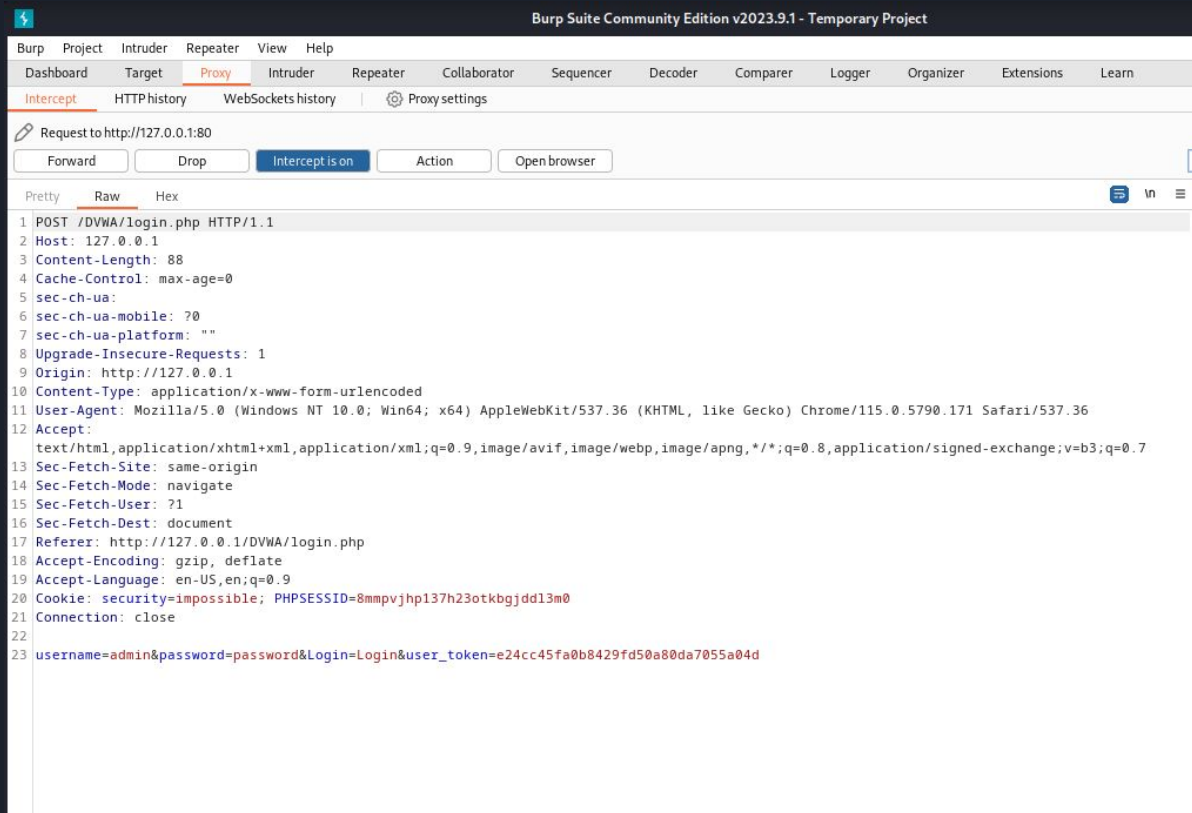




Esercizio S3 L3

configurazione di una DVWA

Per lo svolgimento dell'esercizio sono stati seguiti i passaggi illustrati all'interno delle slides di Pratica, a seguire riporto alcune schermate dei vari processi.



1 x +

Send Cancel < >

Request

Pretty Raw Hex

```
1 GET /DVWA/index.php HTTP/1.1
2 Host: 127.0.0.1
3 Cache-Control: max-age=0
4 sec-ch-ua:
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: ""
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/115.0.5790.171
  Safari/537.36
10 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
  mage/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/DVWA/login.php
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: security=impossible; PHPSESSID=8mmpvjhp137h23otkbgjdd13m0
19 Connection: close
20
21
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Fri, 08 Dec 2023 17:10:46 GMT
3 Server: Apache/2.4.57 (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: 6103
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   <meta http-equiv="Content-Type" content="text/html;
  charset=UTF-8" />
18
19   <title>
    Welcome :: Damn Vulnerable Web Application (DVWA)
  </title>
20
21   <link rel="stylesheet" type="text/css" href="dvwa/css/main.css
  " />
22
23   <link rel="icon" type="image/ico" href="favicon.ico" />
24
25   <script type="text/javascript" src="dvwa/js/dvwaPage.js">
  </script>
26
27 </head>
28
29 <body class="home">
30   <div id="container">
31
32     <div id="header">
33
34       
35
```

0 highlights



Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x 2 x +

Send Cancel < >

Request

Pretty Raw Hex

```
1 GET /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Cache-Control: max-age=0
4 sec-ch-ua:
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: ""
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/115.0.5790.171
  Safari/537.36
10 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
  mage/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/DVWA/login.php
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: security=impossible; PHPSESSID=8mmpvjhp137h23otkgjdd13m0
19 Connection: close
20
21
```

Response

Pretty Raw Hex Render

```
<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='
48a49465c8cafec656820b94b5e562ea' />
</form>
<br />
<div class="message">
  Login failed
</div>
<br />
<br />
<br />
<br />
<br />
<br />
<br />
</div>
<!--<div id="content">-->
<div id="footer">
<p>
  <a href="https://github.com/digininja/DVWA/" target="
_blank">
```

Search... 0 highlights

failed 1 match

Done