تقرير وظيفة الأمن السيبراني الثانية

أمن تطبيقات الويب (Web Application Security)

بيئة العمل: مختبرات SEED Ubuntu

اسم الطالب: عمران خلف الربيدان

الرقم الجامعي: 1722204157

تاريخ التسليم: 2 january 2026

المهمة الأولى: هجوم تزوير الطلب عبر المواقع (CSRF)

بناء الهجوم

تم إنشاء صفحة ويب خبيثة تحتوي على كود JavaScript لتنفيذ هجوم CSRF. الصفحة تظهر كصفحة "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 تلقائيًا عند زيارة الصفحة الخبيثة
- إنشاء نموذج مخفي يحتوي على معلمات تغيير كلمة المرور
- إرسال النموذج تلقائيًا إلى خادم الموقع المستهدف
- تعامل الخادم مع الطلب كأنه صادر من المستخدم نفسه

تحليل طلب HTTP:

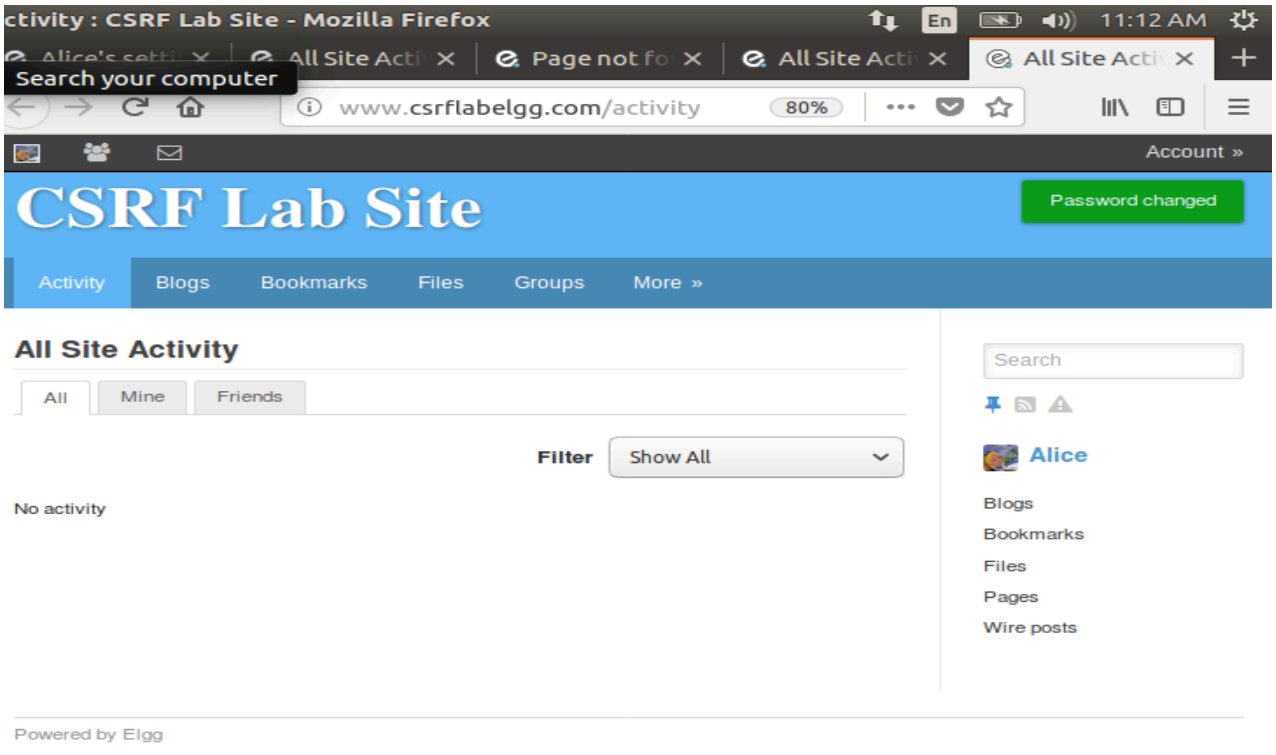
طريقة الطلب: `POST`
الرابط المستهدف:
`http://www.csrflabelgg.com/action/usersettings/save`
المعلمات:

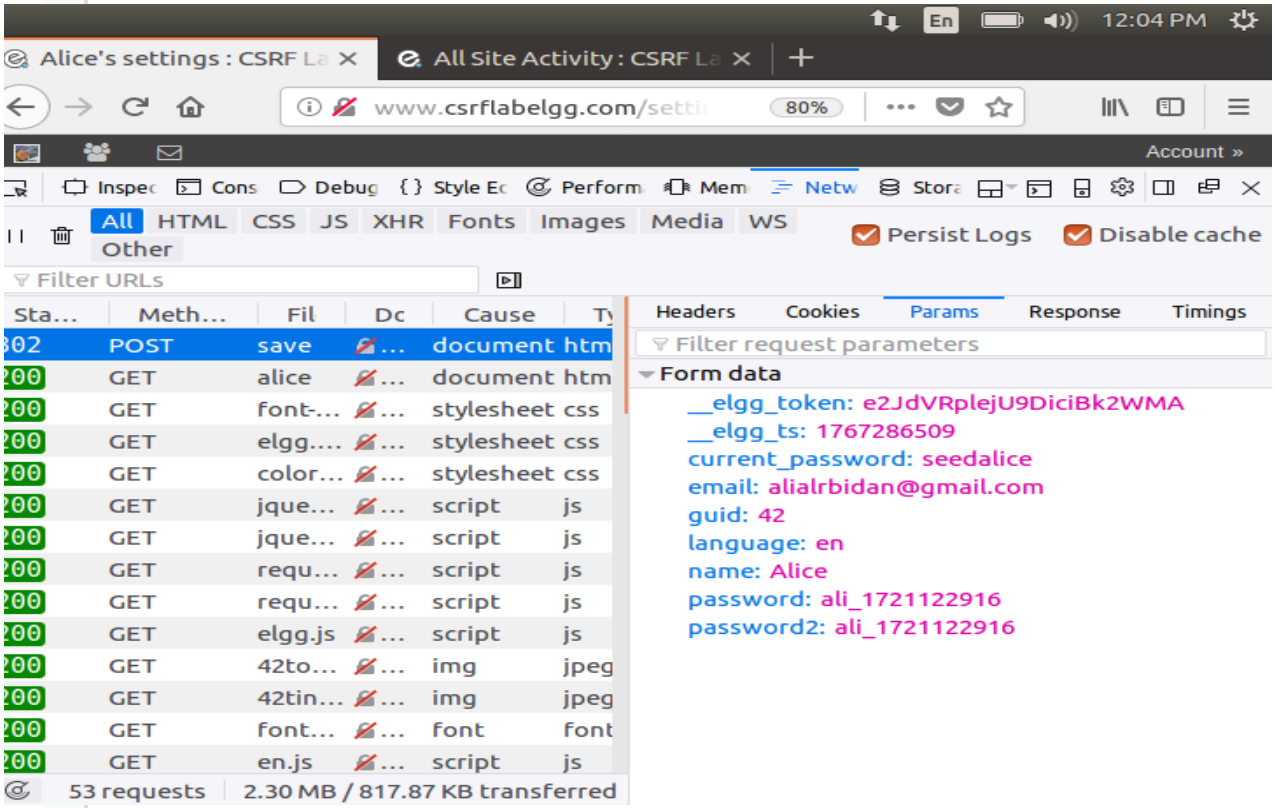
```
guid = "42"
name = "Alice"
language = "en"
email = "omranalrbidan@gmail.com"
password = "omran_1722204157"
password2 = "omran_1722204157"
```

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

إثبات النجاح

لقطة شاشة تثبت نجاح تغيير كلمة المرور:


ctivity : CSRF Lab Site - Mozilla Firefox
11:12 AM
Search your computer
All Site Acti
Page not fo
All Site Acti
All Site Acti
www.csrflabelgg.com/activity
80%
Account »
CSRF Lab Site
Password changed
Activity
Blogs
Bookmarks
Files
Groups
More »
All Site Activity
All
Mine
Friends
Filter
Show All
No activity
Search
Alice
Blogs
Bookmarks
Files
Pages
Wire posts
Powered by Elgg


12:04 PM
Alice's settings : CSRF La
All Site Activity : CSRF La
www.csrflabelgg.com/setti
80%
Account »
All
HTML
CSS
JS
XHR
Fonts
Images
Media
WS
Other
Persist Logs
Disable cache
Filter URLs
Sta...
Meth...
Fil
Dc
Cause
POST save document htm
GET alice document htm
GET font-... stylesheet css
GET elgg.... stylesheet css
GET color... stylesheet css
GET jque... script js
GET jque... script js
GET requ... script js
GET requ... script js
GET elgg.js script js
GET 42to... img jpeg
GET 42tin... img jpeg
GET font... font font
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 JavaScript يستغل ثغرة XSS ليكون ذاتي الانتشار. الكود ينفذ التالي:

- يضيف المستخدم "Charlie" كصديق تلقائيًا عند زيارة الصفحة
- يعرض رسالة تأكيد للمستخدم تفيد بنجاح إضافة الصديق
- يتكاثر ذاتيًا وينتقل إلى الملفات الشخصية للمستخدمين الآخرين

آلية الانتشار

آلية التكرار الذاتي:

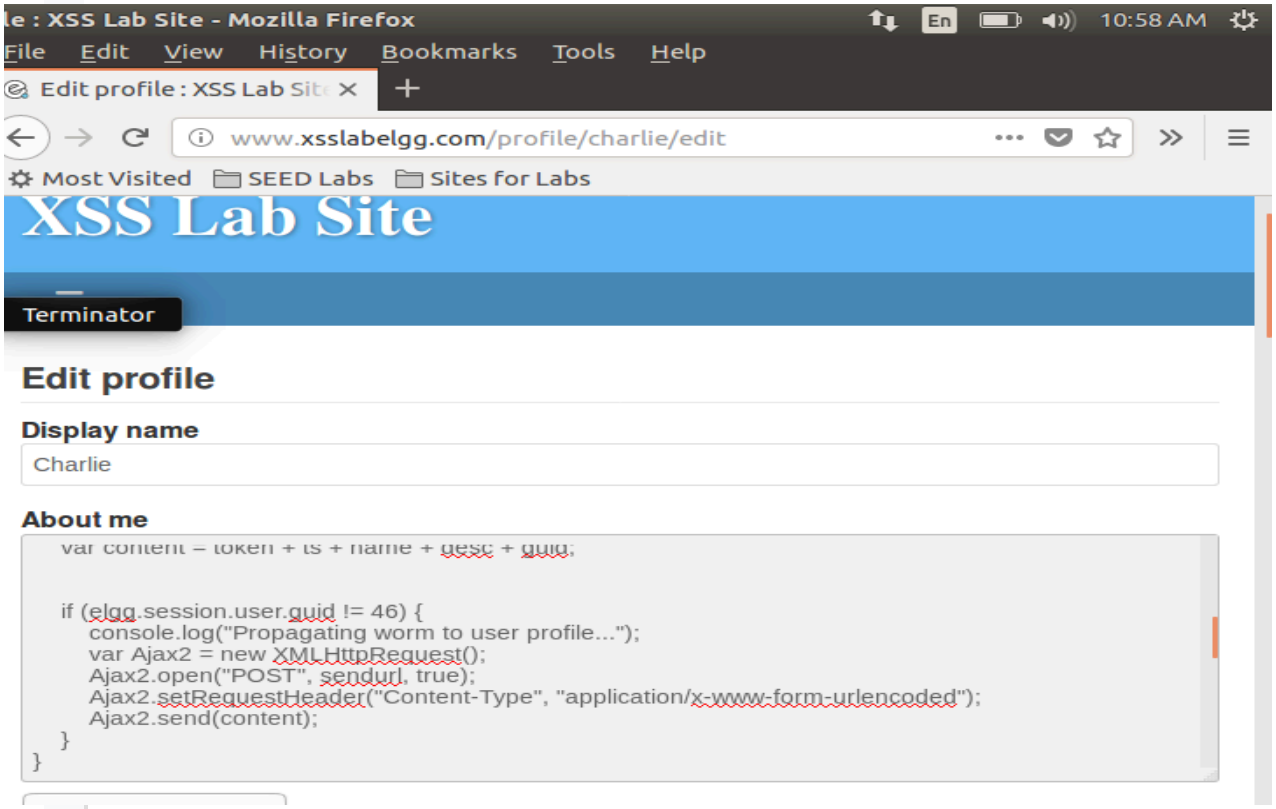
- يستخرج الكود البرمجي نفسه من عنصر script الحالي
- يقوم بتشفير الكود بشكل مناسب للإدراج في حقل الوصف
- يرسل طلب POST لتعديل وصف المستخدم الحالي
- يضيف الكود المشفر إلى وصف المستخدم مع النص "Samy is my hero"
- يستثني المستخدم "Charlie" (ID: 46) لمنع الحلقات اللانهائية

دورة الانتشار:

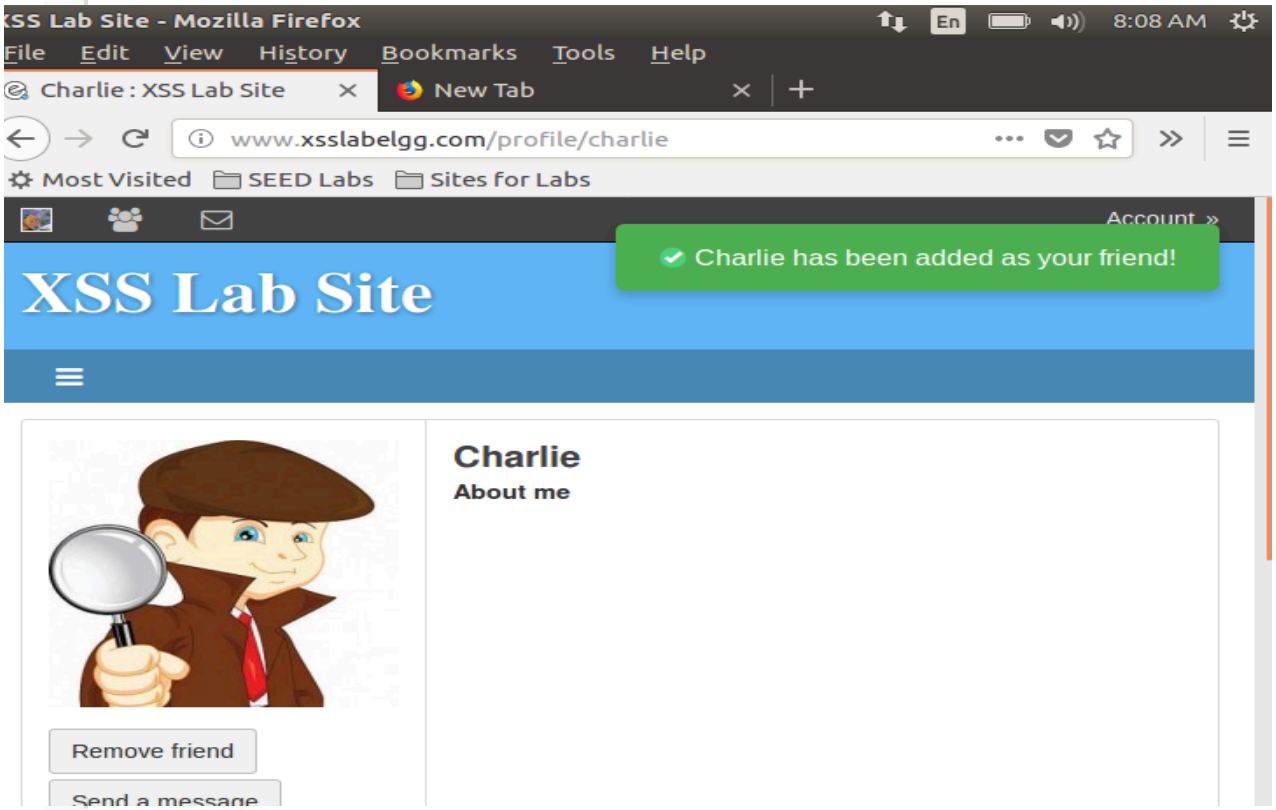
1. المستخدم alice يزور صفحة تحتوي على الدودة (charlie)
2. تضاف "Charlie" تلقائيًا كصديق
3. تنسخ الدودة نفسها إلى وصف المستخدم الزائر (alice)
4. عند زيارة أي مستخدم آخر (samy) لملف هذا المستخدم، تنتقل الدودة إليه
5. تتكرر الدورة مع كل مستخدم جديد

إثبات الانتشار

1- لقطة شاشة تظهر الكود الموجود في حقل ال about في charlie profile



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



3 - بعد ذلك قام samy بزيارة بروفايل alice فاصبح صديق charlie