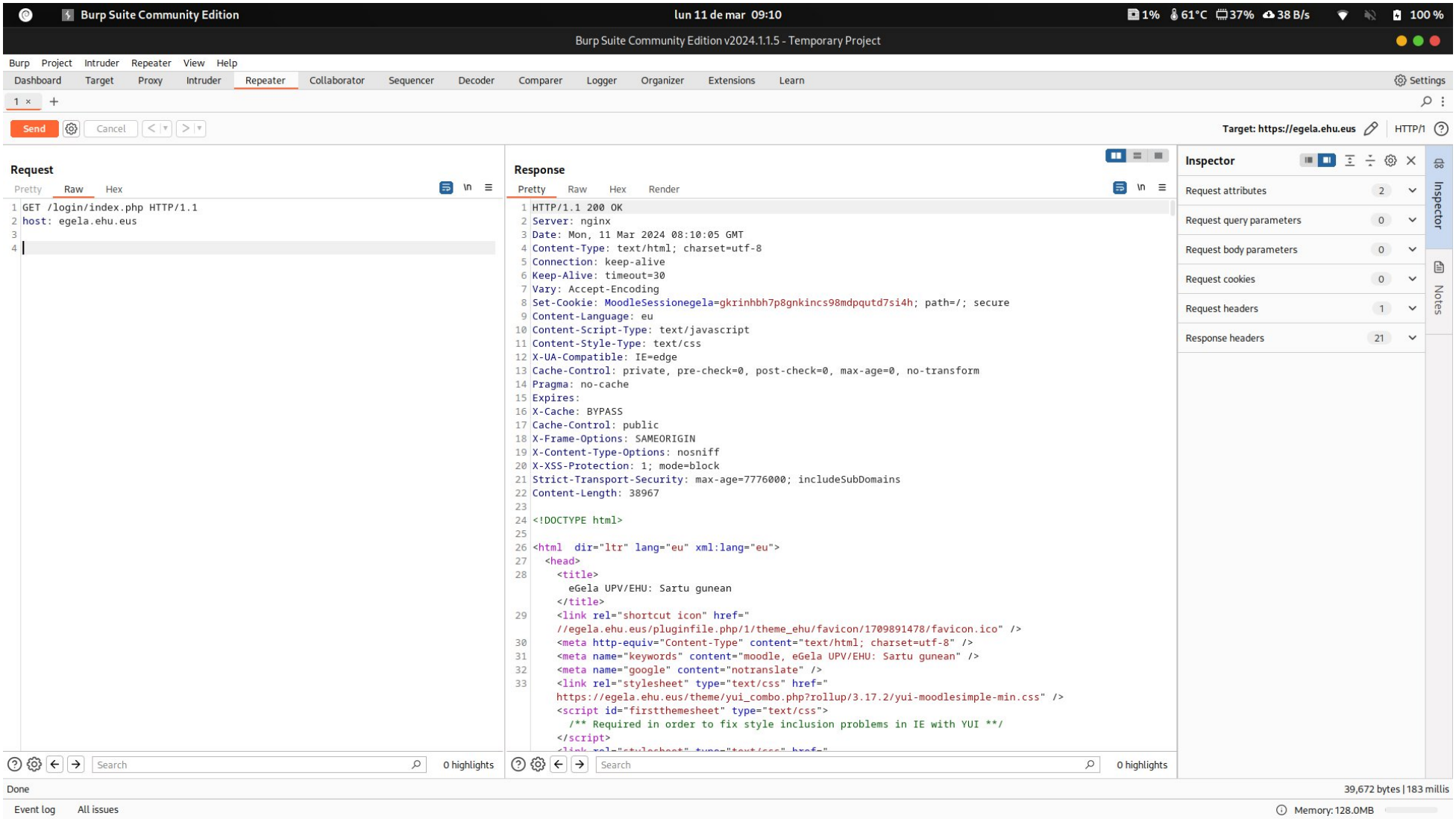
Xabier Gabiña Barañano

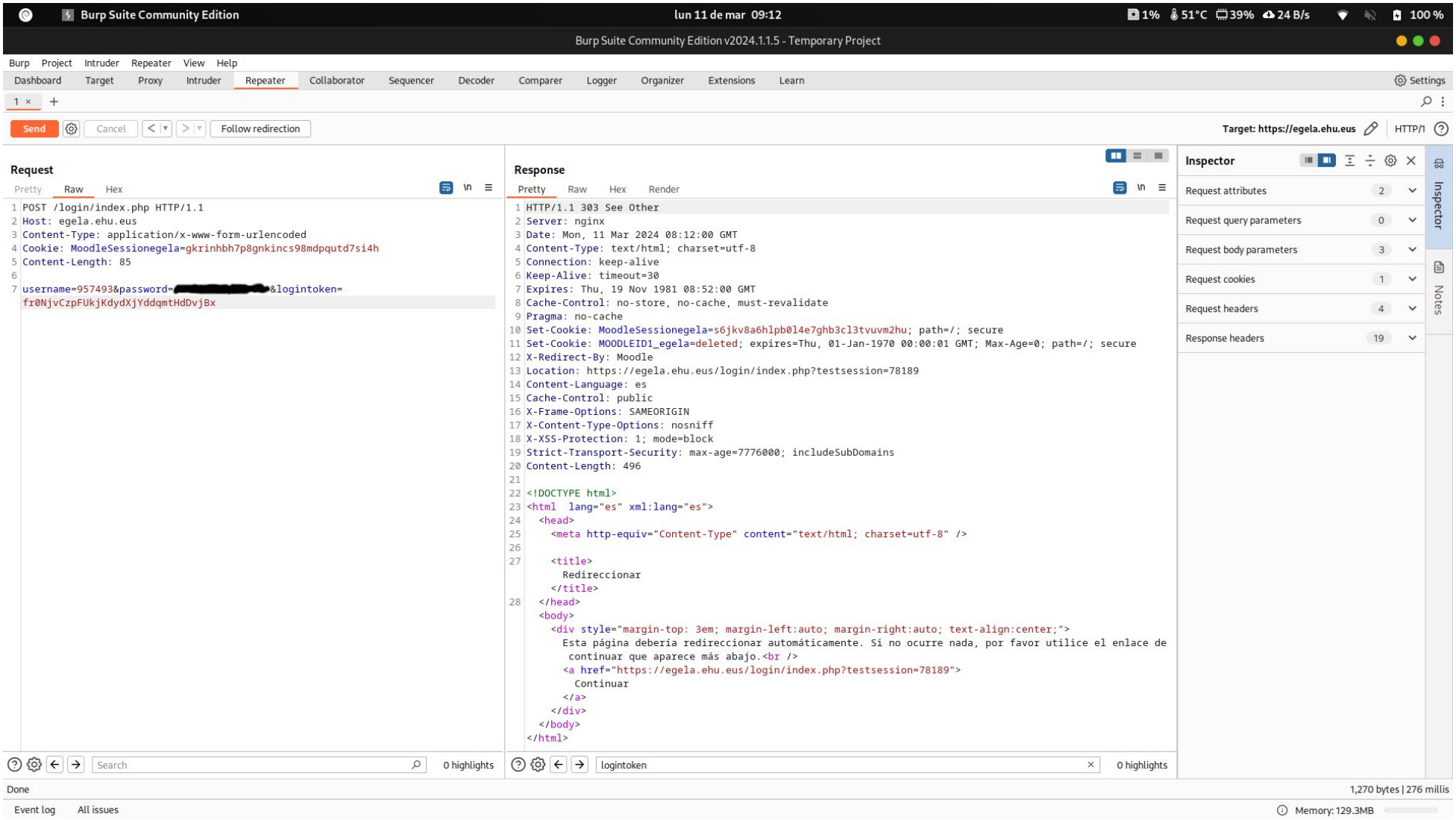
Grupo 1

11/03/2024

Burp – Conectarse a eGela

Conexión a eGela mediante peticiones HTTP usando Burp

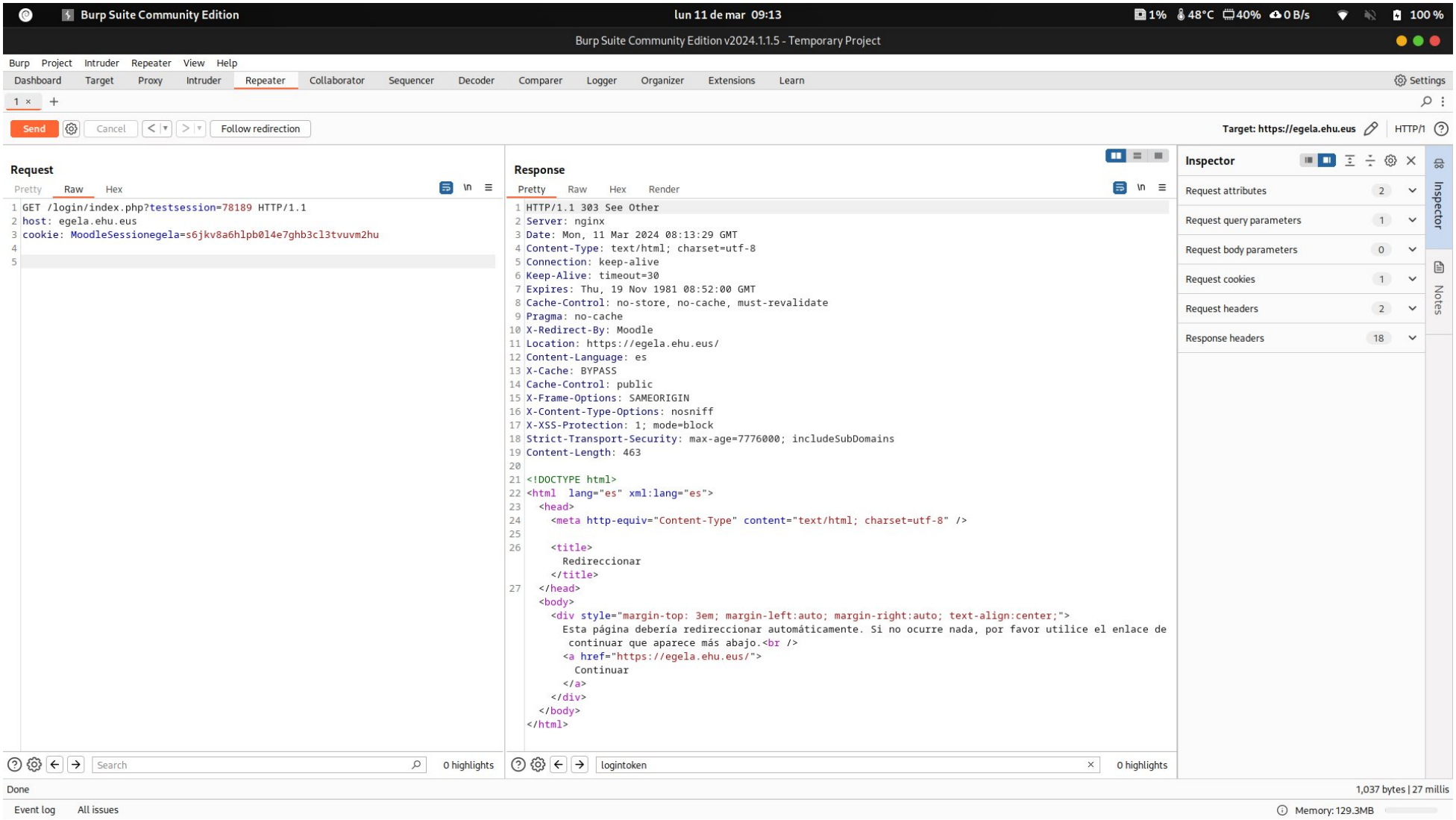

Burp Suite Community Edition
lun 11 de mar 09:10
1% 61°C 37% 38 B/s 100 %
Burp Suite Community Edition v2024.1.1.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Send Cancel
Target: https://egela.ehu.eus HTTP/1
Request
Pretty Raw Hex
GET /login/index.php HTTP/1.1
host: egela.ehu.eus
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 11 Mar 2024 08:10:05 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Keep-Alive: timeout=30
Vary: Accept-Encoding
Set-Cookie: MoodleSessionegela=gkrinhbh7p8gnkincs98mdpqutd7si4h; path=/; secure
Content-Language: eu
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-UA-Compatible: IE=edge
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
Pragma: no-cache
Expires:
X-Cache: BYPASS
Cache-Control: public
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Strict-Transport-Security: max-age=7776000; includeSubDomains
Content-Length: 38967
<!DOCTYPE html>
<html dir="ltr" lang="eu" xml:lang="eu">
<head>
<title>
eGela UPV/EHU: Sartu gunean
</title>
<link rel="shortcut icon" href="
//egela.ehu.eus/pluginfile.php/1/theme_ehu/favicon/1709891478/favicon.ico" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="keywords" content="moodle, eGela UPV/EHU: Sartu gunean" />
<meta name="google" content="notranslate" />
<link rel="stylesheet" type="text/css" href="
https://egela.ehu.eus/theme/yui_combo.php?rollup/3.17.2/yui-moodlesimple-min.css" />
<script id="firstthemesheet" type="text/css">
/** Required in order to fix style inclusion problems in IE with YUI **/
</script>
Search 0 highlights
Search 0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 1
Response headers 21
Inspector
Notes
Done
39,672 bytes | 183 millis
Event log All issues
Memory: 128.0MB


Burp Suite Community Edition
lun 11 de mar 09:12
1% 51°C 39% 24 B/s 100 %
Burp Suite Community Edition v2024.1.1.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
1 ×
Send Cancel Follow redirection
Target: https://egela.ehu.eus HTTP/1
Request
Pretty Raw Hex
1 POST /login/index.php HTTP/1.1
2 Host: egela.ehu.eus
3 Content-Type: application/x-www-form-urlencoded
4 Cookie: MoodleSessionegela=gkrinhbh7p8gnkincs98mdpqutd7si4h
5 Content-Length: 85
6
7 username=957493&password=[redacted]&logintoken=
fr0NjvCzpFUkjKdydXjYddqmtHdDvjBx
Search 0 highlights
Response
Pretty Raw Hex Render
1 HTTP/1.1 303 See Other
2 Server: nginx
3 Date: Mon, 11 Mar 2024 08:12:00 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: keep-alive
6 Keep-Alive: timeout=30
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Set-Cookie: MoodleSessionegela=s6jkv8a6hlpb0l4e7ghb3cl3tvuvm2hu; path=/; secure
11 Set-Cookie: MOODLEID1_egela=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/; secure
12 X-Redirect-By: Moodle
13 Location: https://egela.ehu.eus/login/index.php?testsession=78189
14 Content-Language: es
15 Cache-Control: public
16 X-Frame-Options: SAMEORIGIN
17 X-Content-Type-Options: nosniff
18 X-XSS-Protection: 1; mode=block
19 Strict-Transport-Security: max-age=7776000; includeSubDomains
20 Content-Length: 496
21
22 <!DOCTYPE html>
23 <html lang="es" xml:lang="es">
24 <head>
25 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
26
27 <title>
Redireccionar
</title>
28 </head>
<body>

Esta página debería redireccionar automáticamente. Si no ocurre nada, por favor utilice el enlace de continuar que aparece más abajo.

Continuar

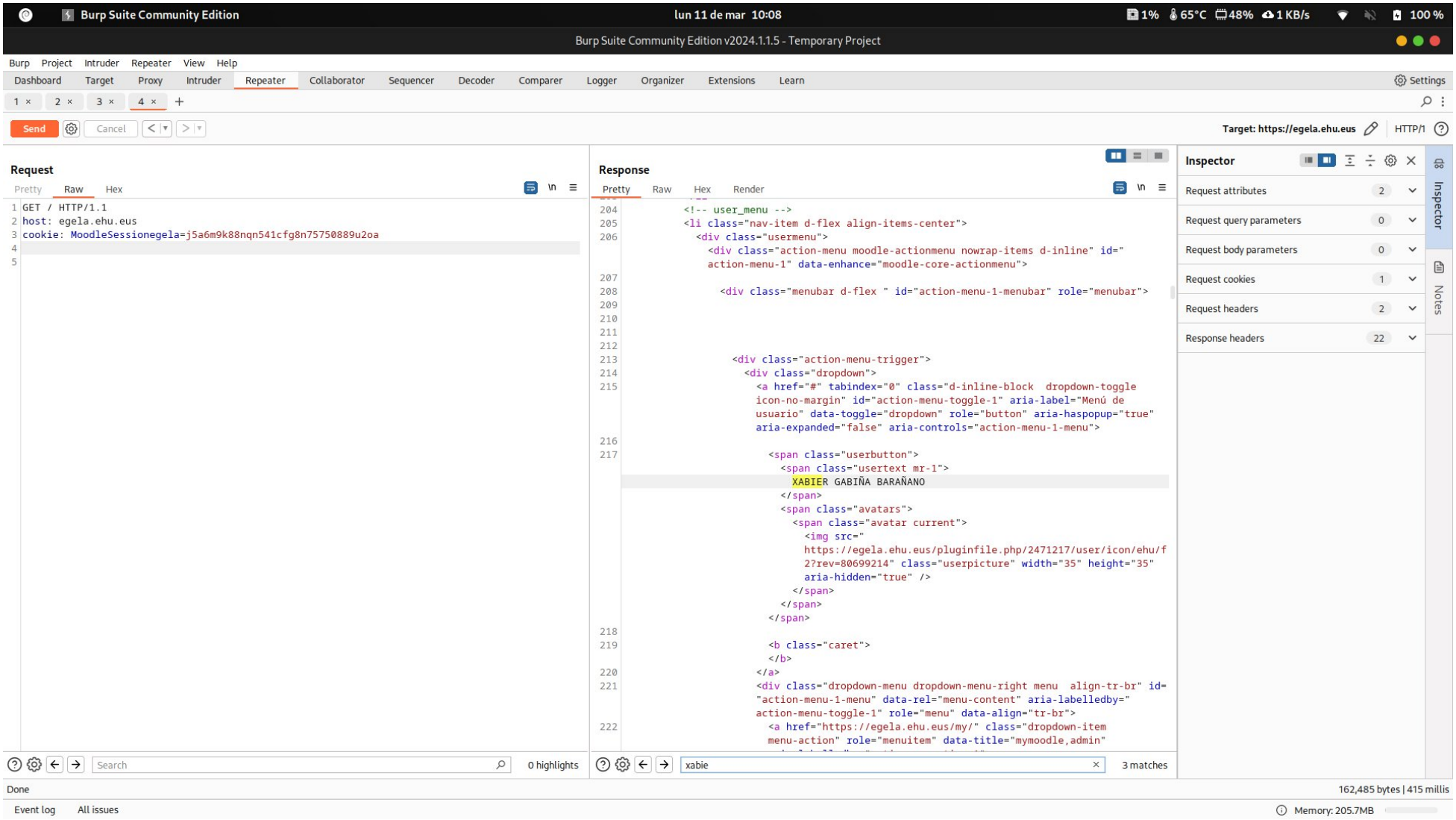
</body>
</html>
logintoken 0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 1
Request headers 4
Response headers 19
Inspector
Notes
Done
1,270 bytes | 276 millis
Event log All issues
Memory: 129.3MB


Burp Suite Community Edition
lun 11 de mar 09:13
1% 48°C 40% 0 B/s 100 %
Burp Suite Community Edition v2024.1.1.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
1 ×
Send Cancel Follow redirection
Target: https://egela.ehu.eus HTTP/1
Request
Pretty Raw Hex
1 GET /login/index.php?testsession=78189 HTTP/1.1
2 host: egela.ehu.eus
3 cookie: MoodleSessionegela=s6jkv8a6hlpb0l4e7ghb3cl3tvuvm2hu
4
5
Search 0 highlights
Response
Pretty Raw Hex Render
1 HTTP/1.1 303 See Other
2 Server: nginx
3 Date: Mon, 11 Mar 2024 08:13:29 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: keep-alive
6 Keep-Alive: timeout=30
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 X-Redirect-By: Moodle
11 Location: https://egela.ehu.eus/
12 Content-Language: es
13 X-Cache: BYPASS
14 Cache-Control: public
15 X-Frame-Options: SAMEORIGIN
16 X-Content-Type-Options: nosniff
17 X-XSS-Protection: 1; mode=block
18 Strict-Transport-Security: max-age=7776000; includeSubDomains
19 Content-Length: 463
20
21 <!DOCTYPE html>
22 <html lang="es" xml:lang="es">
23 <head>
24 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
25
26 <title>
Redireccionar
</title>
27 </head>
<body>

Esta página debería redireccionar automáticamente. Si no ocurre nada, por favor utilice el enlace de continuar que aparece más abajo.

Continuar

</body>
</html>
logintoken 0 highlights
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 2
Response headers 18
Inspector
Notes
Done
1,037 bytes | 27 millis
Event log All issues
Memory: 129.3MB

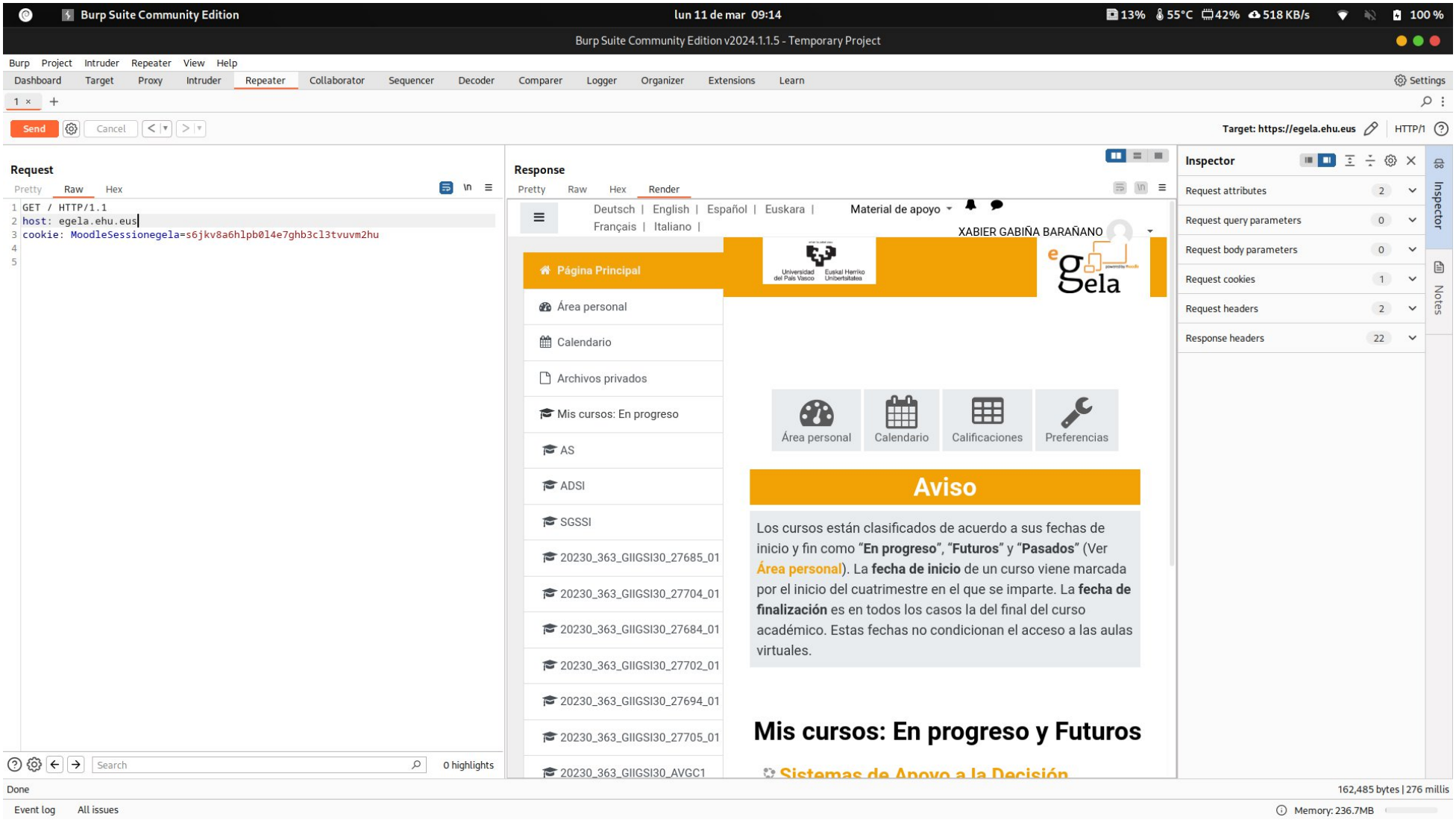

Burp Suite Community Edition
lun 11 de mar 10:08
1% 65°C 48% 1 KB/s 100 %
Burp Suite Community Edition v2024.1.1.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
1 × 2 × 3 × 4 ×
Send Cancel
Target: https://egela.ehu.eus HTTP/1
Request
Pretty Raw Hex
1 GET / HTTP/1.1
2 host: egela.ehu.eus
3 cookie: MoodleSessionegela=j5a6m9k88nqn541cfg8n75750889u2oa
4
5
Search 0 highlights
Response
Pretty Raw Hex Render
204 <!-- user_menu -->
205 <li class="nav-item d-flex align-items-center">
206
<div class="action-menu moodle-actionmenu nowrap-items d-inline" id="
action-menu-1" data-enhance="moodle-core-actionmenu">
207
208
209
210
211
212
213
214
215 <a href="#" tabindex="0" class="d-inline-block dropdown-toggle
icon-no-margin" id="action-menu-toggle-1" aria-label="Menú de
usuario" data-toggle="dropdown" role="button" aria-haspopup="true"
aria-expanded="false" aria-controls="action-menu-1-menu">
216
217

XABIER GABIÑA BARAÑANO

<img src="
https://egela.ehu.eus/pluginfile.php/2471217/user/icon/ehu/f
2?rev=80699214" class="userpicture" width="35" height="35"
aria-hidden="true" />

218
219

220
221 <div class="dropdown-menu dropdown-menu-right menu align-tr-br" id=
"action-menu-1-menu" data-rel="menu-content" aria-labelledby="
action-menu-toggle-1" role="menu" data-align="tr-br">
222 <a href="https://egela.ehu.eus/my/" class="dropdown-item
menu-action" role="menuitem" data-title="mymoodle,admin"
xabie
3 matches
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 1
Request headers 2
Response headers 22
Inspector
Notes
Done
162,485 bytes | 415 millis
Event log All issues
Memory: 205.7MB


Burp Suite Community Edition
lun 11 de mar 09:14
13% 55°C 42% 518 KB/s 100 %
Burp Suite Community Edition v2024.1.1.5 - 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: https://egela.ehu.eus HTTP/1
Request
Pretty Raw Hex
1 GET / HTTP/1.1
2 host: egela.ehu.eus
3 cookie: MoodleSessionegela=s6jkv8a6hlpb0l4e7ghb3cl3tvuvm2hu
4
5
Search 0 highlights
Response
Pretty Raw Hex Render
Deutsch | English | Español | Euskara | Français | Italiano |
Material de apoyo
XABIER GABIÑA BARAÑANO
Página Principal
Área personal
Calendario
Archivos privados
Mis cursos: En progreso
AS
ADSI
SGSSI
20230_363_GIIGSI30_27685_01
20230_363_GIIGSI30_27704_01
20230_363_GIIGSI30_27684_01
20230_363_GIIGSI30_27702_01
20230_363_GIIGSI30_27694_01
20230_363_GIIGSI30_27705_01
20230_363_GIIGSI30_AVGC1
Área personal
Calendario
Calificaciones
Preferencias
Aviso
Los cursos están clasificados de acuerdo a sus fechas de inicio y fin como "En progreso", "Futuros" y "Pasados" (Ver Área personal). La fecha de inicio de un curso viene marcada por el inicio del cuatrimestre en el que se imparte. La fecha de finalización es en todos los casos la del final del curso académico. Estas fechas no condicionan el acceso a las aulas virtuales.
Mis cursos: En progreso y Futuros
Sistemas de Apoyo a la Decisión
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 1
Request headers 2
Response headers 22
Inspector
Notes
Done
162,485 bytes | 276 millis
Event log All issues
Memory: 236.7MB