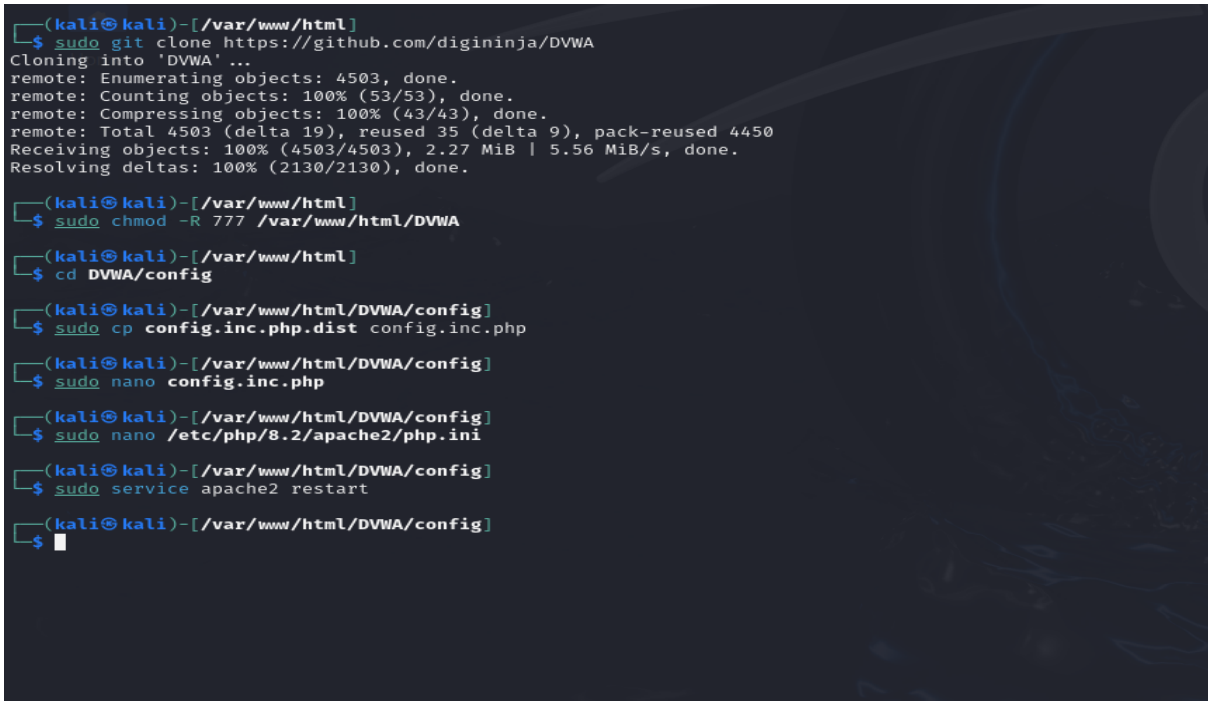
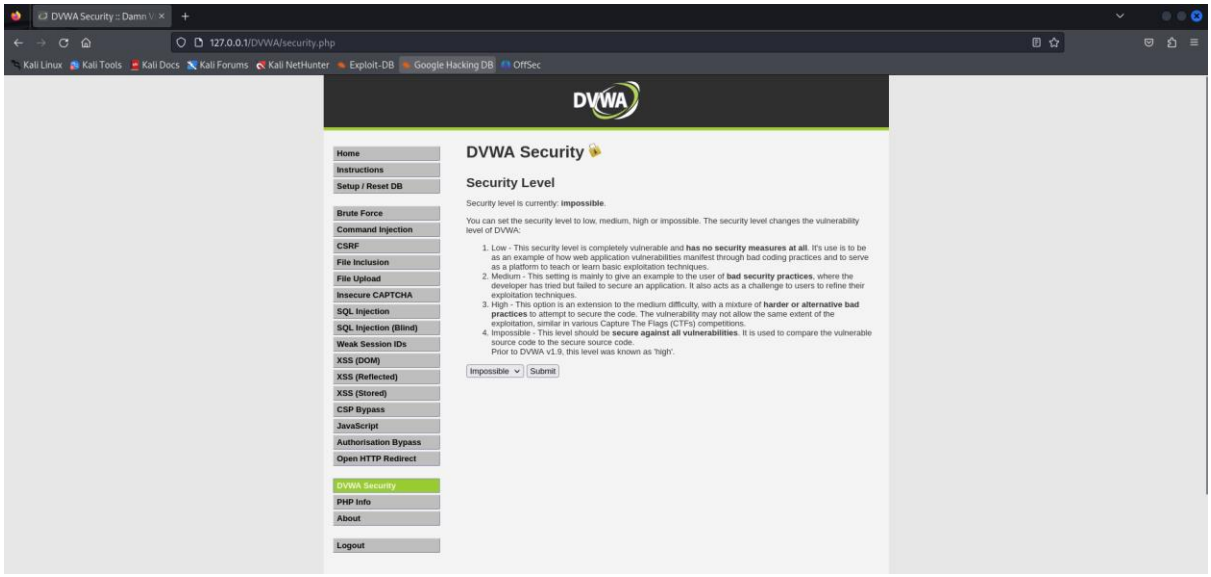
REPORT_TEAM4

Comandi per creare una DWVA:

ovvero una damn vulnerable web application in Kali Linux. La DVWA ci sarà molto utile per i nostri test.

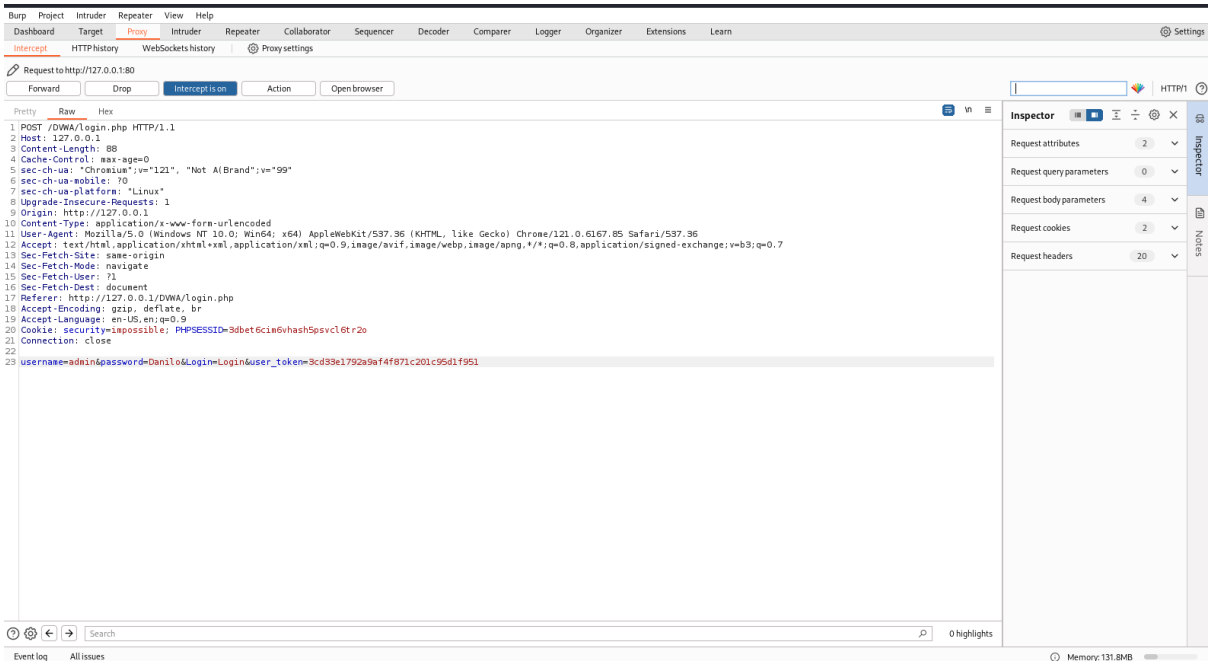


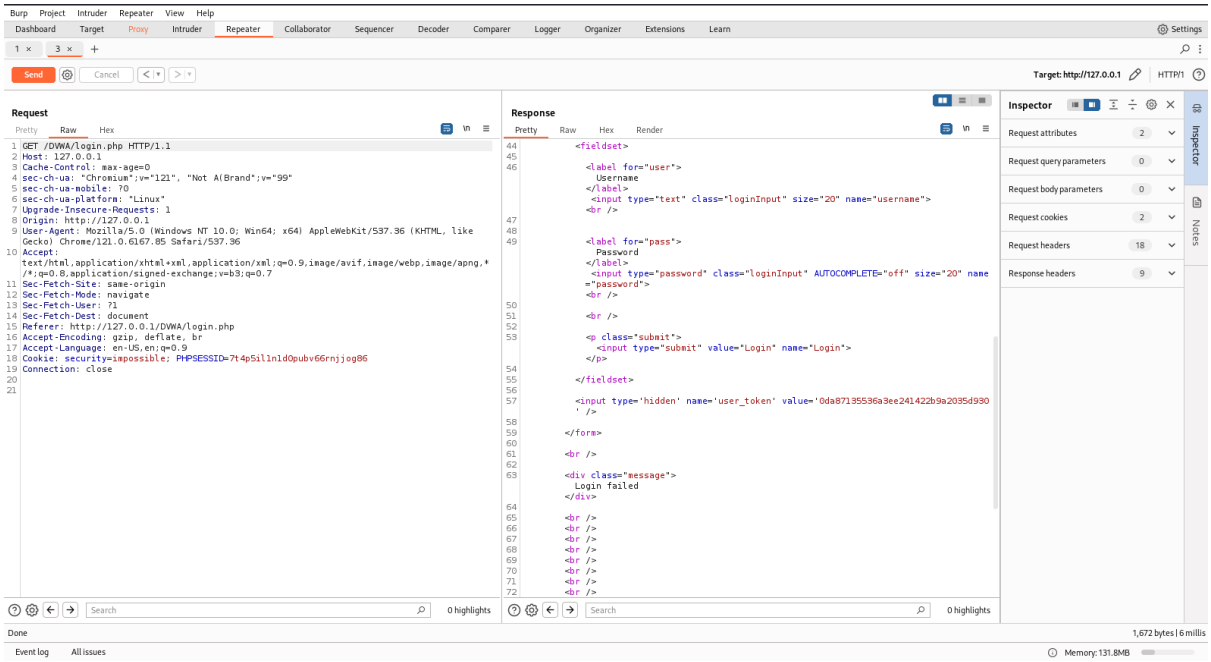
Risposta del codice



Prova con burpsuite:

Cerchiamo di alterare i dati inseriti e procediamo con l'invio del form usando delle credenziali che sappiamo essere incorrette. Prima di procedere con la trasmissione, utilizziamo il tasto destro e scegliamo l'opzione "send to repeater". Dopo aver premuto il pulsante "send" per inviare i dati di accesso e aver seguito il reindirizzamento, otteniamo il risultato previsto: l'accesso non viene concesso con le credenziali sbagliate. Questo fallimento è confermato nel contenuto della risposta HTTP, dove troviamo il messaggio "Login failed".


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Request to http://127.0.0.1:80
Forward Drop Intercept is on Action Open browser
HTTP/1
Pretty Raw Hex
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 88
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
12 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
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
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
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security=impossible; PHPSESSID=3dbet6cim6vhash5psvcl6tr2o
21 Connection: close
22
23 username=admin&password=Danilo&Login=Login&user_token=3cd33e1792a9af4f871c201c95d1f951
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 4
Request cookies 2
Request headers 20
Search 0 highlights
Event log All issues
Memory: 131.8MB


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
1 × 3 ×
Send Cancel
Target: http://127.0.0.1
HTTP/1
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="121", "Not A(Brand";v="99"
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: "Linux"
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/121.0.6167.85 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, br
17 Accept-Language: en-US,en;q=0.9
18 Cookie: security=impossible; PHPSESSID=7t4p5ilnldOpubv66rnjjog86
19 Connection: close
20
21
Response
Pretty Raw Hex Render
44 <fieldset>
45
46 <label for="user">
Username
</label>
<input type="text" class="loginInput" size="20" name="username">

47
48
49 <label for="pass">
Password
</label>
<input type="password" class="loginInput" AUTOCOMPLETE="off" size="20" name="password">

50
51
52
53
<input type="submit" value="Login" name="Login">

54
55 </fieldset>
56
57 <input type='hidden' name='user_token' value='0da87135536a3ee241422b9a2035d930' />
58
59 </form>
60
61
62
63
Login failed

64
65
66
67
68
69
70
71
72
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 18
Response headers 9
Search 0 highlights
Search 0 highlights
Done
1,672 bytes | 6 millis
Event log All issues
Memory: 131.8MB