

# Defending Against SQL Injection

SQL Injection (SQLi) is an attack methodology designed to provide hackers with access to database assets. SQLi takes advantage of poorly secured web applications to create a connection to the database. This is done by inputting a SQL command into an input field of a web application. Once an “injection hole” is found, hackers are free to “explore” the database in search of database vulnerabilities they can exploit.

Network-based defenses, such as Web Application Firewalls (WAFs), are one line of defense against SQLi attacks. However, they are limited by their ability to keep pace with the latest SQLi attack signatures. The experienced hacker will eventually find a way through these perimeter defenses.

## 5 Key Steps to Database Security Process Control

In order to effectively secure their databases, organizations must address five critical requirements:

1. **Isolate Sensitive Databases:** Maintain an accurate inventory of all databases deployed across the enterprise and identify all sensitive data residing on those databases.
2. **Eliminate Vulnerabilities:** Identify and fix vulnerabilities that are exposing the database on a continual basis.
3. **Enforce Least Privileges:** Reset user access controls and privileges to allow access to only the minimum data required for employees to do their jobs.
4. **Monitor for Deviations:** Implement appropriate policies and monitor for any and all activity that deviates from normal and authorized activity.
5. **Respond to Suspicious Behavior:** Alert and respond to any abnormal or suspicious behavior in real-time to minimize risk of attack.

To effectively protect sensitive data assets from SQL Injection attacks, organizations need to add a second line of defense and protect the data where it lives – in the database. DbProtect Precision Database Activity Monitoring (DAM) protects organizations from SQL Injection attacks by:

- Proactively eliminating vulnerabilities that SQLi attackers exploit.
- Continuously monitoring for SQLi signatures indicating an attack.
- Immediately and automatically responding to an SQLi attack.

Precision DAM enables organizations to secure their databases from SQLi attacks by controlling the security processes that impacts sensitive data.

## FOUR STEPS TO COST EFFECTIVE SQL INJECTION PROTECTION

### Step 1: Isolate Sensitive Databases

The first step to effective SQLi protection is to isolate all databases containing sensitive data. Over time, databases become populated with unauthorized databases. These “rogue” databases typically fall outside of IT control and are rarely configured or secured properly. As a result, they create a security risk by giving attackers an easy target to gain a foothold on the network and find access to other databases containing sensitive data.

DbProtect’s Database Discovery feature generates a complete inventory of all databases deployed enterprise-wide. It identifies all production, test, and temporary databases, and more importantly, any unauthorized databases.

DbProtect’s Sensitive Data Discovery identifies and locates all sensitive data residing on those databases. DbProtect helps organizations to protect their sensitive data by:

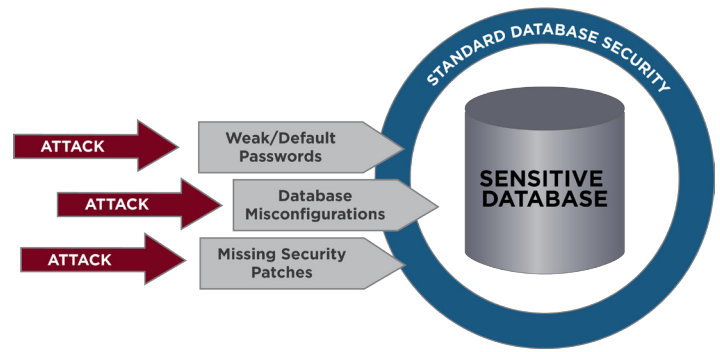
- Ensuring all sensitive data is located on authorized and secured databases.
- Restricting access and use of the sensitive data.
- Identifying and removing any unauthorized databases from their networks.

**Step 2: Eliminate Vulnerabilities**

SQL Injection attacks are used to penetrate network defenses. Once inside, attackers “explore” the network, looking for database vulnerabilities they can exploit to gain access to sensitive data. Default and weak passwords, database misconfigurations, and missing security patches provide easy avenues of attack to the experienced hacker. DbProtect’s Vulnerability Management provides unparalleled database vulnerability assessment, allowing organizations to identify and eliminate vulnerabilities and fix misconfigurations that put their sensitive data at risk.

DbProtect’s powerful Policy Development engine is driven by the SHATTER Knowledgebase, the most comprehensive and up-to-date vulnerability and threat knowledgebase in the industry. SHATTER provides checks on database procedures and functions that are exploitable by SQLi attacks. Each check in the SHATTER knowledgebase provides clear and detailed remediation instructions to insure that the vulnerabilities exposing sensitive data to SQLi attacks are fixed in a timely manner.

**Database Vulnerabilities**

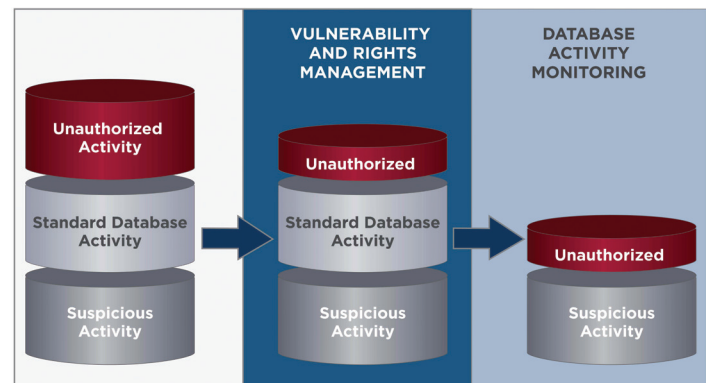


**Step 3. Monitor for Deviations**

DbProtect Database Activity Monitoring (DAM) tracks activity as it hits the database. It watches and evaluates commands, looking for signatures that identify database activity as a possible SQL Injection attack.

DBProtect’s unique approach to DAM is precision monitoring. Precision monitoring employs DbProtect’s powerful policy development engine to streamline monitoring operations to focus on any suspicious activity threatening sensitive data. DbProtect’s precision DAM solution can be customized to a fine level of granularity – A specific activity, performed by a specific user, accessing a specific data, in a specific database. In this way, SQLi attacks are not lost in the noise of other database activity.

**Precision DAM**



Backed by the same SHATTER knowledgebase, DbProtect’s Precision DAM reduces risk and offers best-in-class data protection against SQLi attacks.

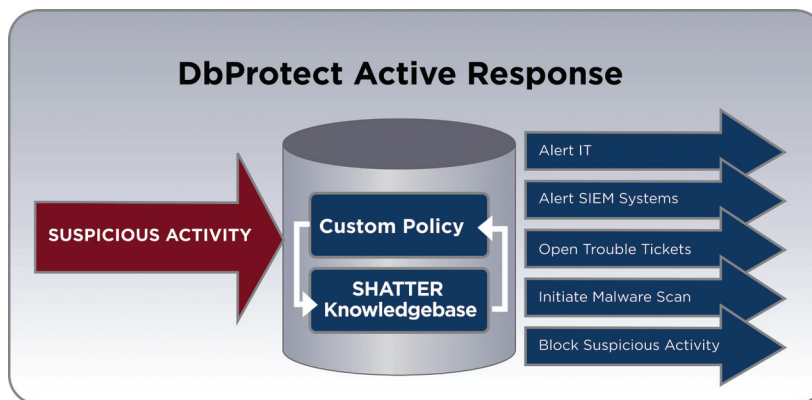
#### Step 4: Respond to Suspicious Behavior

DBProtect's Active Response provides an additional layer of protection against SQL Injection attacks.

Active Response can be configured to take action

when an SQLi signature is identified. For example: When DbProtect recognizes an SQL injection signature, Active Response can be configured to:

- Send an alert to IT Security.
- Notify the SIEM system to correlate database activity with web application logs.
- Initiate a malware scan to remove any injected code.



Active response can be customized to a fine level of granularity – A specific activity, performed by a specific user, accessing specific data, in a specific database.

Incorporating a comprehensive and disciplined program of database security process control and managing these basic steps will help organizations to cost-effectively protect their sensitive data from SQL Injection attacks.

#### ABOUT APPLICATION SECURITY, INC. (APPSECINC)

AppSecInc is a pioneer and leading provider of database security and compliance solutions for the enterprise. By providing strategic and scalable software-only solutions – AppDetectivePro for auditors and IT advisors, and DbProtect for the enterprise – AppSecInc supports the database lifecycle for some of the most complex and demanding environments in the world across more than 1,300 active commercial and government customers.

Leveraging the world's most comprehensive database security knowledgebase from the company's renowned team of threat researchers, TeamSHATTER, AppSecInc products help customers achieve unprecedented levels of data security while reducing overall risk and helping to ensure continuous regulatory and industry compliance.

For more information, please visit: [www.appsecinc.com](http://www.appsecinc.com) | [www.teamshatter.com](http://www.teamshatter.com)

For a free database vulnerability assessment visit: [www.appsecinc.com/downloads/appdetectivepro](http://www.appsecinc.com/downloads/appdetectivepro)

Follow us on Twitter: [www.twitter.com/appsecinc](http://www.twitter.com/appsecinc) | [www.twitter.com/teamshatter](http://www.twitter.com/teamshatter)

**APPLICATION  
SECURITY, INC.**<sup>®</sup>  
[www.appsecinc.com](http://www.appsecinc.com)