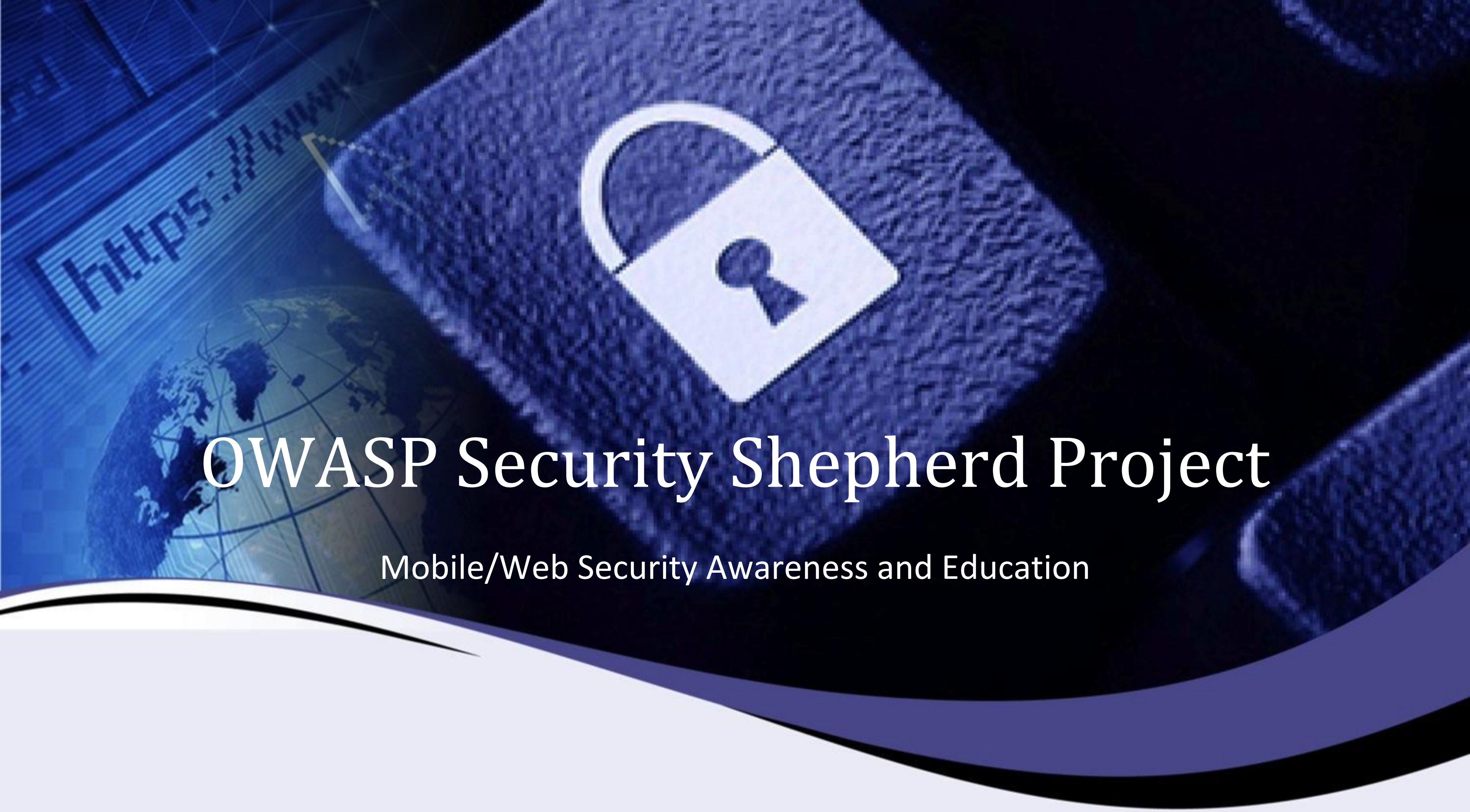


# OWASP Security Shepherd Project

Mobile/Web Security Awareness and Education

OWASP

The Open Web Application Security Project

# About Us

OWASP
The Open Web Application Security Project

## Mark Denihan

@markdenihan

mark.denihan@owasp.org

## Sean Duggan

@duggan4sean

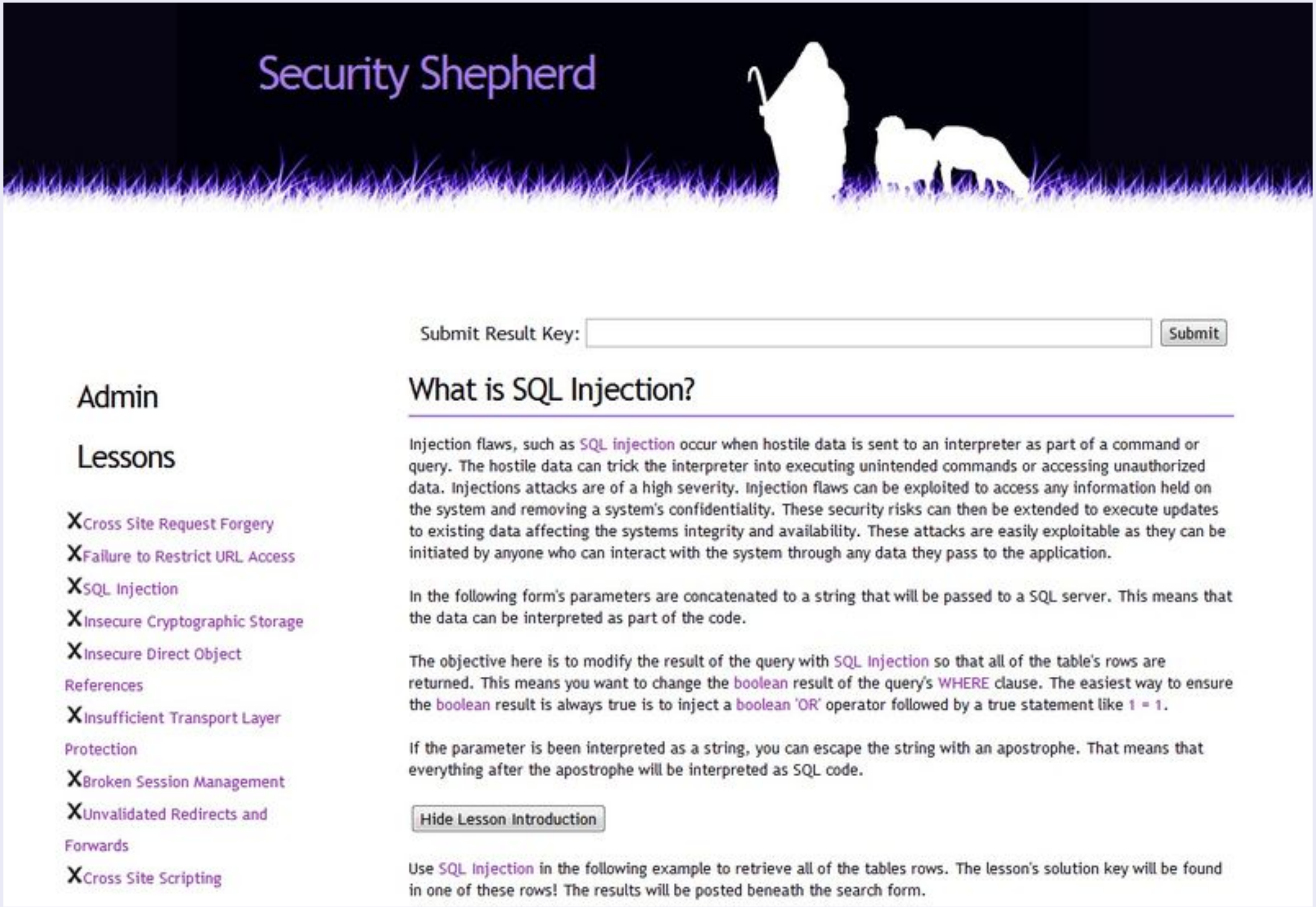
sean.duggan@owasp.org

The opinions expressed in this presentation represent our own and not those of any organisation.

# What is Security Shepherd?

# What is Security Shepherd

OWASP
The Open Web Application Security Project


Security Shepherd
Admin
Lessons
XCross Site Request Forgery
XFailure to Restrict URL Access
XSQL Injection
XInsecure Cryptographic Storage
XInsecure Direct Object References
XInsufficient Transport Layer Protection
XBroken Session Management
XUnvalidated Redirects and Forwards
XCross Site Scripting
Submit
Hide Lesson Introduction

Submit Result Key:

## What is SQL Injection?

Injection flaws, such as SQL injection occur when hostile data is sent to an interpreter as part of a command or query. The hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data. Injections attacks are of a high severity. Injection flaws can be exploited to access any information held on the system and removing a system's confidentiality. These security risks can then be extended to execute updates to existing data affecting the systems integrity and availability. These attacks are easily exploitable as they can be initiated by anyone who can interact with the system through any data they pass to the application.

In the following form's parameters are concatenated to a string that will be passed to a SQL server. This means that the data can be interpreted as part of the code.

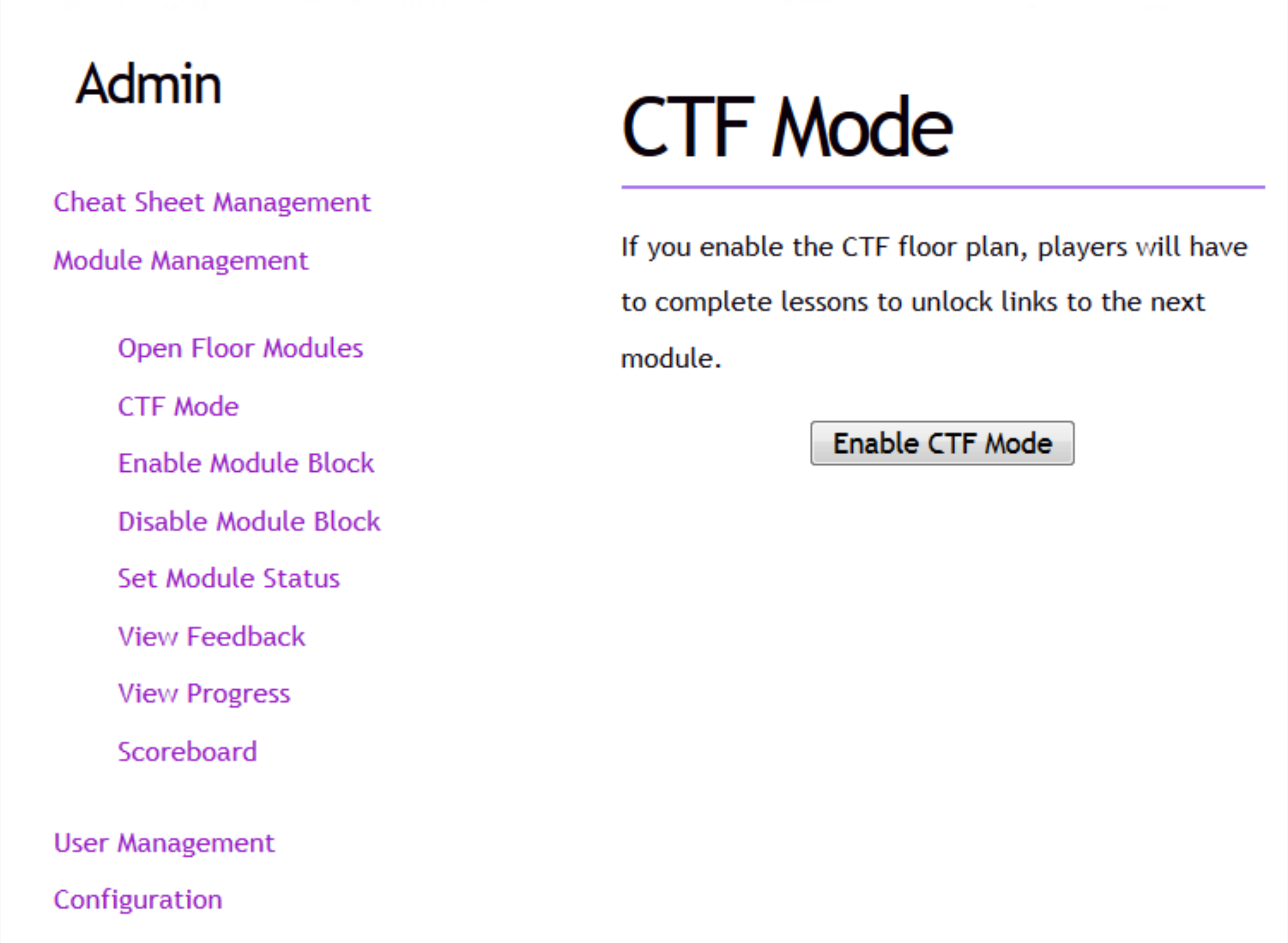
The objective here is to modify the result of the query with SQL Injection so that all of the table's rows are returned. This means you want to change the boolean result of the query's WHERE clause. The easiest way to ensure the boolean result is always true is to inject a boolean 'OR' operator followed by a true statement like 1 = 1.

If the parameter is been interpreted as a string, you can escape the string with an apostrophe. That means that everything after the apostrophe will be interpreted as SQL code.

Use SQL Injection in the following example to retrieve all of the tables rows. The lesson's solution key will be found in one of these rows! The results will be posted beneath the search form.

# The Platform

OWASP
The Open Web Application Security Project

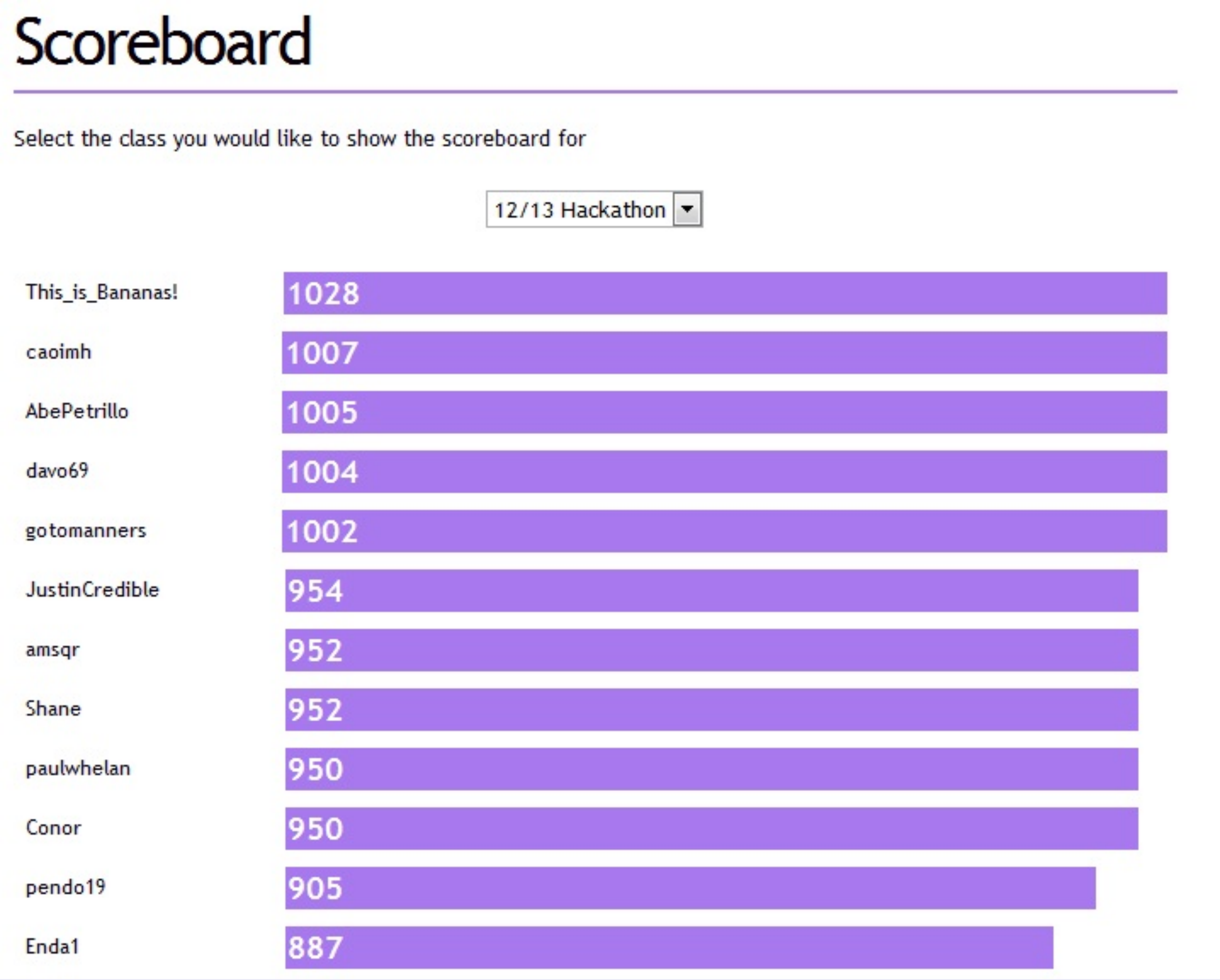


Admin

## CTF Mode

If you enable the CTF floor plan, players will have to complete lessons to unlock links to the next module.

# Learning is a Game



## Scoreboard

Select the class you would like to show the scoreboard for

12/13 Hackathon ▾

| | |
|---|---|
| This_is_Bananas! | 1028 |
| caoimh | 1007 |
| AbePetrillo | 1005 |
| davo69 | 1004 |
| gotomanners | 1002 |
| JustinCredible | 954 |
| amsqr | 952 |
| Shane | 952 |
| paulwhelan | 950 |
| Conor | 950 |
| pendo19 | 905 |
| Enda1 | 887 |

# Shepherd as a CTF

OWASP
The Open Web Application Security Project

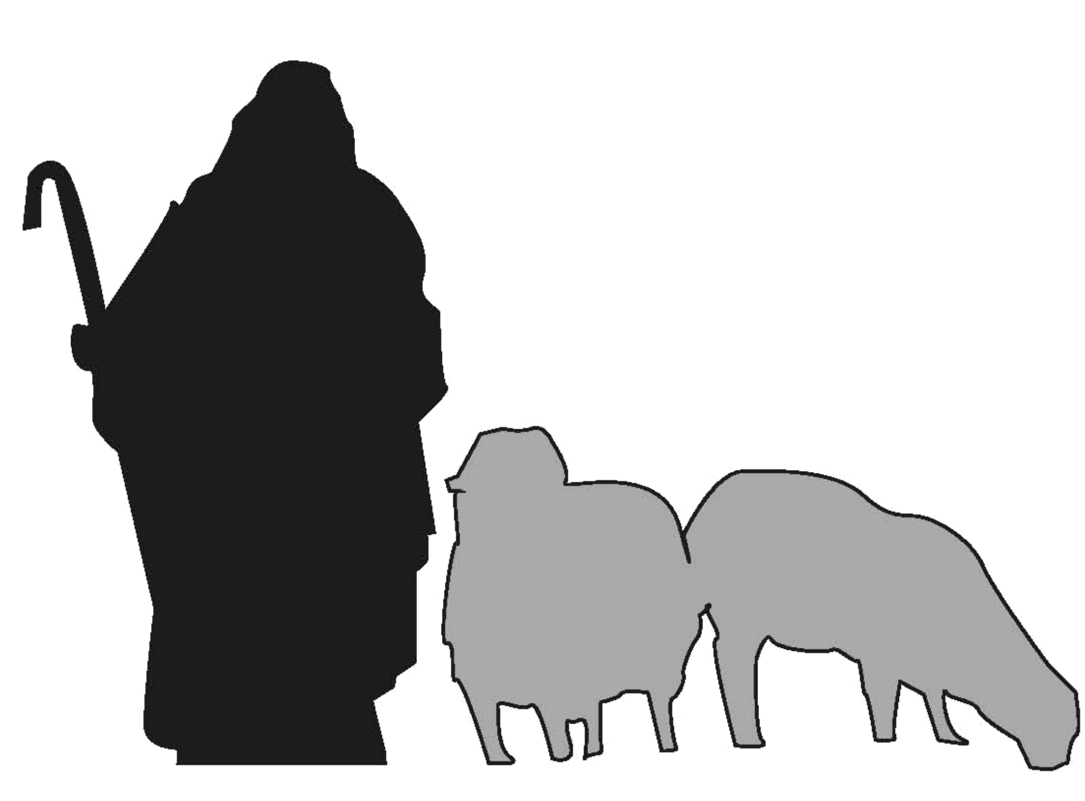
AppSec Ireland 2012

SOURCE
Security Conference And Training

IRISS
Irish Reporting and Information Security Service

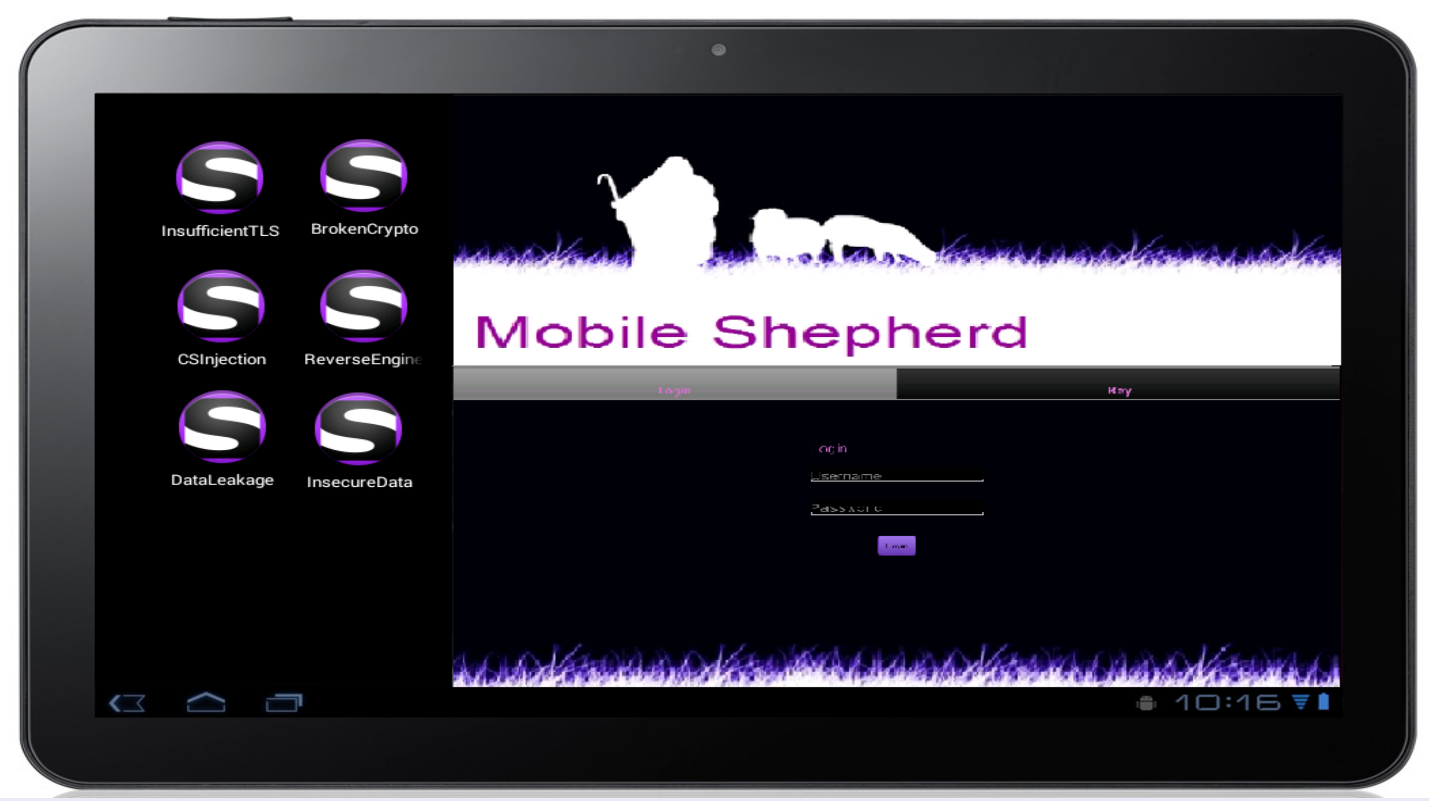
OWASP GLOBAL CTF

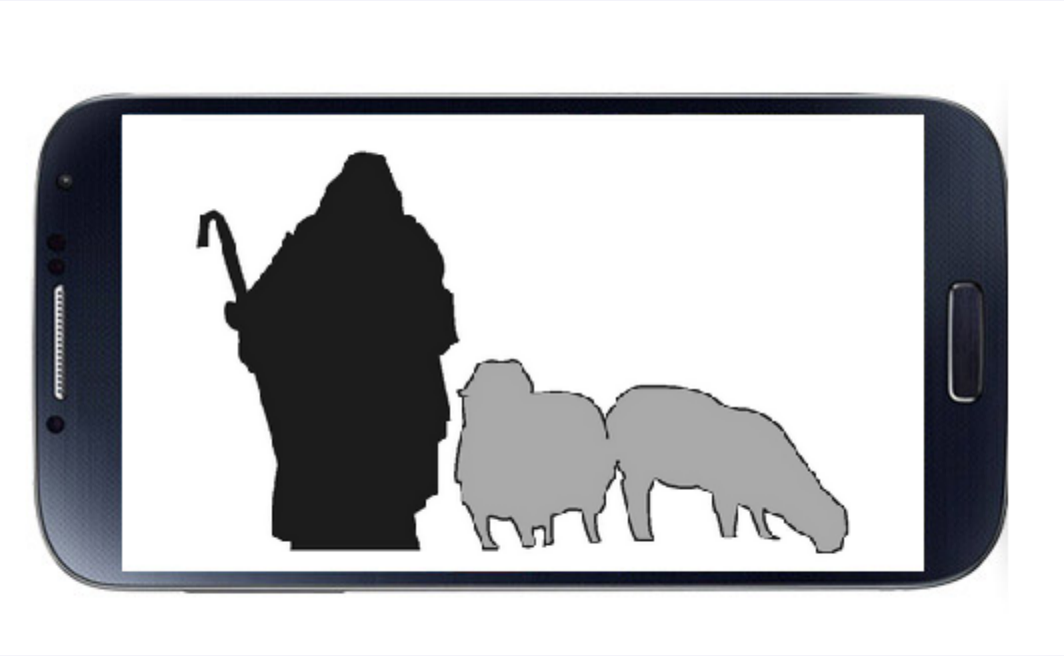
OWASP
The Open Web Application Security Project



## Lesson & Challenge Demonstration

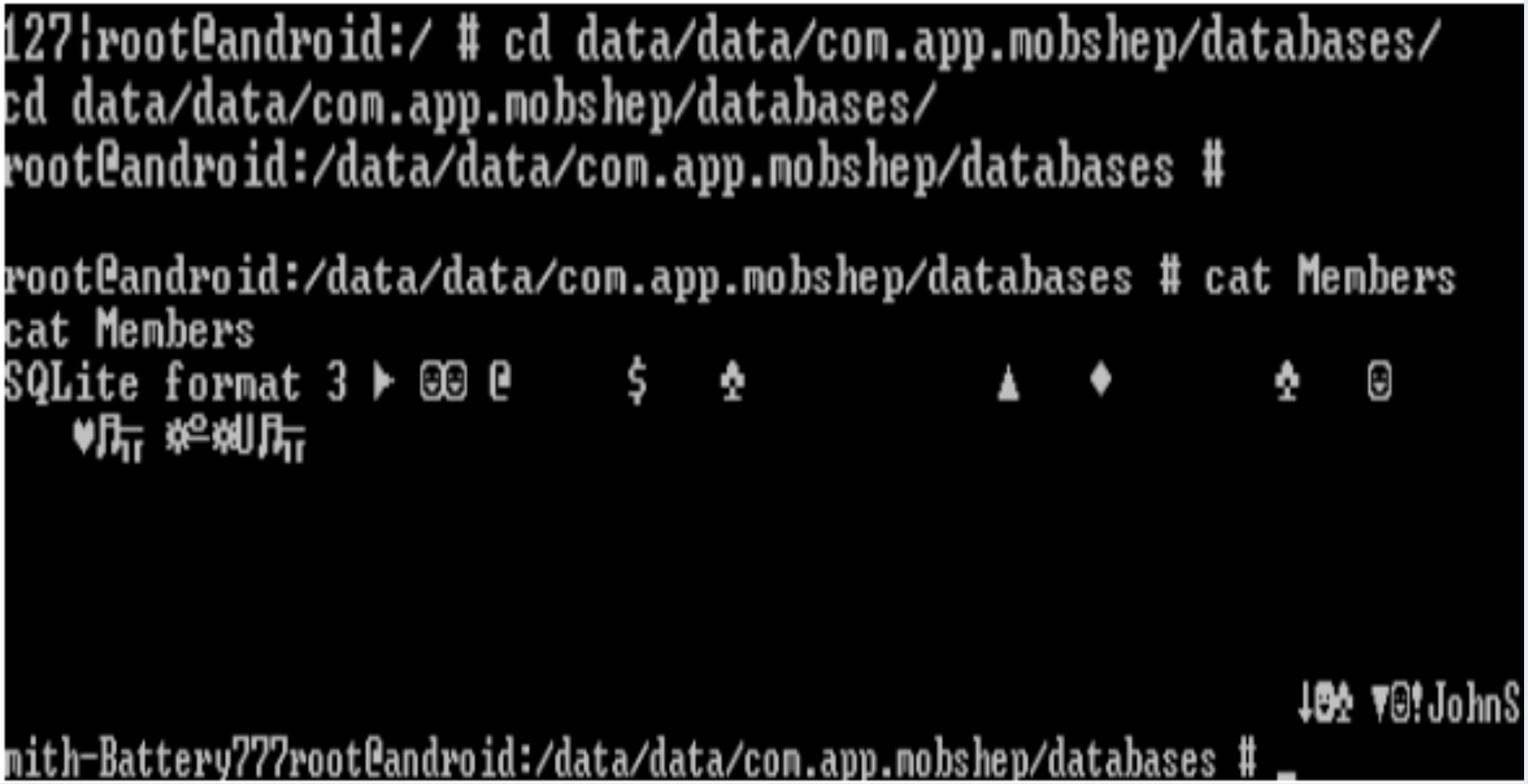
# Mobile Security Awareness





# Lesson & Challenge Demonstration

# Practical Examples - Databases



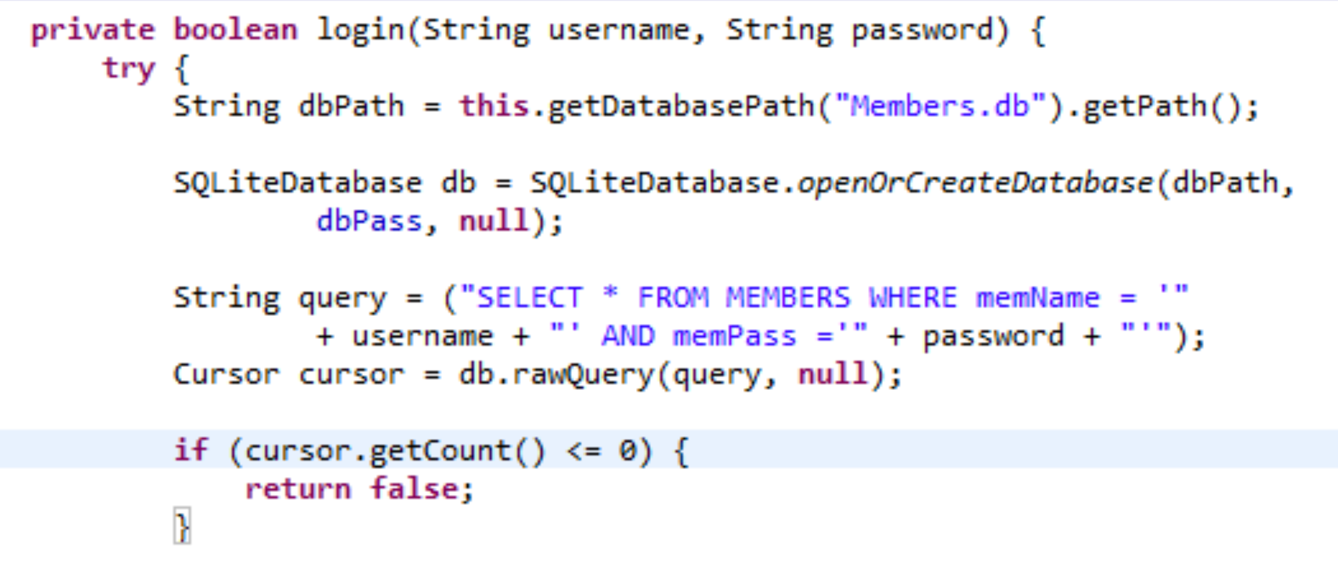
```
127|root@android:/ # cd data/data/com.app.mobshep/databases/
cd data/data/com.app.mobshep/databases/
root@android:/data/data/com.app.mobshep/databases #

root@android:/data/data/com.app.mobshep/databases # cat Members
cat Members
SQLite format 3 ► ☻☻ @     $   ♣              ▲   ♦       ♣   ☻
   ♥╓╖ ☼º☼╙╓╖




                                                               ↓☻♣ ▼☻!JohnS
mith-Battery777root@android:/data/data/com.app.mobshep/databases # _
```

# Practical Examples - Injection



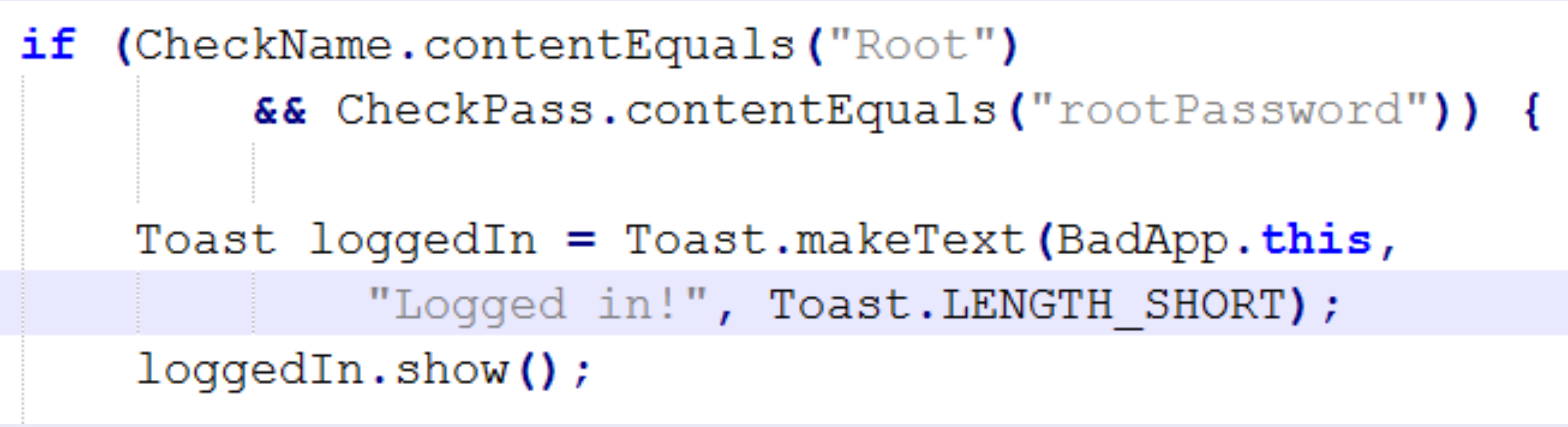
```
private boolean login(String username, String password) {
    try {
        String dbPath = this.getDatabasePath("Members.db").getPath();

        SQLiteDatabase db = SQLiteDatabase.openOrCreateDatabase(dbPath,
                dbPass, null);

        String query = ("SELECT * FROM MEMBERS WHERE memName = '"
                + username + "' AND memPass ='" + password + "'");
        Cursor cursor = db.rawQuery(query, null);

        if (cursor.getCount() <= 0) {
            return false;
        }
```

# Practical Examples - Hard coding



```
if (CheckName.contentEquals("Root")
        && CheckPass.contentEquals("rootPassword")) {

    Toast loggedIn = Toast.makeText(BadApp.this,
            "Logged in!", Toast.LENGTH_SHORT);
    loggedIn.show();
```

# Help Us Build Higher

## Join the Mailing List!

http://bit.ly/shepherdMailingList

# Contact Us

OWASP
The Open Web Application Security Project

## Mark Denihan

@markdenihan
mark.denihan@owasp.org

## Sean Duggan

@duggan4sean
sean.duggan@owasp.org