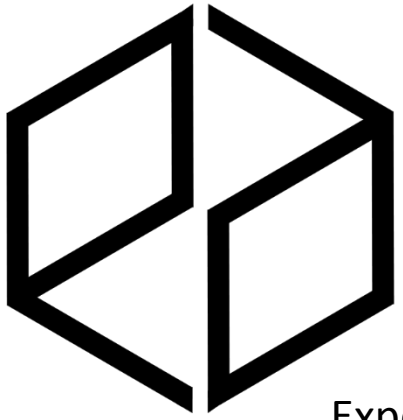
www.pandoralabs.net

PANDORA
SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

OWASP TOP 10: #1 Injection

By @isaacsabas



PANDORA
SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.
www.pandoralabs.net

We are a Security-as-a-Service company

Providing businesses with on-demand IT security controls for them to meet their 24x7 security strategies & requirements.

We Make IT Secure

OWASP

Open Web Application Security Project

OWASP Top 10

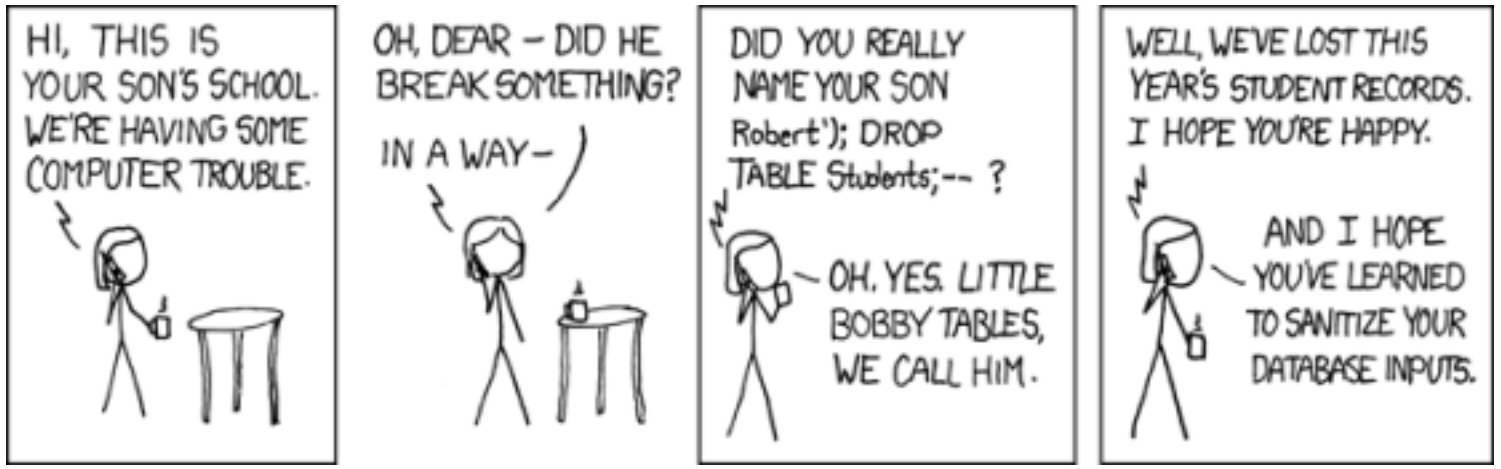
Open Web Application Security Project


A1: Injection
A2: Broken Authentication and Session Management
A3: Cross-Site Scripting (XSS)
A4: Insecure Direct Object References
A5: Security Misconfiguration
A6: Sensitive Data Exposure
A7: Missing Function Level Access Controls
A8: Cross Site Request Forgery (CSRF)
A9: Using Components with Known Vulnerabilities
A10: Unvalidated Redirects and Forwards

OWASP #1

Injection

OWASP Top 10 Vulnerabilities

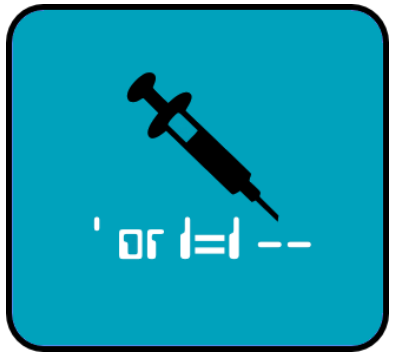


Injection Vulnerability – What is it?

Where it all began.

Different Types of “Injection”

- Involves allowing untrusted or manipulated request, commands or queries to be executed by a web application
- SQL Injection
- Code Injection
- LDAP Injection
- XML Injection
- Many more…



SQL INJECTION

The single most prominent type of injection vulnerability

It's the web app, not the database

**The problem lies not in the database;
but how the web app/site was coded.**

What are the Risks When Exploited?

- Data loss or corruption
- Data theft
- Unauthorized access
- Denial of Service
- System Compromise

Go to http://demo.testfire.net

EXPLOIT DEMO

How simple it is to test for a SQL Injection vulnerability.

Demo

1. Insert a SQL query and review its response
2. Inject SQL query to bypass the login mechanism
3. Login to the web app and looking into some sensitive information
4. Inject SQL query to obtain other data from DB

How to I Prevent Such Vulnerabilities?

- Escape all special characters used by the application
- Input validation/sanitization
- Use widely supported code libraries or frameworks
- Run applications with minimum OS privileges

TIME FOR Q&A

OWASP Top 10 - Injection

Go download WebGoat

https://github.com/WebGoat/WebGoat-Legacy

TRY IT YOURSELF

Some homework for you to learn a bit more.

WebGoat Installation How-To

1. Download Java VM, JDK 1.7
2. Download WebGoat: https://webgoat.atlassian.net/builds/browse/WEB-WGM/latestSuccessful/artifact/shared/WebGoat-Embedded-Tomcat/WebGoat-6.0.1-war-exec.jar
3. Run the .jar file:
    1. java -jar WebGoat-6.0-exec-war.jar
4. Then navigate in your browser to: (http://localhost:8080/WebGoat)
5. Login using guest account
6. Go to: Injection Flaws and complete the following exercises:
    1. String SQL Injection
    2. Add Data with SQL Injection
    3. Blind Numeric SQL Injection

OWASP #1

Injection

OWASP Top 10 Vulnerabilities

www.pandoralabs.net

PANDORA
SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

OWASP TOP 10: #1 Injection

By @isaacsabas