عنوان مقاله:

تشخیص حمله تزریق SQL با استفاده از تکنیکهای یادگیری ماشینی: مروری سیستماتیک بر تحقیقات پیشین

محل انتشار:

هفتمین همایش بین المللی مهندسی برق، علوم کامپیوتر و فناوری اطلاعات (سال: 1401)

تعداد صفحات اصل مقاله: 19

نویسندگان:

ماهیار حسینی – استادیار گروه کامپیوتر موسسه آموزش عالی مارلیک نوشهر

میثم سبحانی – دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات موسسه آموزش عالی مارلیک نوشهر

خلاصه مقاله:

امروزه اینترنت به یکی از الزامات اساسی برای همه زمینه های زندگی روزمره تبدیل شده است. و با رشد روزافزون منابع و داده های موجود بر روی پایگاه های داده، سودجویان زیادی را بر آن داشته که با توجه به اهداف مختلف بخواهند داده های موجود بر روی پایگاه داده را دستکاری یا سرقت کنند . برنامه های کاربردی مبتنی بر وب هم که امروزه درصد بالایی از برنامه ها را تشکیل میدهند، منبع و مقصد ذخیره اطلاعات و داده های با ارزش میباشند. این برنامه های کاربردی با امنیت خیلی بالایی پیاده سازی نمیشوند و معمولا تولیدکنندگان به دلیل کاهش هزینه های تولید نرم افزار، ارزیابیهای امنیتی را انجام نمیدهند. وجود آسیب پذیری در یک برنامه وب، میتواند دریچه ورود مهاجم به آن برنامه و سوء استفاده از آن آسیبپذیری باشد. به منظور به حداقل رساندن حملات موفق به برنامه های وب ، محققان رویکردهای مختلفی برای تامین امنیت و شناسایی آسیبهای ناشی از این گونه حملات ارایه کرده اند. حمله تزریق SQL، که از جمله آسیبرسانترین حملات برنامه های وب هستند معمولا۰ زمانی اتفاق میافتد که مهاجم(ها) داده ها را از سرورهای پایگاه داده تغییر، حذف، خوانش و کپی میکنند. یک حمله موفقیت آمیز تزریق SQL می تواند بر تمام جنبه های امنیتی از جمله محرمانه بودن، یکپارچگی و در دسترس بودن داده ها تاثیر بگذارد. SQL یا Structured Query Language (زبان پرسمان ساخت یافته) برای ارائه پرسمانها به سیستم های مدیریت پایگاه داده استفاده می شود. دانش تشخیص و بازدارندگی حملات تزریق SQL ، که به موجب آن برای بهبود توانایی تشخیص حمله، میتوان از تکنیکهایی از شاخه های مختلف علم استفاده کرد، حوزه تحقیق جدیدی نیست، اما همچنان دارای اهمیت و ارزش است. تکنیکهای هوش مصنوعی و یادگیری ماشینی برای کنترل حملات تزریق SQL آزمایش و استفاده شدهاند که نتایج امیدوارکننده ای را نشان میدهد. در این مقاله سعی شده با نگاهی اجمالی به انواع روش های تزریق، یک طبقه بندی از روش های پژوهشگران، برای دفاع در برابر حملات تزریق SQL، بیان شود. و نیز به بررسی تعدادی از ابزارهای پر کاربرد برای هر روش پرداخته شده است . دستاورد اصلی این مقاله پوشش دادن تحقیقات مرتبط با یادگیری ماشین و مدلهای یادگیری عمیق است که برای شناسایی حملات تزریق SQL استفاده میشوند. با این بررسی سیستماتیک، هدف بنده به روز نگه داشتن محققان و کمک به درک وجه مشترک بین حملات تزریق SQL و مقوله هوش مصنوعی است.

کلمات کلیدی:

تزریق SQL، یادگیری ماشینی، یادگیری عمیق، حملات فریبنده