

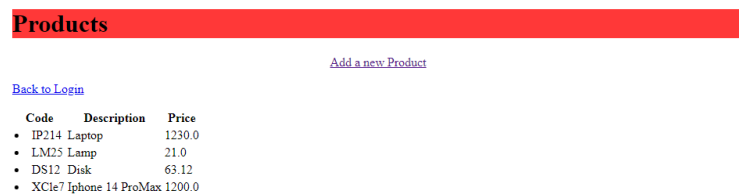
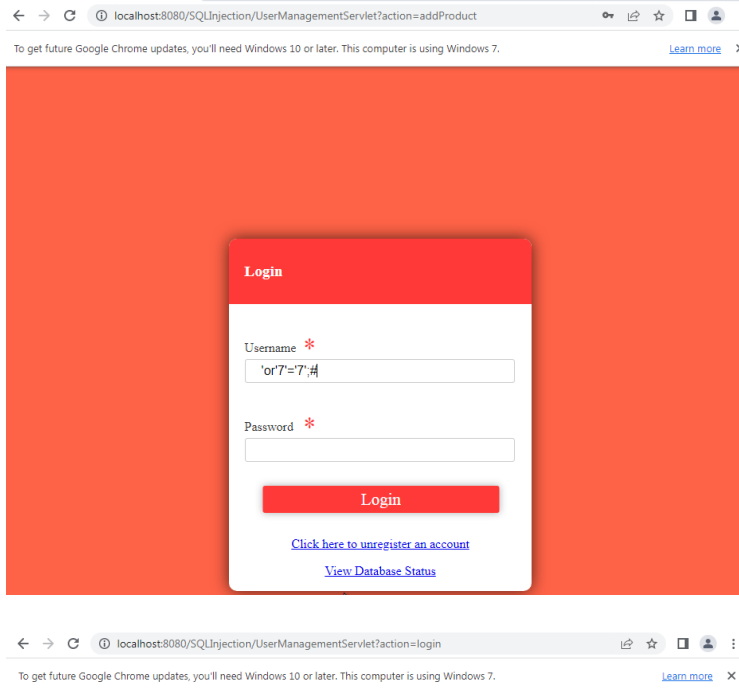
CYSE 450: Ethical Hacking and Penetration Testing

Lab 5: SQL Injection Attack

(1) **Bypass the login screen:** Without using a valid username and password, try to hack into the website login page using the appropriate script or command injection. Try the following script in the **Username** box and keep the **Password** box **empty**.

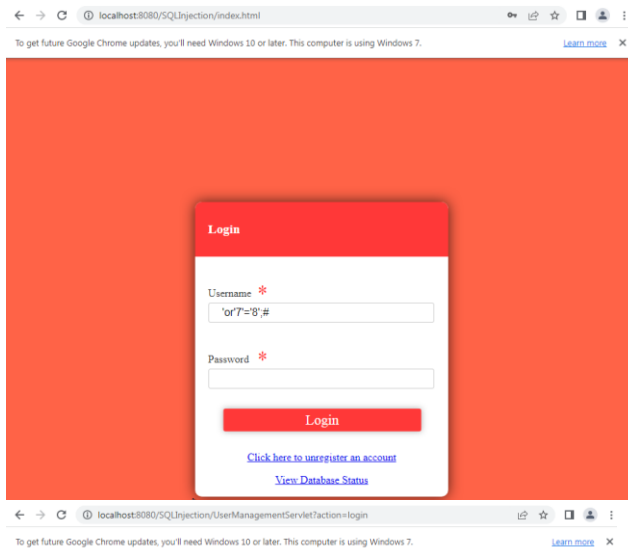
Username: `'or'7'='7';#`

Could you bypass the login hurdle and access the **Products** page? Please take a screenshot of the login page when you entered the script and a screenshot of the **Products** page after bypassing the login page. Include these two screenshots in your submission.



[4 points]

Now, try to replace the script in the **Username** box with `'or'7'='8';#` and try accessing the **Products** page. Did you find any difference here? Again, please take a screenshot of the login page when you entered the script and a screenshot of the **Products** page after bypassing the login page. Include these two screenshots in your submission. [4 points]



Membership Servlet

User does not exist
[Return to Index](#)

In your own words, explain the reasons behind the difference caused by the 2nd script. [2 points]

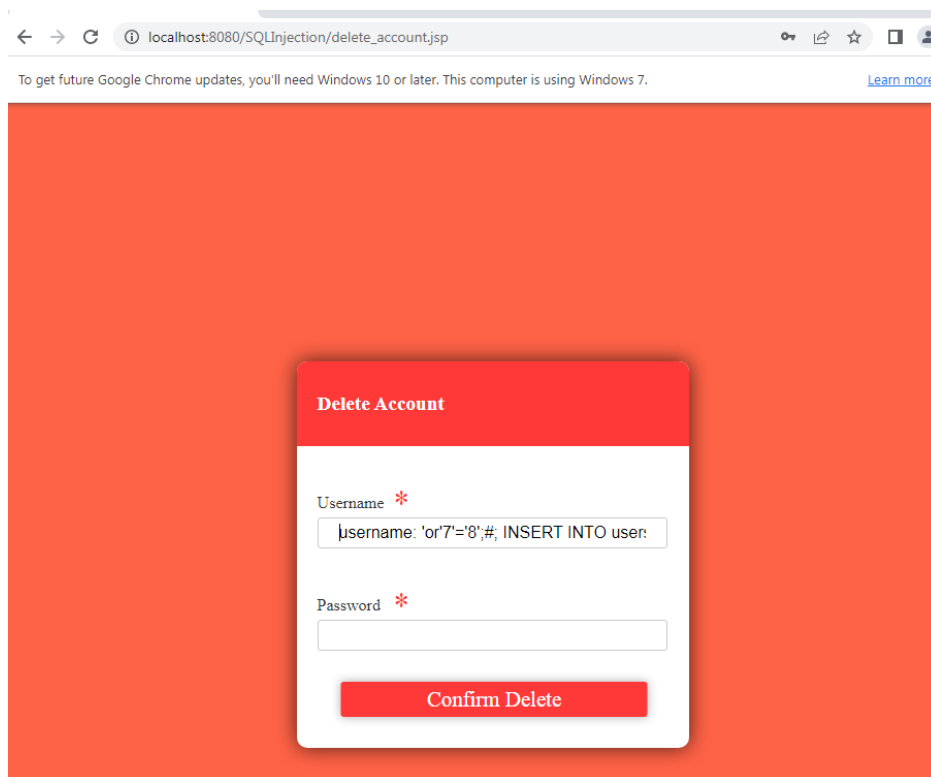
The first script worked because it used `'7'='7'`, which is always true, so the system let me log in without a real username or password. But when I tried the second script with `'7'='8'`, it didn't work because that's false. Since the condition wasn't true, the login failed. That's why only the first one let me bypass the login screen.

(2) Open a backdoor: Once hackers are in, they immediately open backdoors (a way that can be used later to log into the system without hacking it again, such as creating a new account). Let's create a new user account and keep it as a backdoor for the future.

From the **Login** page, click on the link **Click here to unregister an account**, and it will bring you to the **Delete Account** page. In this page, write the following script in the *Username* box and keep the *Password* box empty as usual.

```
Username: 'or'7'='8'; INSERT INTO users(id, firstName, lastName, email, password) VALUES(9, "your_first_name", "your_last_name", "your_email_address", "your_password"); #
```

Note that you should replace the fields **your_first_name**, **your_last_name**, **your_email_address**, and **your_password** with your actual first name, last name, email address and a custom password. **Take a screenshot of the *Delete Account* page with the given script written in the *Username* box and attach it into your submission.** [4 points]



Click on the **Confirm Delete** button and use the view **database status link** to view the *Products* page. **Take a screenshot of the *Products* page and highlight the newly added account information there.** [2 points]

Products

Code	Description	Price
• IP214 Laptop		1230.0
• LM25 Lamp		21.0
• DS12 Disk		63.12
• XCl7 iPhone 14 ProMax		1200.0

ID	firstName	lastName	email	password
• 1	John	Connor	JohnConnor	skynet
• 2	Sarah	Connor	SarahConnor	judgementday
• 3	Jon	Snow	JonSnow	defendthewall
• 4	Alan	Turing	AlanTuring	christopher
• 9	Zufan	Abebe	zabeb001@odu.edu	qweasd123

[Back to Login](#)

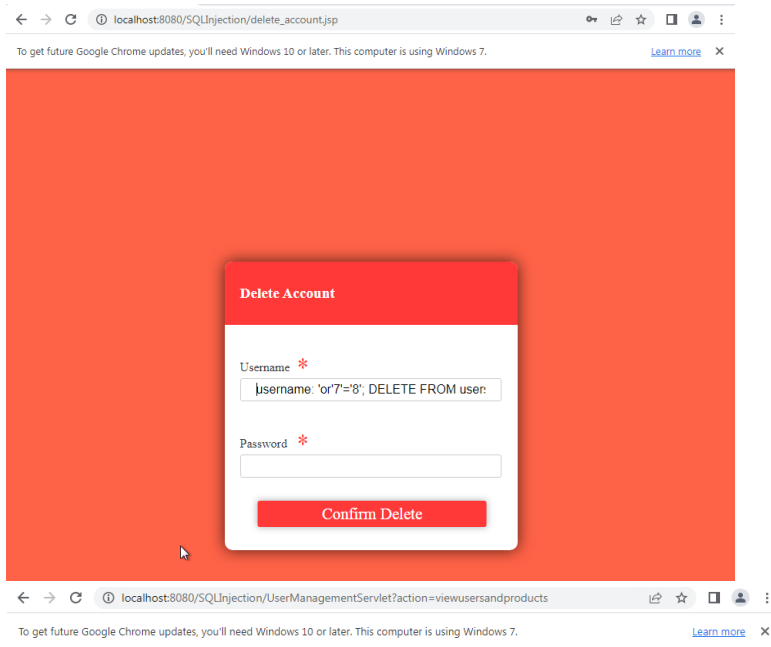
[Restore user and product Database to their original status](#)

Now, using the similar script, add another user with the first name **John** and last name **Smith**. Note that you cannot keep the *id*, *email*, and *password* fields empty. So, choose anything that comes to your mind. After adding the user John Smith, your next task is to remove the user with the **id = 9**.

To do that, from the **Login** page, click on the link **Click here to unregister an account**, and it will bring you to the **Delete Account** page. In this page, write the following script in the *Username* box and keep the *Password* box empty.

Username: 'or'7'='8'; DELETE FROM users WHERE id = 9; #

Take a screenshot of the *Delete Account* page with the given script written in the *Username* box. Take a screenshot of the **Products** page also after following the link *view database status*. Attach both screenshots into your submission. **[4 points]**

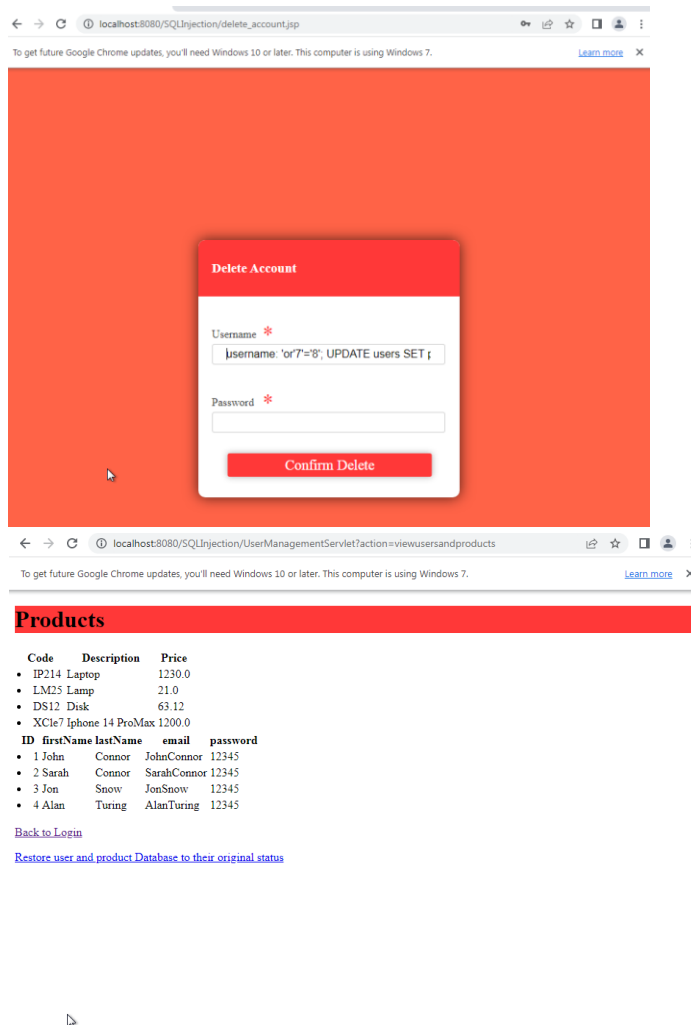


(3) **Take over all customer accounts in the website by setting all of their passwords to '123':** Once a backdoor is created, now you need to attack other customers and hijack their accounts, set all of their passwords to a single value so that you can log into their accounts whenever you please.

To do that, write the following script in the *Username* box in the **Delete Account** page and keep the *Password* box empty:

Username: 'or'7='8'; UPDATE users SET password = '12345'; #

Take a screenshot of the *Delete Account* page with the given script written in the *Username* box. Take a screenshot of the **Products** page also after following the link *view database status*. Attach both screenshots into your submission. [5 points]



Note that the password field for all the user accounts now should be updated into '12345'. Try logging in using a random username from the *Products* page with the password field set at '12345'.

(4) Use XSS attack to run script on a user (victim) if he goes 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 a XSS in its name, when another user logs in and views all products, he will be caught by your trap. In other words, your script in the XSS will run on

his machine. In this task, we will try to plant XSS in the product list by adding a new product that has a script in its name.

First, try logging in as the user John Connor. Now, if you try the password **skynet** for the username **JohnConnor**, you will see an error. That's because you already updated the password for all usernames into '12345' in the previous task. So, you should try logging in with the following credentials:

Username: JohnConnor

Password: 12345

Once you are logged in, try to add a new product following the link **Add a new product**. Use the following information to add the product:

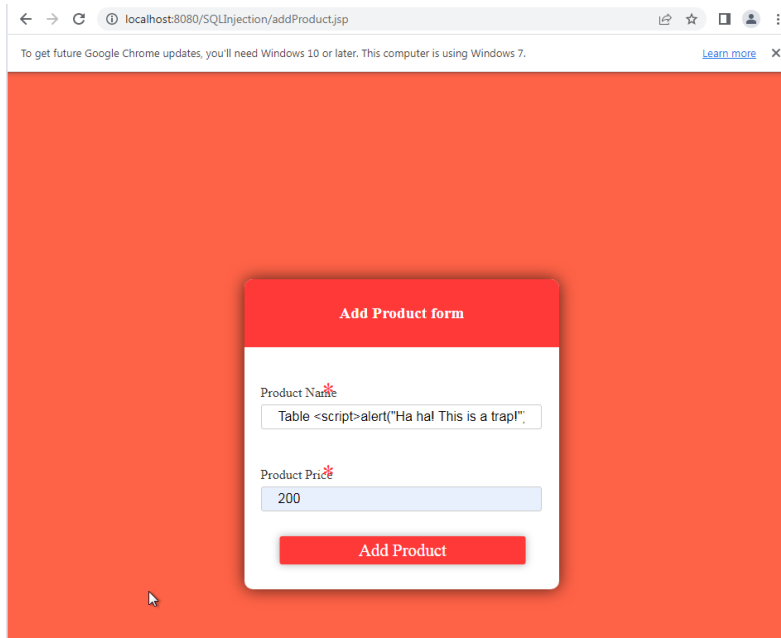
Product Name: Table <script>alert("Ha ha! This is a trap!")</script> **Product**

Price: 200

Take a screenshot of this page and click on the **Add Product** button to add the product. Now, try to login again as Alan Turing with the following credentials:

Username: AlanTuring

Password: 12345



Do you see a pop-up message saying "Ha ha! This is a trap!"? If yes, take a screenshot of the page showing the whole message and include it into your submission along with the previous screenshot. [5 points]

Product Management

localhost:8080/SqliInjection/UserManagementServlet?action=login

localhost:8080 says
Ha hai This is a trap!

OK

[Add a new Product](#)

Code	Description	Price
• IP214	Laptop	1230.0
• LM25	Lamp	21.0
• DS12	Disk	63.12
• XCle7	Iphone 14 ProMax	1200.0
• XCle8	Table	