حمله تزریق کد به پایگاه داده یا sql injection

این حمله روشی است که طی آن داده های ساکن در یک پایگاه داده که از طریق firewall محافظت می شوند، مورد هدف قرار قرار می گیرند.

ایران هشدار - این آسیب پذیری جزء ده آسیب پذیری رایج نرم افزارهای وب در سال ۲۰۰۷ تا کنون بوده است. این حمله روشی است که طی آن داده های ساکن در یک پایگاه داده که از طریق firewall محافظت می شوند، مورد هدف قرار قرار می گیرند. این حمله زمانی که یک مهاجم قادر به اضافه کردن یک سری از عبارت های sql در یک query ، یا دستکاری داده های ورودی کاربر در برنامه مبتنی بر وب باشد، صورت می پذیرد. در واقع در این حمله، فرد مهاجم با استفاده از دانش خود می تواند از نقص امنیتی موجود در کدهایی که برنامه نویس سایت نوشته، استفاده کند و سایت مد نظر خود را در معرض خطر قرار دهد. پس از آن، افشای داده های مهم دیتابیس از قبیل رمزهای عبور و اطلاعات فردی کاربران و ... کمترین کاری است که هکر می تواند انجام دهد.

این آسیب پذیری زمانی که ورودی های منتهی به پایگاه داده محدود نشده باشد، ایجاد می شود و سپس هکر دستوراتی علاوه بر دستورات و درخواست هایی که به سرور ارسال می شود، را به پایگاه داده ارسال می کند و اطلاعات مد نظر خود را از آن خارج می کند. جالب اینجاست که این حمله می تواند با وجود فایر وال و سیستم های تشخیص نفوذ، کار کند و به لایه داده ها دسترسی پیدا کند. در سال های اخیر هدف این حمله ها بیشتر ذخیره کردن داده های مخرب در دیتابیس و انتشار آنها از طریق وب سایت هایی که میزبان این دیتا بیس ها هستند، بوده است. اما گاهی هدف آن سرقت داده های حساس یا تغییر یا تخریب داده ، اجرای دستورات admin روی دیتابیس و یا حتی در مواردی در اختیار گرفتن مکانیزم کل ماشین است.

انواع حملات در injection sql

۱. حملات برنامه ریزی شده
۲. حملات کور

در حملات برنامه ریزی شده، برای بدست آوردن دسترسی نا محدود و غیر مجاز، کدی به صورت مستقیم یا غیر مستقیم به کد کاربر اضافه می شود.

حملات کور، به صورتی است که طی آن مهاجم به اطلاعات حساس تنها با جستجوی یک سری از سوالات درست و نادرست از طریق دستورات sql دسترسی پیدا می کند و سپس اطلاعات بر اساس پاسخ های ارائه شده توسط نرم افزار استخراج می شوند. در واقع مهاجم به جای گرفتن پیام های خطا، به داده های مورد نظر دست می یابد و در این حملات مهاجم شیوه برنامه را تغییر داده و هنگامی که جزئیات پیام خطا و صفحه خطا در برخی از صفحه های عمومی پنهان نباشد، قادر به استخراج اطلاعات برای آماده سازی حمله است.

اداره حراست آموزشکده شهید یزدانپناه سنندج