# 1 SQL Injection

Injection flaws are always one of the most critical and commonplace security vulnerabilities for web applications. So it is no surprise that injection tops the OWASP list. There are various injection flaw types, but by far the most infamous is SQL injection, which has been successfully exploited by hackers for well more than a decade. SQL injection involves an attacker appending SQL database commands within an input field. If the web application code does not sanitize the input, it can allow SQL commands to be executed on the web server, allowing an attacker to bypass network DMZ security, and directly interrogate the back-end database. With SQL injection, an attacker is able to return and steal tables of information, change records, or even delete the entire database.

SQL Injection

http://demo.testfire.net/bank/login.aspx

## Example 1

Add

username as:

' OR 1=1 --

password: Any