12.3.8 SQL Injection Countermeasure Facts

This lesson covers the following topics:

- How to counter SQL injection attacks
- Defense tools

How to Counter SQL Injection Attacks

SQL injections can be quite powerful, so let's look at a few countermeasures that you can use and recommend to your clients. First, let's briefly review four scenarios that make web applications vulnerable to SQL injection attacks.

1. The database server is capable of running operating system commands.
2. A privileged account is being used to connect to the database.
3. Error messaging is enabled and is revealing important information about the system.
4. There is no data validation being completed at the server.

So, how do we fix these things? Since a database server is able to run OS commands, you'll want to be sure that the database server account is being run with minimal rights. Also, you'll want to disable powerful commands that would provide an attacker with too much access to the network. Next, Instead of using a privileged account to connect to the database, you'll want to use a lower privileged account for database connectivity. You'll also want to monitor all database traffic with your intrusion detection system. Because error messages can be used to gather information, you'll want to turn off default error messaging. You could choose to disable error messaging completely, or, if you would prefer to have an error message in place, use a custom error message so you are able to control the information that is shared in the message.

The last (and, arguably, the most important SQL injection countermeasure) is to ensure validation at the server. Limit the size and data type of any input data. Accept only the expected values, and test the content of all string variables. Decline any entry that includes binary input, comment characters, or escape sequences. Enforce type and length checks so that input is viewed as a value and not as a potentially executable code. Ideally, you want to implement various layers of data validation, filtering, and sanitizing. You want to be sure that questionable or unvalidated data does not make it to your web application.

Defense Tools

Tool	Description
IBM Security AppScan	IBM Security AppScan is software that provides application security and risk management for mobile and web applications.
dotDefender	dotDefender is a software firewall for web applications. It works alongside an IPS and other security measures. It examines HTTP and HTTPS traffic. It detects and blocks SQL injection attacks.
WebCruiser	WebCruiser is a vulnerability scanner that looks for SQL injection, XPath injection, and cross-site scripting.