

، سأوجهك بالخطوات التي SQL Injection واكتشاف ثغرة DVWA لإنجاز هذا التحدي باستخدام تطبيق :تحتاجها لتحقيق الهدف المطلوب:

1. DVWA تحميل وتثبيت

- DVWA من GitHub. قم بتحميل
- إذا WAMP أو XAMPP باستخدام أدوات مثل (localhost) ثبت التطبيق على خادم محلي Linux. إذا كنت تستخدم LAMP ، أو Windows كنت تستخدم نظام

2. DVWA إعداد

- :بعد التثبيت، قم بتسجيل الدخول إلى التطبيق باستخدام بيانات الدخول الافتراضية
 - admin :اسم المستخدم
 - password :كلمة المرور
 - (DVWA Security) انتقل إلى إعدادات التطبيق في لوحة التحكم، واضبط مستوى الأمان
- .لسهولة استغلال الثغرات Low على

3. SQL Injection استغلال ثغرة

1. في القائمة الجانبية للتطبيق SQL Injection اختر خيار
2. (User ID). ستظهر واجهة تحتوي على حقل لإدخال رقم المستخدم
3. :جرب إدخال الاستعلام التالي لاختبار الثغرة

' OR '1'='1

- .هذا الاستعلام يستغل ضعف التحقق في الإدخال للوصول إلى قاعدة البيانات
4. إذا كانت الثغرة موجودة، سيعرض التطبيق جميع سجلات المستخدمين الموجودة في قاعدة البيانات.

4. تحليل البيانات وإثبات النجاح

- :التقط لقطات الشاشة التالية
- 1. .(ضار SQL إدخال استعلام) لقطعة توضح استغلال المدخلات
- 2. لقطعة للنتيجة التي تظهر جميع بيانات المستخدمين أو البيانات الحساسة بعد استغلال الثغرة.
- 3. لقطعة توضح تفاصيل قاعدة البيانات التي تمكنت من الوصول إليها

5. رفع مستوى المهارات

- :بعد إثبات استغلال الثغرة، حاول فهم كيفية تأمين التطبيق
 - .mysql_real_escape_string() إضافة فلتر للإدخال: استخدم دوال مثل
 - (Prepared Statements) استخدام استعلامات محضرة
- ضارة.