SQL Injection

تلخيص ثغرت SQL: ثغرة SQL Injection هي ثغرة أمنية شائعة في تطبيقات قواعد البيانات، وتسمح للمهاجم بحقن أوامر SQL ضارة في استعلامات قاعدة البيانات. يمكن أن تؤدي هذه الثغرة إلى استخراج معلومات حساسة أو تعديل قاعدة البيانات أو حذفها بشكل غير مصرح به.

1. فهم SQL: SQL هو لغة برمجة تُستخدم للتحكم في قواعد البيانات. يتم تنفيذ استعلامات SQL لاسترداد أو تحديث أو حذف البيانات في قاعدة البيانات

.2 استعلامات غير آمنة: في بعض التطبيقات، يتم بناء استعلامات SQL باستخدام بيانات المستخدم بدون التحقق من صحتها أو تهيئتها بشكل صحيح. وهنا يحدث خطأ، حيث يمكن للمهاجم إدخال بيانات تحتوي على أوامر SQL ضارة .

.3 نقاط الضعف: تكمن نقاط الضعف في الطرق التي يتم بها تشكيل استعلامات SQL. على سبيل المثال، استخدام تعليمات SQL داخل سلاسل نصية أو عدم التحقق من بيانات المدخلات قبل استخدامها في استعلام

4. أمثلة على الثغرة: على سبيل المثال، افترض أن لدينا صفحة تسجيل الدخول، وعند إدخال اسم المستخدم وكلمة المرور، يتم تشكيل استعلام SQL للتحقق من صحة بيانات المستخدم. إذا كان المطور لا يتحقق من المدخلات بشكل صحيح، يمكن للمهاجم إدخال "OR '1'='1" كقيمة لحقل كلمة المرور، وبذلك ستكون الشرط صحيحة دائمًا، ويتم تجاوز التحقق.

.5 الاستفادة من الثغرة: بعد استغلال ثغرة SQL Injection بنجاح، يمكن للمهاجم تنفيذ أوامر SQL ضارة مثل استرداد قائمة المستخدمين أو حذف البيانات أو تعديلها بشكل غير مصرح به.

لحماية التطبيقات من ثغرة SQL Injection، يجب على المطورين تهيئة وتنظيف بيانات المدخلات وتحقق صحتها قبل استخدامها في استعلامات SQL، واستخدام إجراءات الحماية مثل استخدام تعليمات معدلة مسبقًا (Prepared Statements) أو استخدام ORM (Object-Relational Mapping) لتجنب تشكيل استعلامات SQL يدويًا.