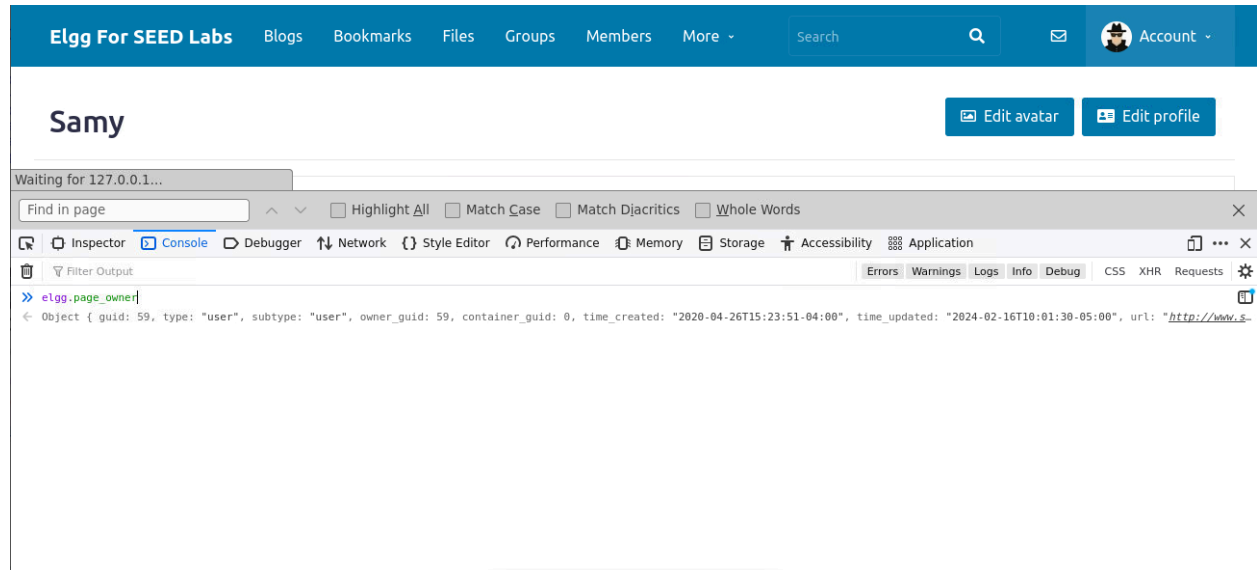


Report on Web Security Assignment

Student ID: 1905092

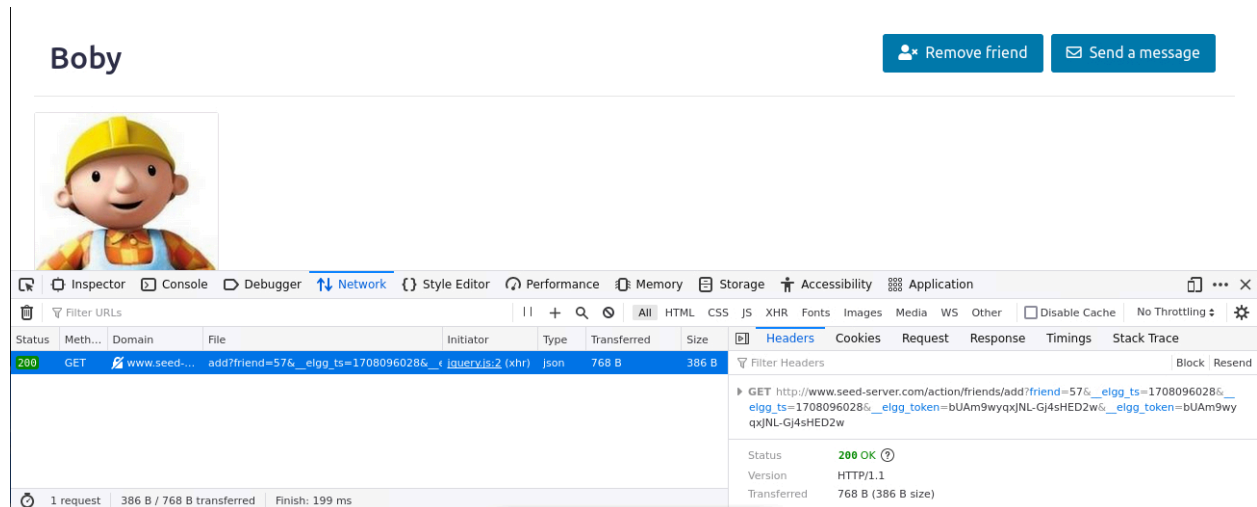
Task 1:



The screenshot shows the Elgg user profile for 'Samy'. The browser's developer console is open, displaying the following JavaScript code and its output:

```
>> elgg.page_owner|  
← Object { guid: 59, type: "user", subtype: "user", owner_guid: 59, container_guid: 0, time_created: "2020-04-26T15:23:51-04:00", time_updated: "2024-02-16T10:01:30-05:00", url: "http://www.s-"
```

Looked for samy's guid



The screenshot shows the Elgg user profile for 'Boby'. The browser's developer console is open, displaying a GET request to the following URL:

```
GET http://www.seed-server.com/action/friends/add?friend=57%__elgg_ts=1708096028%__elgg_token=bUAm9wyqxJNL-Gj4sHED2w%__elgg_token=bUAm9wyqxJNL-Gj4sHED2w
```

The console also shows the status of the request as 200 OK.

Observed the get request when sending friend request.

Task 2:

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More - Search Account -

www.seed-server.com/groups/all

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Filter URLs

| St... | M... | Domain | File | Initiator | Type | Transferred | Size | Headers | Cookies | Request | Response | Timings | |
|-------|-------|----------|----------------------|---------------|------|-------------|-------|---|---------|---------|----------|---------|--|
| 302 | PO... | www.s... | edit | document | html | 4.36 kB | 19... | POST http://www.seed-server.com/action/profile/edit | | | | | |
| 200 | GET | www.s... | alice | document | html | 4.41 kB | 19... | Status: 302 Found | | | | | |
| 200 | GET | www.s... | 56large.jpg | img | jpeg | cached | 6... | Version: HTTP/1.1 | | | | | |
| 200 | GET | www.s... | jquery.js | script | js | cached | 0 B | Transferred: 4.36 kB (19.47 kB size) | | | | | |
| 200 | GET | www.s... | jquery-ui.js | script | js | cached | 0 B | Referrer Policy: strict-origin-when-cross-origin | | | | | |
| 200 | GET | www.s... | require_config.js | script | js | cached | 78... | Request Priority: Highest | | | | | |
| 200 | GET | www.s... | require.js | script | js | cached | 0 B | DNS Resolution: System | | | | | |
| 200 | GET | www.s... | elgg.js | script | js | cached | 0 B | Response Headers (397 B) | | | | | |
| 200 | GET | www.s... | favicon-128.png | Favicon... | png | cached | 4... | Cache-Control: must-revalidate, no-cache, no-store, private | | | | | |
| 200 | GET | www.s... | favicon.svg | Favicon... | svg | cached | 6... | Connection: Keep-Alive | | | | | |
| 200 | GET | www.s... | sprintf.js | require.js... | js | cached | 0 B | Content-Length: 406 | | | | | |
| 200 | GET | www.s... | en.js | require.js... | js | cached | 0 B | Content-Type: text/html; charset=UTF-8 | | | | | |
| 200 | GET | www.s... | weakmap-polyfill.js | require.js... | js | cached | 0 B | Date: Fri, 16 Feb 2024 16:41:44 GMT | | | | | |
| 200 | GET | www.s... | formdata-polyfill.js | require.js... | js | cached | 0 B | expires: Thu, 19 Nov 1981 08:52:00 GMT | | | | | |
| 200 | GET | www.s... | widgets.js | require.js... | js | cached | 0 B | Keep-Alive: timeout=5, max=100 | | | | | |
| 200 | GET | www.s... | init.js | require.js... | js | cached | 37... | Location: http://www.seed-server.com/profile/alice | | | | | |
| | | | | | | | | pragma: no-cache | | | | | |
| | | | | | | | | Server: Apache/2.4.41 (Ubuntu) | | | | | |

25 requests 59.46 kB / 8.76 kB transferred Finish: 2.71 s DOMContentLoaded: 2.45

Observed the post request when editing own profile.

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More - Search Account -

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Filter URLs

| St... | M... | Domain | File | Initiator | Type | Transferred | Size | Headers | Cookies | Request | Response | Timings | |
|-------|-------|----------|----------------------|---------------|------|-------------|-------|---|---------|---------|----------|---------|--|
| 302 | PO... | www.s... | edit | document | html | 4.36 kB | 19... | Filter Request Parameters | | | | | |
| 200 | GET | www.s... | alice | document | html | 4.41 kB | 19... | Request payload | | | | | |
| 200 | GET | www.s... | 56large.jpg | img | jpeg | cached | 6... | Content-Disposition: form-data; name="accesslevel[mobile]" | | | | | |
| 200 | GET | www.s... | jquery.js | script | js | cached | 0 B | 2 | | | | | |
| 200 | GET | www.s... | jquery-ui.js | script | js | cached | 0 B | Content-Disposition: form-data; name="website" | | | | | |
| 200 | GET | www.s... | require_config.js | script | js | cached | 78... | http://www.cf.com | | | | | |
| 200 | GET | www.s... | require.js | script | js | cached | 0 B | Content-Disposition: form-data; name="accesslevel[website]" | | | | | |
| 200 | GET | www.s... | elgg.js | script | js | cached | 0 B | 1 | | | | | |
| 200 | GET | www.s... | favicon-128.png | Favicon... | png | cached | 4... | Content-Disposition: form-data; name="twitter" | | | | | |
| 200 | GET | www.s... | favicon.svg | Favicon... | svg | cached | 6... | www.twitter.com | | | | | |
| 200 | GET | www.s... | sprintf.js | require.js... | js | cached | 0 B | Content-Disposition: form-data; name="accesslevel[twitter]" | | | | | |
| 200 | GET | www.s... | en.js | require.js... | js | cached | 0 B | 1 | | | | | |
| 200 | GET | www.s... | weakmap-polyfill.js | require.js... | js | cached | 0 B | Content-Disposition: form-data; name="guid" | | | | | |
| 200 | GET | www.s... | formdata-polyfill.js | require.js... | js | cached | 0 B | 56 | | | | | |
| 200 | GET | www.s... | widgets.js | require.js... | js | cached | 0 B | | | | | | |
| 200 | GET | www.s... | init.js | require.js... | js | cached | 37... | | | | | | |

25 requests 59.46 kB / 8.76 kB transferred Finish: 2.71 s DOMContentLoaded: 2.45

Task 3:

UI mockup showing a post form and network inspector. The post form has a text input "What's happening?", a "Post" button, and a "140 characters remaining" indicator. Below the form, it shows the post is by "Alice" and says "Let's see what happens". The network inspector shows a list of requests, with the selected request being a POST to "http://www.seed-server.com/action/thewire/add". The response headers are visible, showing a 302 Found status and various headers like Cache-Control, Connection, Content-Length, and Content-Type.

Observed the post request when making a wire post.

UI mockup showing the same post form, but the network inspector is expanded to show the request payload. The request payload is a JSON object containing a token, a timestamp, and a body. The response is also visible, showing a 302 Found status and various headers like Cache-Control, Connection, Content-Length, and Content-Type.