با نظارت بر پایگاه داده می توانید تزریق SQL را تشخیص دهید. تزریق SQL به سختی قابل شناسایی است زیرا حمله پرس و جوهای اصلی را در پایگاه داده انجام می دهد ، هنگامی که مهاجم از آسیب پذیری برای انجام کارهای اضافی مانند تغییر محتوای پایگاه داده برای دسترسی ممتاز استفاده می کند ، بیشتر حملات شناسایی می شوند. از آنجا که تشخیص این تزریقات SQL دشوار است ، انجام اقدامات پیشگیرانه مهم است.

ساده ترین راه برای محافظت از خود در برابر تزریق SQL این است که اطمینان حاصل کنید همه اجزای خود را به روز نگه دارید. بیشتر مهاجمان به آسیب پذیری هایی که در نسخه های جدید اجزا components برطرف شده اند اعتماد می کنند ، بنابراین وب سایت هایی را که در نسخه های قدیمی و آسیب پذیر باقی مانده اند ، هدف قرار می دهند. هرچند این همه حملات را شامل نمی شود: برخی از مهاجمان می توانند از آسیب پذیری های روز صفر یا نامشخص برای به خطر انداختن وب سایت ها استفاده کنند. در چنین مواردی ، باید به محافظت عمومی از تزریق SQL مانند CloudProxy ، Sucuri Web Application اعتماد کنید. فایروال وب سایت داده های حمله را در شبکه Sucuri با هم مرتبط می کند تا درخواست های انجام شده برای تزریق SQL را شناسایی کند و آنها را قبل از رسیدن به وب سایت مسدود کند.

مزایای WAF

1. این قوانین به صورت رشته ای مطابقت ندارند ، اما در درختی از گره های SQL تجزیه می شوند و با ساختار منطقی و نه تفسیر نمادین ، ​​با لیست های مجاز / انکار مجموعه مطابقت دارند.

2. شما می توانید در مرحله آزمایش بتا "گردش کار عادی" یک برنامه فایروال را بیاموزید ، قوانین را تنظیم کنید و آن را در محیط تولید آزاد کنید.

3. چنین دیوار آتش یک نکته عالی برای ارسال گزارش ها و رویدادهای نقابدار به سیستم های SIEM / IDS علاوه بر WAF و نظارت بر پایگاه داده است.

4. می توانید ترکیبی خاص از قوانین را تنظیم کنید تا برخی از درخواست ها را به جای پایگاه داده تولید واقعی ، به پایگاه داده honeypot هدایت کنید.