تقرير وظيفة الأمن السيبراني الثانية

أمن تطبيقات الويب (Web Application Security)

بيئة العمل: مختبرات SEED Ubuntu

اسم الطالب: علي نايف الربيدان

الرقم الجامعي: 1721122916

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 كصفحة "404 Not Found" لتضليل المستخدم بينما تنفذ الهجوم في الخلفية.

الهدف المحقق

تم تغيير كلمة المرور الخاصة بالمستخدم "Alice" إلى: **ali_1721122916**

تحليل آلية العمل

آلية عمل الهجوم:

- يستغل الهجوم جلسة المستخدم المصادق عليها مع الموقع المستهدف
- عند زيارة الصفحة الخبيثة، ينفذ JavaScript تلقائيًا
- ينشئ نموذج (form) مخفيًا يحتوي على معلمات تغيير كلمة المرور
- يرسل النموذج تلقائيًا إلى خادم الموقع المستهدف
- يتعامل الخادم مع الطلب كأنه صادر من المستخدم نفسه

تحليل طلب HTTP:

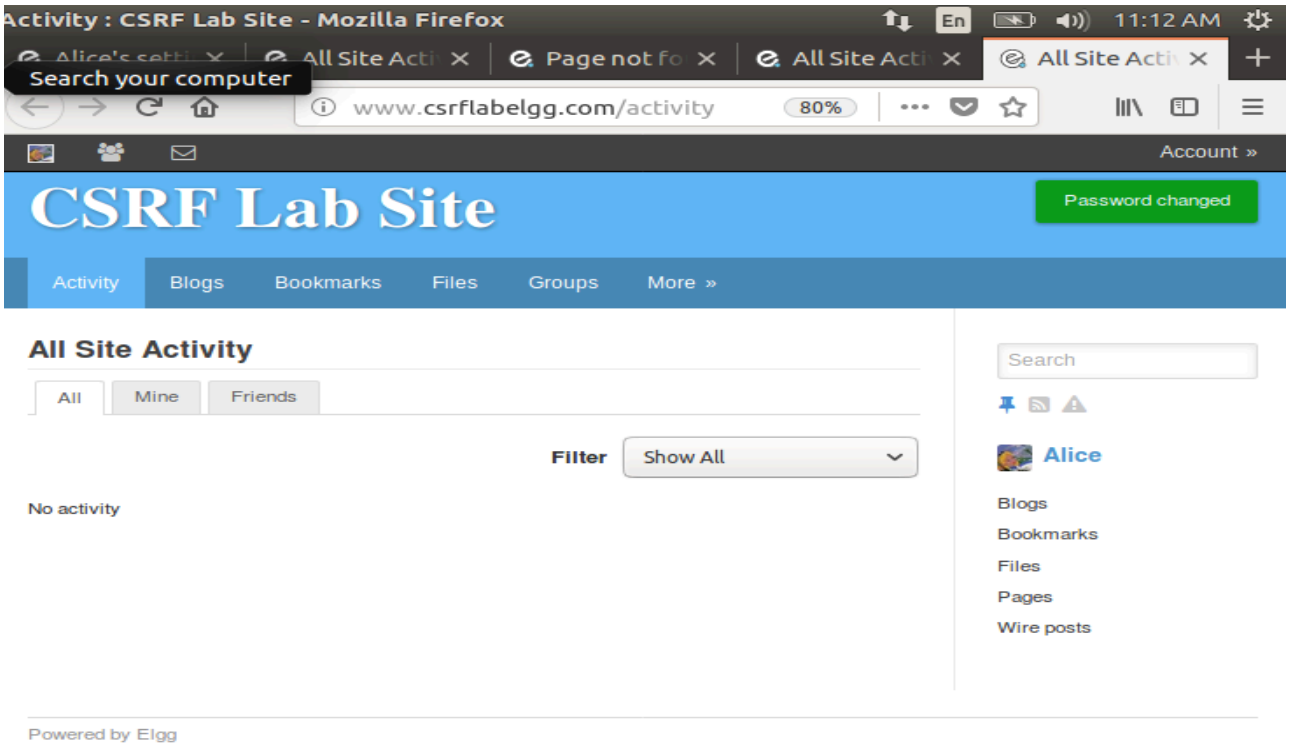
- **طريقة الطلب:** POST
- **الرابط المستهدف:** http://www.csrflabelgg.com/action/usersettings/save
- **المعلمات الأساسية:** guid, name, email, password, password2

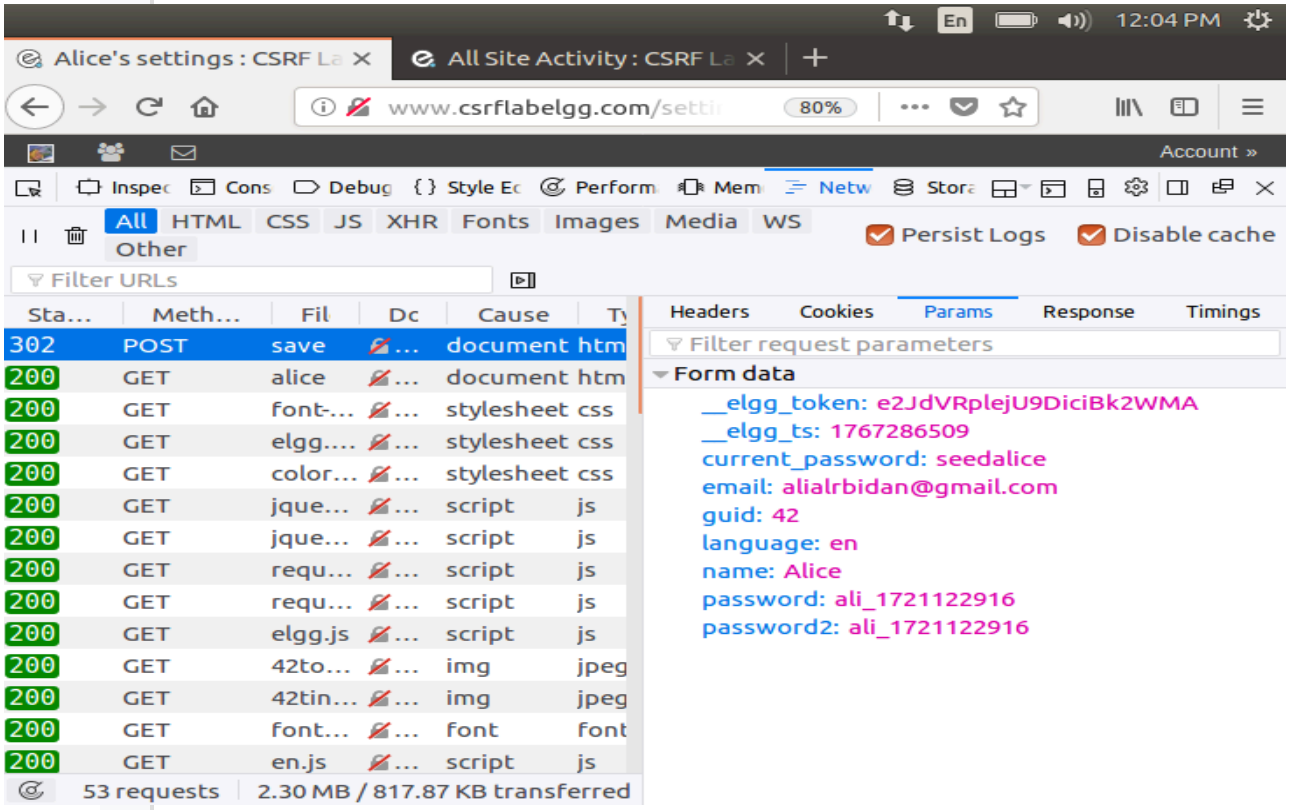
```
;addField("guid", "42")

;addField("name", "Alice")

;addField("language", "en")

;addField("email", "alialrbidan@gmail.com")

;addField("password", "ali_1721122916")

;addField("password2", "ali_1721122916")
```

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

إثبات النجاح

لقطة شاشة تثبت نجاح تغيير كلمة المرور:


Activity : CSRF Lab Site - Mozilla Firefox
11:12 AM
Search your computer
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 »
Inspec
Cons
Debug
Style Ec
Perform
Mem
Netw
Stora
All
HTML
CSS
JS
XHR
Fonts
Images
Media
WS
Other
Persist Logs
Disable cache
Filter URLs
Sta...
Meth...
Fil
Dc
Cause
302 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 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:

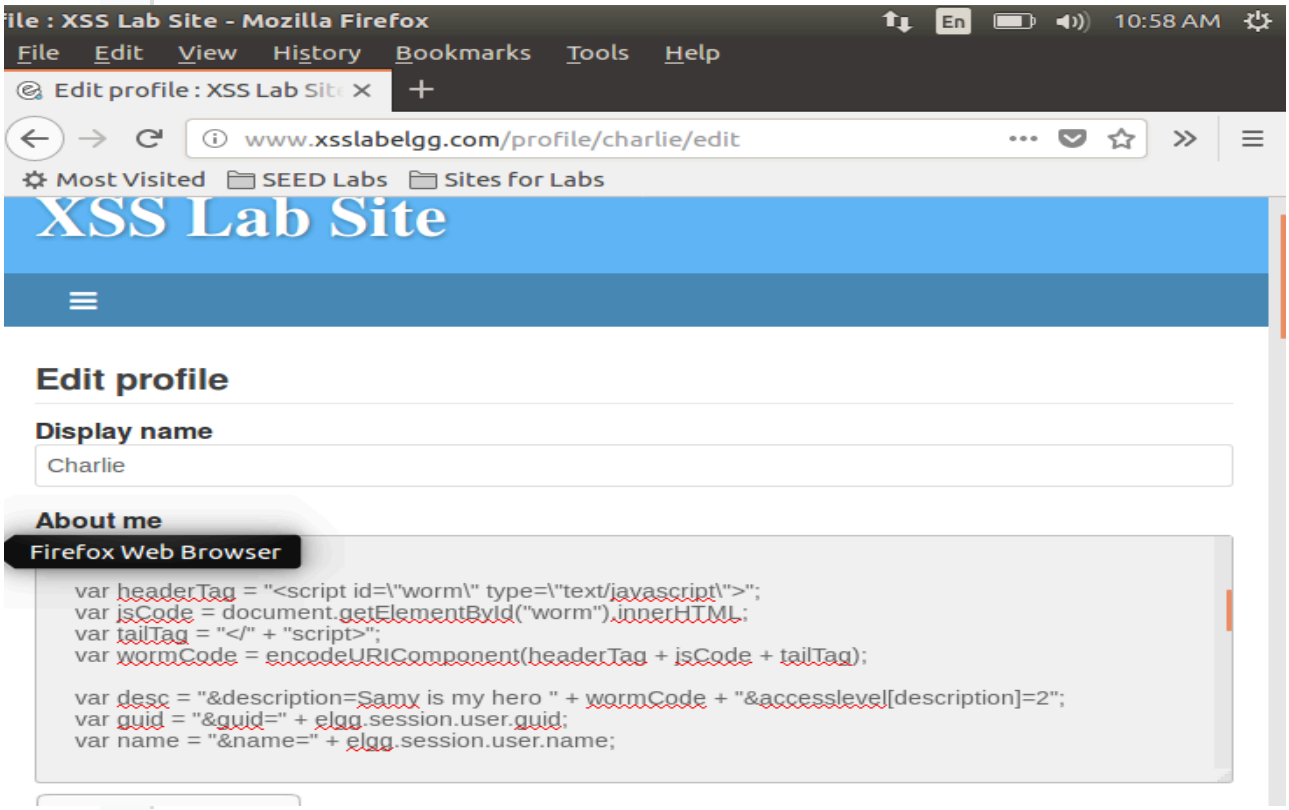
1. المستخدم samy يزور صفحة تحتوي على الدودة (charlie)
2. تضاف "Charlie" تلقائيًا كصديق
3. تنسخ الدودة نفسها إلى وصف المستخدم الزائر (samy)
4. عند زيارة أي مستخدم آخر (alice) لملف هذا المستخدم، تنتقل الدودة إليه

5. تتكرر الدورة مع كل مستخدم جديد

إثبات الانتشار

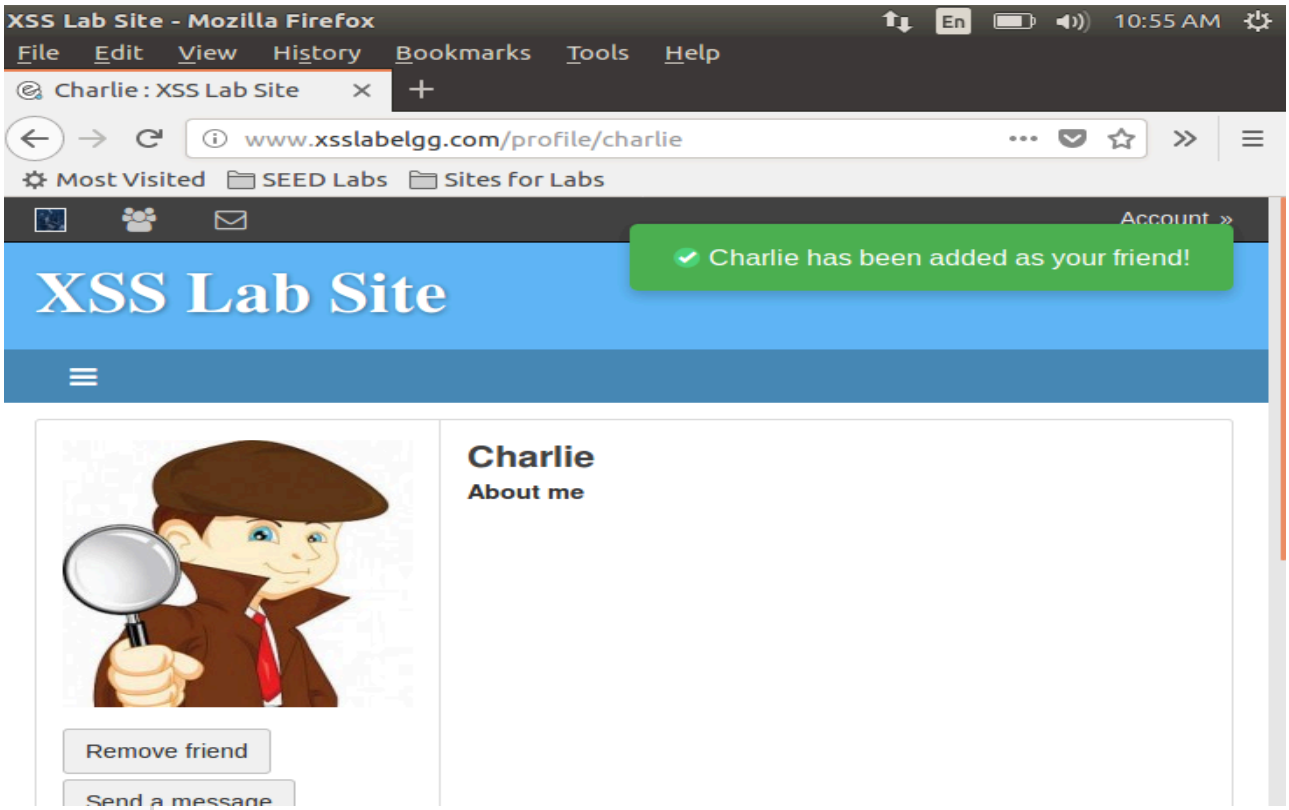
لقطات شاشة توضح تزايد قائمة الأصدقاء:

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

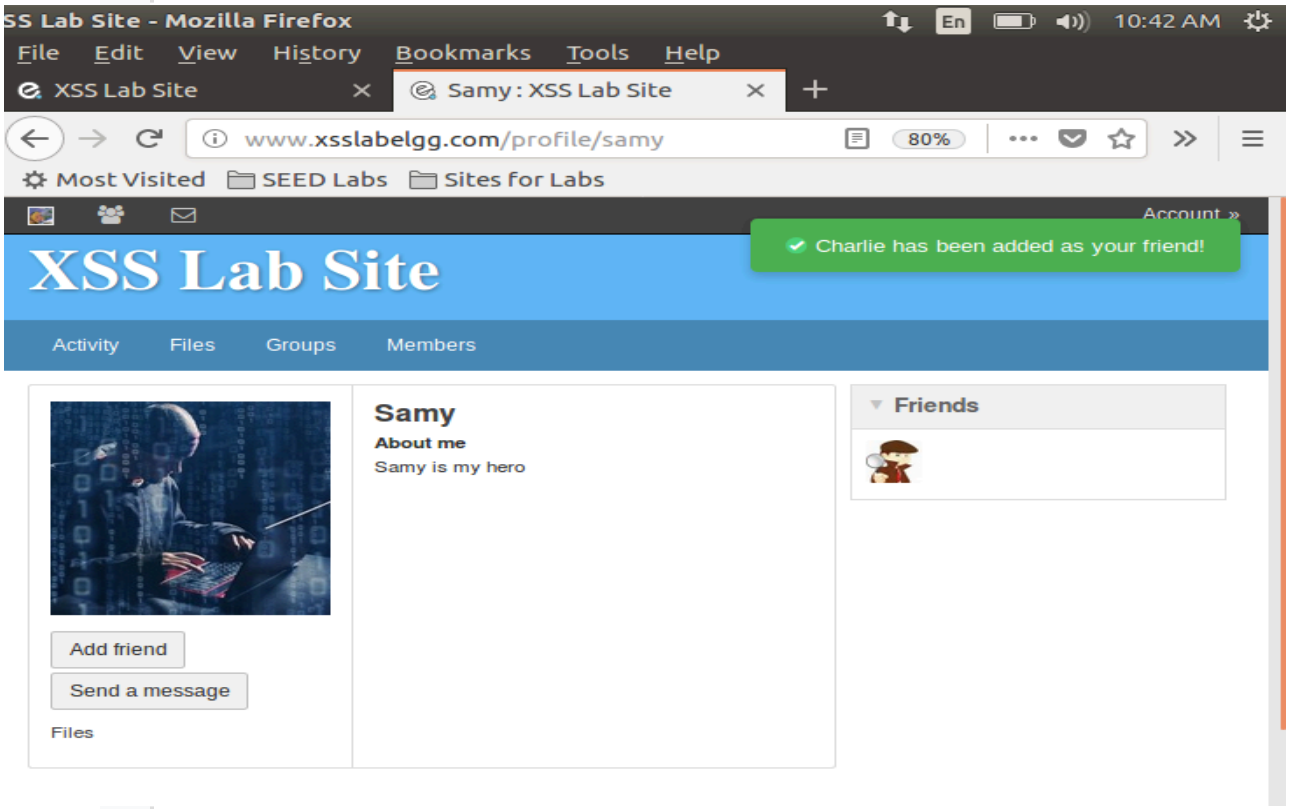


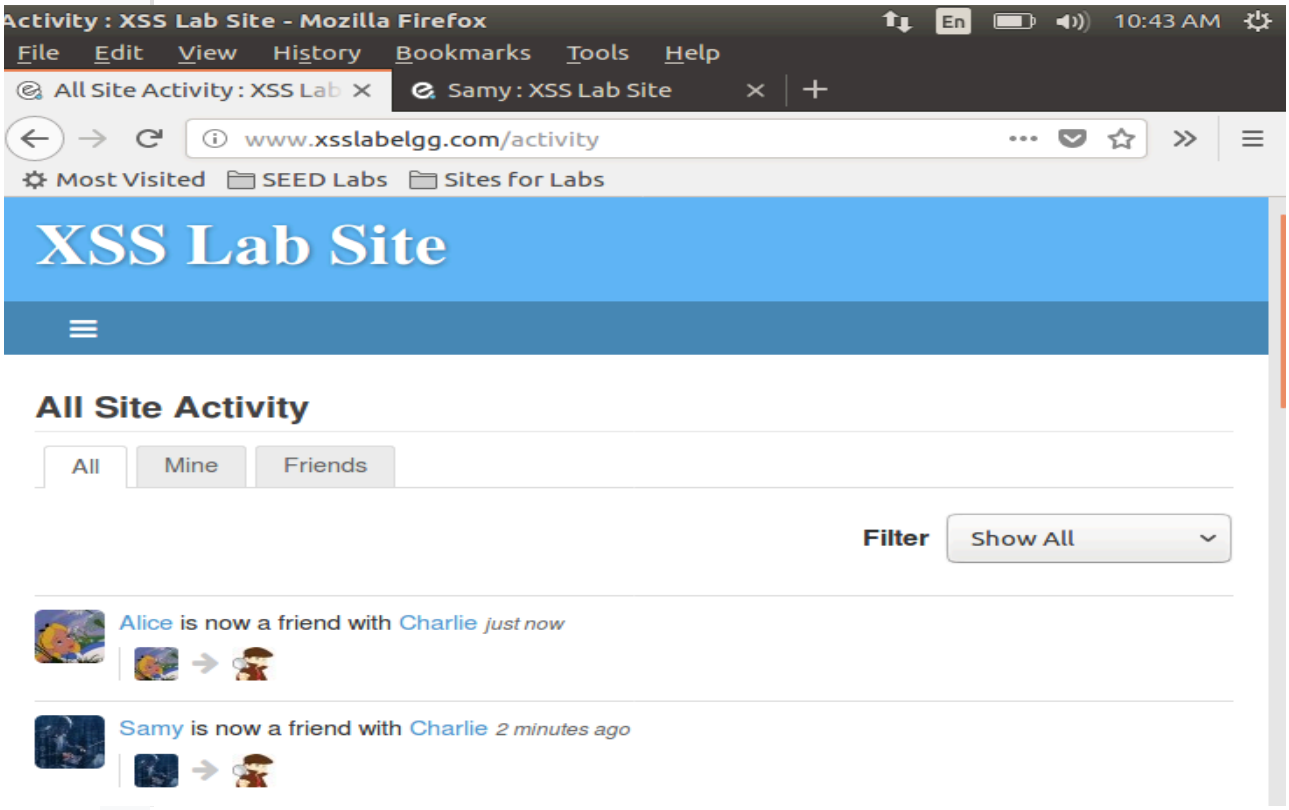
2 - هنا قام سامي بزيارة charlie profile بمجرد الدخول للصفحة اصبح سامي صديق شارلي وانتقلت ثقرة ال XSS الى بروفايل سامي

هنا الكود ليس ضاهرا للامان



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




Activity : XSS Lab Site - Mozilla Firefox
En
10:43 AM
File Edit View History Bookmarks Tools Help
All Site Activity : XSS Lab
Samy : XSS Lab Site
www.xsslabelgg.com/activity
Most Visited
SEED Labs
Sites for Labs
XSS Lab Site
All Site Activity
All
Mine
Friends
Filter
Show All
Alice is now a friend with Charlie just now
Samy is now a friend with Charlie 2 minutes ago