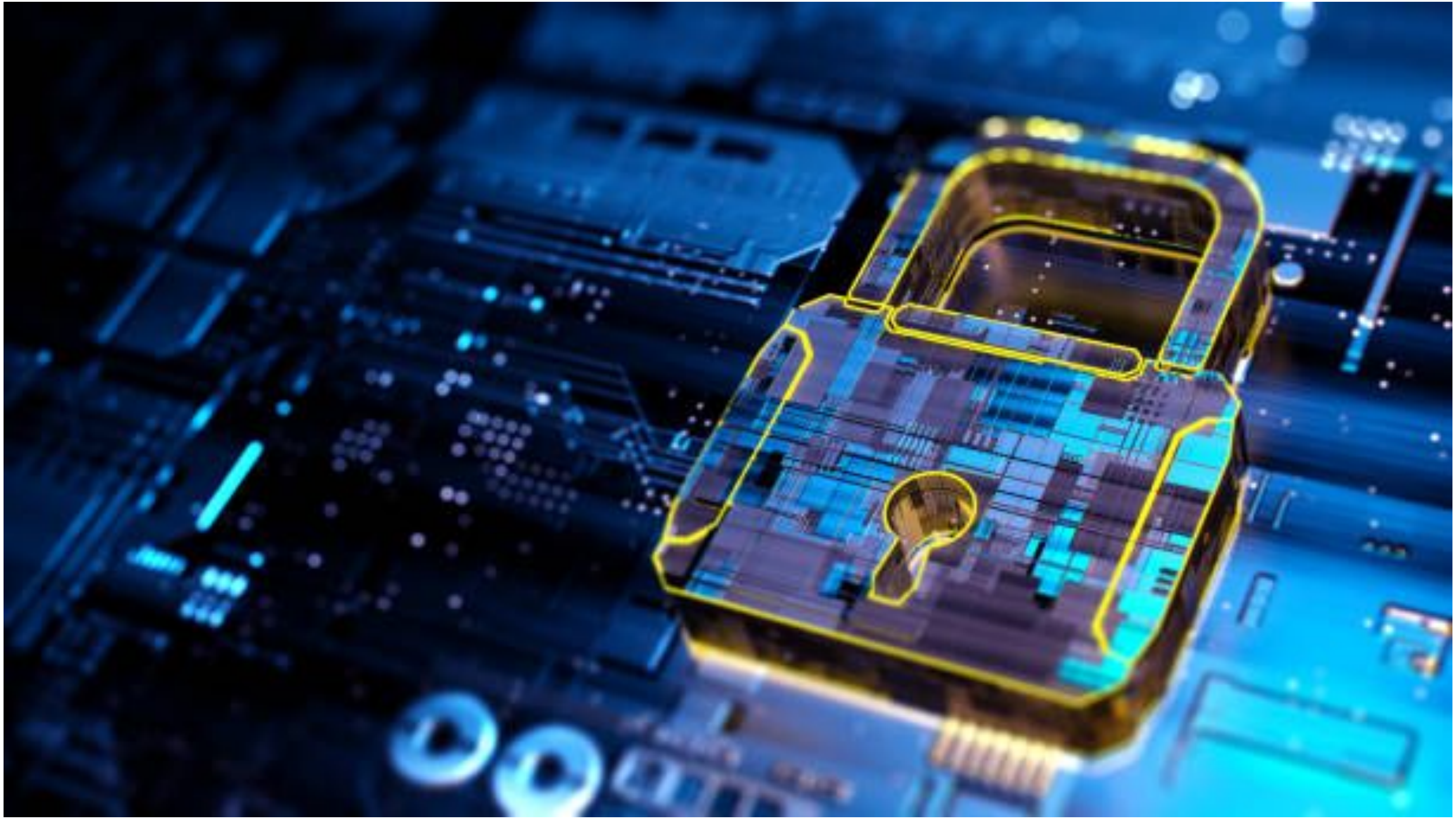
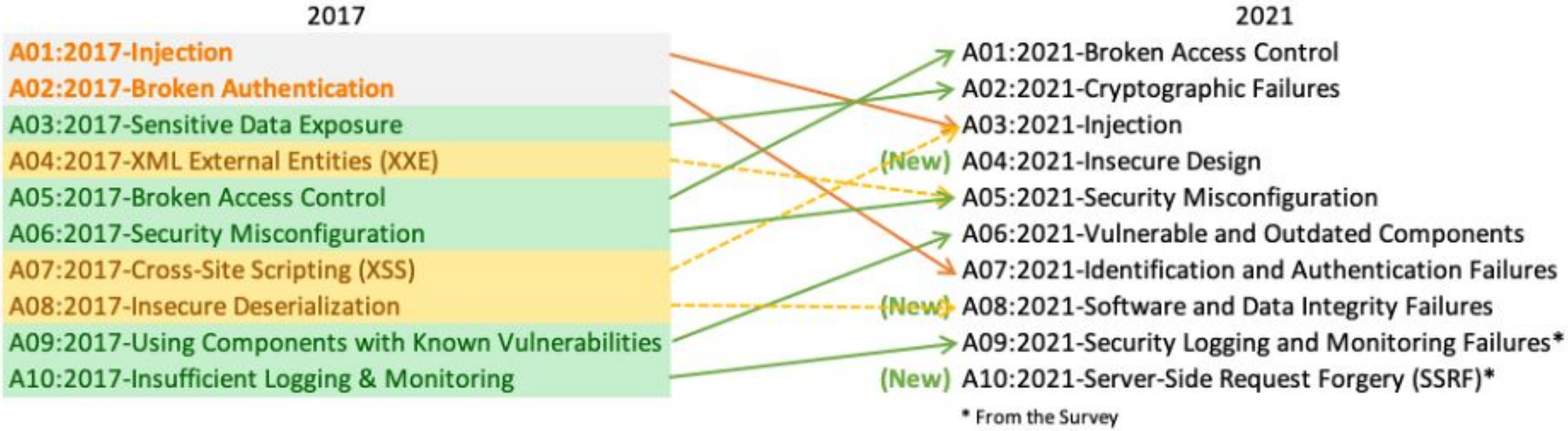
SQL Injection

Sivana Hamer - sivana.hamer@ucr.ac.cr
Escuela de Ciencias de la Computación

UNIVERSIDAD DE COSTA RICA



OWASP es una fundación que determina los problemas de seguridad más frecuentes en aplicaciones



2017

A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

2021

A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

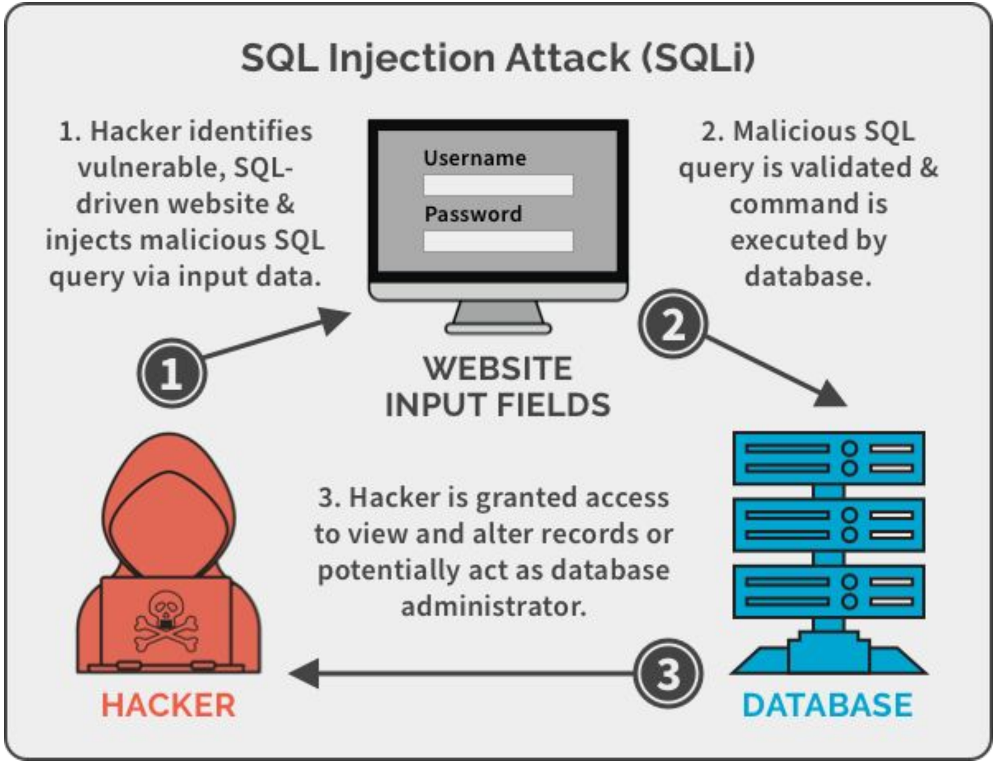
Hay distintas maneras en que se puede proteger un sistema

Prevención

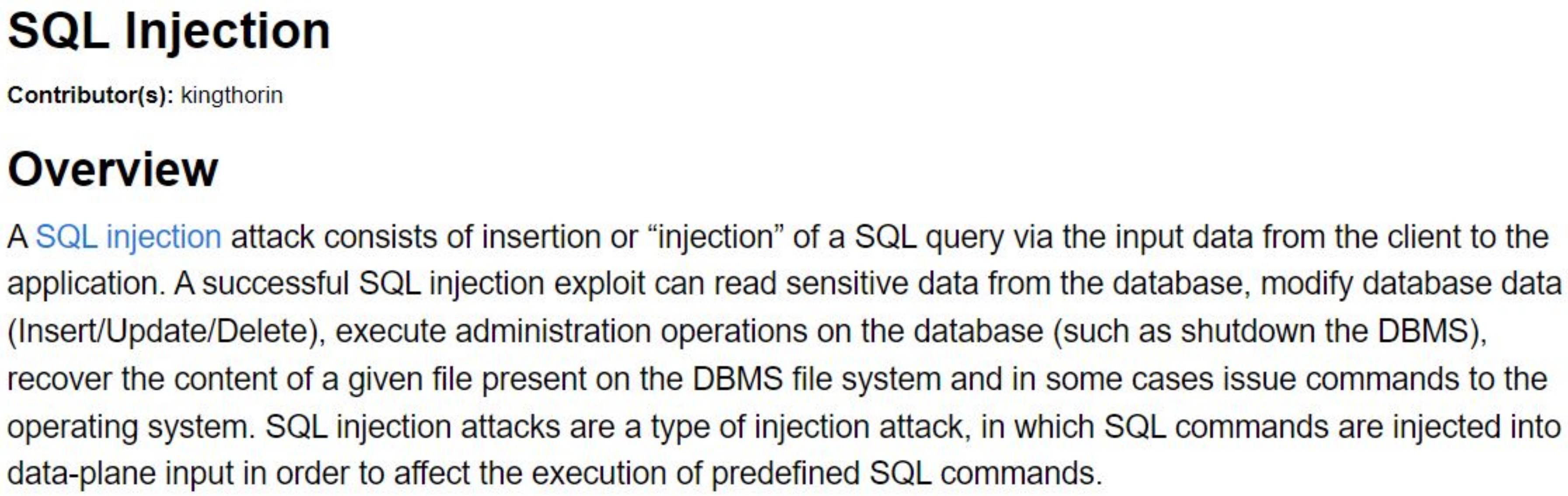
Detección

En general se busca considerar ambas medidas, pero prevenir ayuda a que no suceda el ataque

Con SQL injection se inyecta desde la app código para ejecutar un query en la base de datos


SQL Injection Attack (SQLi)
1. Hacker identifies vulnerable, SQL-driven website & injects malicious SQL query via input data.
Username
Password
2. Malicious SQL query is validated & command is executed by database.
1
2
WEBSITE INPUT FIELDS
3. Hacker is granted access to view and alter records or potentially act as database administrator.
3
HACKER
DATABASE

LIVE DEMO



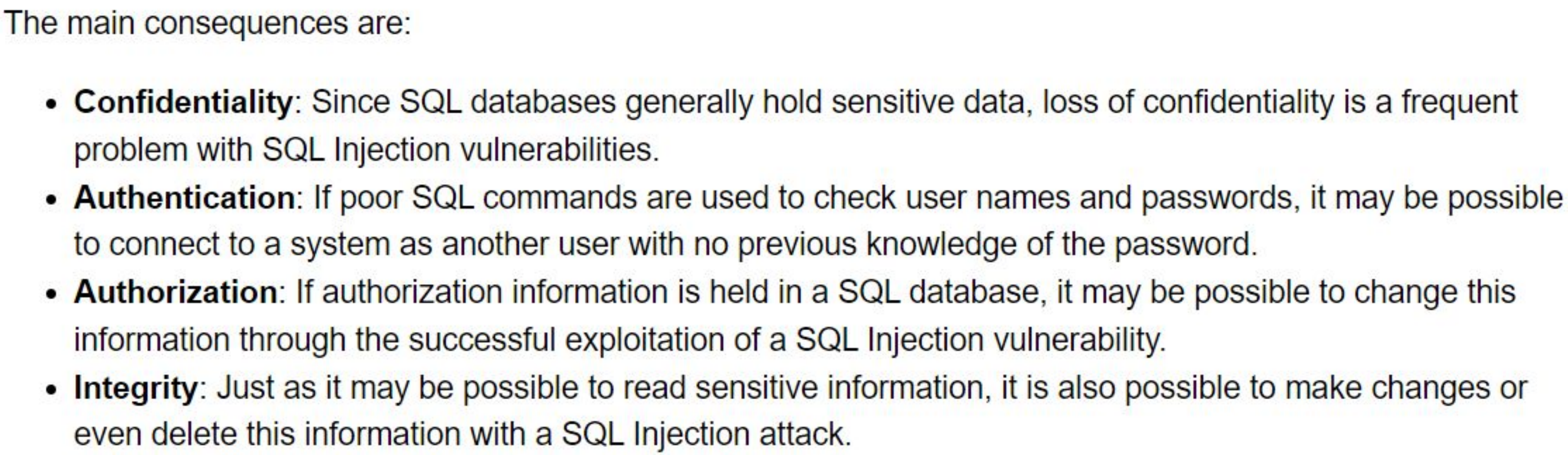
SQL Injection

Contributor(s): kingthorin

Overview

A SQL injection attack consists of insertion or “injection” of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands.

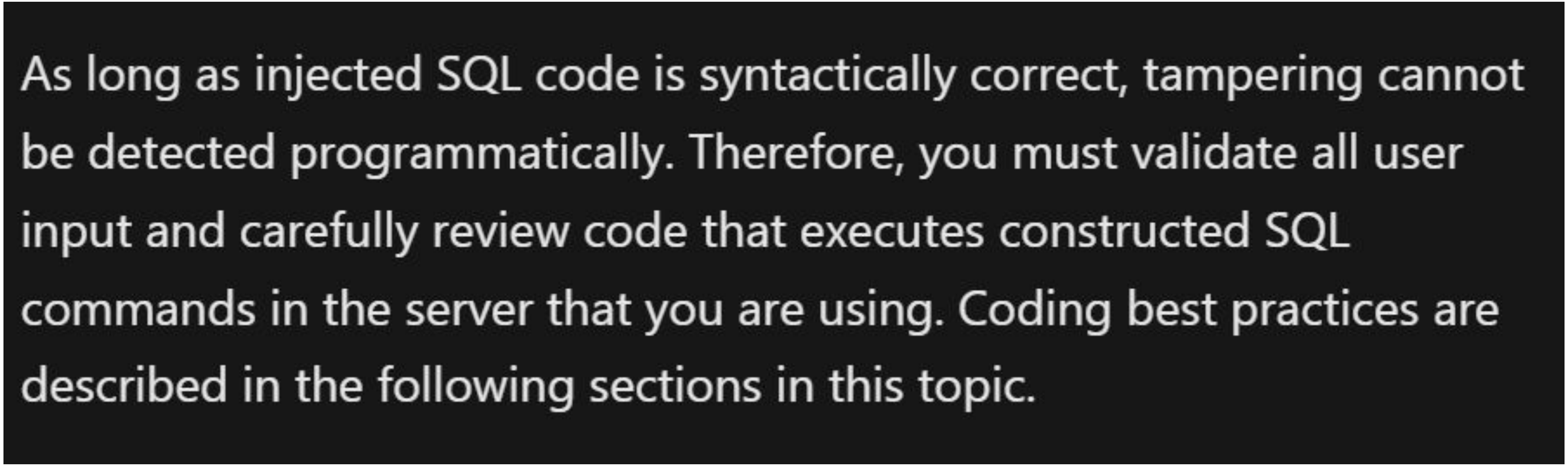
@OWASP



The main consequences are:

- **Confidentiality**: Since SQL databases generally hold sensitive data, loss of confidentiality is a frequent problem with SQL Injection vulnerabilities.
- **Authentication**: If poor SQL commands are used to check user names and passwords, it may be possible to connect to a system as another user with no previous knowledge of the password.
- **Authorization**: If authorization information is held in a SQL database, it may be possible to change this information through the successful exploitation of a SQL Injection vulnerability.
- **Integrity**: Just as it may be possible to read sensitive information, it is also possible to make changes or even delete this information with a SQL Injection attack.

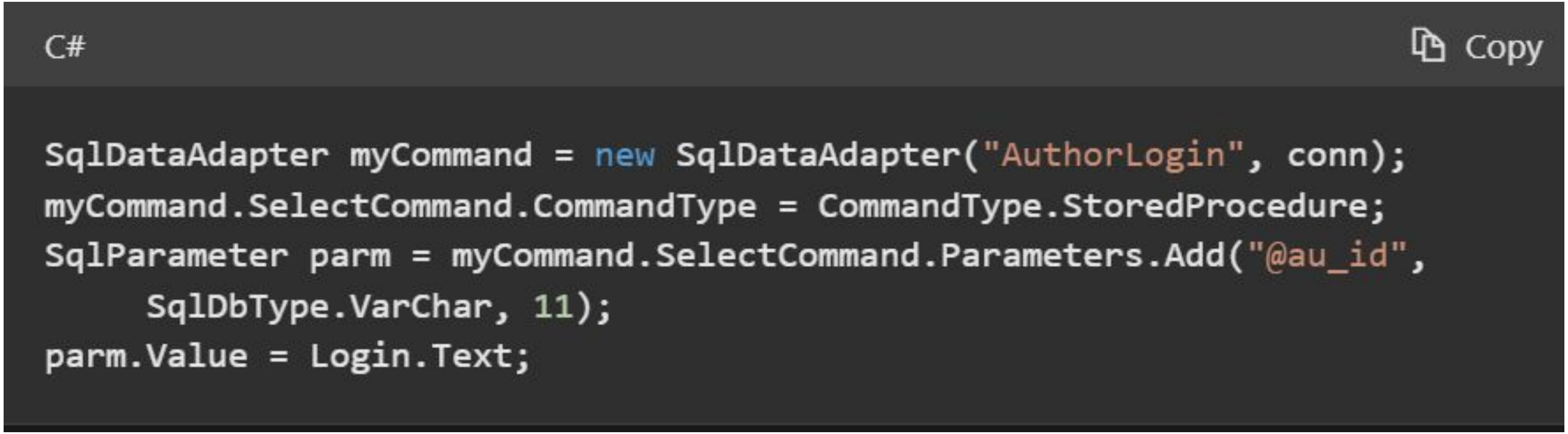
@OWASP



As long as injected SQL code is syntactically correct, tampering cannot be detected programmatically. Therefore, you must validate all user input and carefully review code that executes constructed SQL commands in the server that you are using. Coding best practices are described in the following sections in this topic.

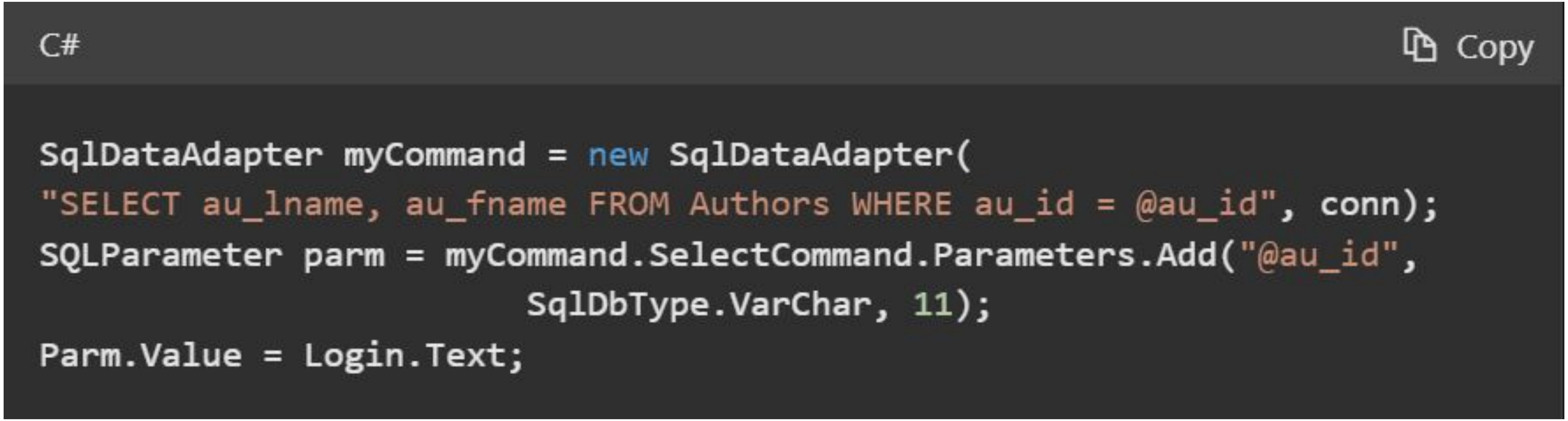
@Microsoft

Se puede verificar los tipos de datos que se pasan a procedimientos almacenados



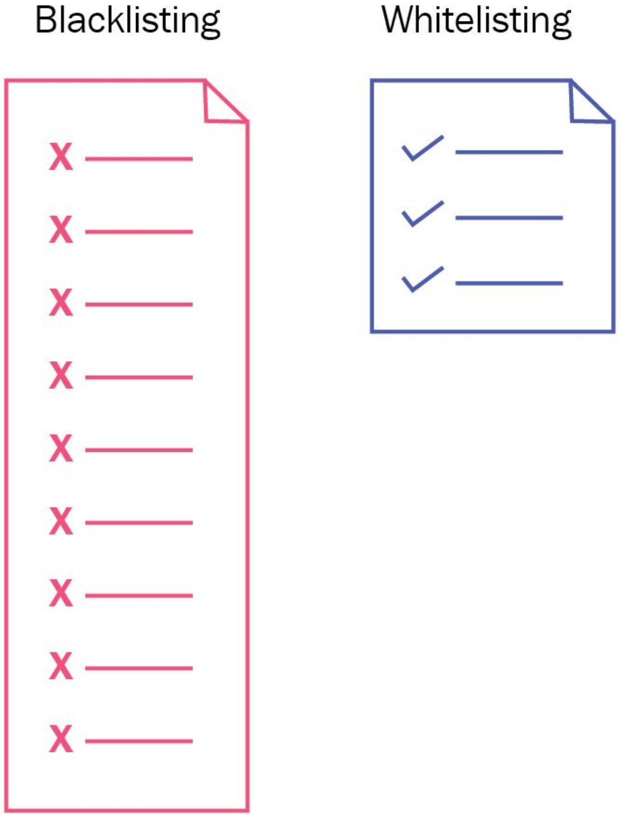
```
SqlDataAdapter myCommand = new SqlDataAdapter("AuthorLogin", conn);
myCommand.SelectCommand.CommandType = CommandType.StoredProcedure;
SqlParameter parm = myCommand.SelectCommand.Parameters.Add("@au_id",
     SqlDbType.VarChar, 11);
parm.Value = Login.Text;
```

Se puede utilizar parámetros igualmente sin procedimientos almacenados

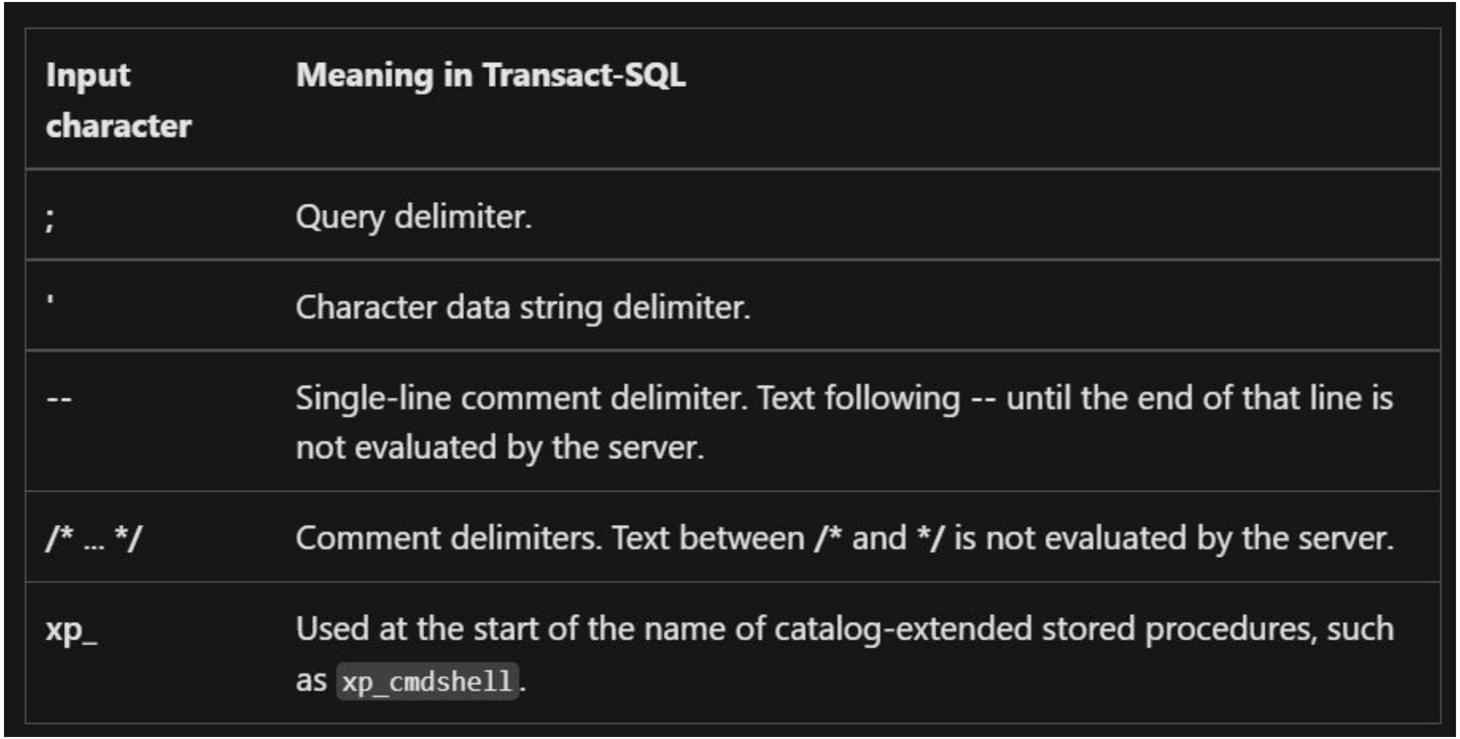


```
SqlDataAdapter myCommand = new SqlDataAdapter(
"SELECT au_lname, au_fname FROM Authors WHERE au_id = @au_id", conn);
SQLParameter parm = myCommand.SelectCommand.Parameters.Add("@au_id",
                        SqlDbType.VarChar, 11);
Parm.Value = Login.Text;
```

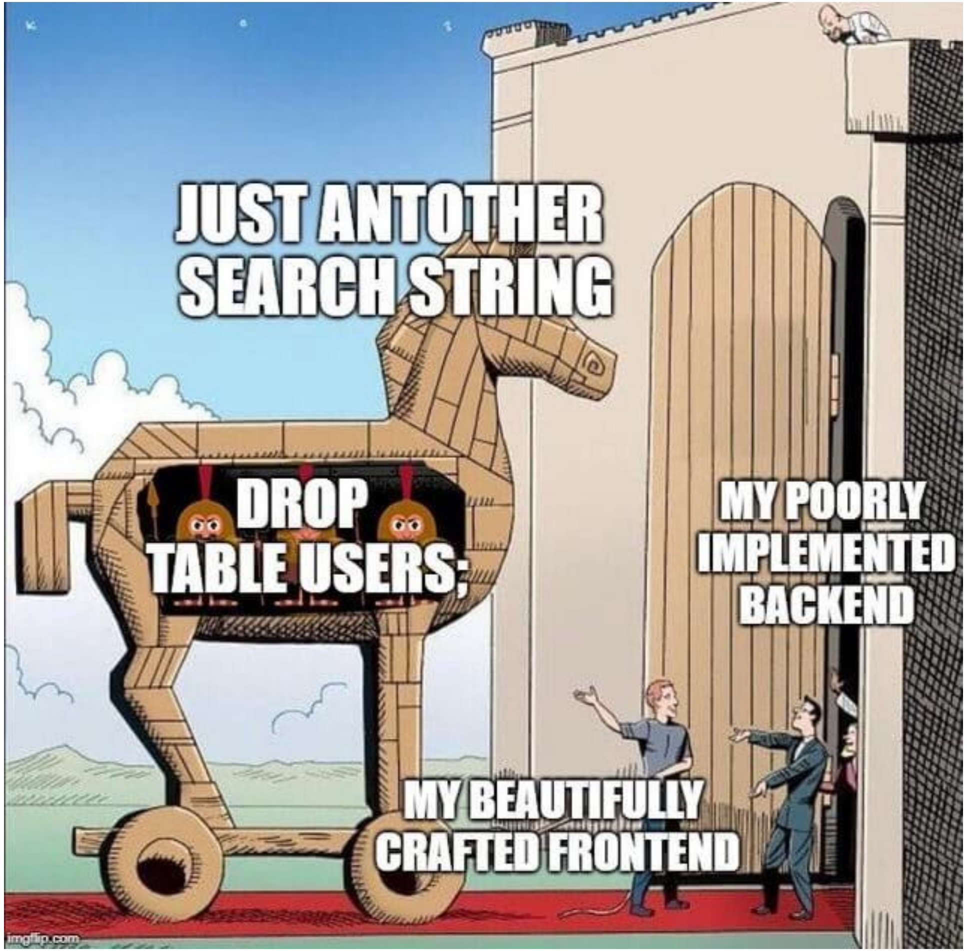
Hay una diferencia entre whitelisting y blacklisting



Hay que tener cuidado con las siguientes entradas que provienen de personas usuarias



Input character	Meaning in Transact-SQL
;	Query delimiter.
'	Character data string delimiter.
--	Single-line comment delimiter. Text following -- until the end of that line is not evaluated by the server.
/* ... */	Comment delimiters. Text between /* and */ is not evaluated by the server.
xp_	Used at the start of the name of catalog-extended stored procedures, such as `xp_cmdshell`.



JUST ANTOTHER
SEARCH STRING
DROP
TABLE USERS;
MY POORLY
IMPLEMENTED
BACKEND
MY BEAUTIFULLY
CRAFTED FRONTEND
imgflip.com

Referencias

- OWASP. (2021). OWASP Top Ten. Recuperado de: https://owasp.org/www-project-top-ten/
- OWASP. (s.f). SQL Injection. Recuperado de : https://owasp.org/www-community/attacks/SQL_Injection
- ¿Qué es SQL injection y Cómo afecta los SQL Query?. (s.f.). Recuperado de: https://estradawebgroup.com/Post/-Que-es-SQL-injection-y-Como-afecta-los-SQL-Query-/4273
- Microsoft. (2021). SQL Injection. Microsoft sql documentation. [Online]. Available: https://owasp.org/www-community/attacks/SQL_Injection