ITIS 6200/8200 Principles of Information Security and Privacy

Project 2: SQL and XSS Attacks

The goal of this project is to let you practice SQL injection and XSS attacks in the web. A webpage and back-end database are provided in our virtual machine environment.

Download the Virtual Machine (https://drive.google.com/file/d/1PfHfV_sKGTWp6agZx8an8Z7EjvLsfnQN/view?usp=sharing)
The following video (SQLi attacks introduction (https://youtu.be/VmjVYPiCtgU)) will help you with the project. In the instructions we link some tips back to certain period of the video.

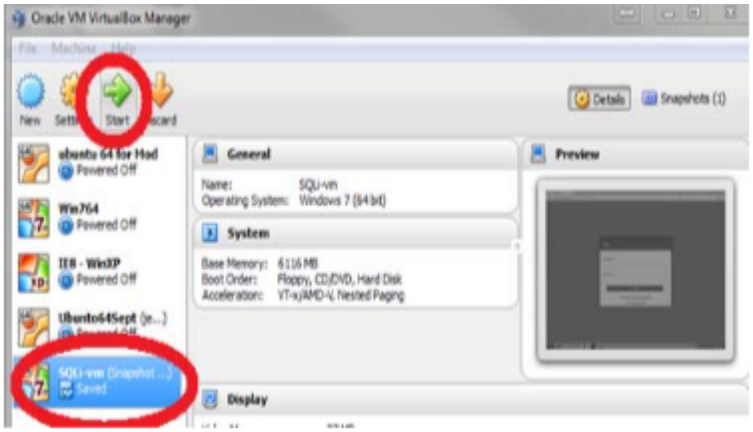
Objective

The objective of the project is to provide a hands-on experience to students so that they have a better understanding of web security and SQL injection attacks. At the same time, we want to show how such attacks are executed. For this purpose, we prepared a virtual machine that has a web application that is connected to a database. This provides a safe environment to try and experiment with such attacks. Recall to experiment with these attacks only in such safe and isolated environments.

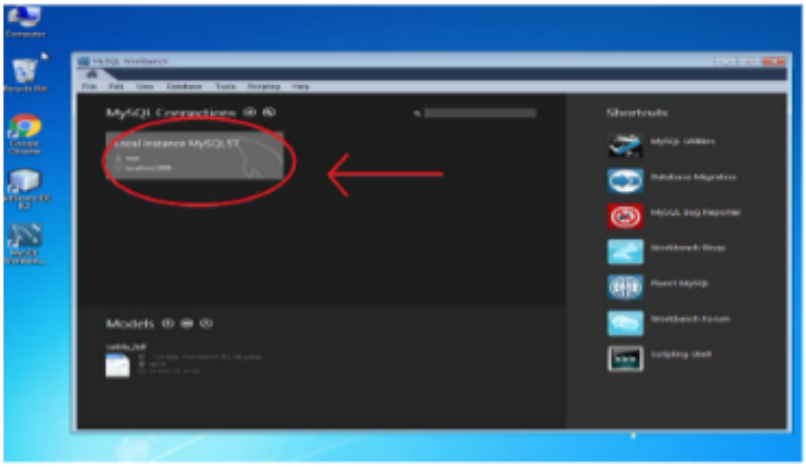
Tasks

Installing

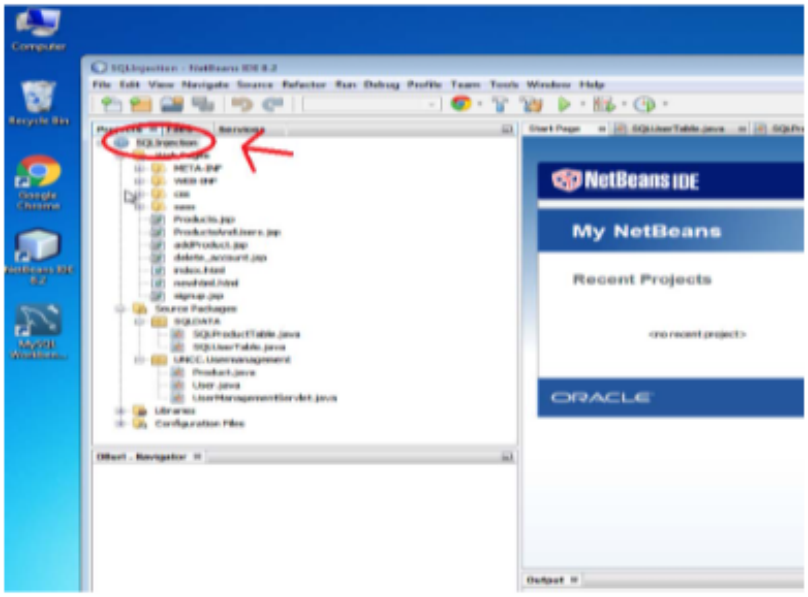
1. Download and install **VirtualBox**. Suggested version: **VirtualBox 6.1**
2. Download the virtual machine zip file that you will be using through the provided link -- Go to File and choose Import appliance
3. Navigate to unzipped directory and find the folder SQLi-vm then choose the file SQLi-vm and click ‘open’
4. Once loaded, select the virtual machine and click start:



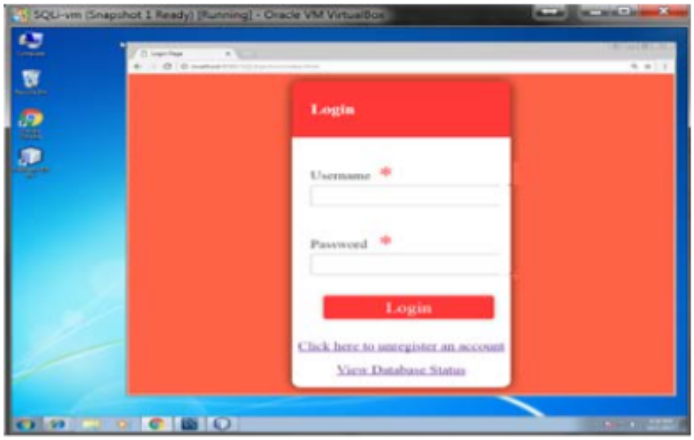
5. Start MySQL Workbench. After the Virtual machine finishes loading, you should be able to see the desktop. There is an icon for MySQL on the desktop, double click it to start the application. Once it starts, double click the ‘local instance’ (red in picture) and enter the password **root** if asked for a password.



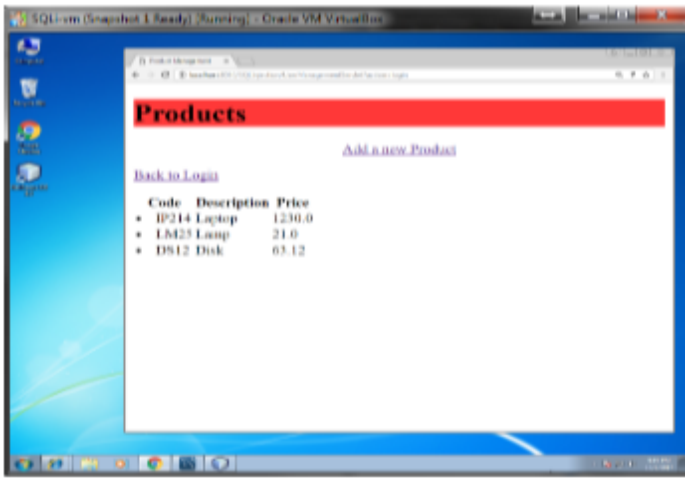
6. Start Netbeans and Run web app. The desktop has another icon for NetBeans IDE, you can double click it to start the application. Then, right click SQLInjection project (red in picture) and choose run.



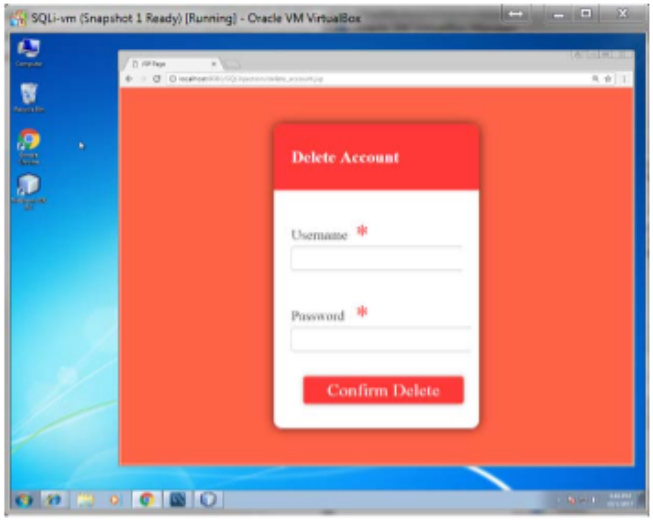
7. Navigate the web app. Once you hit 'run' you should be able to see the new virtual environment and the login screen of the web application.



You should be able to login using the following credentials: Username: **JohnConnor** Password: **skynet**. When you successfully login, you will be able to view a list of products, and you can add new products through the link add a new product.



You can also delete an account from the database using click here to unregister, where you will be asked for your username and a password:



8. The view database status link at the main screen will show you the SQL tables in the database and their structures, understanding tables' structures is vital to launch sql attacks.
9. This website shows many variations to sql commands. (https://www.w3schools.com/sql/) You can observe some examples there.

Hacking the Website

1. Bypass the login screen. Without using a username and password, hack into the website login page using the appropriate script or command injection. Tip: login bypass in the blind sql injection attack discussed in the video (~5th minute).
2. Open a backdoor. Once a hacker is in, they immediately open a backdoor (a way that they can use later to log into the system without hacking it again, such as creating a new account). Therefore, in this task, you should create a new user account and keep it as a backdoor.
3. Take over all customer accounts in the website by setting all of their passwords to '123'. Once a backdoor is created, now you need to attack other customers and hijacking their accounts, set all of their passwords to one value so you can log into their accounts whenever you please.
4. Use XSS attack to run script on a user (victim) if they go to view products page. An XSS attack is like planting a trap, you plant it, and then you wait for a victim to step on it. So if you add a new product that has an XSS in its name, then when another customer logs in and views all products, he will be caught by your trap, or in other words, your script in the XSS will run on his machine. In this task, plant XSS in the product list by adding a new product that has a script in its name. Tip: some XSS attacks that target client browsers discussed in the video (~5:28th minute).
5. Wipe the products database. Sometimes, a hacker wants to destroy things rather than steal them (Denial of Service attacks). This could be done by wiping the database. In this task, you should delete all products. After successfully deleting all products, you should see an empty list of products when you log in. Tip: some sql injection attacks that target removing tables discussed in the video (~4th minute).
6. Wipe the users database. In this task, you should delete all user accounts. After successfully deleting all users, you should not be able to login using any account. Tip: some sql injection attacks that target removing tables discussed in the video (~4th minute).

Tips and Cautions

1. If you destroy the website before completing the tasks, then you can restore the entire website to its original status by using the restore link inside view database status on the main page.
2. The view database status is not a function that exists in real life scenario, but we added it so you can see the effects of your attacks there. So please do not use the accounts (usernames and passwords) there to execute any of your attacks. You can use either JohnConnor account or a backdoor account that you create as in Task 2.

Submission Instructions

For tasks 1-6 please take a screenshot of the attack effect on the website and provide the script that you used to hack into it (**6 scripts + screenshots**).