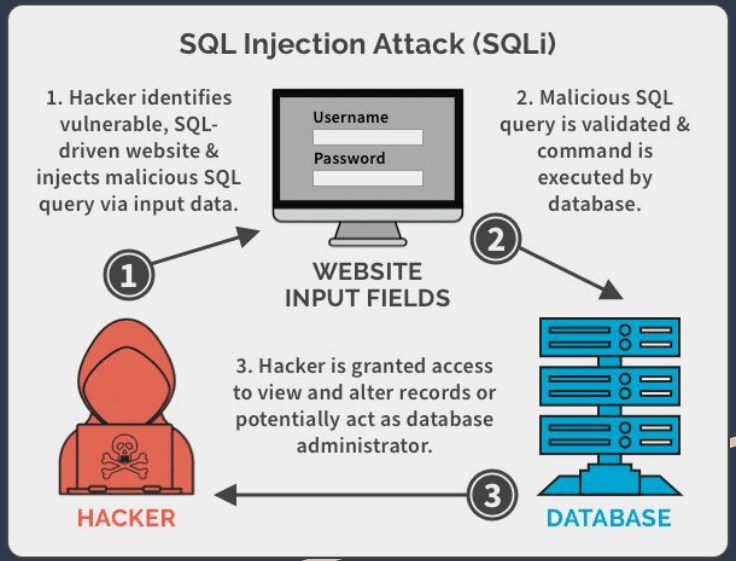
# SQL Injection

Jarrell Jackson
Caden Roberson

# What Is it

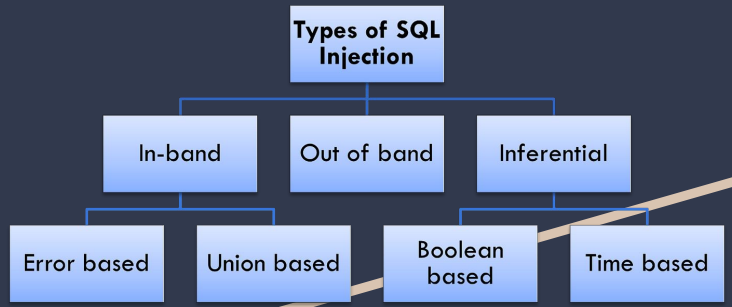

SQL (Structured Query Language) is a programming language that is used to store and process data in a relational database. Relational databases store information in a tabular form meaning that different data attributes are presented in rows and columns. SQL injection is the process of using malicious code to access information that was not supposed to be displayed.

# How Is It Done?




SQL injection happens when the application accepts a malicious user input and then uses it as a part of a SQL statement to query a backend database. An attacker can inject SQL control characters and command keywords (e.g., single quote (‘), double quote (“), equal (=), comment (- -), etc.). Using these control characters with common SQL commands (e.g., SELECT, FROM, DELETE, etc.) enables access or retrieval of data elements from a backend database server.

# Popular Types/Variants




- In-band SQL injection
  - Error-based SQL injection (the attacker causes error messages to appear on a database causing the attacker to gain information from the error messages.)
  - Union-based SQL injection (fuses multiple segments to get a single HTTP response which can be used by the attacker.)
- Inferential SQL Injection (aka Blind SQL injection)
  - Boolean Injection (The attacker sends out a SQL query prompting the return of a result. Based on the result, the information within the HTTP response will either be changed or unchanged. The attacker can then work out to see if the message generated was true or false.)
- Out-of-band injection
  - Performed when the attacker can't use the same channel to gather information when its too slow. These techniques count on DNS or HTTP requests to transfer data to an attacker

# Notable Events


- GhostShell attack
- Turkish government (SQL injection was used to breach a website and erase debt from agencies)
- 7-Eleven Breach (Penetrated corporate systems and stole upwards of 130 million credit card numbers )
- HBGary breach

# Mitigation Techniques

- System updates
- RBAC (role based access control)
- Input validation
- Error reporting
- Firewall
- Regular scanning (catch vulnerabilities before they do any damage)

# Links

https://www.synopsys.com/glossary/what-is-sql-injection.html.

https://brightsec.com/blog/sql-injection-attack/.

https://www.acunetix.com/websitesecurity/sql-injection/.

https://www.imperva.com/learn/application-security/sql-injection-sqli/#:~:text=SQL%20injections%20typically%20fall%20under,data%20and%20their%20damage%20potential.