

OWASP TOP 10

Injection

Insufficient
Logging

Broken
Authenticatio
n

Using components
with vulnerabilities

Sensitive data
exposure

Insecure
Deserialization

XML External Entity

Cross Site
Scripting

Broken Access
Control

Security
Misconfiguration

Injection - Definition

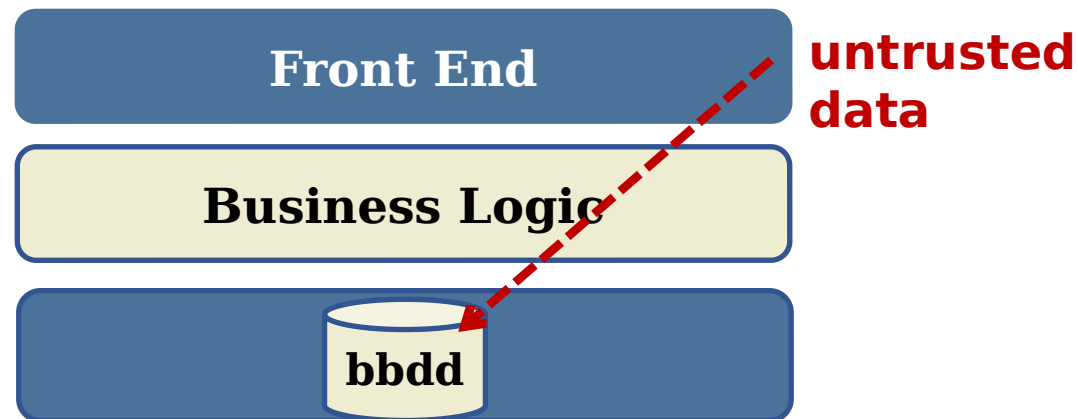
Injection happens when **untrusted data** is sent to an interpreter as part of a **command or query**. The attacker's hostile data can trick the interpreter into executing **unintended commands or accessing data** without proper authorization.

If the injection affects our database then we talk about **SQL Injection**.

If the injection affects our logs then we talk about **Log Injection**.

If the injection executes some commands of our system then we talk about **Command Injection**.

And there are more injection issues as LDAP injection, XPATH injection.




Injection - demo

Vulnerable Chess Game

You can try SQL Injection in this page ;-)

According to the OWASP TOP TEN: it is risk #1, more info [here](#)



Username

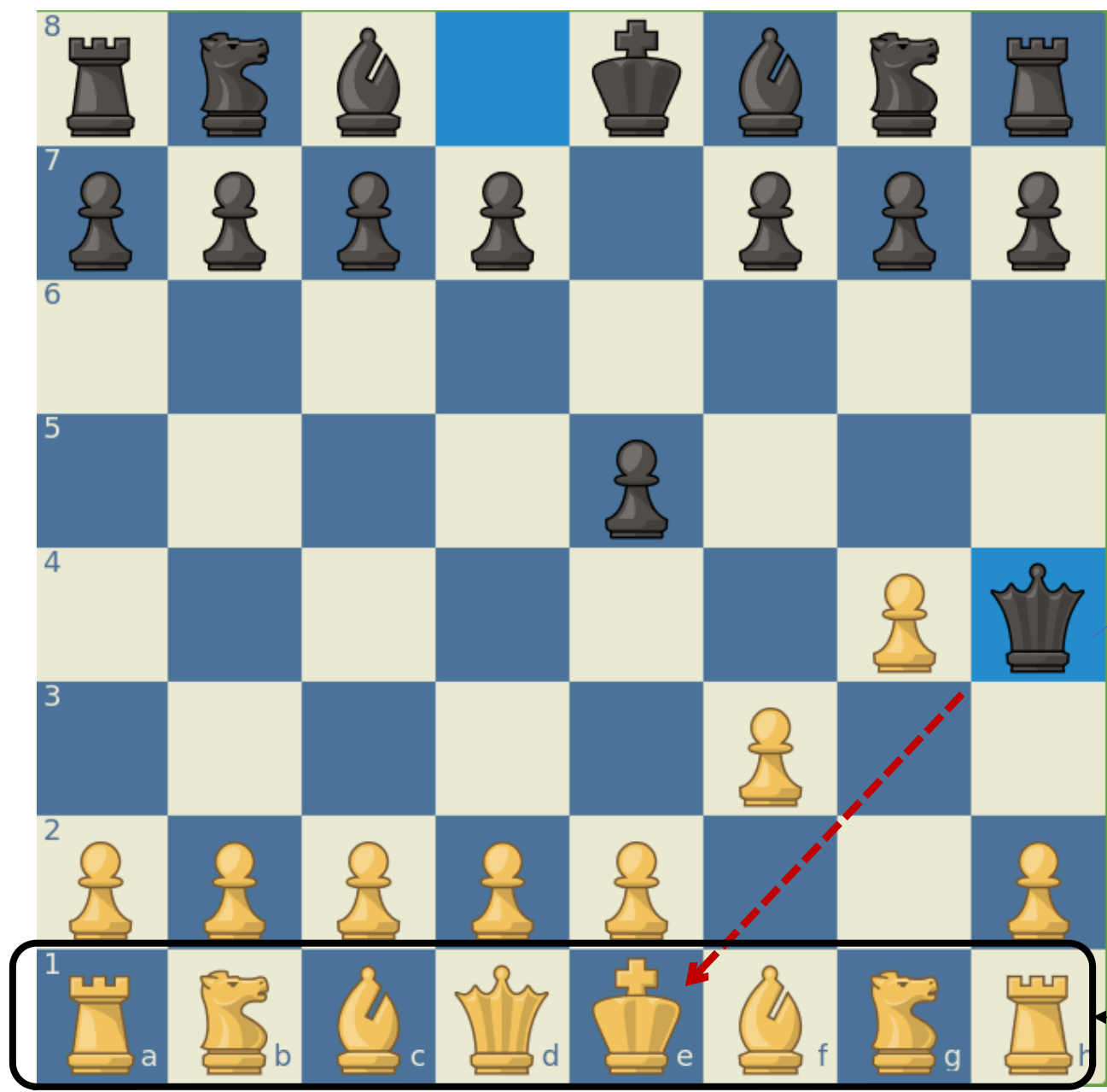
Password

Login

HINT 1. username: user' or '1'='1 Password: Whatever

HINT 2. username: whatever Password: 'UNION select * from user where '1'='1

Injection
Chess
comparison



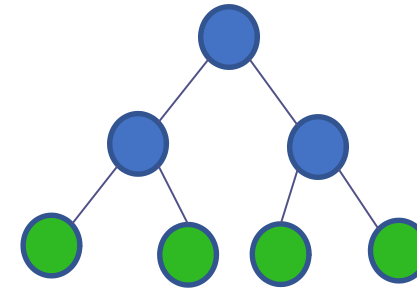
**Bad defense,
no one can
stop the
attack.**

**It is the
fastest check
mate of the
history.**

backend

Injection: solutions

- Validate each input. “Don’t trust in the end user”
 - Whitelist
 - Regular expression
 - String length
 - Data type
- Use modern frameworks
- Use prepared statements (SQL Injection)
- Use stored procedure (SQL Injection)



https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html