

Manager's Technical Guide To SQL Injection

Threat Assessment

- Exploitation Status: Actively Exploited
- Threat Level: High
- Risk Factors: Exposure of confidential information, Possible arbitrary code execution

Threat Overview:

SQL injection is an attack from the family of input validation attacks. In this situation, an attacker attempts to place SQL commands or functions into input variables on an application, form or website. The attacker hopes that to use these commands to gain access to the underlying database or operating system and manipulate that access in some way. Successful exploitation of this vulnerability can result in the attacker having complete access the data held in the database, complete control over the database functionality (even allowing modification or destruction of all or part of the data) and/or the attacker gaining complete control over the underlying operating system. If the attacker gains control over the operating system, that access could be leveraged to completely compromise the entire network.

Threat Details

Attackers actively comb the web for new victims to employ SQL Injection against. Any web-based application can be vulnerable if not correctly implemented to protect against this form of attack, if a SQL database is in use by the application, form or system. Firewalls and network intrusion detection systems may offer little protection against these attacks, since the majority of the attack traffic is legal protocol communication, looks like normal SQL communication from an application and is often encrypted with SSL. Probes for the attack appear as attempts to use control characters (' " ; ` /, etc.) in variable input from forms or applications. Using these input characters often causes the application or web form to display database or ODBC errors which alert the attackers to the presence of the vulnerability and often assist them in refining their exploitation techniques.

Suggested Mitigation

All user input needs to be checked on the SERVER SIDE for SQL control characters (' ` ; /, etc.) prior to being passed into the database connector or application for processing. User input, in this instance, is defined as ANY AND EVERY input variable received and processed by the application. Server side checking is required to resolve these issues as all client side applications and code should be considered optional and may or may not be executed by the end user. It is trivial for an attacker to mitigate client side protection mechanisms or input parsing. With appropriate server side parsing of all user input SQL injection attacks are easily and completely mitigated.

Further Information and Assistance:

For more information on this or any other type of vulnerability or attacker exploitation, please feel free to contact MicroSolved or one of our SecureAssure™ partners via email or phone. One of our Security Experts will be happy to talk with you about any questions you may have. MSI has specialized in information security assessments, penetration testing, security awareness and data asset protection for more than a decade. Contact us today for all of your information security needs.

