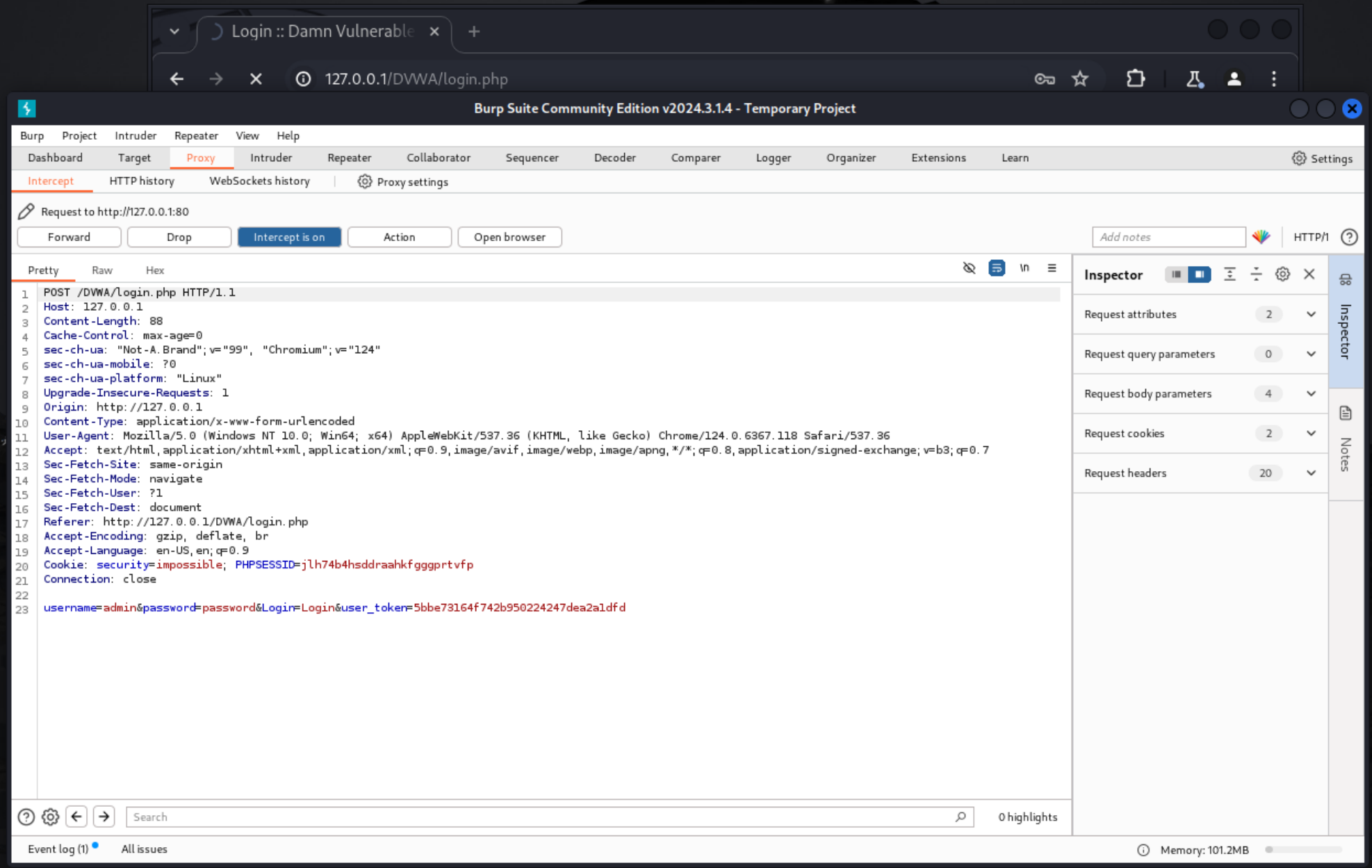
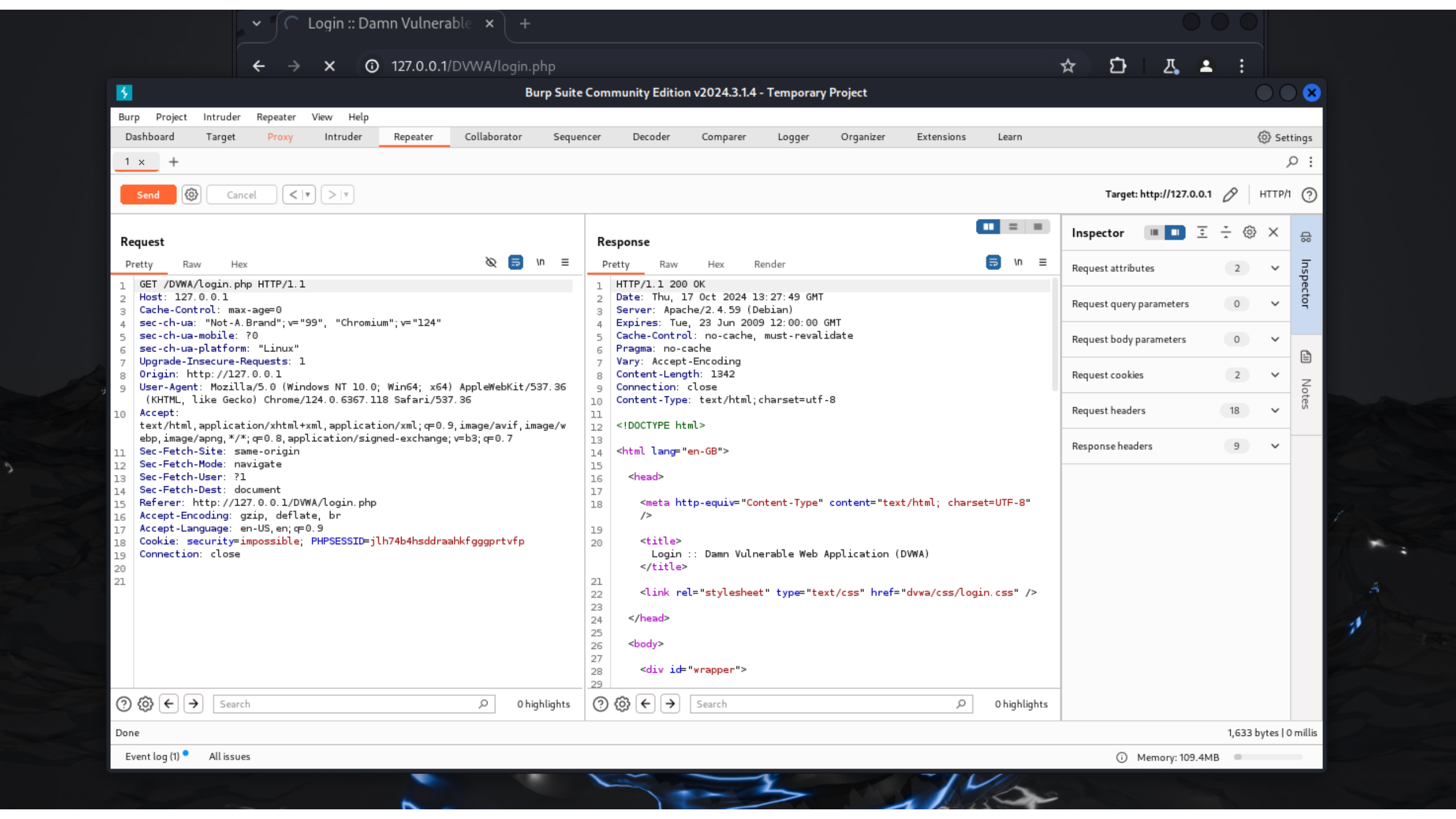

Login :: Damn Vulnerable
127.0.0.1/DVWA/login.php
Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Request to http://127.0.0.1:80
Forward Drop Intercept is on Action Open browser
Add notes 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: "Not-A.Brand";v="99", "Chromium";v="124"
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/124.0.6367.118 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=jlh74b4hsddraahkfgggprtvfp
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=5bbe73164f742b950224247dea2a1dfd
Search 0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 4
Request cookies 2
Request headers 20
Inspector Notes
Event log (1) All issues
Memory: 101.2MB


Login :: Damn Vulnerable
127.0.0.1/DVWA/login.php
Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Send Cancel
Target: http://127.0.0.1 HTTP/1
Request
Pretty Raw Hex
GET /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Cache-Control: max-age=0
sec-ch-ua: "Not-A.Brand";v="99", "Chromium";v="124"
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/124.0.6367.118 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=impossible; PHPSESSID=jlh74b4hsddraahkfgggprtvfp
Connection: close
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Date: Thu, 17 Oct 2024 13:27:49 GMT
Server: Apache/2.4.59 (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>

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
1,633 bytes | 0 millis
Event log (1) All issues
Memory: 109.4MB

Nell’esercizio odierno è stata configurata una DVWA, ovvero una damn vulnerable web application, sulla macchina Kali. Dopo aver effettuato i corretti passaggi di installazione e averne verificato il funzionamento, tramite l’utilizzo di burp suite è stata effettuata un’intercettazione della pagina. Giuti alla pagina di login Burpsuit ci mostrerà tutto ciò che succede dietro le quinte, quindi i processi richiesti come GET e POST, nonché la password inserita in chiaro insieme al nome utente, i quali era possibile modificare. A scopo didattico le due credenziali sono state quindi modificate ed inoltrate ad un «reapeter» del programma burp, nel quale è stato effettuato un test di accesso, risultato negativo come da aspettative, a causa delle credenziali modificate.