

Nombre: Diego Marta Hurtado

Asignatura: Sistemas Web

Grupo: 2

Fecha de Entrega: 04/03/2024

Nombre de la Entrega: Parte uno Practica de Laboratorio 2 (BurpSuite)

Descripción breve:

El siguiente documento contiene una serie de capturas de pantalla en las que se va mostrando los pasos seguidos y ejecutados para llevar a cabo la primera parte de la práctica de laboratorio número 2.

Dentro de algunas imágenes aparecen diferentes recuadrados en color rojo indicando las partes que son necesarias para la siguiente petición.

Primera Petición:

Interface of Burp Suite Community Edition v2023.3.3 - Tempora...

Menu: Dashboard, Target, Proxy, Intruder, Repeater, Window, Help

Sub-menu: Comparer, Logger, Extensions, Learn

Repeater Tab: 4 x, 5 x, 6 x, 7 x, +

Buttons: Send, Cancel, Follow redirection

Target: <https://egela.ehu.eus> HTTP/1

Request

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host: egela.ehu.eus
3
4
```

Inspector

Request attributes: 2

Request query parameters: 0

Request body parameters: 0

Request cookies: 0

Request headers: 1

Response headers: 19

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 303 See Other
2 Server: nginx
3 Date: Mon, 04 Mar 2024 08:51:46 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: keep-alive
6 Keep-Alive: timeout=30
7 Set-Cookie: MoodleSessionegela=
  co28712s832i4oh6knrist2b0jpk0lbe; path=/; secure
8 Expires: Thu, 19 Nov 1981 08:52:00 GMT
9 Cache-Control: no-store, no-cache, must-revalidate
10 Pragma: no-cache
11 X-Redirect-By: Moodle
12 Location: https://egela.ehu.eus/login/index.php
13 Content-Length: 1117
14 X-Cache: BYPASS
15 Cache-Control: public
```

Done 1,117 bytes | 76 millis

Segunda Petición:

4 x

5 x

6 x

7 x

+

Send

Cancel

Target: https://egela.ehu.eus HTTP/1

Request

Pretty

Raw

Hex

1 GET /login/index.php HTTP/1.1

2 Host: egela.ehu.eus

3

4

Inspector

Selection

32 (0x20)

Selected text

o2r7elhmFuBGSfX9Drs5VVTQrbw4PWmY

Request attributes

2

Request query parameters

0

Request body parameters

0

Request cookies

0

Request headers

1

Response headers

21

Response

Pretty

Raw

Hex

Render

1 HTTP/1.1 200 OK

2 Content-Type: text/html; charset=utf-8

3 Date: Mon, 04 Mar 2024 08:53:18 GMT

4 Content-Type: text/html; charset=utf-8

5 Connection: keep-alive

6 Keep-Alive: timeout=30

7 Vary: Accept-Encoding

8 Set-Cookie: MoodleSessionegela=spnbb12n2s85of9avlfmjrvkvhljda02; path=/; secure

9 Content-Language: eu

10 Content-Script-Type: text/javascript

11 Content-Style-Type: text/css

12 X-UA-Compatible: IE=edge

13 Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform

14 Pragma: no-cache

logintoke

1 match

Done

39,697 bytes | 265 millis

Response

Pretty

Raw

Hex

Render

128 e_ehu/logintopimage/1709188990/screenshot.png" class="img-fluid" alt="eGela">

129 </div>

130 <form class="m-t-l ehuloginform" action="https://egela.ehu.eus/login/index.php" method="POST" role="form">

131 <input type="hidden" name="logintoken" value="o2r7elhmFuBGSfX9Drs5VVTQrbw4PWmY">

132 <label for="username">

133 Erabiltzaile-izena

134 </label>

135 <div class="input-group">

136 <div class="input-group-addon">

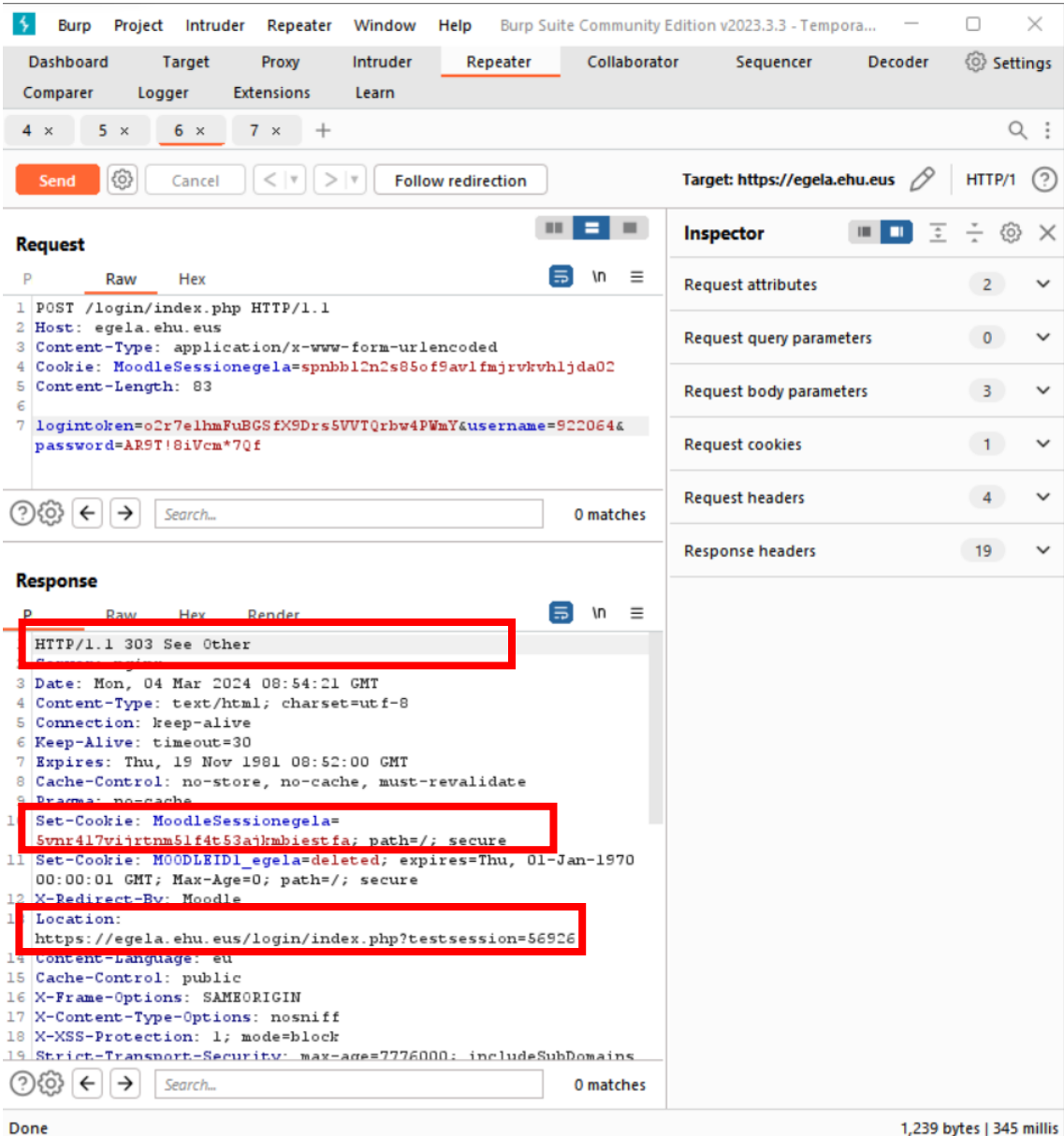
logintoke

1 match

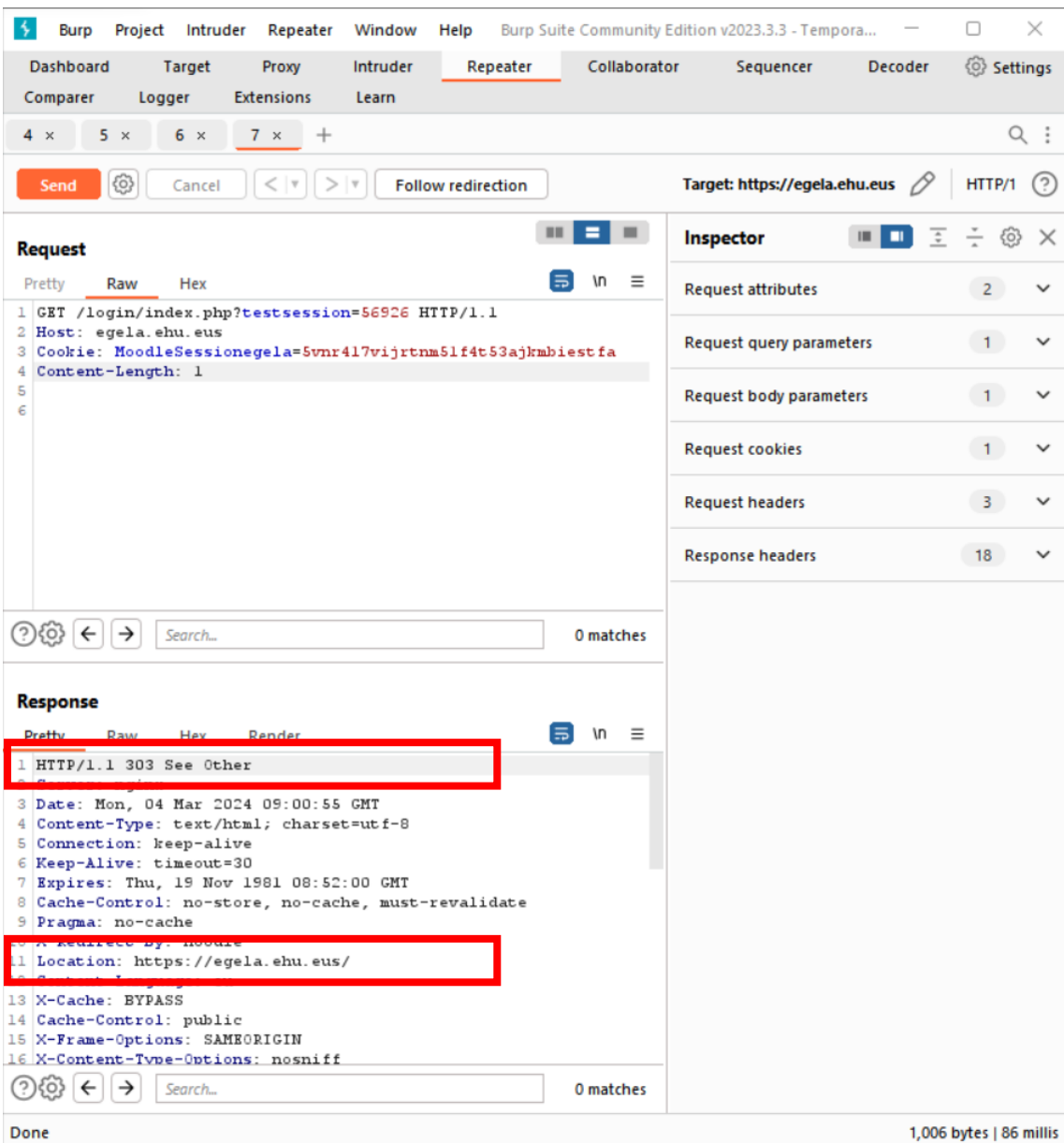
Done

39,697 bytes | 265 millis

Tercera petición:



Cuarta petición:



Última petición:

The screenshot displays the Burp Suite Repeater interface. The top menu bar includes options like Burp, Project, Intruder, Repeater, Window, Help, and Burp Suite Community Edition v2023.3.3. The Repeater tab is active, showing a list of requests with tabs for 4x, 5x, 6x, 7x, and 8x. The selected request is a GET / HTTP/1.1 to the target https://egela.ehu.eus. The request details show the Host and Cookie (MoodleSessionegela=5vnr4l7vijrtnm5lf4t53ajkrmbiestfa).

The Response section shows the HTML content of the request. A red box highlights a snippet of HTML code within a <div class="logininfo"> container. The highlighted code is as follows:

```
<div class="logininfo">
  <a href="
    https://egela.ehu.eus/user/profile.php?id=56926" title="Ikusi
    profila">
    DIEGO MARTA HURTADO
  </a>
  barruan da (<a href="
    https://egela.ehu.eus/login/logout.php?sesskey=EbxWHp8Gyt">
    Irten
  </a>
  )
</div>
```

The Inspector panel on the right shows the selected text "DIEGO MARTA HURTADO" and various request attributes, query parameters, body parameters, cookies, headers, and response headers.

At the bottom, the status bar indicates "Done" and "150,681 bytes | 976 millis".