الأدوات والثغرات فى الأمن السيبرانى

سلطان الحربي

CSRF

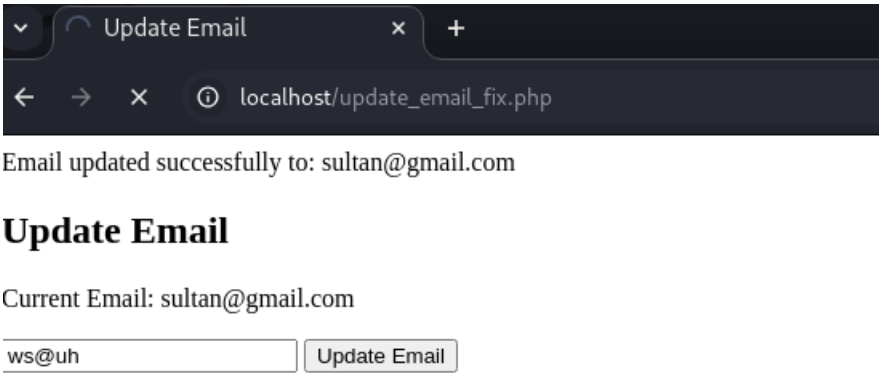
ثغرة CSRF اختصارًا لـ **(Cross-Site Request Forgery)**هي ثغرة في أمان تطبيقات الويب تسمح للمهاجم بتنفيذ طلبات غير مصرح بها نيابة عن المستخدم دون علمه. تحدث الثغرة عندما يقوم المهاجم بإجبار متصفح المستخدم على إرسال طلب إلى موقع مستهدف حيث يكون المستخدم قد قام بتسجيل الدخول بالفعل، ويمتلك جلسة نشطة **(Session)**.

الأدوات المستخدمة:

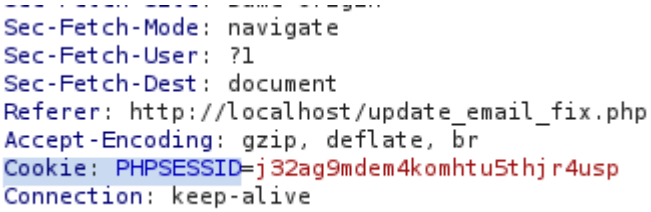
Burp suite-1

msCSRF -2

تم تصميم موقع بسيط لاختبار الاختراق عليه



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



قمنا بتشغيل الاداه ومن ثم ارسال طلب مزيف وتم بنجاح

مثال على كود برمجي بدون token معرض للاختراق

```php
<?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

```php
// بيانات تسجيل الدخول الثابتة
$correct_username = 'admin';
$correct_password_hash = password_hash('password123', PASSWORD_DEFAULT); // ر 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_ha
        $_SESSION['username'] = $username;
        $_SESSION['email'] = 'user@example.com'; // البريد الإلكتروني الأولي

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