کنگره بین المللی علوم و مهندسی
آلمان – هامبورگ
اسفند ماه ۱۳۹۶

تشخیص آسیب‌پذیری‌های منشأ حمله‌ی تزریق SQL در صفحات وب با استفاده از فازر بهینه

رضا خرمی[۱]*، مسعود باقری[۲]

۱- دانشجوی کارشناسی ارشد، دانشگاه جامع امام حسین، rkhorami@ihu.ac.ir
۲- استادیار گروه کامپیوتر، دانشگاه جامع امام حسین، m.bagheri@ihu.ac.ir

چکیده

وجود آسیب‌پذیری در یک برنامه‌ی وبی، می‌تواند دریچه‌ی ورود مهاجم به آن برنامه و سوء استفاده از آن آسیب‌پذیری باشد. از این‌رو در این پایان‌نامه، راه‌کاری جهت شناسایی آسیب پذیریری برنامه‌های وبی ارائه شده است. اهمیت مساله، ممانعت از حمله تزریق SQL به برنامه‌های وبی از طریق منافذ موجود در این برنامه‌ها و پایگاه‌داده‌های مورد استفاده‌ی آنها است. در این پایان نامه سعی بر آن است که با استفاده از روش فازینگ جعبه سیاه و تولید موارد آزمون مناسب و بهینه بتوانیم آسیب پذیری برنامه‌های وبی را به عنوان دسته ای عظیم از انواع مختلف نرم افزار، بدون در نظر گرفتن کد منبع آن ها، و فقط با استفاده از URL(متد GET) بدست آوریم. از این‌رو مساله اصلی، ایجاد فازر تشخیص آسیب‌پذیری با قدرت تشخیص آسیب بالا است.در این راستا در این پایان نامه طراحی و پیاده سازی فازر با استفاده از یک فرایند دو مرحله‌ای می‌باشد؛ در مرحله‌ی اول با استفاده از تکنیک‌های داده‌کاوی تکه‌سازی، خوشه‌بندی و دسته‌بندی، نام صفحات و پارامترهایی که بیشتر حائز اهمیت هستند از دیتاست بردار حملات استخراج می‌شود با این‌کار دیگر نیاز به تزریق موارد آزمون به تمام پارامترهای ارسالی به یک صفحه کمتر و باعث افزایش سرعت فاز می‌شود. در مرحله‌ی دوم با توجه به نوع پایگاه داده، قانون‌هایی برای تولید موارد آزمون بهینه ساخته شده است که تولید تست را از حالت تصادفی خارج کرده است. میزان موفقیت روش مذکور در مرحله‌ی اول کار در تشخیص نقاط آسیب‌پذیری ۷۹ درصد و در قسمت انجام عمل فازینگ، دقت ۱۰۰ درصد تنها با بردار وردی GET، نسبت به ابزارهای مشابه تشخیص آسیب‌پذیری حداقل با ۱۱ بردار ورودی، بر روی برنامه‌ی وبی مرجع آسیب‌پذیری به دست می‌آید.

واژه‌های کلیدی: آسیب پذیری نرم افزار، برنامه‌های وبی، تزریق SQL، فازر.

۱- مقدمه

مطابق گزارش‌های آماری در حال حاضر بیش از ۷۰ درصد حملاتی اینترنتی از طریق وب انجام می‌شود و بنابراین بخش عمده‌ای از تهدیدات از عدم تأمین امنیت کافی در برنامه‌های کاربردی به طور خاص برنامه‌های کاربردی تحت وب ناشی می‌گردد[۱].

امروزه یکی از حملات شایع و خطرناکی که بر روی برنامه‌های تحت وب انجام می‌گیرد، حمله تزریق SQL می‌باشد. این حمله توسط مؤسسه تحقیقاتی OWASP[۱] در سال ۲۰۱۳ و ۲۰۱۷، جایگاه اول در میان حملات تحت وب را داراست[۲].

[۱] Open Web Application Security Project (http://www.owasp.org)