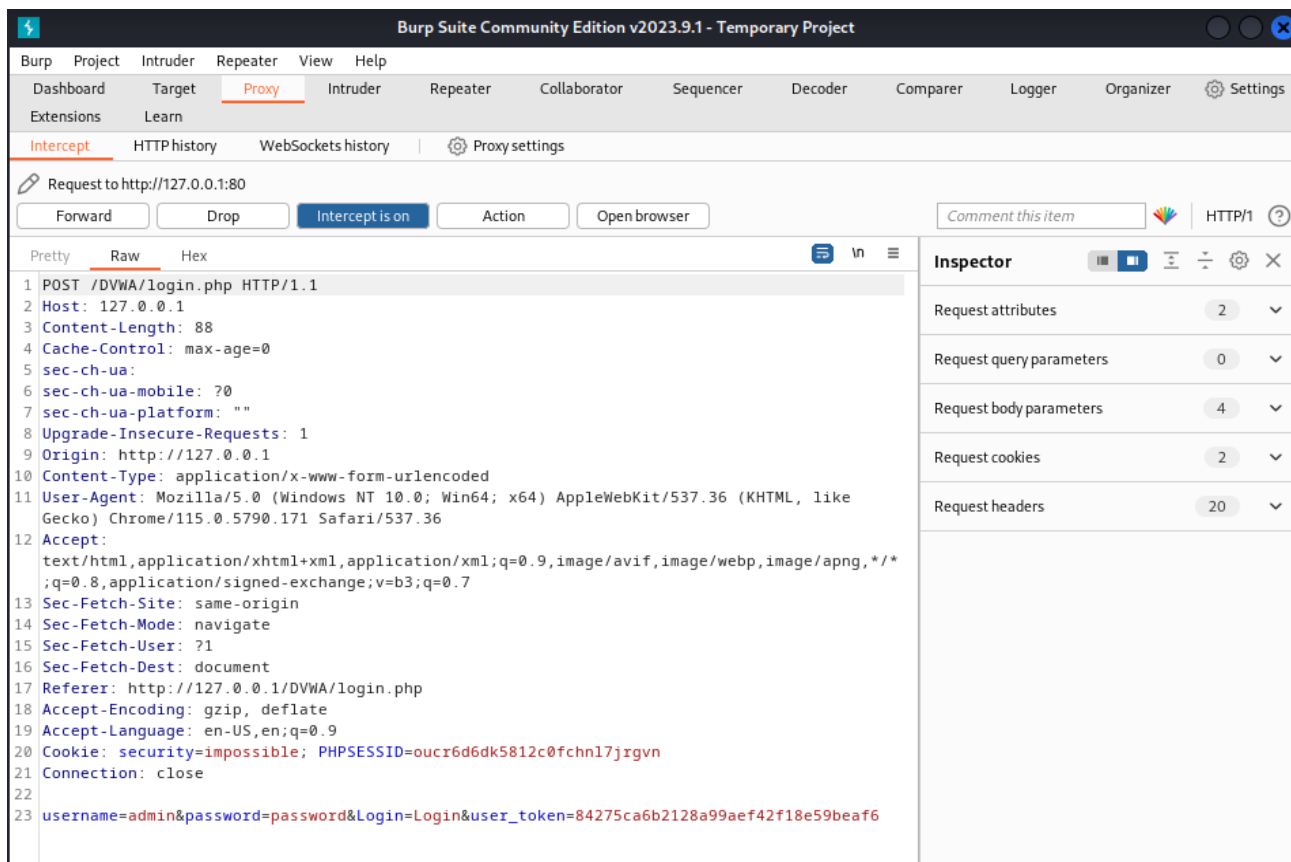


La DVWA è stata installata e configurata con successo.



Burp suite è un proxy (fa da filtro), progettata per testare la sicurezza delle applicazioni web. In questo caso abbiamo aperto l'applicazione web DVWA su Chromium, e abilitando "Intercept" e premendo "Forward", siamo riusciti a vedere cosa accade al sito quando io mi connetto. Alla prima riga abbiamo il metodo POST, che è un'operazione nel protocollo HTTP utilizzata per inviare dati da un client (come un browser) a un

server. A differenza del metodo GET, i dati non sono visibili nell'URL ma vengono inviati nel corpo della richiesta.

Successivamente dal browser abbiamo digitato le nostre credenziali, che sono risultate visibili su Burp suite.

The screenshot displays the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane on the left shows an HTTP 1.1 POST request to `/DVWA/login.php`. The 'Response' pane on the right shows the corresponding HTML response. The 'Inspector' pane on the far right provides a summary of the request and response attributes.

Request:

```
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Cache-Control: max-age=0
4 sec-ch-ua:
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: ""
7 Upgrade-Insecure-Requests: 1
8 Origin: http://127.0.0.1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
10 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
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: http://127.0.0.1/DVWA/login.php
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: security=impossible; PHPSESSID=oucr6d6dk5812c0fchnl7jrgvn
19 Connection: close
20
21
```

Response:

```
50 <input type="password" class="
51 loginInput" AUTOCOMPLETE="off"
52 size="20" name="password">
53 <br />
54 <br />
55 <p class="submit">
56 <input type="submit" value="
57 Login" name="Login">
58 </p>
59 </fieldset>
60
61 <input type='hidden' name='
62 user_token' value='
63 2166a719d1ae8252856508523d908ef9'
64 />
65 </form>
66
67 <br />
68
69 <div class="message">
70 Login failed
71 </div>
72
73 <br />
```

Inspector:

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 2
- Request headers: 18
- Response headers: 9

Abbiamo provato a digitare credenziali errate. Come ci aspettavamo con le credenziali errate non riusciamo ad entrare, infatti nel body della http response (riga 63 di destra) leggiamo «Login failed».