

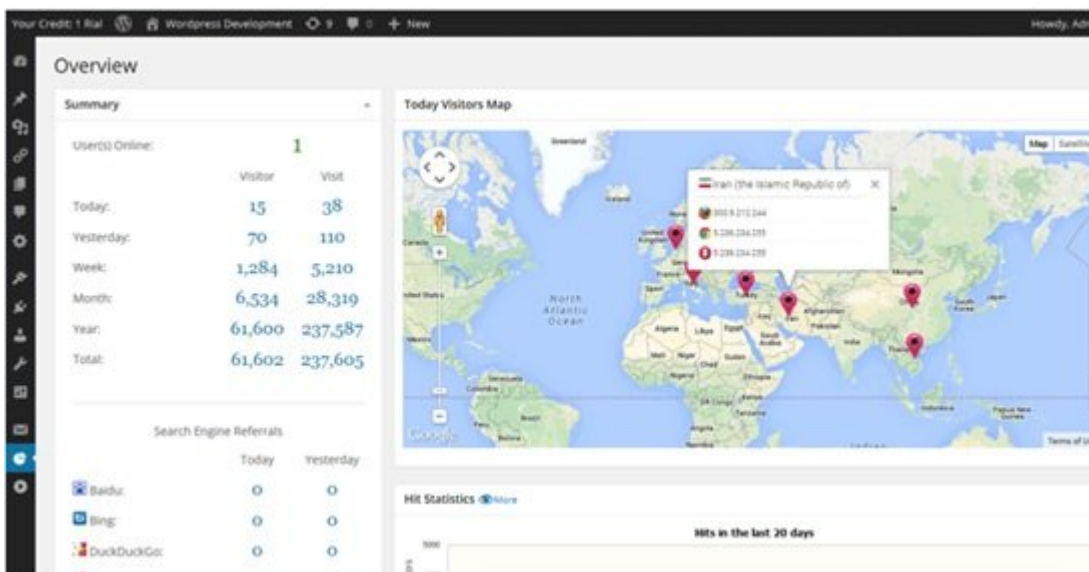
# WordPress Hacking

## SQL Injection Attack



کارشناسان امنیتی به تازگی گزارش کرده‌اند یک آسیب‌پذیری تزریق کد SQL را در یکی از معروف‌ترین افزونه‌های وردپرس شناسایی کرده‌اند. این افزونه که روی بیش از 300 هزار سایت وردپرس نصب شده است اکنون این سایت‌ها را در معرض یک حمله هکری جدی قرار داده است. هکرها به واسطه این آسیب‌پذیری قادر هستند به بانک اطلاعاتی کامل یک سایت دسترسی پیدا کرده یا بدتر از آن کنترل یک سایت را به دست آورند.

آسیب‌پذیری تزریق کد SQL در افزونه WP Statistics که در ارتباط با آمارگیری مورد استفاده قرار می‌گیرد شناسایی شده است. افزونه یاد شده به مدیران سایت‌ها این توانایی را می‌دهد تا اطلاعات و جزئیاتی در ارتباط با تعداد کاربران آنلاینی که روی سایت آن‌ها قرار دارند، تعداد بازدیدها، تعداد بازدیدکنندگان و همچنین اطلاعات آماری مرتبط با سایت خود را به دست آورند. گروه امنیتی Sucuri که موفق شده است این آسیب‌پذیری را شناسایی کند در پستی نوشته است: «آسیب‌پذیری تزریق کد SQL یکی از باگ‌های مرتبط با برنامه‌های کاربردی تحت وب است که به هکرها اجازه می‌دهد محاوره‌های مخرب SQL را از طریق فیلدهای ورودی به سایت‌ها تزریق کرده، در ادامه مکان قرارگیری بانک‌های اطلاعاتی کلیدی را به دست آورده و در نهایت به سرقت اطلاعات بپردازند. آسیب‌پذیری فوق همچنین به یک هکر اجازه می‌دهد یک دسترسی از راه دور تأیید نشده به سایت‌ها را به دست آورد.»



آسیب‌پذیری تزریق کد SQL در افزونه WP Statistics درون چند تابع معروف منجمله `wp_statistics_searchengine_query` قرار دارد. پژوهشگران این شرکت امنیتی اعلام داشته‌اند: «این آسیب‌پذیری به واسطه فقدان مقداردهی اولیه داده‌هایی به وجود می‌آید که از سوی کاربران وارد می‌شود. طیف گسترده‌ای از

مقادیری که از سوی کاربران وارد می‌شود در قالب آرگومان‌های ورودی برای بسیاری از توابع این افزونه ارسال می‌شود. اگر پارامترهای ورودی مورد اعتبارسنجی قرار بگیرند در این حالت آرگومان‌های وارد شده مشکلی به وجود نخواهند آورد.» wp\_statistics\_searchengine\_query یکی از این توابع آسیب‌پذیر است که درون فایل includes/functions/functions.php قرار دارد.

## مطلب پیشنهادی



**سرآغازی بر امن‌تر کردن ارتباطات کاربران  
سیسکو و اپل با مشارکت یکدیگر بیمه سایبری ارائه می‌کنند**

این تابع امتیازات اضافی که به کاربر تخصیص داده می‌شود را مورد بررسی قرار نمی‌دهد. در نتیجه یک کاربر عادی این شانس را پیدا می‌کند تا محاوره‌هایی را به درون بانک اطلاعاتی وارد کرده و در ادامه کدهای مخرب خود را روی بانک اطلاعاتی به مرحله اجرا در آورد. پژوهشگران Sucuri به‌طور محرمانه این نقص را به تیم توسعه‌دهنده افزونه WP Statistics گزارش داده‌اند و تیم مربوطه وصله مورد نظر را در قالب جدیدترین نسخه این افزونه یعنی نسخه 12.0.8 عرضه کرده است. اگر شما نیز یک نسخه آسیب‌پذیر از افزونه فوق را روی سایت خود نصب کرده‌اید و به کاربران اجازه ثبت نام داده‌اید، باید بدانید که در معرض خطر قرار دارید. در نتیجه به شما توصیه می‌شود در اولین فرصت ممکن افزونه خود را به‌روزرسانی کنید.

## تاریخ انتشار:

14 تیر 1396

نشانی منبع:

<https://www.shabakeh-mag.com/security/8541/%D9%BE%D9%84%D8%A7%DA%AF%DB%8C%D9%86-%D9%88%D8%B1%D8%AF%D9%BE%D8%B1%D8%B3-%D8%A8%D8%A7-300-%D9%87%D8%B2%D8%A7%D8%B1-%D9%85%D8%AE%D8%A7%D8%B7%D8%A8%D8%8C->

%D8%B1%D8%AE%D9%86%D9%87-%D8%AA%D8%B2%D8%B1%DB%8C%D9%82-  
%DA%A9%D8%AF-sql-%D8%AF%D8%A7%D8%B1%D8%AF