

Hands-on B1: Predicting Threats

Read the following report from the national technology security coalition (also available for download from the stream site);

<https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf>

Deliverables [3 Marks]:

Please hand-in a short report detailing:

1. What are the most significant cyber security concerns in 2020 shifted from 2019?
2. In your opinion, what were the top 3 most significant security issues in 2019 and why did you choose these?
3. Which of the recent technologies are most exploited and why do you think they become the growing target?

Hands-on B2: Password Cracking

Users' passwords are typically stored not in their plaintext form, but in their digest (or hashed) form. In this exercise, the student experiments to break into passwords by cracking the password hashes.

You are given the FIVE different hash values as following. You will need to crack these hash values in order to recover the original words that were used to produce the hash in the first place.

During the lab, you can use this website (or other websites of your choosing) for password cracking:

<https://crackstation.net/>

The hash values that you need to crack are:

- [1]. 81dc9bdb52d04dc20036dbd8313ed055
- [2]. e91e6348157868de9dd8b25c81aebfb9

- [3]. b273b0604664ef525ef83046d1b79659
- [4]. 7110eda4d09e062aa5e4a390b0a572ac0d2c0220
- [5]. c84c50d5a767a23bda0ea5ca348fed54c6db9aab

Deliverables [3 Marks]:

Please hand-in a short report detailing:

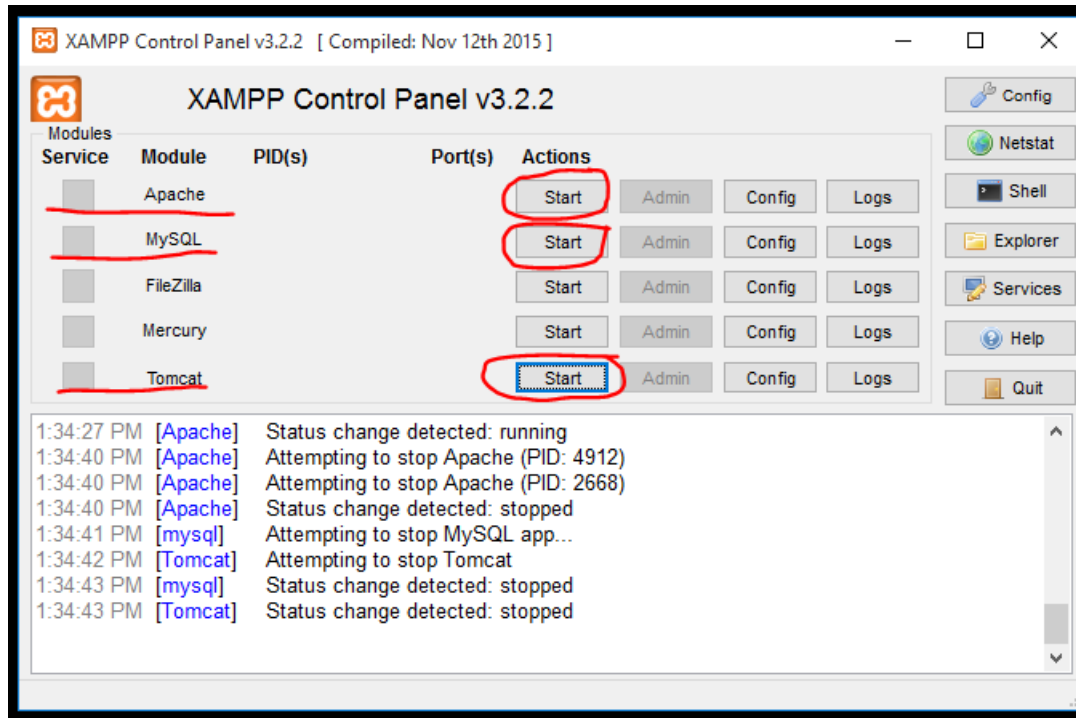
1. What is hash? How is it related to password? How is it used for password cracking?
2. Submit your result of hash cracking, including the original word used for the hash and the type of hash function. If one or more of those hashes cannot be cracked, please state that you did not manage and your opinion about why it was not cracked.
3. Create at least 2 hash digests. You can use a tool like this: <http://www.fileformat.info/tool/hash.htm>. Submit your original word, corresponding hash digest, and hash function.

Hands-on B3: Exploiting Web

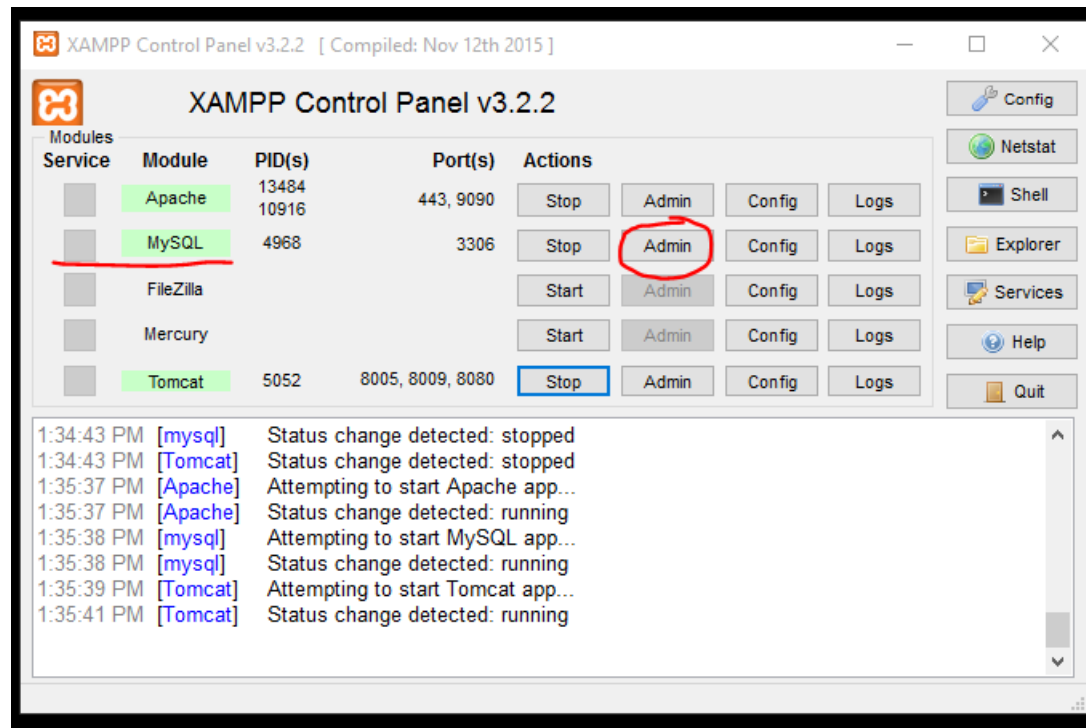
In this exercise, the student finds a different ways to exploit web application vulnerabilities to attempt unauthorized access to user's sensitive data.

Set up:

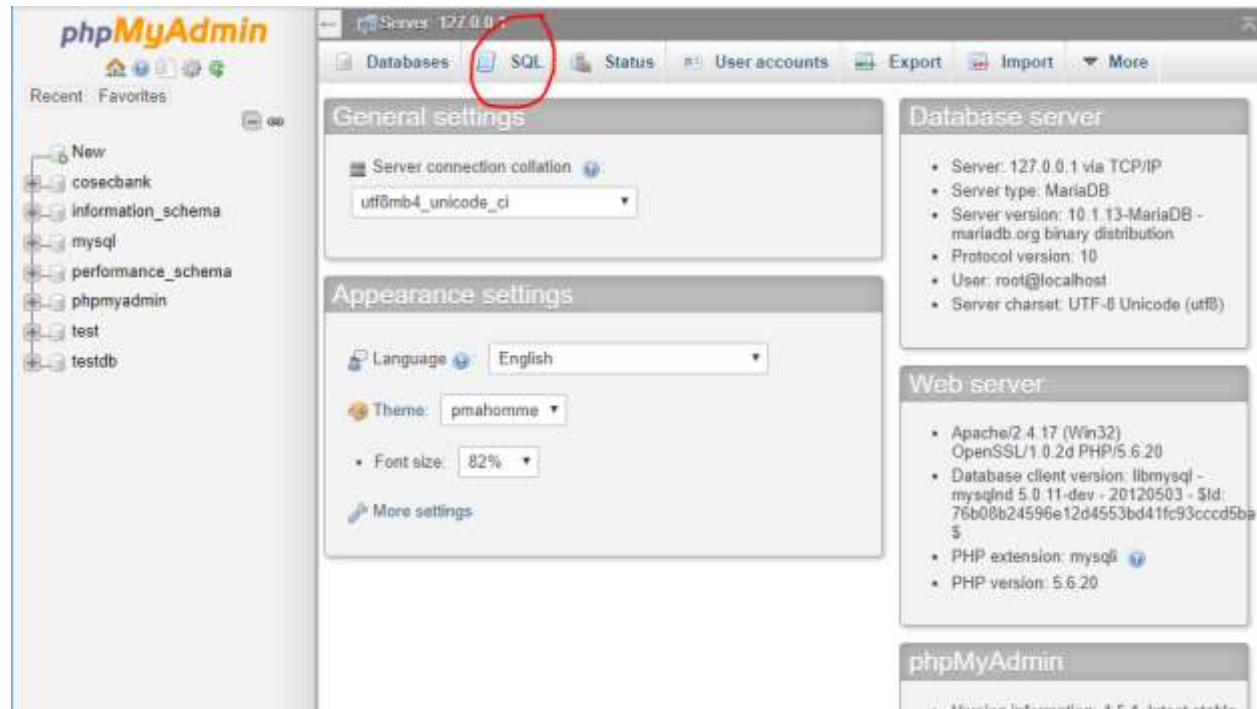
1. Download [CosecBank.zip](#) from the course stream website. Move it to [xampp/tomcat/webapps](#) directory, extract it by right click on the file/click 7-zip/Extract to CosecBank\
2. Download [mysql-connector-java-5.1.43-bin.jar](#) from the course stream website. Move it to under [xampp/tomcat/lib](#) directory.
3. Open XAMPP control panel. Run Apache, MySQL, Tomcat:



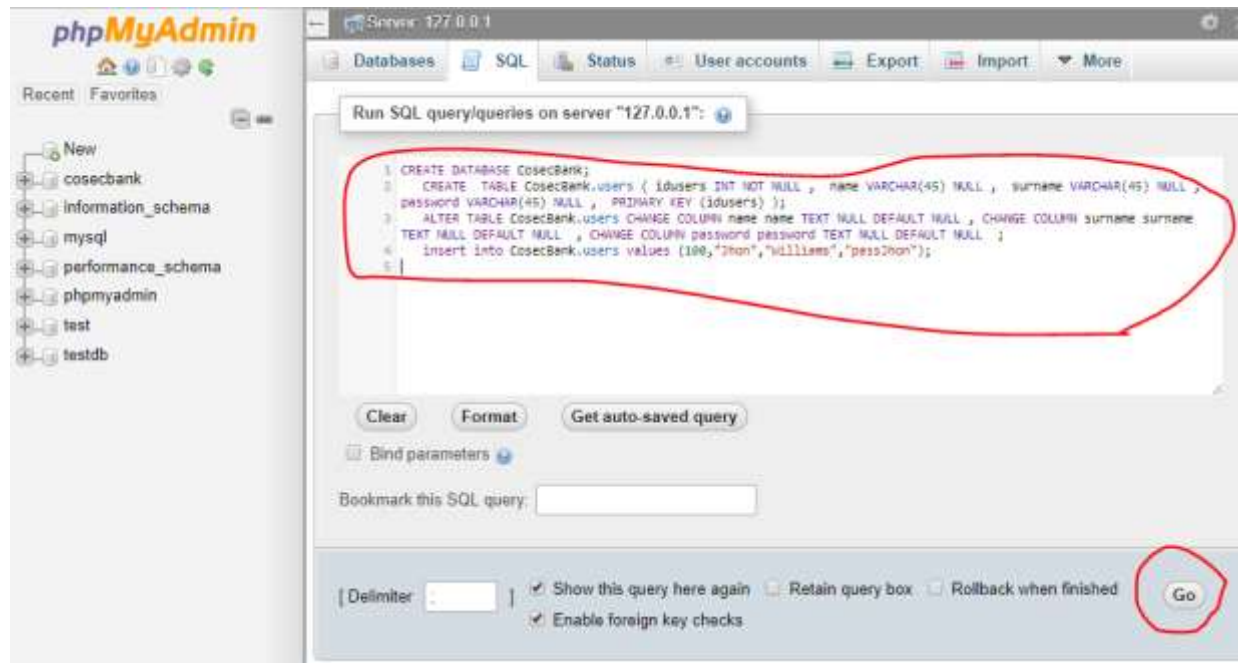
Open XAMPP control panel. Click Admin next to MySQL icon.



This will bring phpMyAdmin on your browser. Click SQL menu.



Run the following sql statement and click "go".



CREATE DATABASE CossecBank;

```
CREATE TABLE CossecBank.users ( idusers INT NOT NULL , name VARCHAR(45) NULL , surname VARCHAR(45)
NULL , password VARCHAR(45) NULL , PRIMARY KEY (idusers) );
```

```
ALTER TABLE CossecBank.users CHANGE COLUMN name name TEXT NULL DEFAULT NULL , CHANGE
COLUMN surname surname TEXT NULL DEFAULT NULL , CHANGE COLUMN password password TEXT NULL DEFAULT
NULL ;
```

```
insert into CossecBank.users values (100,"Jhon","Williams","passJhon");
```

Deliverables [4 Marks]

1. Let's assume that someone else was already logged in. Describe what attack is attempted by the following sequence and the way the attack is executed.

Type url in your browser: <http://localhost:8080/CosecBank/index.jsp>. Click register.

Log in

Log in

Name

Password

Log in

Register

COSEC - BANK

In the register page.

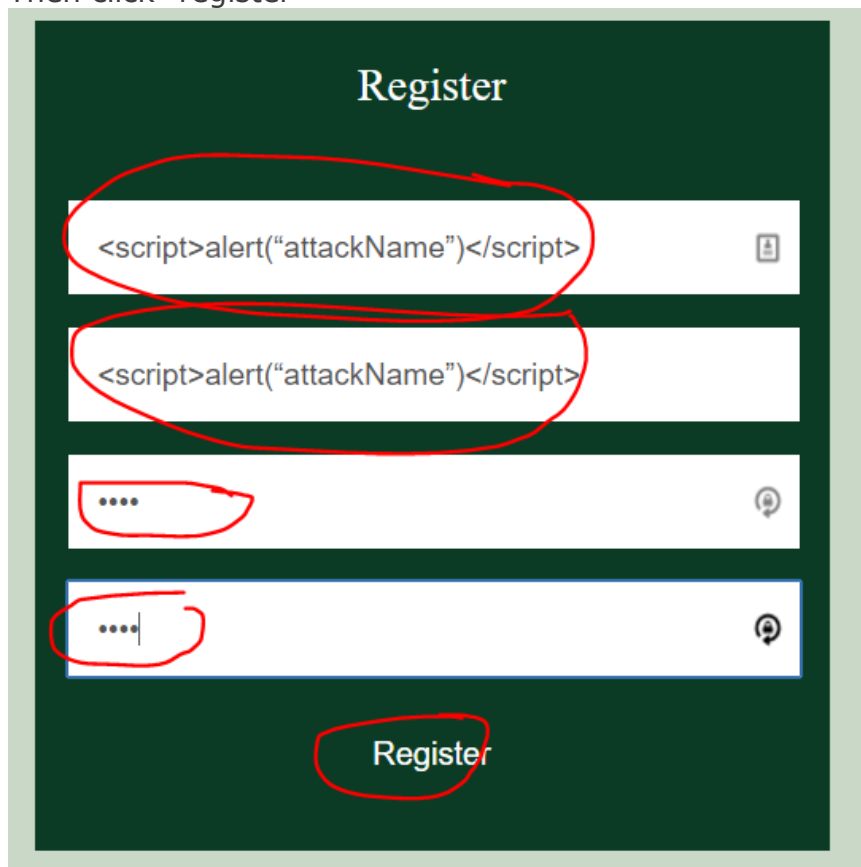
Enter : `<script>alert("attackName")</script>` in the "name" field

Enter : `<script>alert("attackSurname")</script>` in the "Surname" field

Enter : pass in the "Password" field

Enter : pass in the "Confirmed Password" field

Then click "register"



The image shows a 'Register' form with a dark green background. The title 'Register' is at the top. There are four input fields and a 'Register' button at the bottom. Red circles and arrows highlight the following elements:

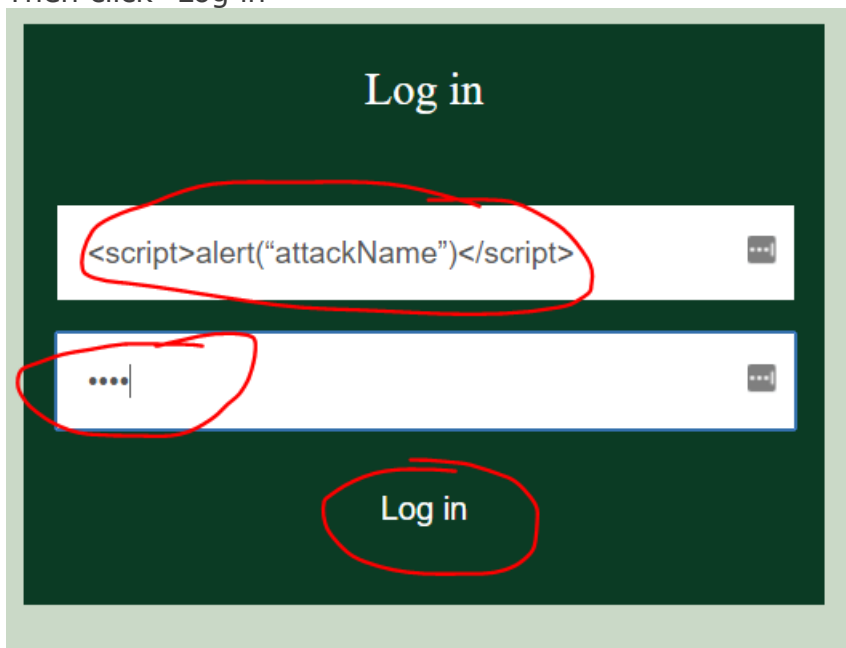
- The first input field (Name) containing the text `<script>alert("attackName")</script>`.
- The second input field (Surname) containing the text `<script>alert("attackName")</script>`.
- The third input field (Password) containing four dots.
- The fourth input field (Confirmed Password) containing four dots.
- The 'Register' button at the bottom.

In the log in page.

Enter : `<script>alert("attackName")</script>` in the "name" field

Enter : pass in the "password" field

Then click "Log in"



Log in

`<script>alert("attackName")</script>`

pass

Log in

2. Describe what attack is attempted by the following sequence and the way the attack is executed.

Type url in the browser: http://localhost:8080/CosecBank/login.jsp?name=test union select * from users;

*if you are new to SQL, read here: <https://en.wikipedia.org/wiki/SQL> and here https://en.wikipedia.org/wiki/SQL_syntax

