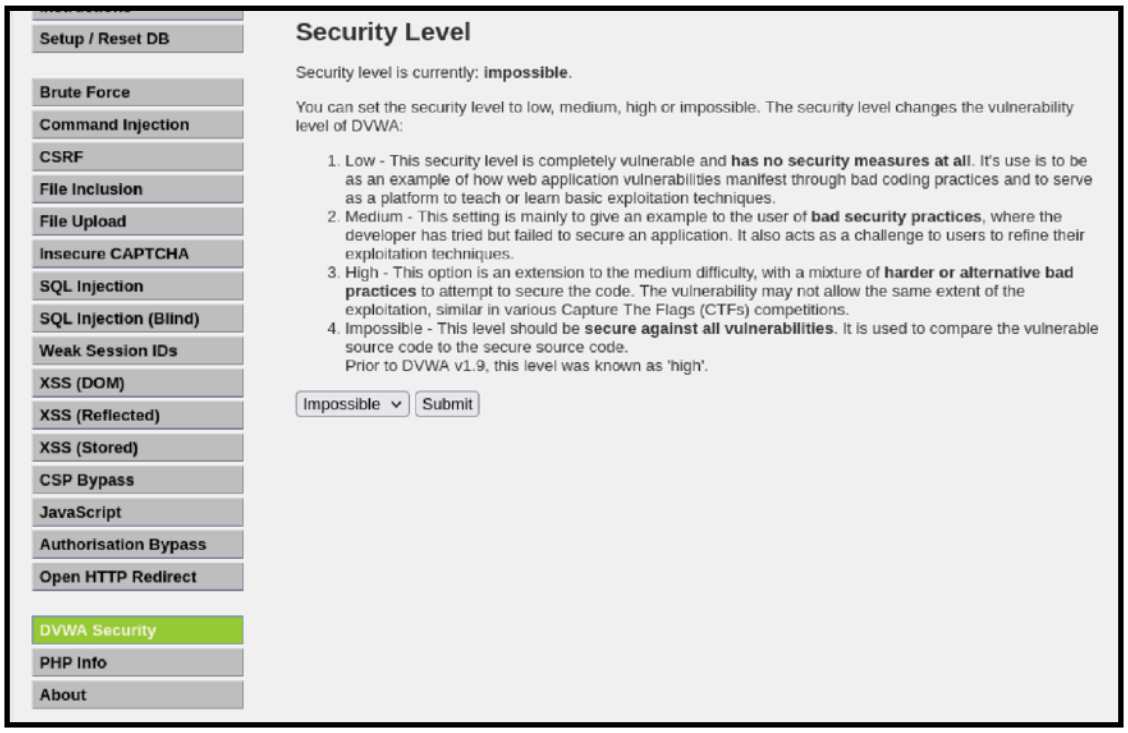
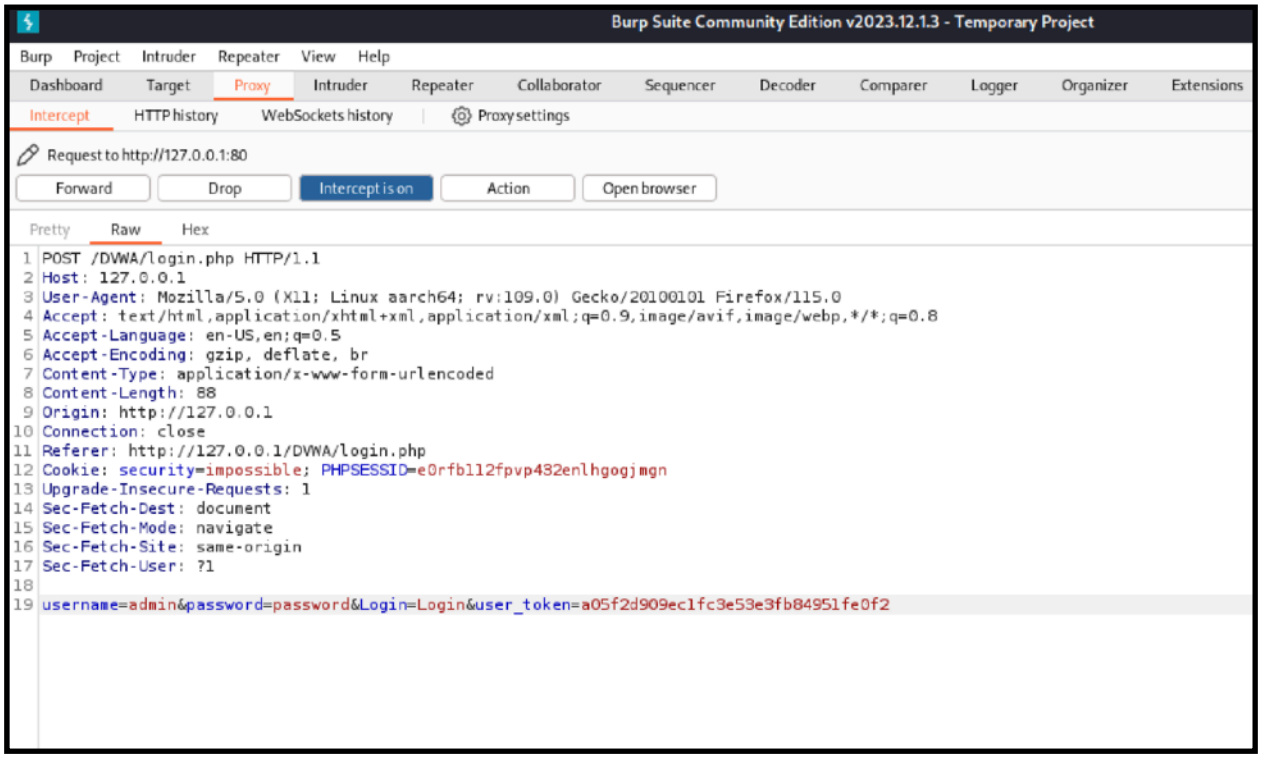
M2_W8D2



Intercettazione del traffico con BURP SUITE sulla pagina di Log In



Request

Pretty Raw Hex

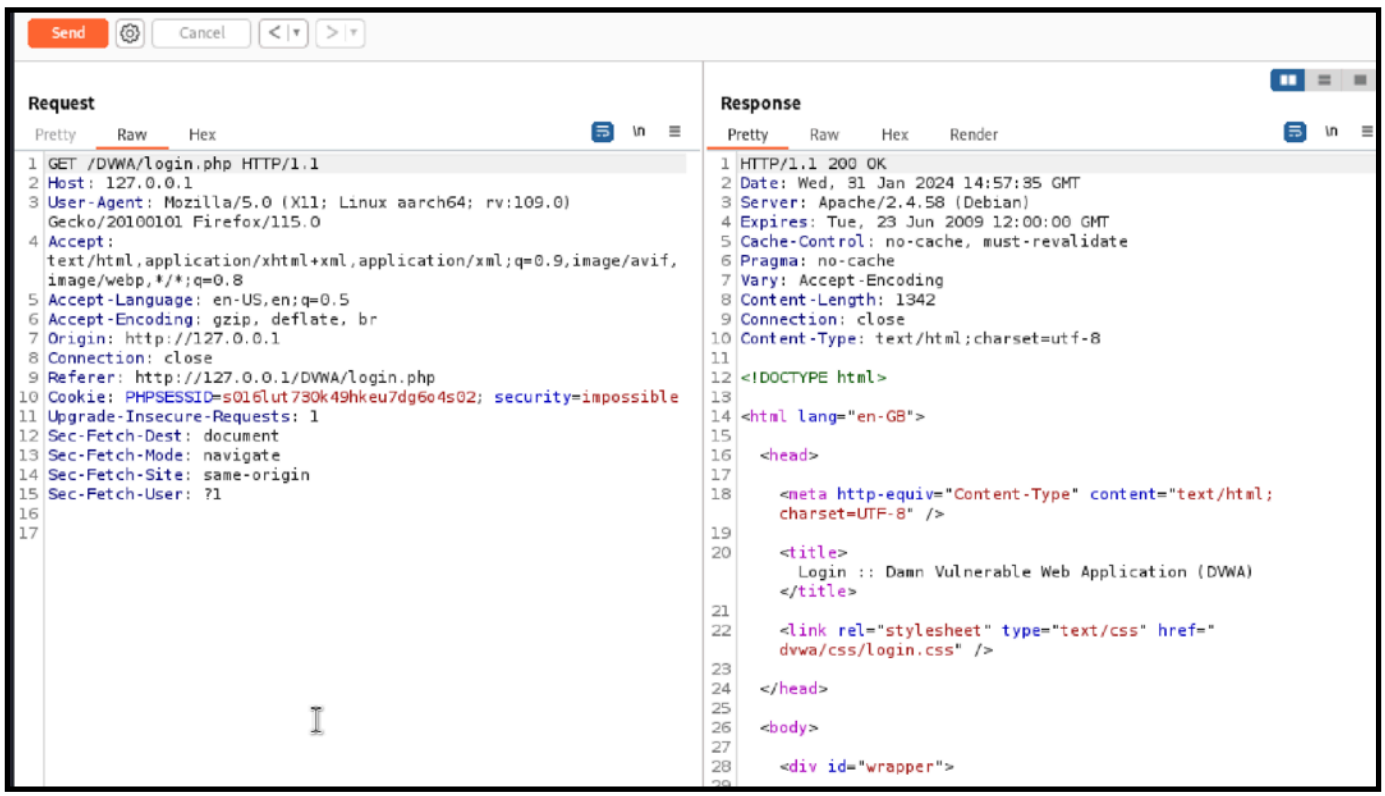
```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 85
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/DVWA/login.php
Cookie: PHPSESSID=gps8h3qlu54lm43ikuvorga9sq; security=low
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

username=pippo&password=baudo&Login=Login&user_token=
241b09dc0114fed071718c37cbaca492
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 302 Found
Date: Wed, 31 Jan 2024 14:30:47 GMT
Server: Apache/2.4.58 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=q53usfe19h4q7h9ckq56jl2d7g; expires=Thu, 01
 Feb 2024 14:30:47 GMT; Max-Age=86400; path=/
Location: login.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```



Send Cancel

Request

Pretty Raw Hex

```
GET /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/DVWA/login.php
Cookie: PHPSESSID=s016lut730k49hkeu7dg6o4s02; security=impossible
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Wed, 31 Jan 2024 14:57:35 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="wrapper">
```