مفهوم sql injection چیست؟

حالا ببینیم باگ sql چیست sql injection .یا sqli آسیب امنیتی وب است که به هکر اجازه مداخله در کوئری های دیتابیس را می‌دهد. مثلا هکرها دیتایی که در حالت عادی دسترسی به آن نیست را می‌بینند. ممکن است دیتایی باشد که متعلق به کس دیگری است یا دیتایی باشد که فقط خود برنامه امکان دسترسی به آن را دارد. در بسیاری موارد مهاجم این دیتا را پاک می‌کند یا تغییر می‌دهد در نتیجه روی محتوا و یا رفتار برنامه تاثیر می‌گذارد.

هر وب سایت و برنامه وبی که از دیتابیس sql مثل MySQL و Oracle و SQL Server استفاده می‌کند در معرض آسیب این حمله است Sql .زبان کوئری‌ها است که برای مدیریت اطلاعات ذخیره شده در دیتابیس‌ها طراحی شده است. پس با استفاده از آن می‌توان دسترسی و اصلاح و حذف اطلاعات را انجام داد. حتی می‌توان از دستورات sql برای اجرای برخی دستورات سیستم عاملی استفاده کرد. در نتیجه حمله sql injection موفق، عواقب زیادی دارد.

نکته مهم این است که باگ sql اصلا به دلیل ضعف sql نیست بلکه برنامه‌نویس‌ها با اشتباهات برنامه‌نویسی راه را برای هکرها و انجام تزریق sql هموار می‌کنند.

هکر ابتدا به دنبال ورودی‌های کاربری آسیب‌پذیر در صفحه وب یا برنامه وب می‌گردد چون بدین ترتیب می‌تواند مستقیم وارد کوئری sql شود. هکر، محتوای ورودی که malicious payload نامیده می‌شود و کلید اصلی حمله است را آماده می‌کند. پس از اینکه هکر این محتوا را وارد می‌کند، دستورات SQL مخرب در دیتابیس اجرا می‌شود.

در SQL Injection امکان اجرای SQL statement های مخرب فراهم می‌شود. این استیت منت‌ها کنترل دیتابیس سرور پشت برنامه وب را به دست می‌گیرند. هکرها از SQLi استفاده می‌کنند تا به صفحه وب، برنامه وب و بازیابی محتوای کل دیتابیس sql دست یابند تا بتوانند رکوردهای دیتابیس را اضافه و اصلاح و حذف کنند.

تاثیرات حمله sql injection موفق چیست؟

برخی مواقع مهاجم از انواع حملاتsql injection استفاده می‌کند تا سرور و دیگر زیرساخت‌ها را از سرویس خارج کند یا حمله دایس DoS – انجام دهد. همچنین دسترسی به سیستم عامل باعث می‌شود هکر بتواند به شبکه داخلی شما نفوذ کند. برای استفاده از خدمات تعمیر سرور hp و ارتقای آن روی لینک بزنید.

یک حمله موفق sql injection دسترسی کامل به تمام اطلاعات دیتابیس سرور را به هکر می‌دهد و روی دسترسی‌های غیرمجاز به اطلاعات حساس تاثیر می‌گذارد مثلا پسوردها، اطلاعات کارت اعتباری، اطلاعات مشتری و اطلاعات شخصی کاربر. بسیاری از هک‌های اطلاعات محرمانه در سال‌های اخیر با استفاده از انواع حملات sql injectionانجام شده است. برخی مواقع، مهاجم به سیستم های دولتی نفوذ می‌کند و در اصطلاح بک دور دارد در نتیجه مدت‌ها می‌تواند از اطلاعات استفاده کند بدون اینکه کسی متوجه شود.

هکر با تغییر در رکوردهای دیتابیس به اهداف خود می‌رسد مثلا در برنامه‌های مالی، انتقال وجه بین حساب‌ها انجام می‌دهد. با حذف رکوردی‌های دیتابیس و حتی جدول‌های آن، ممکن است برنامه از دسترس خارج شود تا زمانی که دیتابیس با استفاده از بکاپ‌ها ری‌استور شود. حتی ممکن است با بکاپ‌ها هم کامل نتوان دیتای کامل را به دست آورد.

انواع sql injection

انواع حملات sql injection عبارتند از:

۱. UNION
۲. Error Based
۳. Blind
٤. تزریق sql کور به دو روش Boolean وTime

نقص‌های برنامه‌نویسی، حفره‌های امنیتی وب سایت و نرم‌افزار، امکان ترزیق کد توسط هکر را فراهم می‌کند. ضعف در برنامه‌نویسی، استفاده نادرست از متغیرهای کنترل نشده، و استفاده از دستورات نامطمئن و غیراصولی، کامپایلر را به سمت اجرای دستورات غیرمجاز سوق می‌دهد. به مثال زیر دقت کنید.

کوئری‌های Select دارای قسمت‌های زیر هستند:

۱. دستور :Select انتخاب ستون‌های مورد نظر
۲. دستور :Fromکدام جدول برای انتخاب ستون‌های مورد نظر استفاده شود.
۳. دستور :Whereشروط کوئری که **تزریق sqlاز این طریق انجام می‌شود.**
٤. عبارات و پارامترهای دیگر

اگر هکر در فیلد یوزرنیم عبارت ۱۰۵ OR ۱=۱ را وارد کند، کوئری select به شکل زیر خواهد بود:

```
SELECT * FROM Users WHERE UserId = ۱۰۵ OR ۱=۱;
```

چون همیشه ۱=۱ است، تمام ردیف‌های جدول Users را برمی‌گرداند.

اگر از دستور زیر استفاده شود هکر با یک دستور ساده، توانسته به تمام نام‌های کاربری و پسوردها دست یابد:

```
SELECT UserId,  Name,  Password FROM Users WHERE UserId = ۱۰۵ or ۱=۱;
```

اگر هکر در فیلد پسورد عبارت password’ OR ۱=۱ را وارد کند، کوئری select به شکل زیر خواهد بود:

```
SELECT id FROM users WHERE username='username' AND password='password' OR ۱=۱'
```

چون همیشه ۱=۱ است، در نتیجه اولین id از جدول Users را برمی‌گرداند و اصلا مهم نیست username و password چی هستند. معمولا اولین کاربر در جدول کاربران، کاربر ادمین است. بدین ترتیب هکر نه تنها به دیتابیس دسترسی یافته است بلکه امتیازات ادمین را هم دارد.

جلوگیری از حمله sql injection

برای جلوگیری از حمله sql injection و مقابله با باگ موارد زیر را در نظر بگیرید:

۱. اعتبارسنجی ورودی، افزایش امنیت فرم‌ها برای جلوگیری از ورود کوئری غیرمجاز و بررسی دایمی اطلاعات ورودی قبل از ارسال آنها به دیتابیس به عنوان Query مثلا اینکه کاراکترهای غیرمجاز نداشته باشد یا ورودی مستقیم نگیرد.
۲. ایجاد چند کاربر با دسترسی های مختلف به دیتابیس
۳. توجه کنید پیغام‌های خطایی که به کاربر نمایش داده می‌شود. مثلا "نام کاربری نمی‌تواند شامل اعداد باشد" هکر را آگاه می‌کنید که نباید در نام کاربری اعداد وارد کند. طوری این پیغام‌ها را طراحی کنید که نقاط ضعف سایت برای هکر نمایان نشود.
٤. آپدیت محتوای سایت به جدیدترین نسخه
٥. بررسی منظم دسترسی کاربران به دیتابیس. این کار باعث می‌شود اگر کاربری هک شده باشد، متوجه شوید و دسترسی آن را قطع کنید.
٦. افزایش امنیت سایت و هاست و دیتابیس آن
۷. استفاده از پسوردهای قوی و پیچیده برای دیتابیس