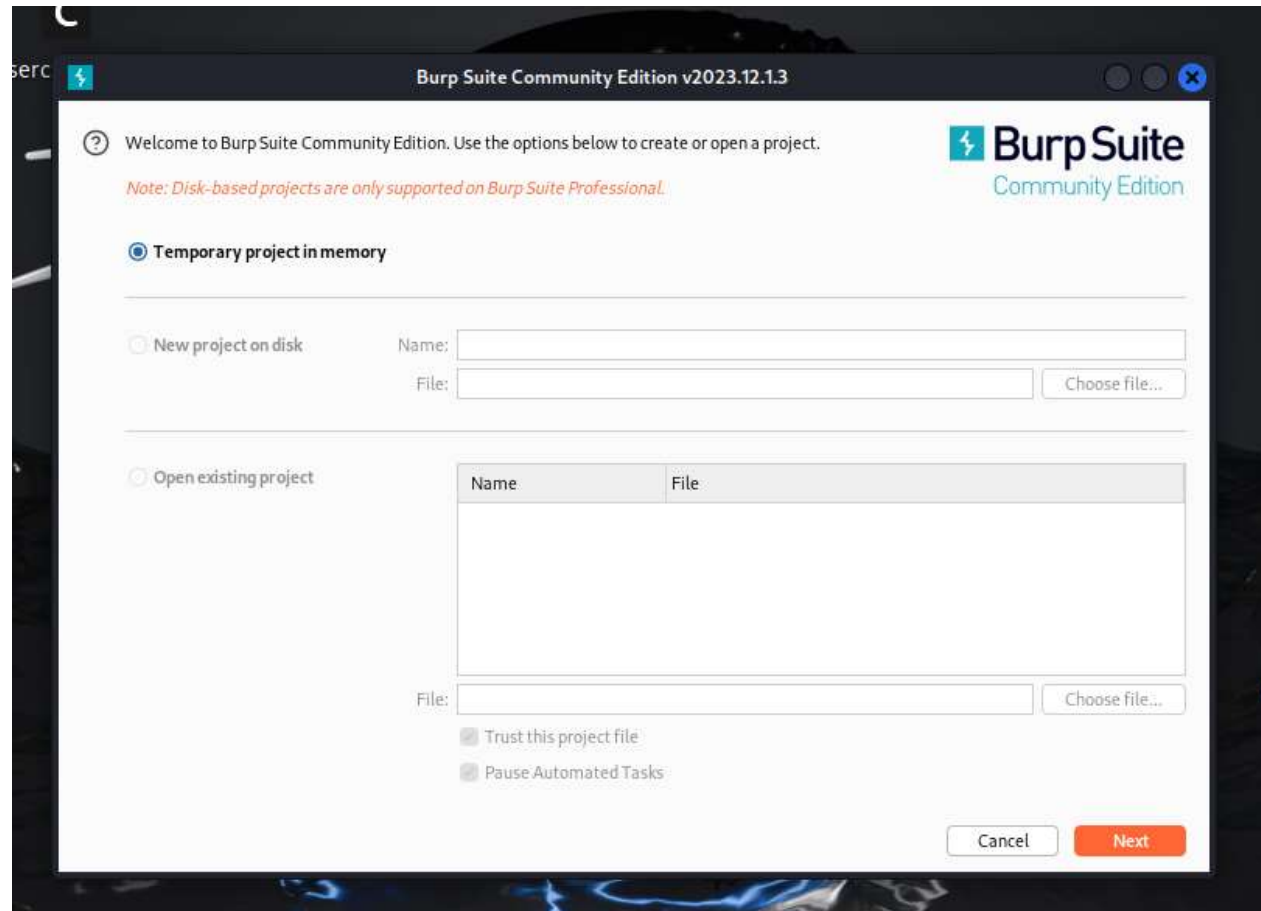


## LABORATORIO EPICODE

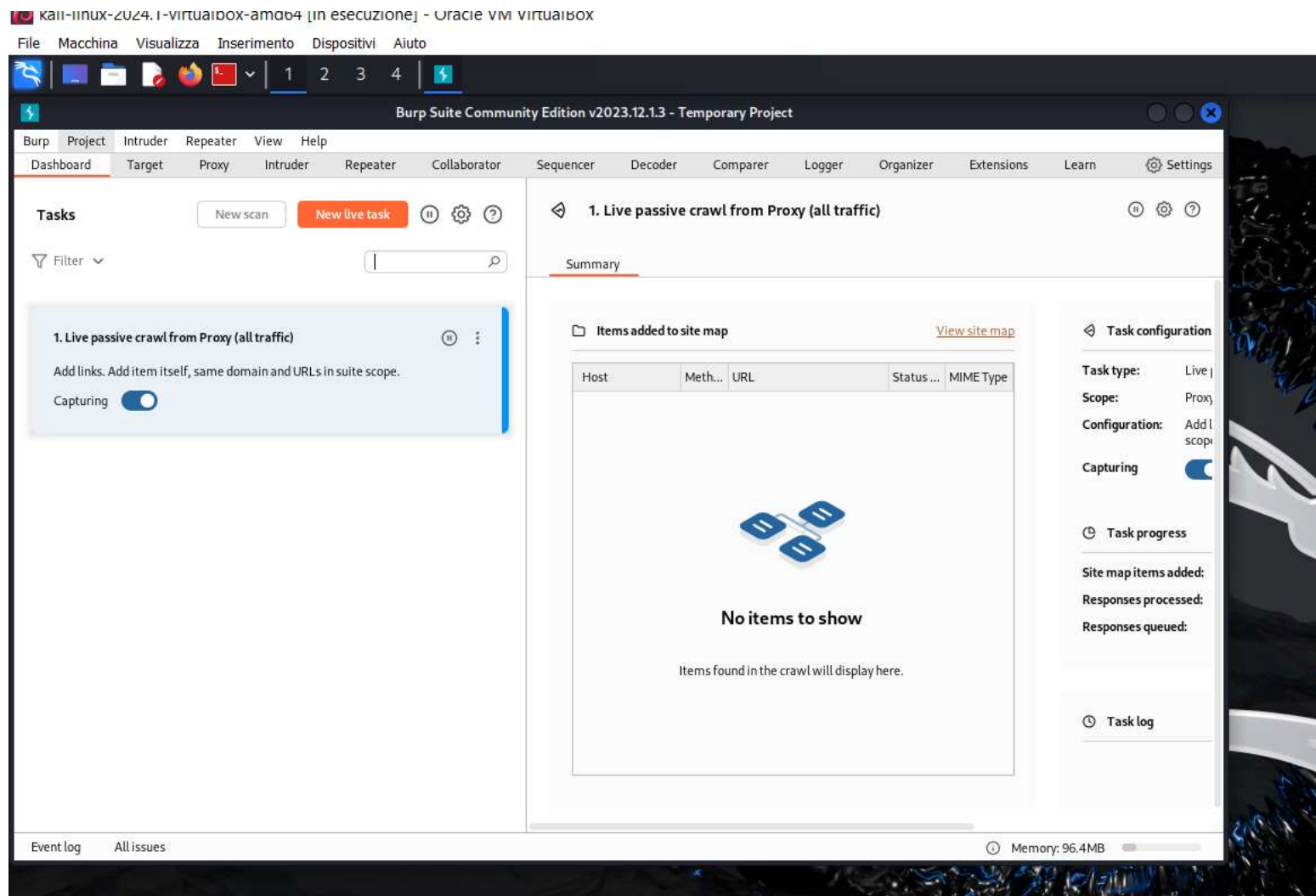
**Traccia:** Nella lezione pratica di oggi vedremo come configurare una DVWA – ovvero damn vulnerable web application in Kali Linux. La DVWA ci sarà molto utile per i nostri test.

Nel laboratorio di oggi abbiamo provato ad installare una DVWA per poter effettuare dei test, nello specifico con BurpSuite in modo da poter rintracciare credenziali di Login sulla DVWA stessa e provare a modificare lo user e la password. Di seguito i passaggi per intercettare e di seguito effettuare le modifiche opportune.

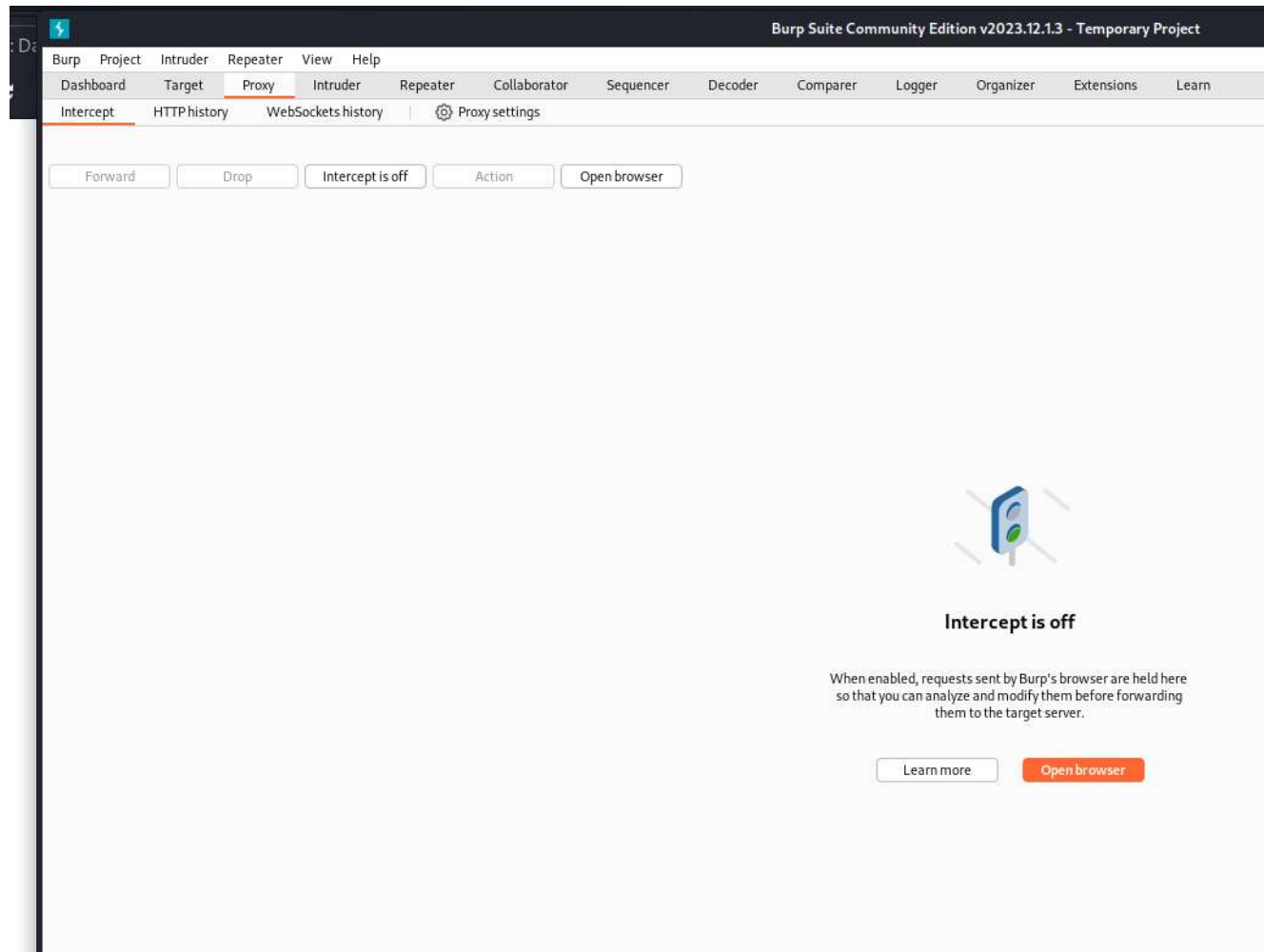
### STEP 1: Aprire BurpSuite



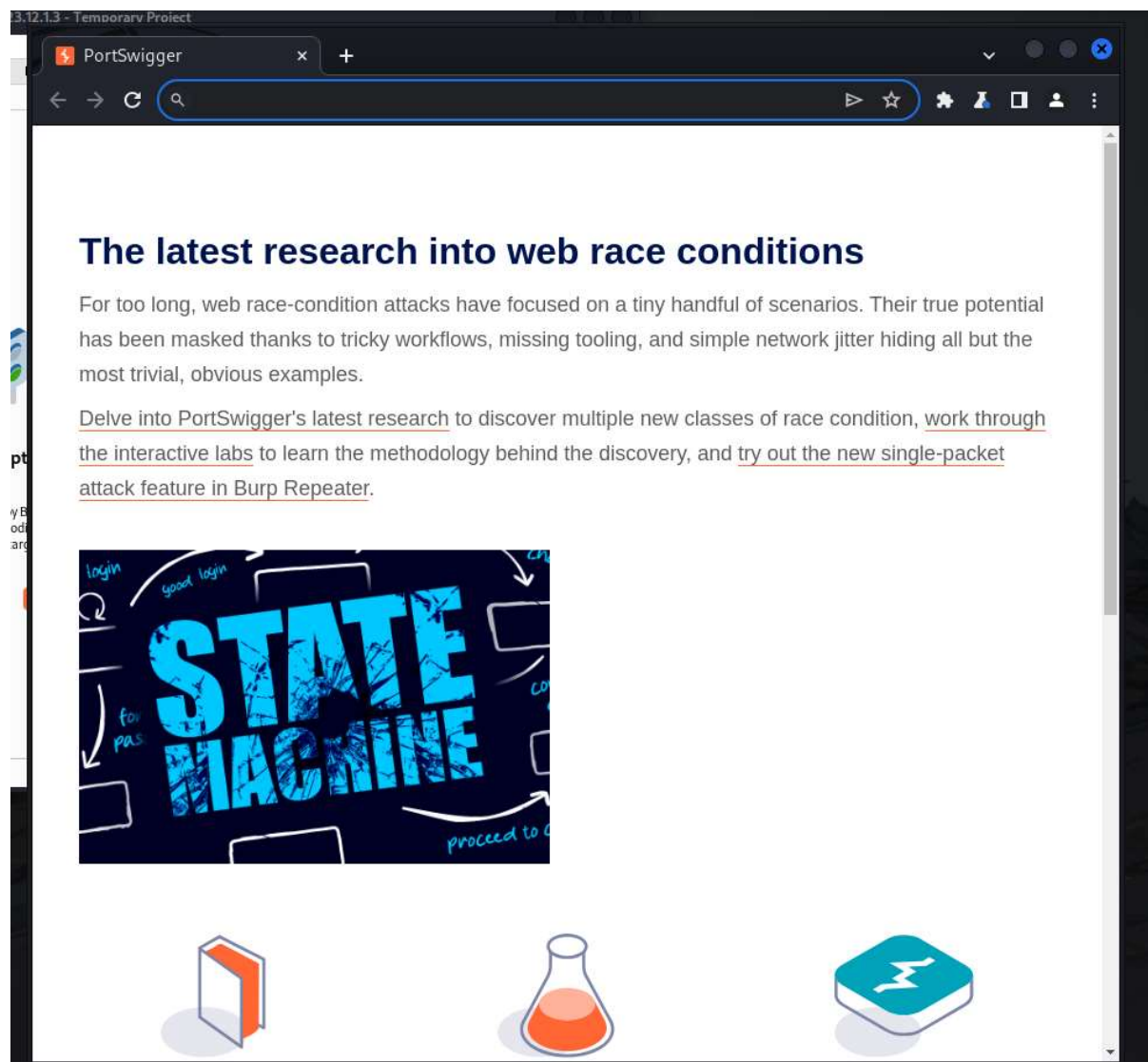
## STEP 2: Avviare BurpSuite



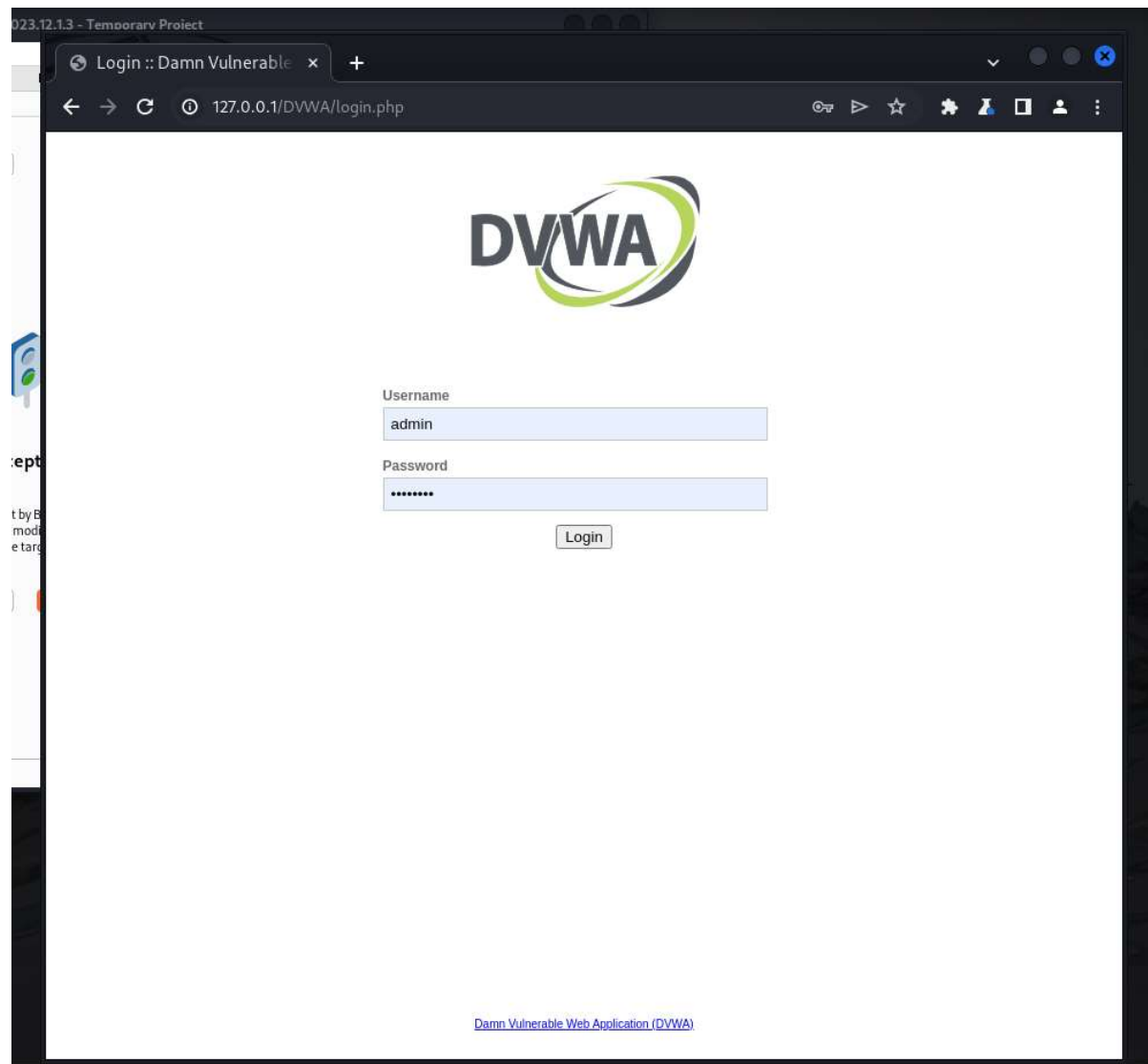
**STEP 3:** Cliccare su Proxy e aprire il browser per poter successivamente intercettare



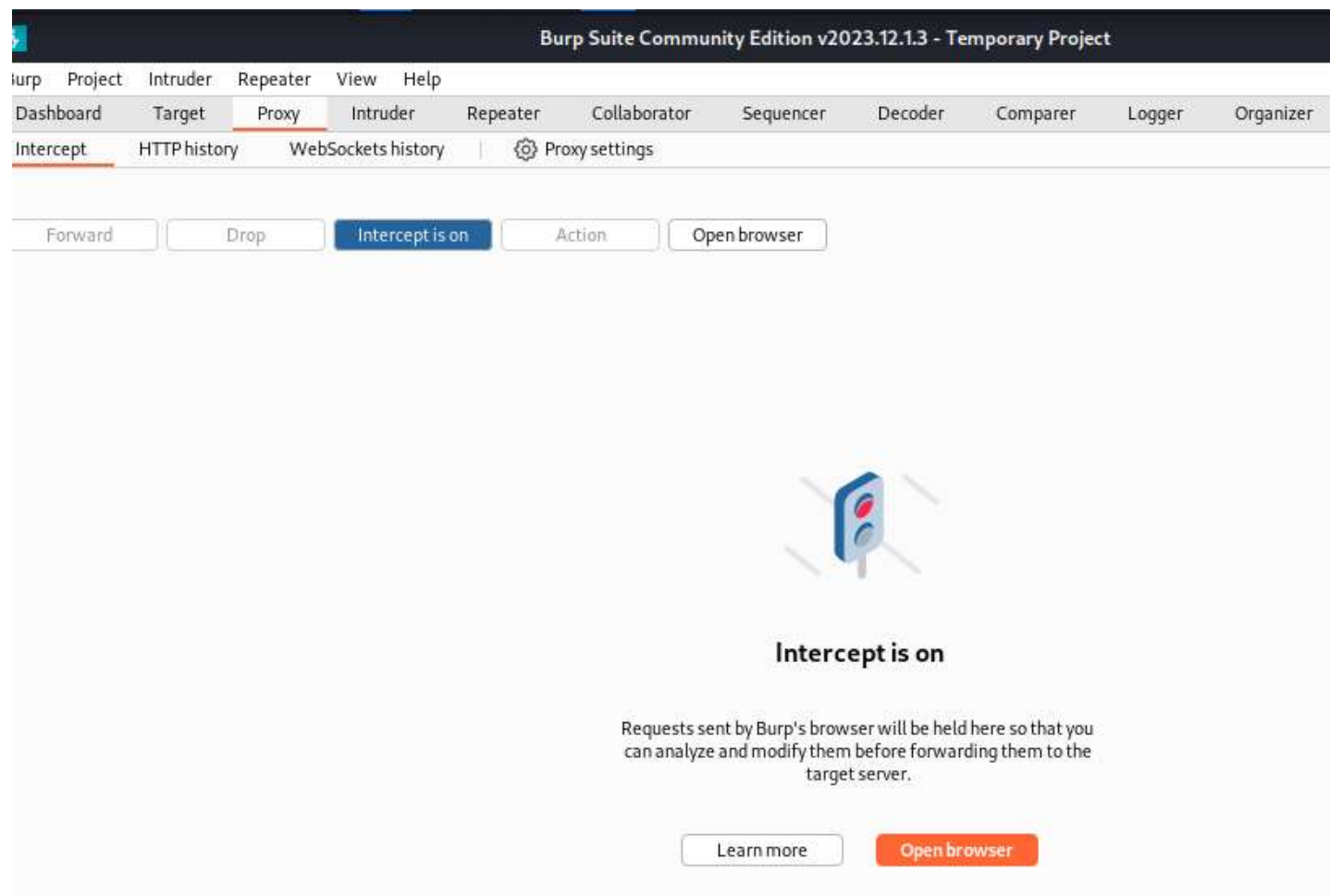
**STEP 4:** Inserire il browser nella barra di ricerca



**STEP 6:** Ricercare la pagina della DVWA sull'indirizzo 127.0.0.1/DVWA/login.php



## STEP 7: Attivare l'intercettazione di BurpSuite



**STEP 9:** Effettuare il login dalla pagina della DVWA ed ecco che vengono intercettati i dati visualizzando lo user e la password in chiaro

The screenshot displays the Burp Suite interface with the 'Proxy' tab selected. The 'Intercept' sub-tab is active, showing a request to `http://127.0.0.1:80`. The 'Intercept is on' button is highlighted. The request details are shown in the 'Pretty' view, and the 'Inspector' panel on the right is open, showing the 'Request body' tab.

**Request details:**

- Method: POST
- URL: /DVWA/login.php
- Host: 127.0.0.1
- Content-Length: 88
- Cache-Control: max-age=0
- sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"
- sec-ch-ua-mobile: ?0
- sec-ch-ua-platform: "Linux"
- Upgrade-Insecure-Requests: 1
- Origin: http://127.0.0.1
- Content-Type: application/x-www-form-urlencoded
- 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
- 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
- Sec-Fetch-Site: same-origin
- Sec-Fetch-Mode: navigate
- Sec-Fetch-User: ?1
- Sec-Fetch-Dest: document
- Referer: http://127.0.0.1/DVWA/login.php
- Accept-Encoding: gzip, deflate, br
- Accept-Language: en-US,en;q=0.9
- Cookie: security=low; PHPSESSID=kbs3g6suk7jv16ab7s7inmrn47
- Connection: close

**Request body (application/x-www-form-urlencoded):**

```
username=admin&password=password&Login=Login&user_token=82722f94320e40ffe1c8091a89701417
```

## STEP 10: Modifichiamo le credenziali

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action Open browser

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=low; PHPSESSID=kbs3g6suk7jv16ab7s7inmrn47
21 Connection: close
22
23 username=ciao&password=ciao&Login=Login&user_token=82722f94320e40ffe1c8091a89701417
```

Inspector

- Request attributes
- Request query parameters
- Request body parameters
- Request cookies
- Request headers



1 x2 x3 x4 x5 x+

SendCancel<>

Request

PrettyRawHex

1 GET /DWA/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/DWA/login.php

16 Accept-Encoding: gzip, deflate, br

17 Accept-Language: en-US,en;q=0.9

18 Cookie: security=low; PHPSESSID=kbs3g6suk7jv16ab7s7inm47

19 Connection: close

20

21

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK

2 Date: Tue, 23 Apr 2024 13:55:02 GMT

3 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: 1342

9 Connection: close

10 Content-Type: text/html; charset=utf-8

11

12 <!DOCTYPE html>

13

14 <html lang="en-GB">

15

16 <head>

17

18 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

19

20 <title>

21 Login :: Damn Vulnerable Web Application (DVWA)

22 </title>

23

24 <link rel="stylesheet" type="text/css" href="dvwa/css/login.css" />

25

26 </head>

27

28 <body>

29

30 <div id="wrapper">

31

32 <div id="header">

33

34 <br />

35

36 <p>

37 

38 </p>

39

40 <br />

41

42 </div>

43 <!--div id="header"-->

0 highlights0 highlights