SQL Injection Scenario

NETGLADIATOR

SQL Injection is a form of web application intrusion used by hackers to attempt to subvert your databases. In this white paper, we briefly discuss the SQL Injection scenario, provide an example of how it is used, explain how NetGladiator stops the attack, and tie this in to your overall layered security approach.

SQL Injection Description

SQL Injection is one of the most common and dangerous attacks web applications face today. The attack takes advantage of weakly-coded pages that interface with a back-end database. A hacker will use this weakness to run custom database queries to gather information, modify the database entries, or insert malicious code. The result can be a total compromise of your most sensitive data.

Example

Assume you have an ecommerce store that lists products on the following URL: http://www.mystore.com/products.php. If a user wants to view a certain product, they might end up at the following URL: http://www.mystore.com/products.php?id=74.

This is a clue to the attacker that a database lookup is occurring. Likely with the following query: SELECT * FROM content WHERE id=74. If SQL Injection is possible, the attacker can use this knowledge to modify the above SQL query, possibly like this: http://www.mystore.com/products.php?id=74 AND (SELECT 1 FROM(Select Count(*), Concat(CHAR (58,58,58), (Version()), floor(rand(0)*2), CHAR (58,58,58))x FROM Information_Schema>. Now the query to the database becomes: SELECT * FROM content WHERE id=74 AND (SELECT 1 FROM(Select Count(*), Concat(CHAR (58,58,58), (Version()), floor(rand(0)*2), CHAR (58,58,58))x FROM Information_Schema.

If this is successful, the page will print out the version of mysql running on the server. This results in a proof-of-concept for the attacker, and many other, more damaging queries can be executed. Information gathering is almost always the initial phase for any attack. For the attacker, it is critical to find out as much information as possible about your web server and the technologies that run on it. What is discovered in this phase is often the basis of the actual attack.

How NetGladiator Stops This Attack

NetGladiator looks for database keywords in the requests destined for your web servers. The assumption is that database keywords like SELECT, FROM, and WHERE would never be in a valid URL. NetGladiator will stop this attack right away, blocking the offending IP address and alerting an administrator to the attack. The NetGladiator is a key device in a layered security approach. Its behavior-based anomaly detection identifies potential attackers through recognizing unusual patterns of behavior, as hackers explore and utilize your website much differently than a normal user.

Layer This With...

To prevent SQL Injection, it's very important to validate and sanitize the input from a form or URL before the database query is executed. This includes escaping strings, validating length, and checking the type of input to make sure it matches expected values.

When developing an IT security policy and implementing security controls, the single most important thing to consider is how the different controls you use will layer within your security profile. Because no single piece of equipment or software will be able to thwart 100% of attacks, good layering provides the best chance to stop a hacker from their ultimate goal.

To Learn More...

We would be a happy to discuss the NetGladiator technology, to help you to determine if this is the right solution for you. Please email ips@apconnections.net or call us at **303.997.1300 x123**.

About APconnections, Inc.

APconnections is an innovation-driven technology company that delivers best-in-class network traffic management solutions to give our customers better networks, with zero maintenance, at the best prices. We specialize in turn-key bandwidth shaping and intrusion prevention system (IPS) appliances.

Since 2003, APconnections' mission has been to provide simple turn-key network optimization appliances to any network topology. Our products are simple to install, easy to use, require little maintenance, and are offered at the best prices.

APconnections is based in Lafayette, Colorado, USA. We released our first commercial offering in July 2003, and since then thousands of customers all over the world have put our products into service. Today, our flexible and scalable solutions can be found in many types of public and private organizations of all sizes across the globe, including: Fortune 500 companies, major universities, K-12 schools, Internet providers, law firms, hotels, hospitals, libraries, business centers, small businesses, non-profits, military, and government agencies on six (6) continents.