

تقرير: تحدي الأسبوع الثالث - استغلال ثغرة DVWA في SQL

المقدمة والاعتذار

أود بدايةً الاعتذار عن عدم تمكيني من توفير البحث مدعومًا بالصور التوضيحية كما هو مطلوب، وذلك بسبب تواجدي في منطقة تعاني من انقطاع مستمر للكهرباء بالإضافة إلى ضعف شديد في شبكة الاتصال، مما جعل من الصعب جدًا رفع أو إرسال الصور في الوقت الحالي.

وعلى الرغم من هذه الظروف الخارجية عن إرادتي، إلا أنني بذلت كل جهدي في البحث والدراسة المتواصلة لفهم الثغرة بشكل عملي، وتمكنت من الوصول إلى الحلول المطلوبة مع توثيقها نصيًا بالتفصيل في هذا التقرير، على أمل أن يعوض ذلك عن نقص الصور.

- تعريف عام بالتحدي

،وتثبيته وتشغيله في بيئة محلية، GitHub تطبيق الويب الضعيف للغاية) من DVWA التحدي يطلب تحميل تطبيق للوصول إلى بيانات حساسة في قاعدة البيانات SQL Injection ومن ثم استغلال إحدى الثغرات المتاحة وهي ثغرة

- الخطوات التفصيلية

الخطوة الأولى

DVWA تحميل وتثبيت

الرسمي GitHub من مستودع DVWA تقوم بتنزيل تطبيق

تم فك ضغط الملف ووضعه في المسار التالي

C:\xampp\htdocs\DVWA

بنجاح MySQL و Apache وتفعيل خدمتي XAMPP تم تشغيل برنامج

الخطوة الثانية

: إعداد قاعدة البيانات

:عبر المتصفح، تم الدخول للرابط

<http://localhost/DVWA/setup.php>

.لتجهيز قاعدة البيانات الخاصة بالتطبيق Create/Reset Database تم الضغط على زر

الخطوة الثالثة

: تسجيل الدخول

:عبر الرابط DVWA تم تسجيل الدخول إلى

<http://localhost/DVWA>

:بيانات الدخول الافتراضية المستخدمة

admin : اسم المستخدم

password : كلمة المرور

الخطوة الرابعة

SQL Injection : تحديد واستغلال ثغرة

SQL Injection. بعد تسجيل الدخول، ومن القائمة الجانبية، تم اختيار خيار

.وهو الحقل المستهدف بالتجربة، User ID ظهرت صفحة تحتوي على حقل إدخال

الخطوة الخامسة

: تنفيذ استغلال الثغرة

:تم إدخال الكود التالي في الحقل

1' OR '1'=1

حيث يتم تجاوز التحقق من المدخلات، ويتم جلب جميع البيانات SQL Injection هذا الاستعلام يستغل وجود ثغرة من جدول المستخدمين بدون أي شروط

الخطوة السادسة

: استخراج البيانات المسربة

بعد تنفيذ الاستعلام، ظهرت بيانات جميع المستخدمين (أسماء المستخدمين وكلمات المرور) المخزنة في قاعدة البيانات.

- اللقطات المطلوبة التوضيحية

نظرًا للظروف الفنية التي تم ذكرها سابقًا، لم أتمكن من التقاط وإرفاق الصور التوضيحية. لكن الخطوات السابقة موثقة بشكل نصي دقيق، ويمكن إعادة تطبيقها عمليًا والحصول على نفس النتائج

- الدروس المستفادة

DVWA. تعلمت كيفية إعداد بيئة اختبار آمنة باستخدام

.وكيف يمكن استغلالها SQL Injection فهمت آلية عمل ثغرات

.تعلمت أهمية التحقق من مدخلات المستخدم لحماية الأنظمة من هذه الثغرة

.والتعامل مع تطبيقات الاختبار XAMPP اكتسبت خبرة عملية في تشغيل خوادم محلية عبر

الخاتمة

رغم ضعف الشبكة وانقطاع الكهرباء المتكرر، إلا أنني حرصت على إكمال هذا التحدي بأفضل صورة ممكنة مع شرح تفصيلي لجميع الخطوات والحلول التي توصلت إليها من خلال دراستي وبحثي المستمر

آمل أن يكون هذا التقرير يعكس الجهد المبذول رغم الظروف وأتمنى أن ينال قبولكم