



NJCCIC

NJ CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

SQL Injection: A Common, Yet Avoidable, Attack Vector

October 28, 2015

TLP: WHITE | *The NJCCIC assesses that organizations using Structured Query Language (SQL) for database management systems are at a high risk for SQL injection (SQLi) attacks unless the appropriate mitigation strategies are applied.* SQL is the standard computer language used to conduct various functions such as querying and modifying data in relational database management systems. SQLi is a cyber tactic that exploits a vulnerability in a database application that does not properly validate or encode user input. An attacker inserts malicious SQL statements into a text entry field which then allows the actor to manipulate, exfiltrate, or delete data stored on a backend server. Without adequate cybersecurity measures in place, SQLi attacks can remain undetected for long periods, providing threat actors ample time to identify the most valuable data to steal, such as customer's Social Security and credit card numbers.

- On October 22, 2015, a United Kingdom Internet Service Provider and mobile carrier, [TalkTalk](#), announced a large-scale breach of servers which housed personal and financial information on up to four million customers. Hackers used SQLi to initiate the attack and demanded a ransom of approximately \$122,000 in Bitcoin to not publicly release TalkTalk's customer data. Though unconfirmed, the SQLi attack was reportedly accompanied by a [denial-of-service](#) (DoS) attack that prevented legitimate users from visiting the targeted site.
- A Kosovo citizen, [Ardit Ferizi](#), was indicted on October 6, 2015 for allegedly hacking into the servers of a US web hosting company and stealing the personal information of over 1,300 US service members and federal employees. The FBI believes SQLi was used to obtain the information. The stolen data was later found in the possession of [Junaid Hussain](#), a British citizen and alleged leader of the Islamic State in Syria and Iraq's cyber operations, who was later killed by a US drone strike in August.
- On August 11, 2015 nine individuals were [indicted](#) in New Jersey and New York federal courts for running an international hacking ring designed to steal unreleased press releases and execute profitable stock trades based on this information. From January 2010 to November 2013, the group allegedly used an SQLi attack against [Marketwired](#), a press release distributor. The hacking group generated upwards of \$30 million in profits.

Injection vulnerabilities are very common and, according to the [InfoSec Institute](#), SQLi is not only one of the most exploited flaws, but considered one of the top five vulnerabilities with potential for severe impact. Some of the most commonly used databases rely on the SQL language, such as Oracle and Microsoft SQL Server. SQL vulnerabilities are easily detected and exploited, and are therefore a soft target for both criminal and state-sponsored threat actors.

- In a study released by the [Ponemon Institute](#) in October 2014, 65 percent of respondents had experienced one or more SQLi attacks in the last year. These attacks successfully evaded their perimeter defenses and required, on average, 140 days to detect and 68 days to remediate. Though well-documented since the late 1990s, SQLi still accounts for more than 20 percent of all web vulnerabilities, according to cybersecurity vendor [Veracode](#).

Mitigation

The NJCCIC recommends a comprehensive [defense-in-depth](#) strategy to [protect against SQLi](#). It is advised to avoid using dynamic SQL when possible, provide the least necessary account privileges to those who require database access, and ensure that database software vendors evaluate the code and fix security flaws in any custom applications. Implementing a web application firewall (WAF) will provide protection at the web server (back-end) and web application (front-end) layers. Blacklist potentially malicious values, and whitelist safe values and characters to prevent malicious commands from being executed. Encrypting or hashing passwords and other sensitive data will increase the likelihood of maintaining data integrity in the event of a breach. Lastly, it is vital to keep all systems and software updated with security patches.

Traffic Light Protocol: **WHITE** information may be distributed without restriction.