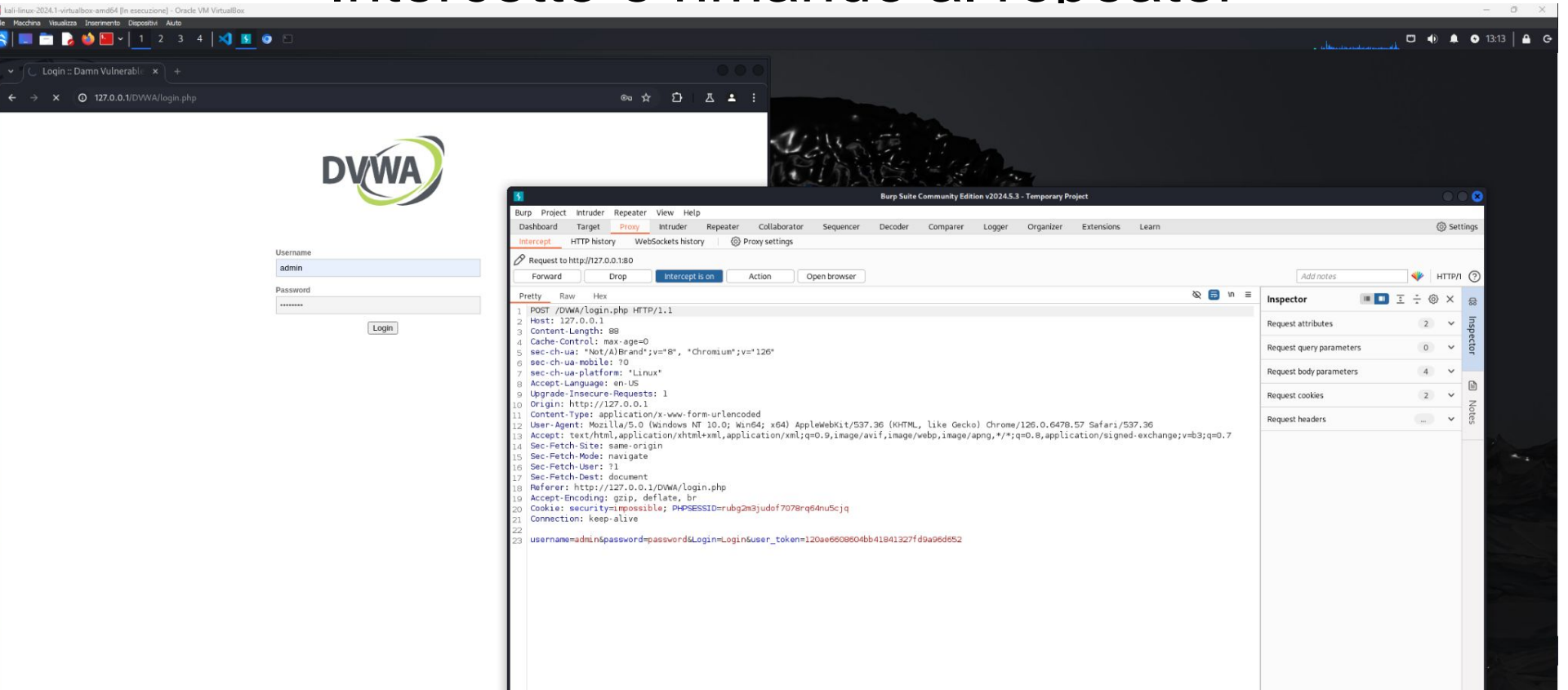
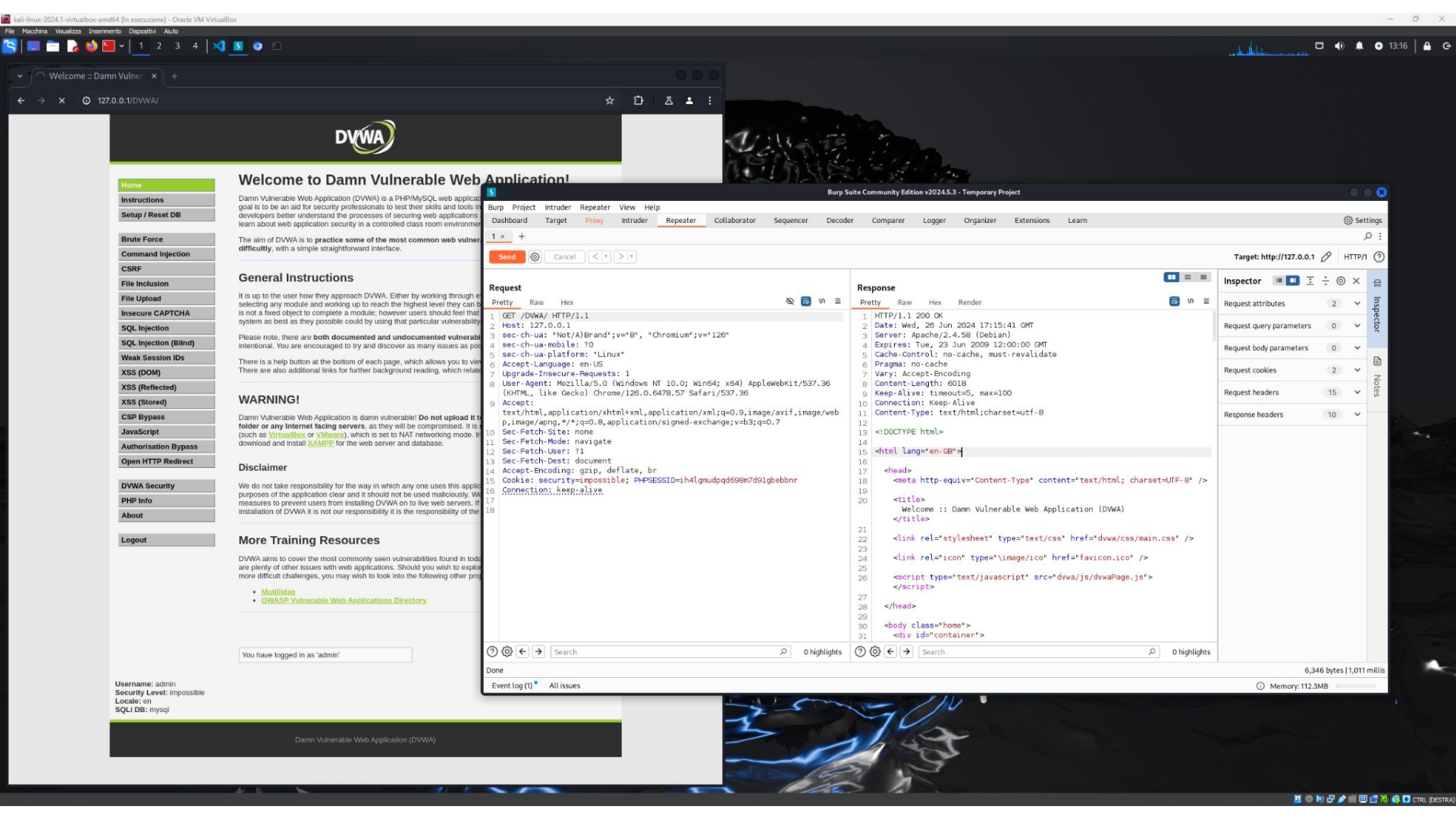
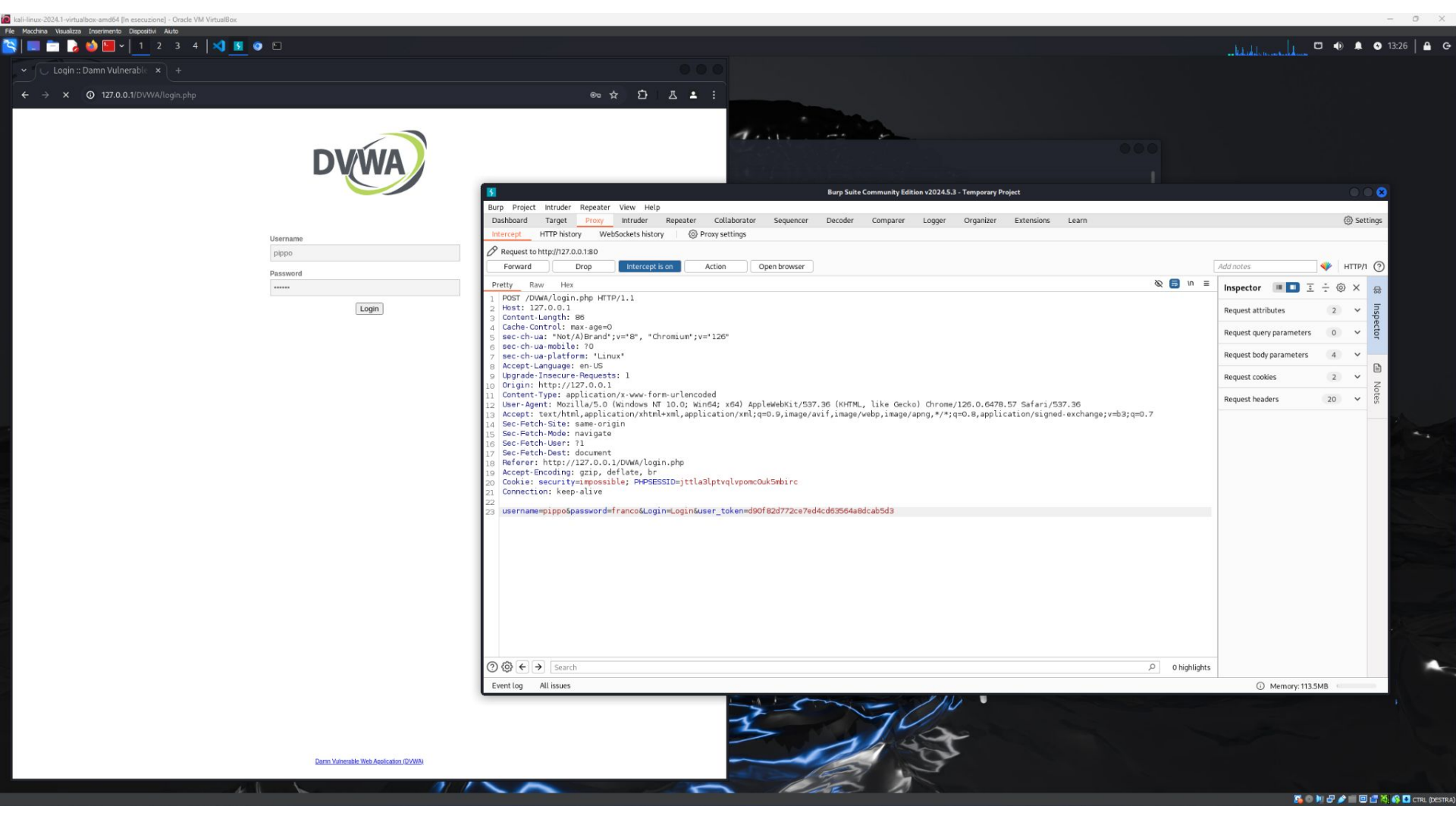
Intercetto e rimando al repeater




kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Welcome :: Damn Vulner
127.0.0.1/DVWA/
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Welcome to Damn Vulnerable Web Application!
General Instructions
WARNING!
Disclaimer
More Training Resources
Mutillidae
OWASP Vulnerable Web Applications Directory
You have logged in as 'admin'
Username: admin
Security Level: impossible
Locale: en
SQLi DB: mysql
Damn Vulnerable Web Application (DVWA)
Burp Suite Community Edition v2024.5.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel
Target: http://127.0.0.1
HTTP/1
Request
Pretty Raw Hex
GET /DVWA/ HTTP/1.1
Host: 127.0.0.1
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 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: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Cookie: security=impossible; PHPSESSID=ih4lgmudpqd698m7d91gbebbnr
Connection: keep-alive
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2024 17:15:41 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: 6018
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
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>
Welcome :: Damn Vulnerable Web Application (DVWA)
</title>
<link rel="stylesheet" type="text/css" href="dvwa/css/main.css" />
<link rel="icon" type="\image/ico" href="favicon.ico" />
<script type="text/javascript" src="dvwa/js/dvwaPage.js">
</script>
</head>
<body class="home">

Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 15
Response headers 10
Search 0 highlights
Done
6,346 bytes | 1,011 millis
Event log (1)
All issues
Memory: 112.3MB


kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Login :: Damn Vulnerable
127.0.0.1/DVWA/login.php
DVWA
Username
pippo
Password
Login
Damn Vulnerable Web Application (DVWA)
Burp Suite Community Edition v2024.5.3 - 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
Pretty Raw Hex
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 86
4 Cache-Control: max-age=0
5 sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Accept-Language: en-US
9 Upgrade-Insecure-Requests: 1
10 Origin: http://127.0.0.1
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
13 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
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://127.0.0.1/DVWA/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: security=impossible; PHPSESSID=jttla3lptvqlvpomc0uk5mbirc
21 Connection: keep-alive
23 username=pippo&password=franco&Login=Login&user_token=d90f82d772ce7ed4cd63564a8dcab5d3
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: 113.5MB

Burp Suite Community Edition v2024.5.3 - 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

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response timer
1	http://127.0.0.1	GET	/DVWA/			200	6536	HTML		Welcome :: Damn Vulnerable Web ...			127.0.0.1		13:24:40 26 Jun 2024	8080	34
2	http://127.0.0.1	GET	/DVWA/logout.php			302	337	HTML	php				127.0.0.1		13:25:44 26 Jun 2024	8080	2
3	http://127.0.0.1	GET	/DVWA/login.php			200	1715	HTML	php	Login :: Damn Vulnerable Web Appl...			127.0.0.1		13:25:51 26 Jun 2024	8080	8
4	http://127.0.0.1	GET	/favicon.ico			404	487	HTML	ico	404 Not Found			127.0.0.1		13:25:52 26 Jun 2024	8080	1
5	http://127.0.0.1	GET	/DVWA/			302	337	HTML					127.0.0.1		13:25:58 26 Jun 2024	8080	3
6	http://127.0.0.1	GET	/DVWA/login.php			200	1669	HTML	php	Login :: Damn Vulnerable Web Appl...			127.0.0.1		13:26:01 26 Jun 2024	8080	6
7	http://127.0.0.1	POST	/DVWA/login.php	✓		302	476	HTML	php				127.0.0.1	PHPSESSID=l9pom5g8sqs...	13:26:21 26 Jun 2024	8080	14
8	http://127.0.0.1	GET	/DVWA/login.php			200	1708	HTML	php	Login :: Damn Vulnerable Web Appl...			127.0.0.1		13:26:39 26 Jun 2024	8080	3

Request

Pretty Raw Hex

```
GET /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 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
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US
Referer: http://127.0.0.1/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Cookie: security=impossible; PHPSESSID=l9pom5g8sqs8q3u361p86e0f1s
Connection: keep-alive
```

Search 0 highlights

Response

Pretty Raw Hex Render

```
            </label>
             <input type="password" class="loginInput" AUTOCOMPLETE="off" size="20" name="password">
            <br />

            <br />

            <p class="submit">
              <input type="submit" value="Login" name="Login">
            </p>

          </fieldset>

          <input type='hidden' name='user_token' value='ae5e3eecfeabcaa983dc73fef720c015' />

        </form>

        <br />

        <div class="message">
          Login failed
        </div>

        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />

      </div >
       <!--<div id="content">-->

      <div id="footer">

        <p>
          <a href="https://github.com/digininja/DVWA/" target="_blank">
            Damn Vulnerable Web Application (DVWA)
          </a>
        </p>

      </div>
       <!--<div id="footer"> -->
```

Search 0 highlights

Inspector

Selection 12 (0xc)

Selected text

Login failed

Request attributes 2

Request cookies 2

Request headers 17

Response headers 10

Inspector Notes

Event log All issues

Memory: 113.5MB