CyberDefenses
Information Assurance

Protect Your Organization Now
☎ Call (512) 255-3700

# SQL Injection Attacks Put Businesses at Risk for Data Breaches

December 29, 2014 in CyberDefenses Blog

In June 2013, UK-based travel firm Worldview Ltd. was the victim of a systematic cyber-attack that targeted an SQL vulnerability and let hackers capture credit card information for more than 3,800 customer accounts over a 10-day period. The company not only lost the trust of its customers, but was subject to a fine by the UK Information Commissioner's Office (ICO), which felt the hack could have been avoided had Worldview been more thorough in conducting security updates on its website.

Worldview's site was built on the WordPress platform, but cyber criminals do not discriminate when it comes to content management systems. This past November, developers of the Drupal open source CMS issued an emergency advisory after discovering an SQL injection vulnerability potentially affecting up to a million websites using 7.x versions prior to version 7.32.

These and other SQL injection attacks provide a cautionary tale to CEOs and IT Managers alike, and an unwelcome reminder of the need to rigorously manage data security.

**A Time-Tested Tool**
SQL injection attacks insert malicious SQL statements into a form field, URI stem, or cookie value for a Web application, creating a pathway through which cyber criminals can access otherwise secure content, or even take control of the server on which the database is housed. Although experts say this technique has been around since at least 1998, the ever-expanding use of Web-based platforms and recent spate of attacks on high-profile retailers, such as Target and Neiman Marcus, has business owners on edge.

Even seasoned developers have struggled to ensure the security of open source systems, like WordPress and Drupal, which require continual maintenance and updates to keep stealthy cyber criminals at bay. Although Drupal 7 was developed in such a way as to sanitize queries executed against the database to prevent SQL injection, a vulnerability in the API allowed hackers to send specially crafted requests that could "lead to privilege escalation, arbitrary PHP execution, or attacks," the initial Drupal advisory explained.

In the case of Worldview Ltd., however, the vulnerability had existed for years—since 2010, in fact—and was only recently discovered during a routine security update after having already been leveraged by hackers. According to the ICO, cyber criminals were able to crack into the travel company's WordPress system because the weak default passwords had never been changed, something that easily could have been avoided with proper training and oversight.

**Steps to Safeguard Your Data**
"Organizations must act now to avoid one of the oldest hackers' tricks in the book," said a spokesperson from the ICO following the SQL injection attack on Worldview, adding, "If you don't have the expertise in-house, then find someone who does," or you may be subject to fines and reputational damage as a result of a serious data breach.

In a survey of nearly 600 IT and IT security professionals conducted by the Ponemon Institute and DB Networks, the majority recommended continuous monitoring of the database network, advanced database activity monitoring, and database encryption to defend against SQL injection attacks and avoid mega data breaches. Although the recommendations are sound, the same survey showed that most firms allocate only a small part of their IT budget to database security.

Small and mid-size businesses often hire independent contractors to build their website and set up data networks, and lack the financial and staff resources to ensure that security updates are managed properly. Larger companies, in contrast, may have an IT team in-house, but their time is often spent managing enterprise software systems, and they may lack the expertise to monitor database activity, manage website updates, or develop strategies to improve data security. In both cases, contracting a cyber security firm can help ensure that sensitive systems are continually updated, and proper safeguards are in place to prevent an SQL injection or other cyber attack.

CyberDefenses, Inc. provides both consulting services for security system analysis, design and development, as well as IT staff augmentation for firms needing additional expertise in-house. Our highly trained experts maintain the highest security clearances and certifications, such as CISM, CISSP, CAP and PMP, and can assess the risks and vulnerabilities your company faces to put the proper security systems in place. To learn more about how we can help you protect sensitive data and safeguard your organization's website against attack, call 512-255-3700 or contact us online.

Recent Articles

- 5 Strategies for Protecting Data on the Cloud
- SQL Injection Attacks Put Businesses at Risk for Data Breaches
- What to Do if Your Company Gets Hacked
- 4 Strategies to Minimize Risk of a Data Breach
- Why Neiman Marcus' New CIO Matters to Your Business
- Secret Service Offers Cybersecurity Guidelines for Executives
- Malvertising on the Rise as the Holidays Approach

Services

- ✓ Information Management
- ✓ Information Assurance
- ✓ Forensics
- ✓ Business Transformation and Change
- ✓ Management
- ✓ Vitalization, Architecture and Infrastructure
- ✓ System Development and Integration
- ✓ Project Planning and Execution
- ✓ Government Business
- ✓ Process Outsourcing