

Proposer par moi ze3ma hahaha pour chapitre 1

Nseblkmok ?ghamel te3 zbi

**Table of contents**

**General introduction............................................................................................. 1**

### **Chapter 1: SQL Injection and Modern Detection Approaches…………2**

#### **1.1 Introduction**

#### **1.2 Understanding Web Applications and Databases**

* definition of web applications brk

#### **1.3 SQL Injection:Definition and Mechanisms**

* 1.3.1 Whatis SQL Injection?
* 1.3.2 How SQL Injection Works
* 1.3.3 Impact of SQL Injection Attacks

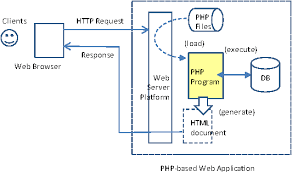
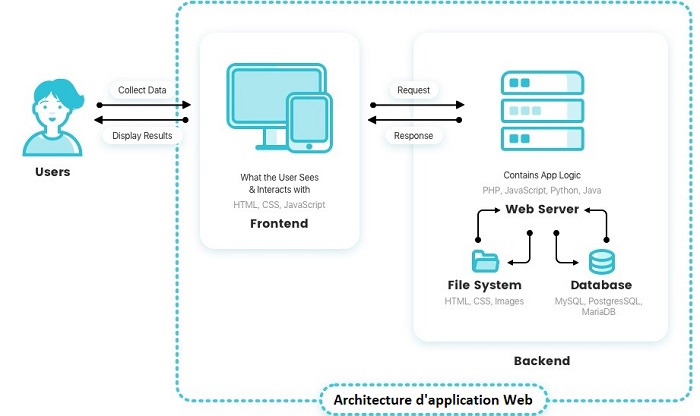
#### **1.4 Techniques of SQL Injection**

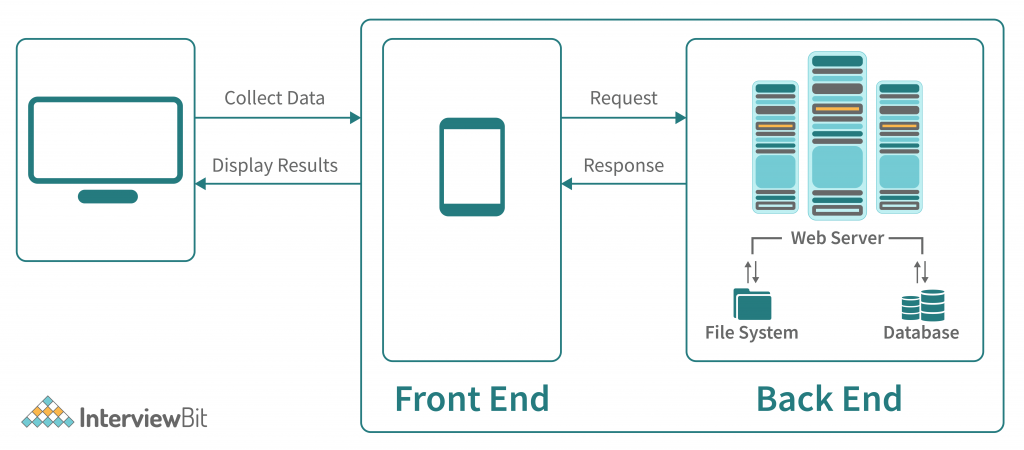
* 1.4.1 Tautology-Based SQL Injection
* 1.4.2 Error-Based SQL Injection
* 1.4.3 Blind SQL Injection
  + 1.4.3.1 Content-Based Blind SQL Injection
  + 1.4.3.2 Time-Based Blind SQL Injection
* 1.4.4 Union-Based SQL Injection
* 1.4.5 Other Advanced Techniques

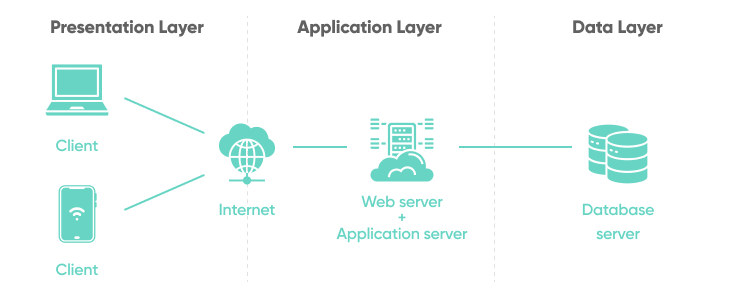
#### **1.5 Traditional Defense Mechanisms Against SQL Injection**

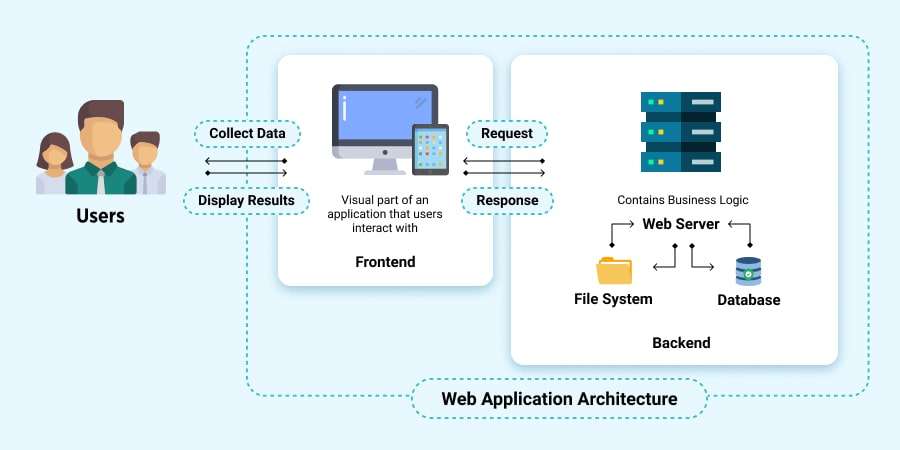
* 1.5.1 Input Validation and Sanitization
* 1.5.2 ParameterizedQueries and PreparedStatements
* 1.5.3 EscapingSpecialCharacters
* 1.5.4 Web Application Firewalls (WAF)
* 1.5.5 Limitations of Traditional Methods

#### **1.6 Conclusion**









Refernces

1 sql inejction (<https://www.red-gate.com/hub/product-learning/redgate-monitor/picking-over-the-bones-of-a-sql-injection-attack?utm_source=DBW&utm_medium=pubemail>)

2 types de ijection (<https://portswigger.net/web-security/sql-injection>)

HADA yvdg bzf te3 ia detactor mdlou text mktoub b ia yglbou mktoup humain (<https://www.humanizeai.pro/>)

W hada 9a7boun ymdlk pourcentage te3 ia (<https://app.gptzero.me/>)

##### 1.4.3.2 Time-Based Blind SQL Injection

* **Detailed Explanation:** SQL queries include time-delay functions to infer query results based on the time taken to execute.
* **Extended Example:**

' OR IF(1=1, SLEEP(5), 0) --

* **Impact:**
  + Data extraction without error messages.
  + Performance degradation during attacks.
* **Countermeasures:**
  + Implement query limits.
  + Use ORM frameworks.

#### 1.4.4 Union-Based SQL Injection

This method leverages the UNION SQL operator to combine the results of multiple queries, retrieving data from other tables.

* **Detailed Explanation:** Attackers add malicious queries to original SQL statements, exploiting the UNION operator to fetch data.
* **Extended Example:**

' UNION SELECT null, username, password FROM users --

* **Impact:**
  + Complete database extraction.
  + Theft of sensitive information.
* **Countermeasures:**
  + Validate query structures.
  + Restrict database permissions.

#### 1.4.5 Other Advanced Techniques

* **Second-Order SQL Injection:** Stores malicious SQL in the database, executed during subsequent operations.
* **Out-of-Band SQL Injection:** Transmits data through DNS/HTTP requests.
* **Stored Procedure Injection:** Targets database procedures for exploitation.

SQL injection attacks can lead to catastrophic consequences. Implementing robust defenses such as prepared statements, input validation, and comprehensive security audits is essential to protect web applications from such vulnerabilities.