**CH8 SQL injection exploitation and defense**

**Objectives**

* Define SQL injection exploitation
* Identify ways intruders gather information from a network infrastructure
* Describe common strategies for exploiting database infrastructure
* Identify common SQL statements and SQL constructs used to exploit weaknesses
* Apply exploitation for the purpose of identifying infrastructure weaknesses
* Identify defense strategies against SQL injection exploits

**Exploitation and information gathering**

* Exploitation
* Act of using system vulnerabilities for the purpose of gaining access or control
* Does not always result in control

Depends on effectiveness of SQL query injection techniques and usefulness of generated output

* To defend a system from successful exploitation:
* Security professional must be aware of means to derive information

And what information to protect

**Information that aids in exploitation**

* Locating a weakness

First step in intrusion process

* Example: attacker gains access to database
* But does not have knowledge of its connects
* Goal: construct theoretical picture of infrastructure
* Gathering details aids goal of obtaining access
* Database schema
* Overall logical structure of objects within the database
* Includes stored procedures, table, views, and users
* Information about the database
* Knowing database vendor and version is necessary
* With vendor/version info, attacker can infer:
* SQL language syntax to use to construct injections
* Available default procedures
* Method of processing queries
* Storage mechanisms utilized
* Large portion of the schema
* Identifying the vendor
* Easy for the knowledgeable intruder
* Multiple clues needed to ascertain database vendor and type
* Clues that aid intruders in identifying vendor
* The scripting language
* Database vendors often lean toward one or two language
* Example: PHP used to communicate with MySQL
* .NET used by SQL Server
* Oracle has a relationship with Java Script
* The platform
* Microsoft SQL Server based on foundation of Microsoft Windows Server 2008

Indication of Windows points to SQL Server

* Open source operating systems often used to support MySQL and Oracle
* Platform provides only one small clue

Every configuration is built on unique needs

* The database response
* Provides most reliable means to identify database
* Differences in syntax and error format exist between database
* Error code can be a valuable piece of information

Vendor’s Web site provides information on error codes

* Identifying the version
* Can be equally important to identify as the vendor
* Gives insight into system capabilities
* Intruder can take advantage of known vulnerabilities for a given version
* Once database vendor is identified:
* Locating version number can be an easy task
* Standard queries used to return version number of that system
* Example of command to discover version in SQL Server:

SELECT@@VERSION

* Return version of SQL server, processor, operating system, service pack, and build
* Possible results of injecting statement as a string parameter within a Web application
* Results returned:
* If application input or output has not been filtered
* If expected parameter is a string
* Error returned:
* If statement is constructed incorrectly
* If expected parameter is a number
* Message may provide the necessary information
* Nothing returned:
* If application filters input or output
* If application is configured to handle error messages in this way
* Intruder will need to use trial and error approach
* Other types of standard statements
* Statements to determine database name, location, and language being used
* Administrators should become familiar with these statements
* Helps understand the amount of information that may be gathered during exploitation

**Extracting the real data**

* Techniques presented in previous section allow intruders to gather basic information needed
* Based on knowledge gained about the database:
* Intruder can construct meaningful queries to gather data
* Exploitation attack equipped to move deeper into the system
* Targets can be located and data extracted

**Statement exploits**

* Endless number of SQL statements can be injected into the database
* Intruder has capability to access database as a typical user
* Access is restricted by privileges of the user
* Next section explores common statements used in SQL injection attacks
* Assumes attacker is working under restricted conditions

**Using union**

* UNION statements
* Powerful tools of SQL injection attacks
* Intruder attaches his or her own queries onto preexisting legitimate statements
* UNION operator combines two or more SQL statements
* Revisiting Yum grocer example

http://www/yum.com/index.asp?category=dairy union select Table\_Name from Information\_Schema.Tables—