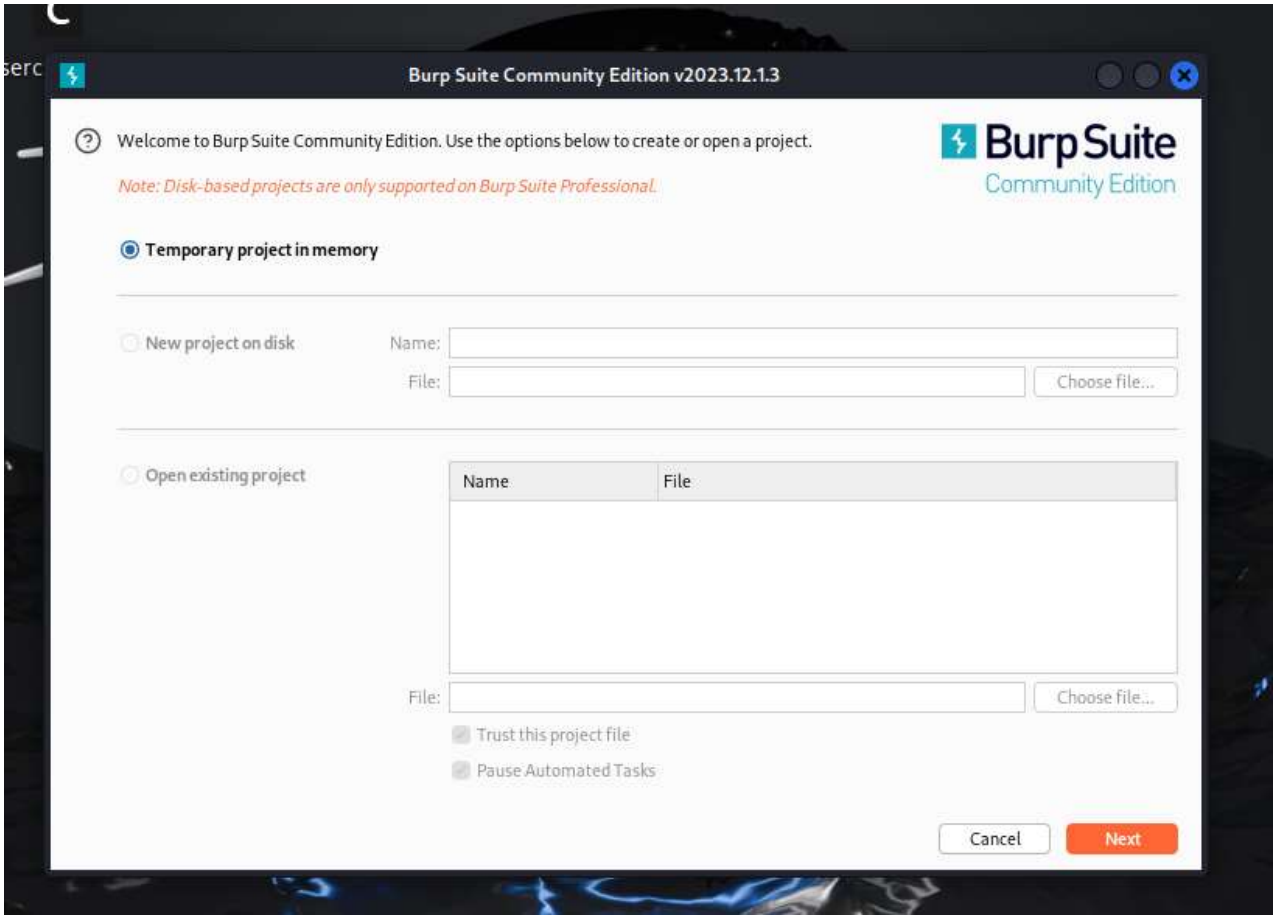
LABORATORIO EPICODE

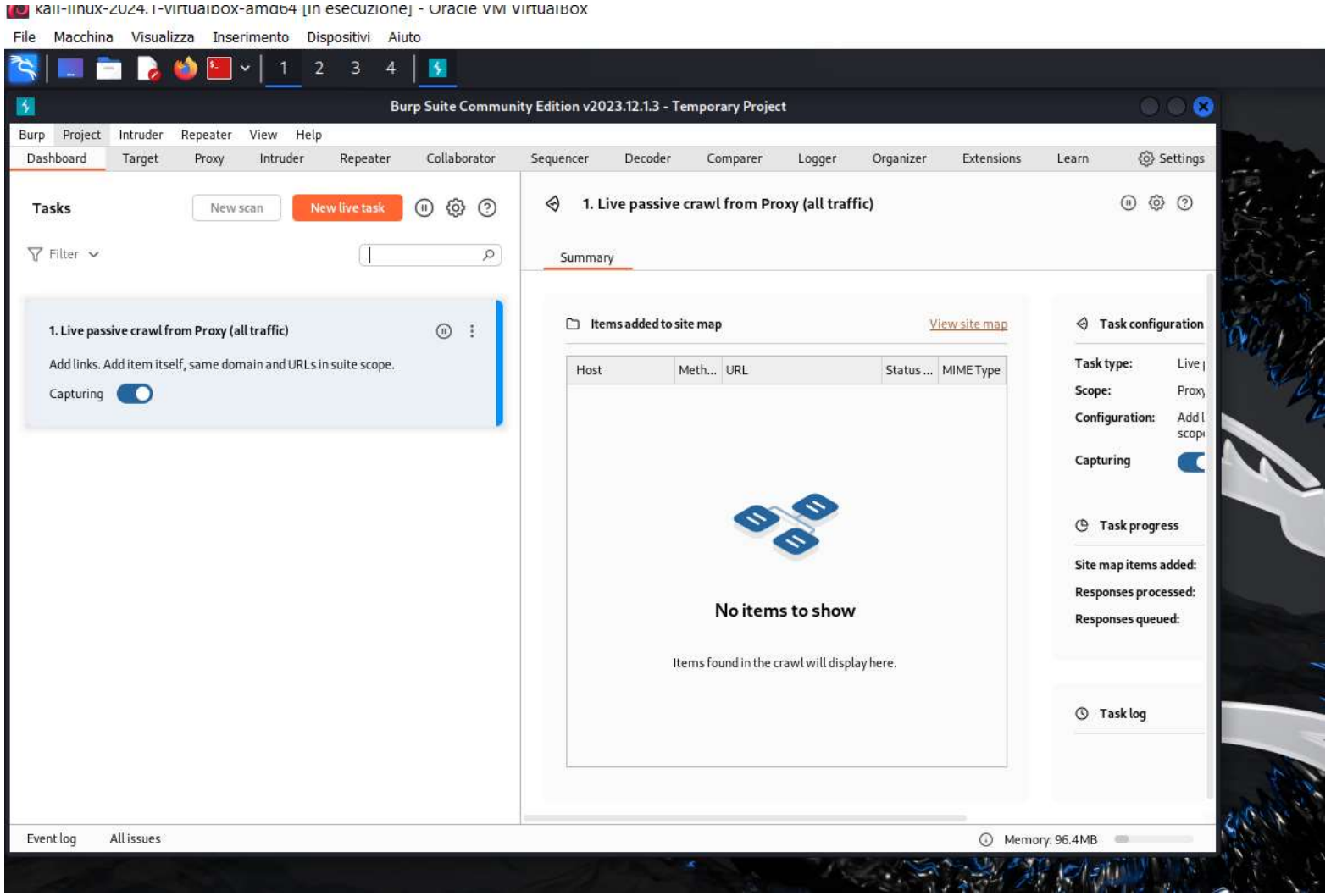
Traccia: Nella lezione pratica di oggi vedremo come configurare una DVWA – ovvero damn vulnerable web application in Kali Linux. La DVWA ci sarà molto utile per i nostri test.

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.

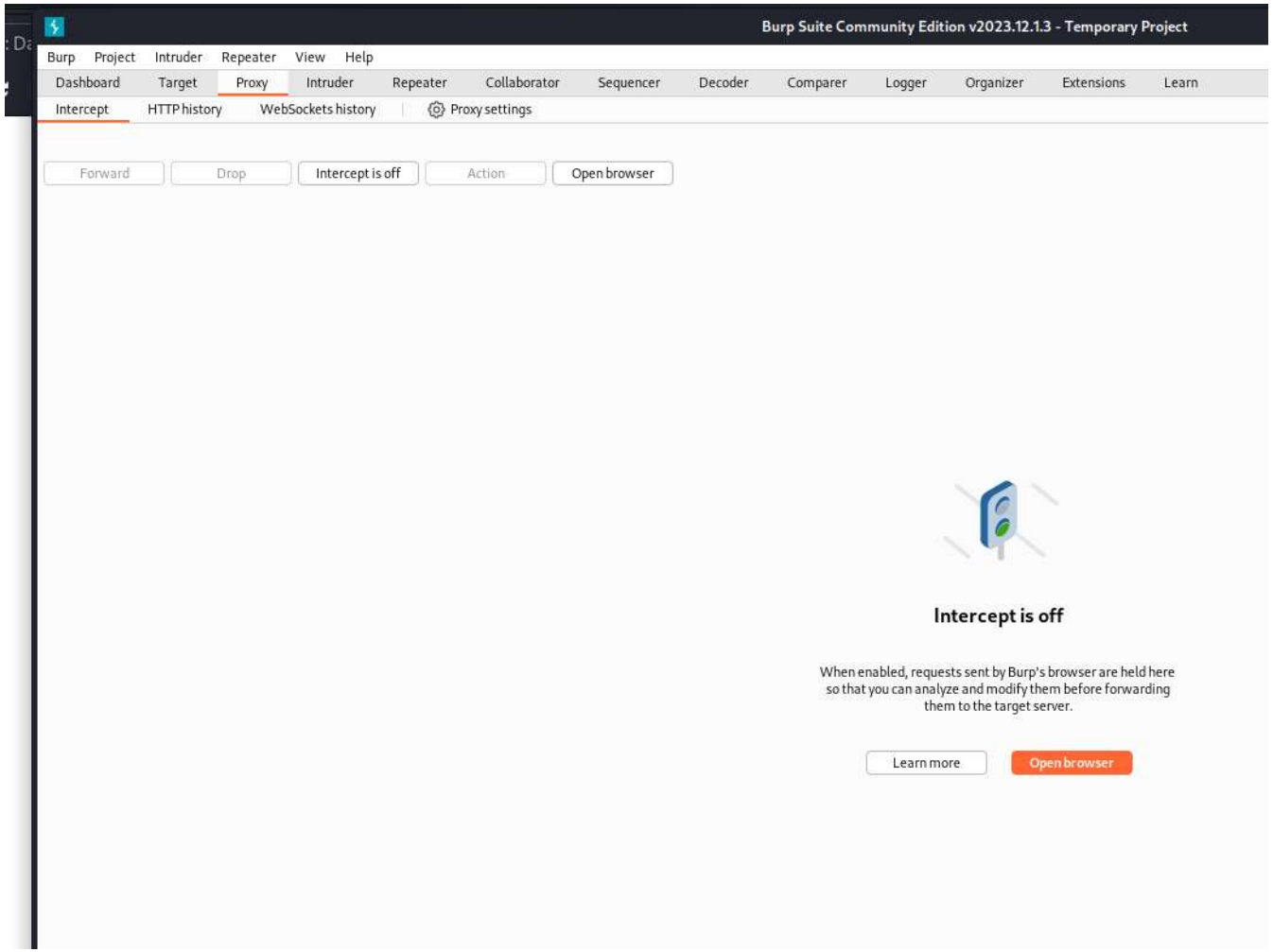
STEP 1: Aprire BurpSuite



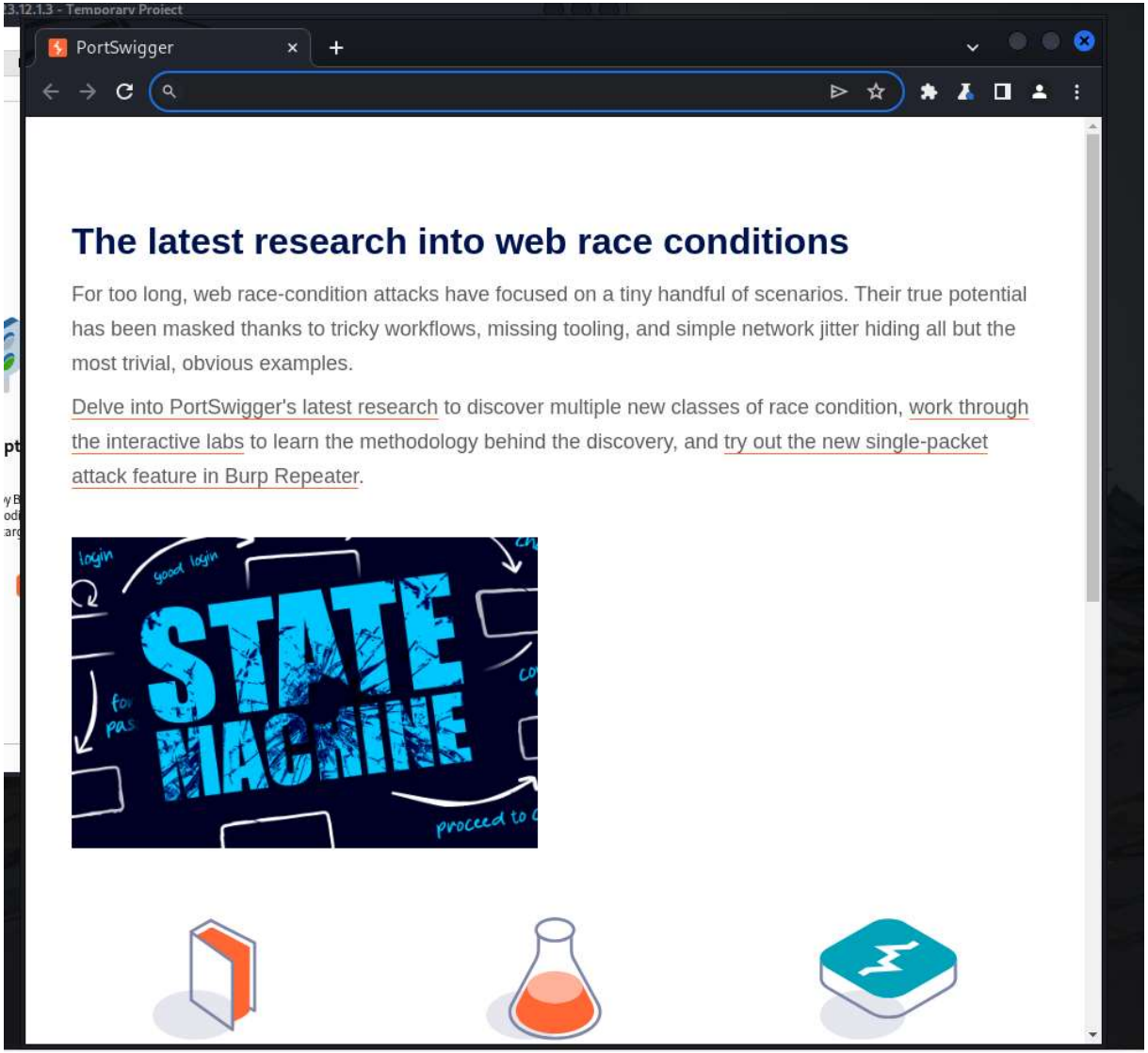
STEP 2: Avviare BurpSuite



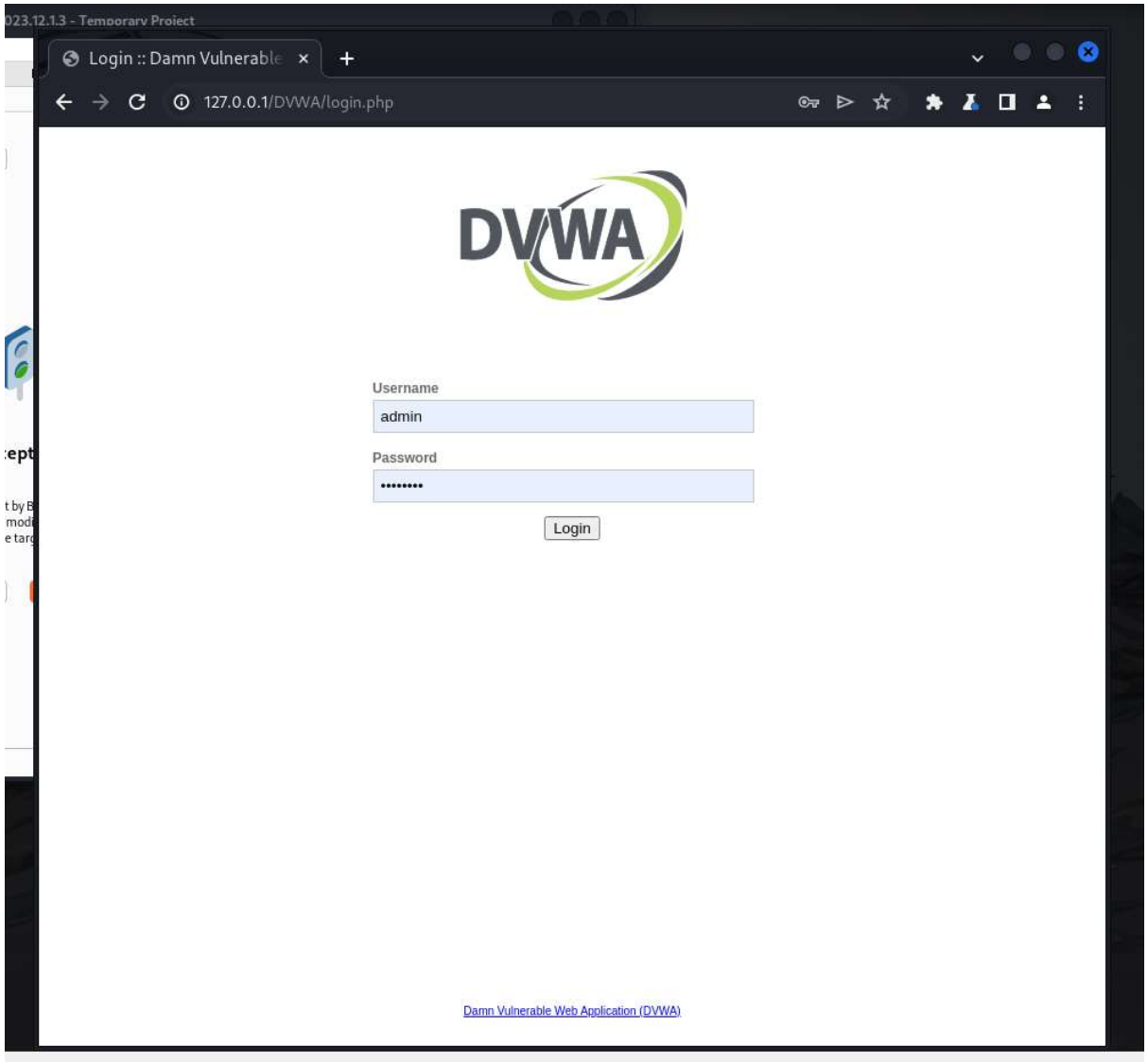
STEP 3: Cliccare su Proxy e aprire il browser per poter successivamente intercettare



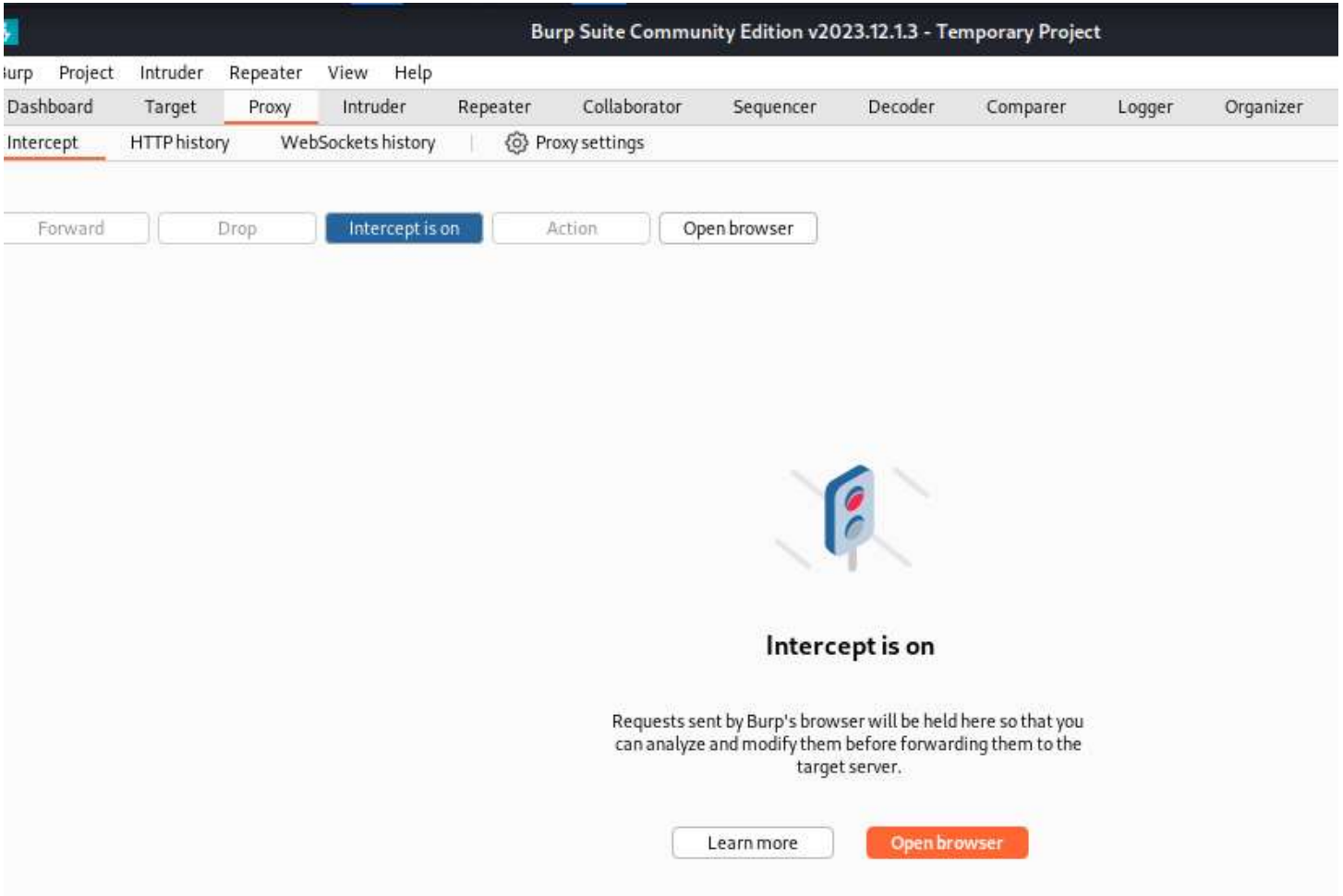
STEP 4: Inserire il browser nella barra di ricerca



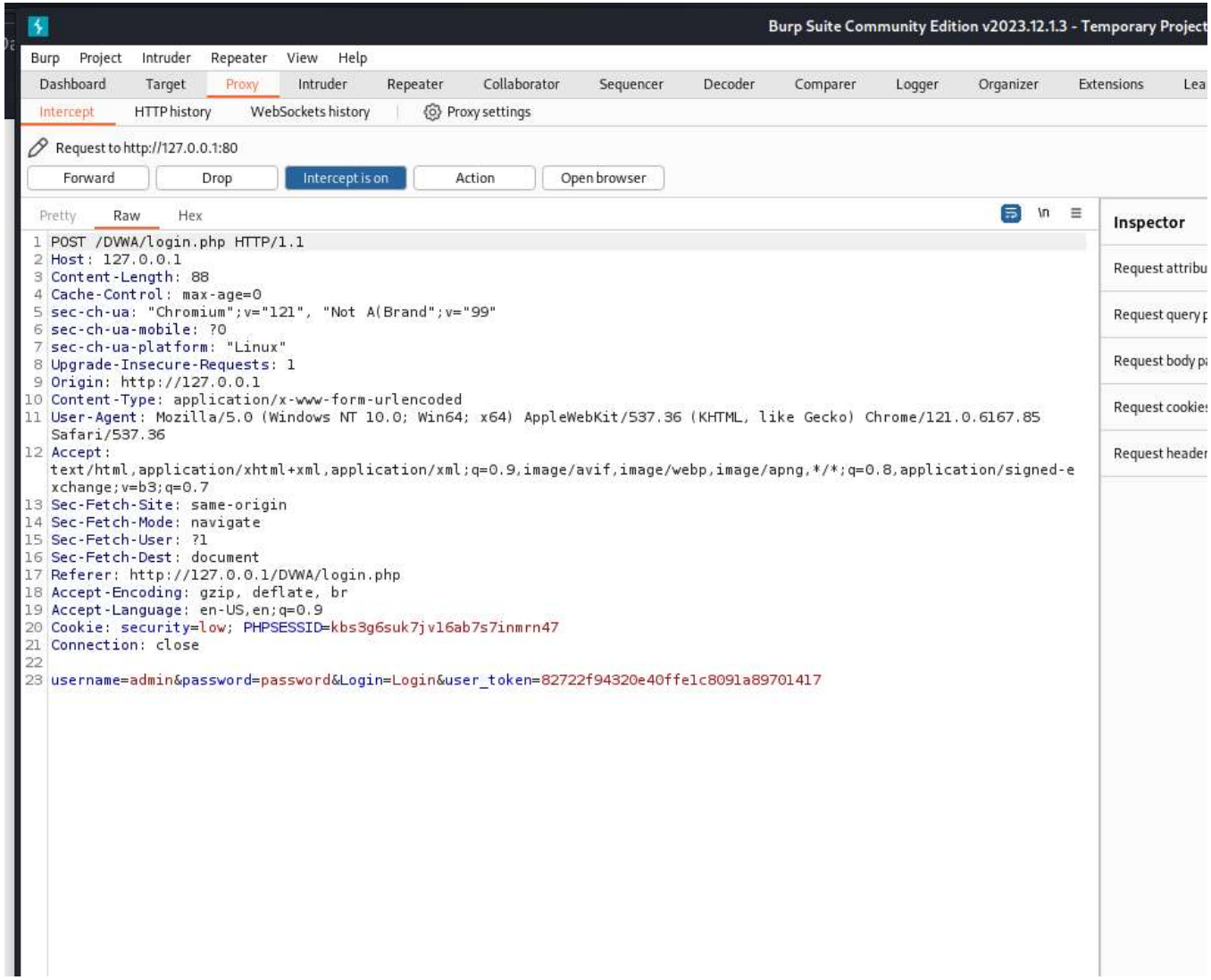
STEP 6: Ricercare la pagina della DVWA sull'indirizzo 127.0.0.1/DVWA/login.php



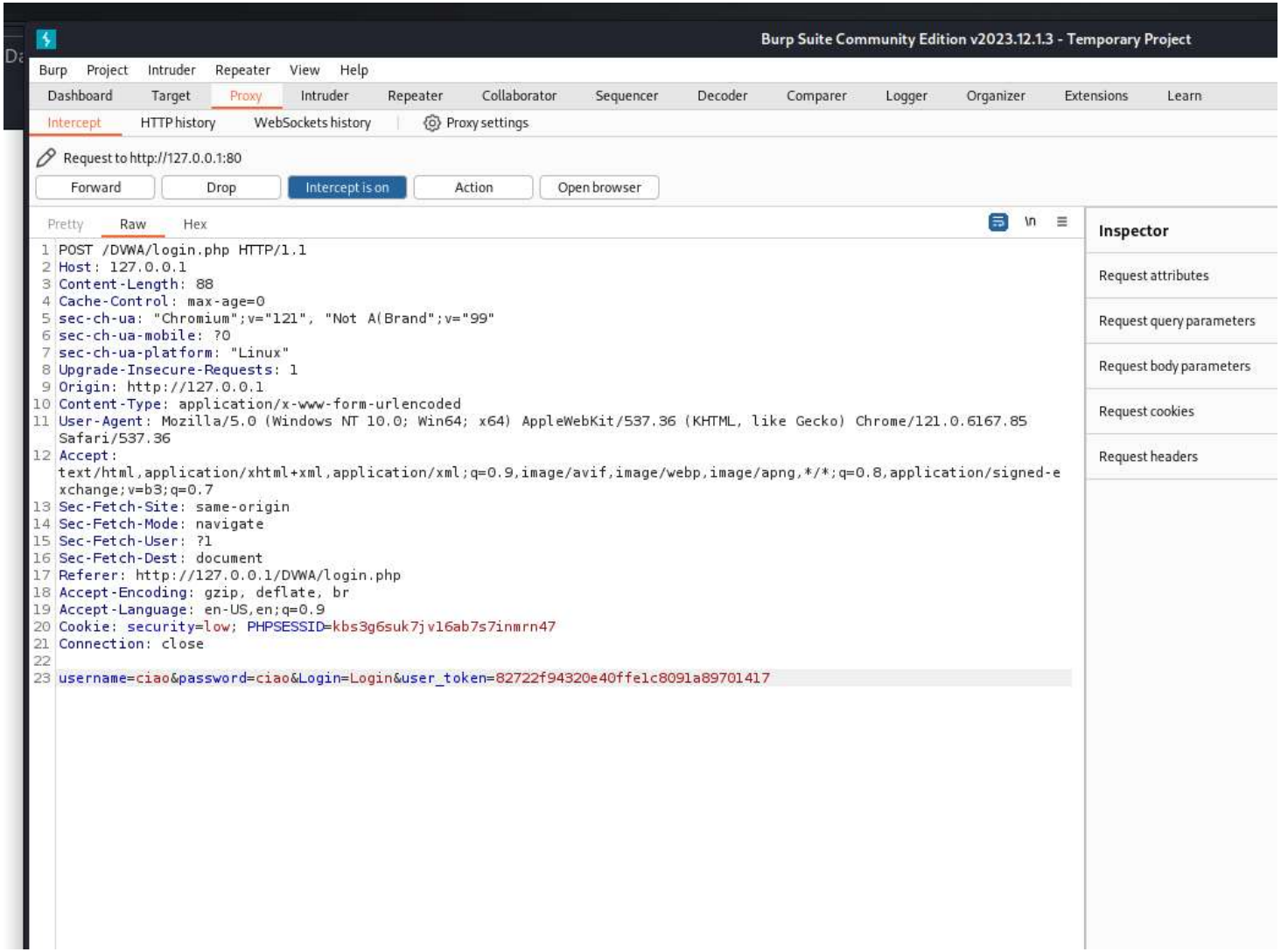
STEP 7: Attivare l'intercettazione di BurpSuite

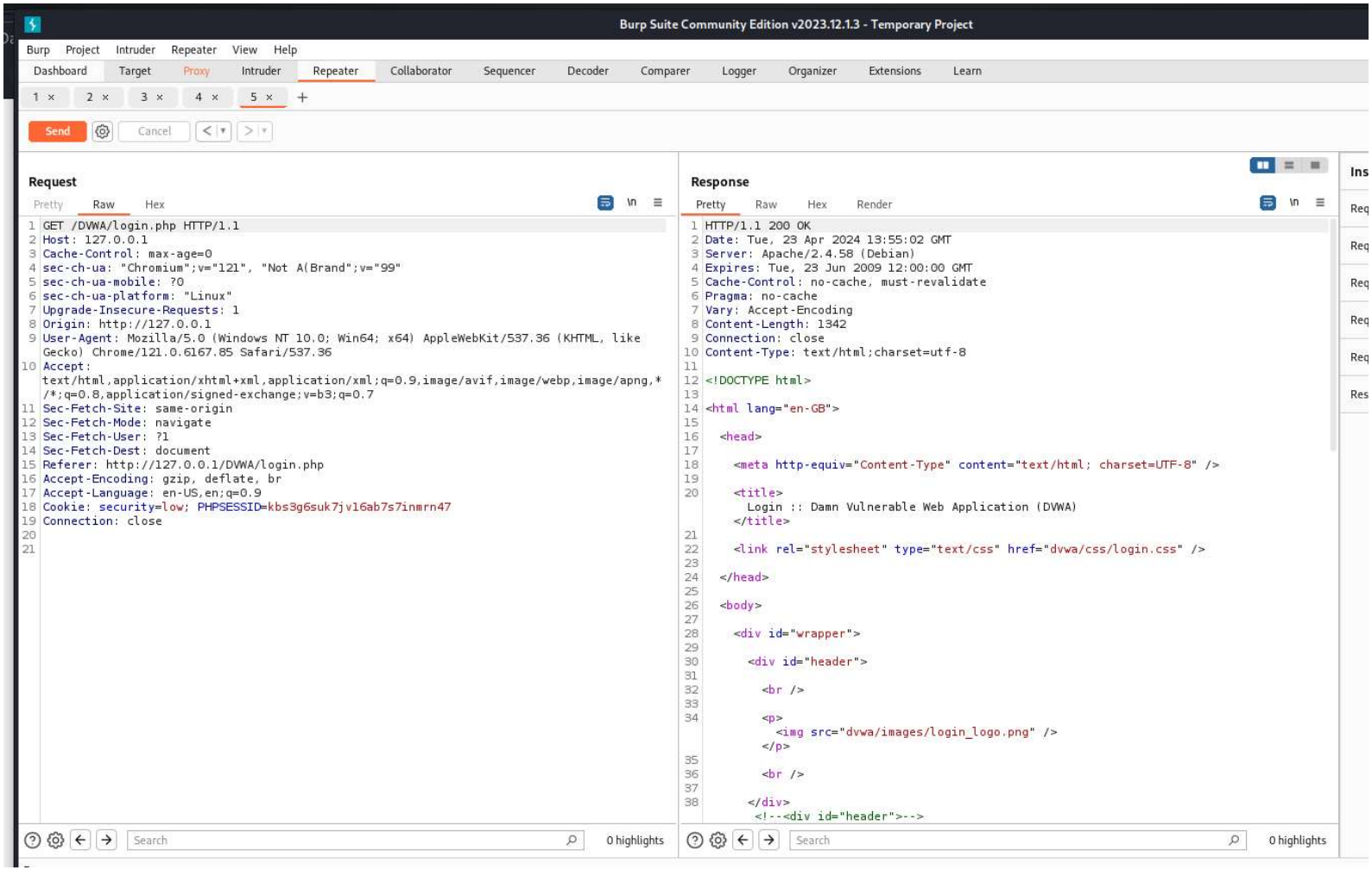


STEP 9: Effettuare il login dalla pagina della DVWA ed ecco che vengono intercettati i dati visualizzando lo user e la password in chiaro



STEP 10: Modifichiamo le credenziali




Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 × 2 × 3 × 4 × 5 ×
Send Cancel
Request
Pretty Raw Hex
GET /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
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
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
Search
0 highlights
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Date: Tue, 23 Apr 2024 13:55:02 GMT
Server: Apache/2.4.58 (Debian)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1342
Connection: close
Content-Type: text/html;charset=utf-8
<!DOCTYPE html>
<html lang="en-GB">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>
Login :: Damn Vulnerable Web Application (DVWA)
</title>
<link rel="stylesheet" type="text/css" href="dvwa/css/login.css" />
</head>
<body>

<!--<div id="header">-->
Search
0 highlights