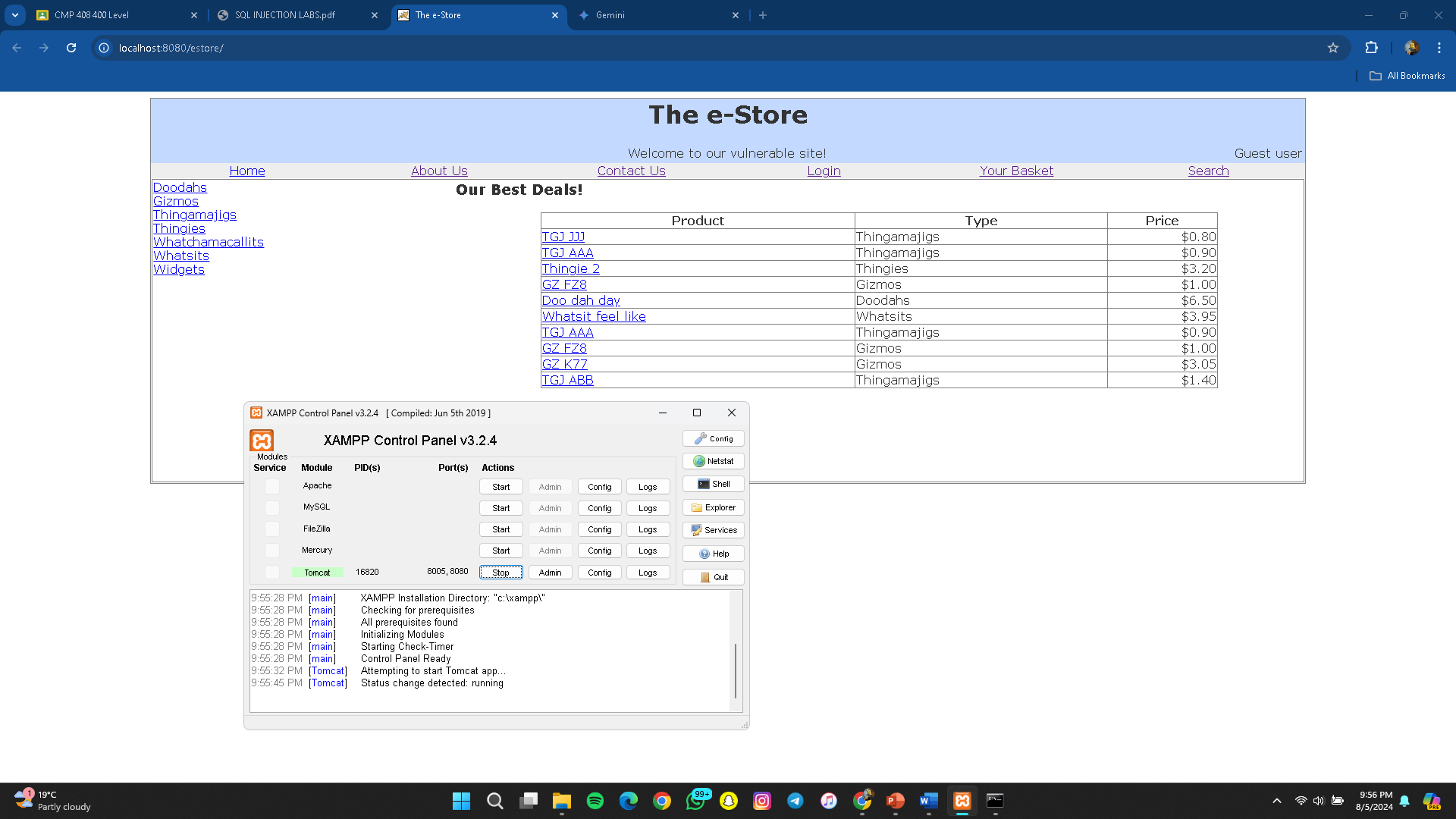
**CMP 408 INFORMATION SECURITY**

**SQL INJECTION LAB**

**IKEMKA ROMASON ROMANUS**

**BHU/20/04/05/0016**

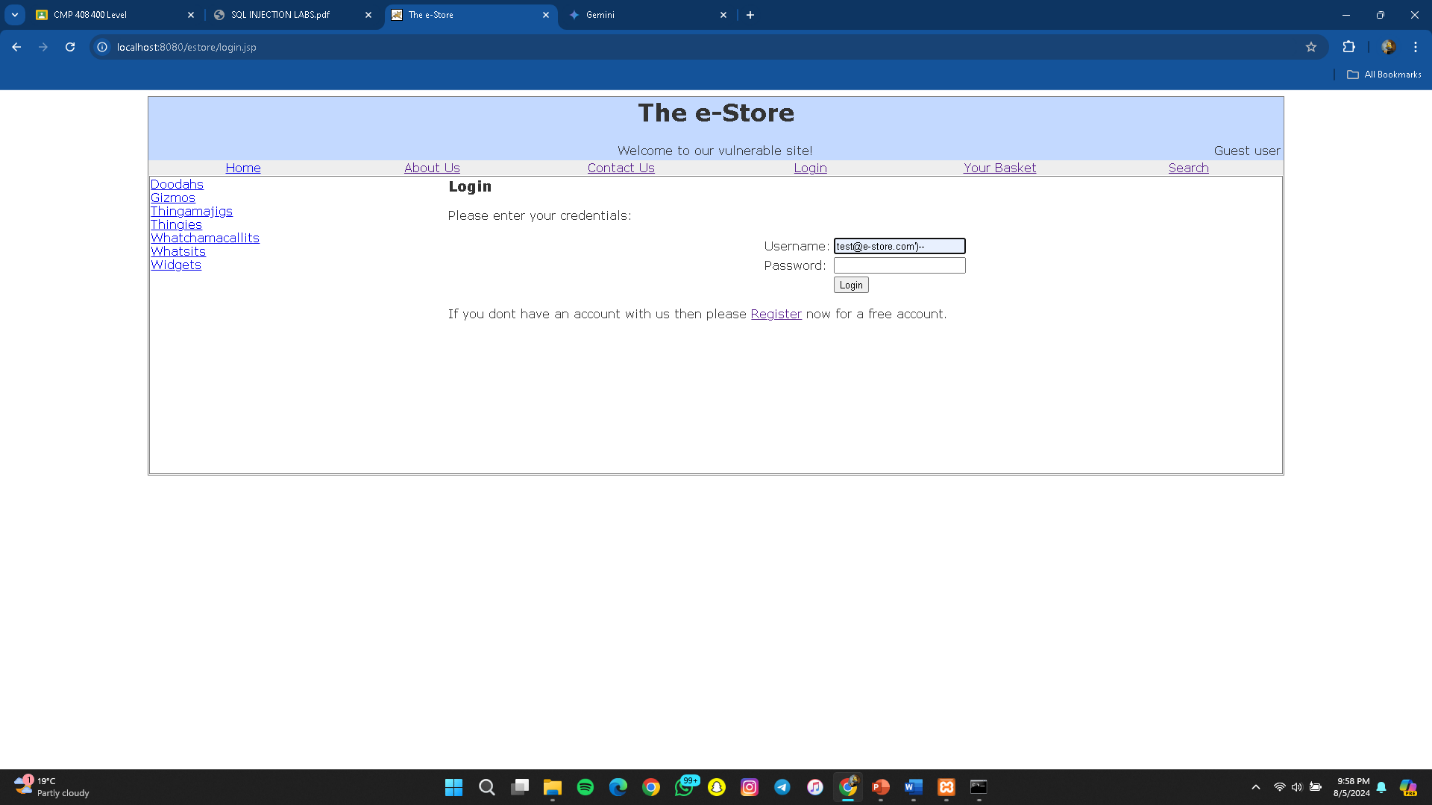
Set up and start the lab by installing XAMPP and starting TOMCAT.  
Access the e-Store through the URL: <http://localhost:8080/estore/>

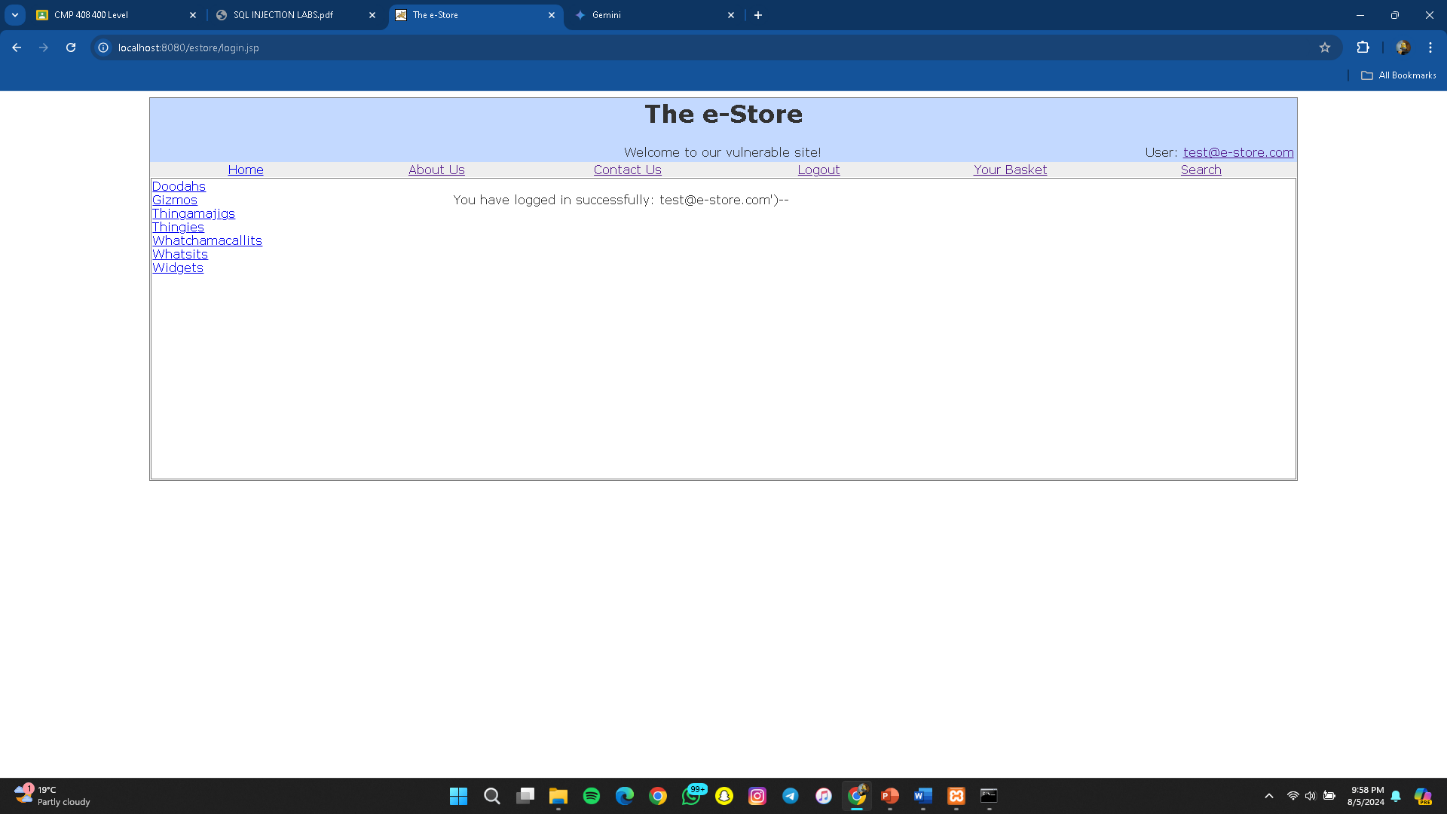


**Challenge 1**

Login as [test@e-store.com](mailto:test@e-store.com)

Using sqlInjection an unsanitized login input form can be exploited to access a user profile using only the provided username and an sql statement to manipulate the login form.



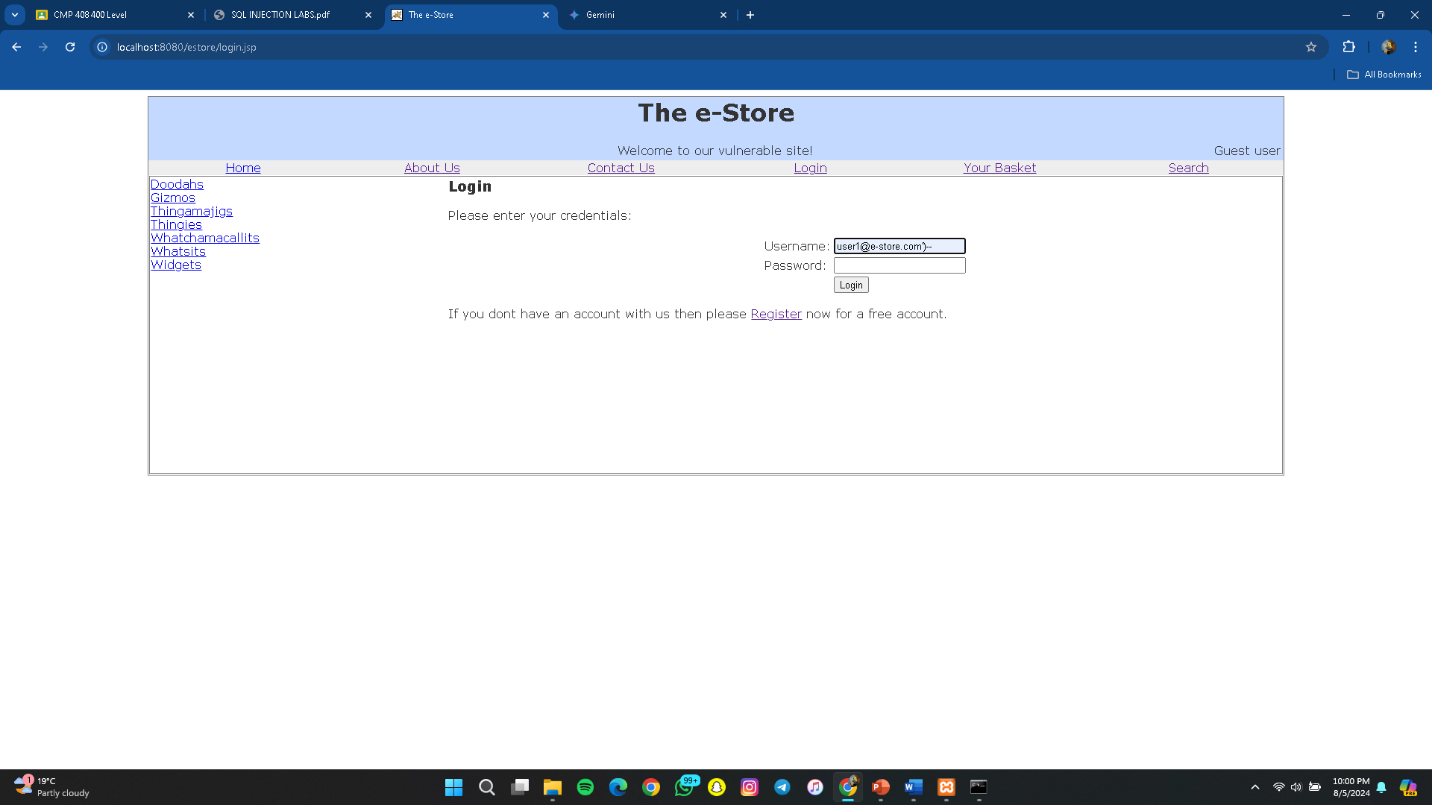


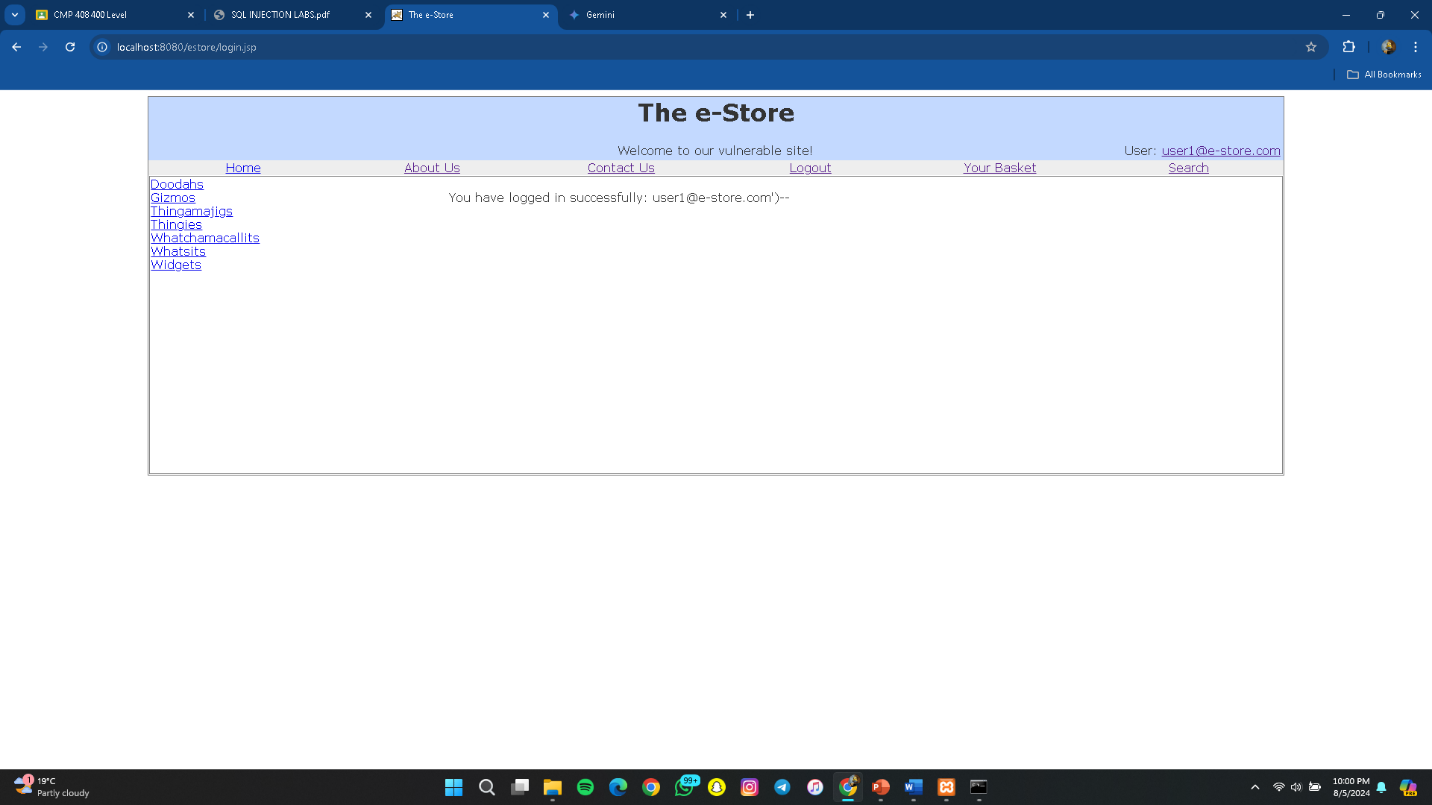
Using “ test@e-store’) – “ in the login username form affects the SQL code of the site and the – symbol is a comment tag in SQL and causes the database to log in without needing a password as long as a valid username is used.

**Challenge 2**

Login as user1[@e-store.com](mailto:test@e-store.com)

Using sqlInjection an unsanitized login input form can be exploited to access a user profile using only the provided username and an sql statement to manipulate the login form.



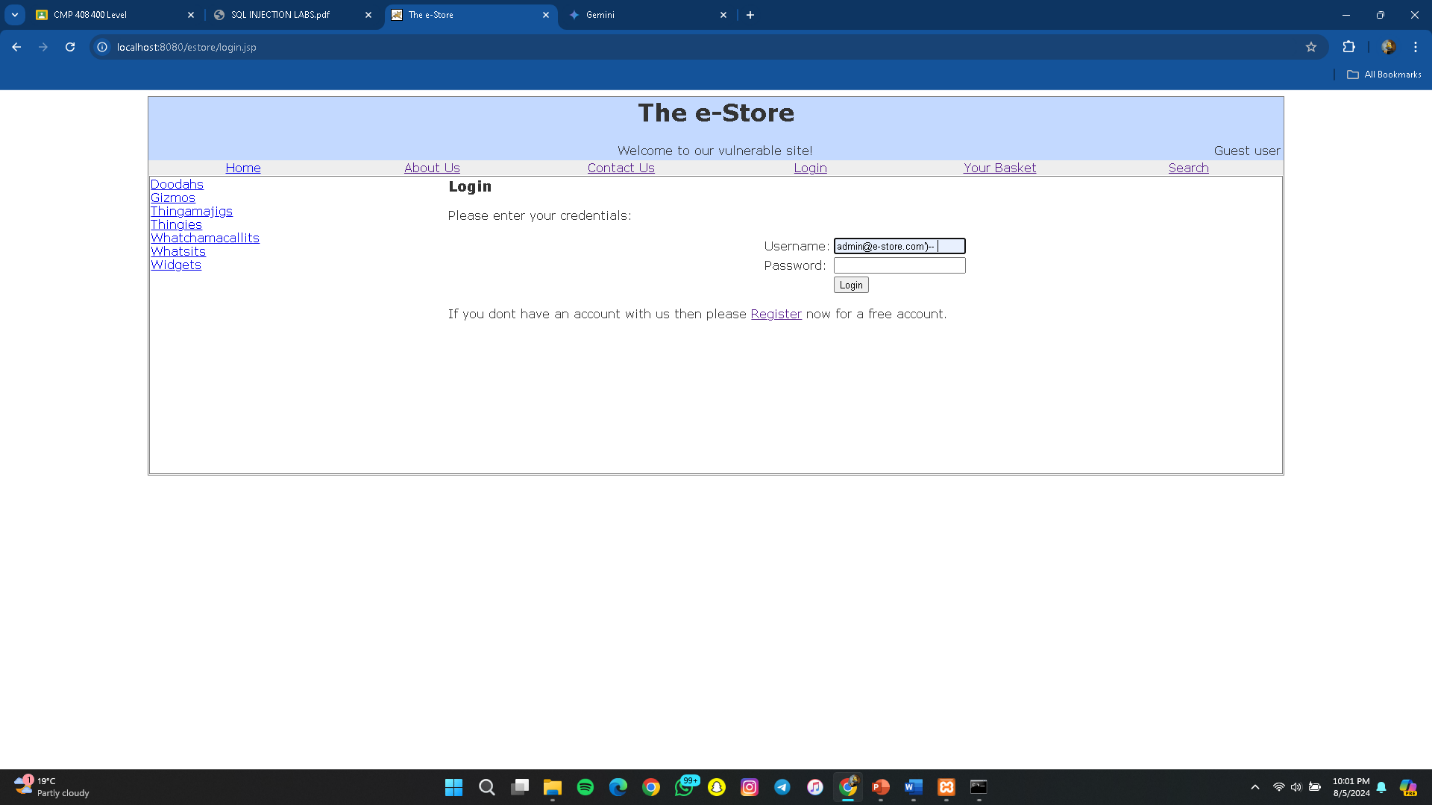


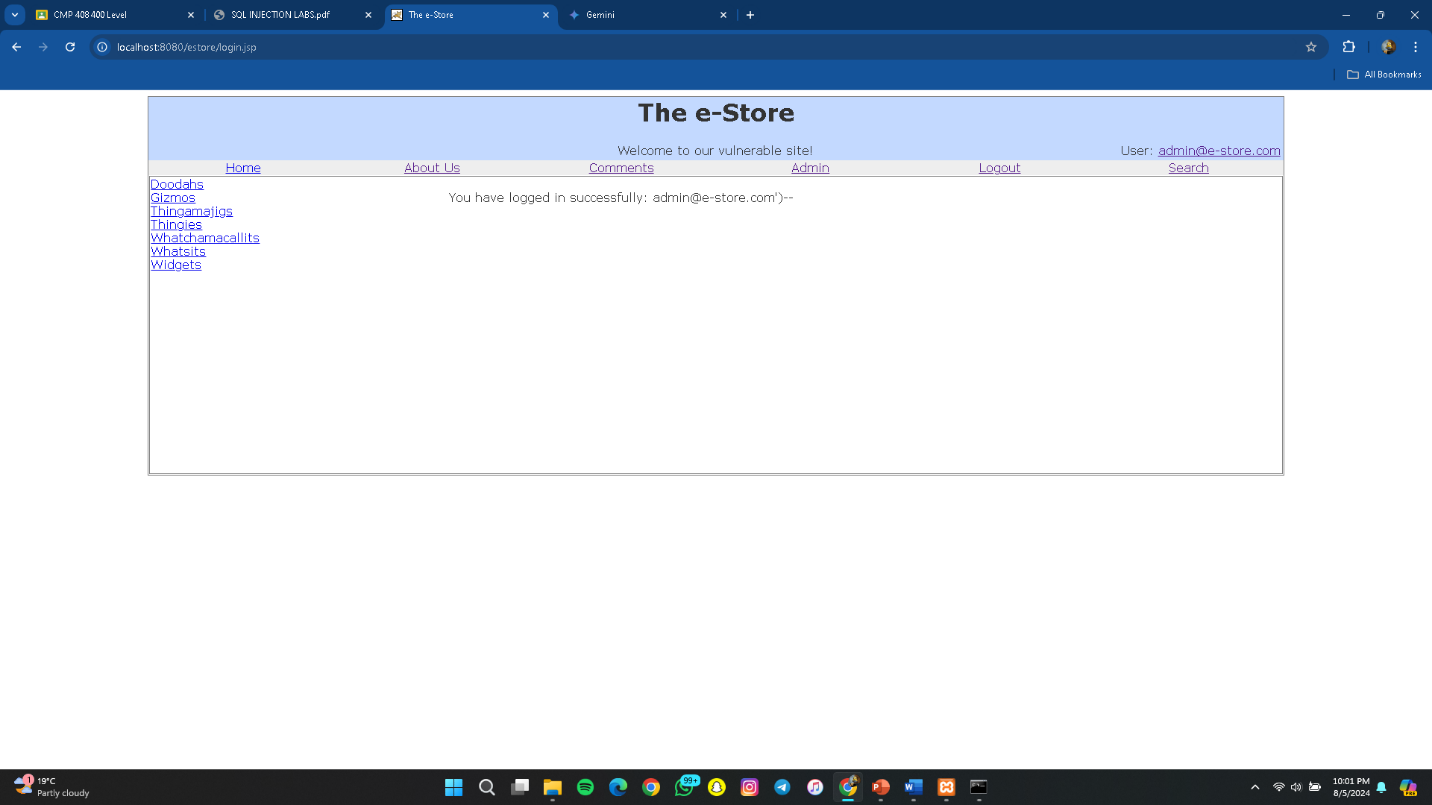
Using “ user1@e-store’) – “ in the login username form affects the SQL code of the site and the – symbol is a comment tag in SQL and causes the database to log in without needing a password as long as a valid username is used..

**Challenge 3**

Login as admin[@e-store.com](mailto:test@e-store.com)

Using sqlInjection an unsanitized login input form can be exploited to access a user profile using only the provided username and an sql statement to manipulate the login form.



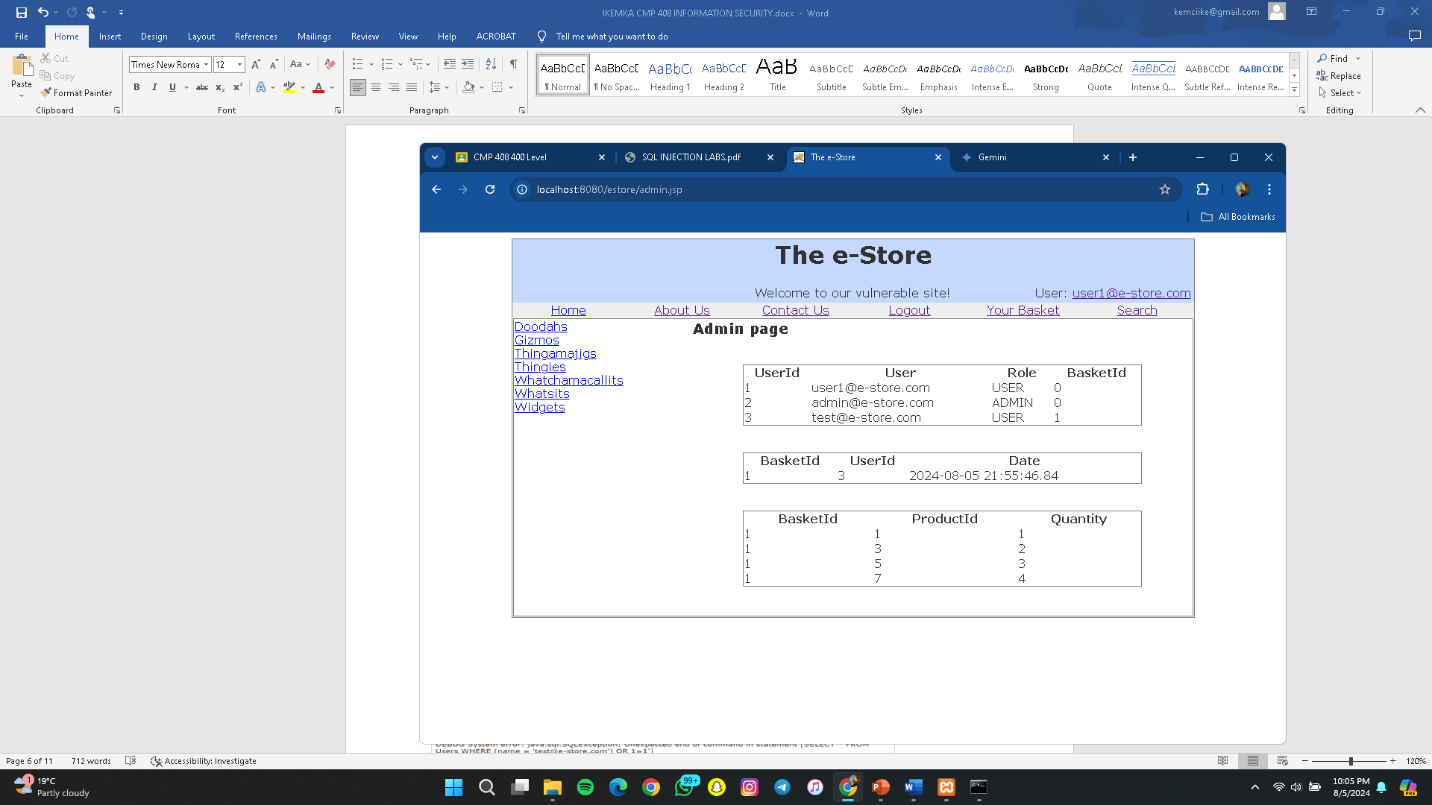


Using “ admin@e-store’) – “ in the login username form affects the SQL code of the site and the – symbol is a comment tag in SQL and causes the database to log in without needing a password as long as a valid username is used.

**Challenge 4**

Find hidden content as a non-admin user

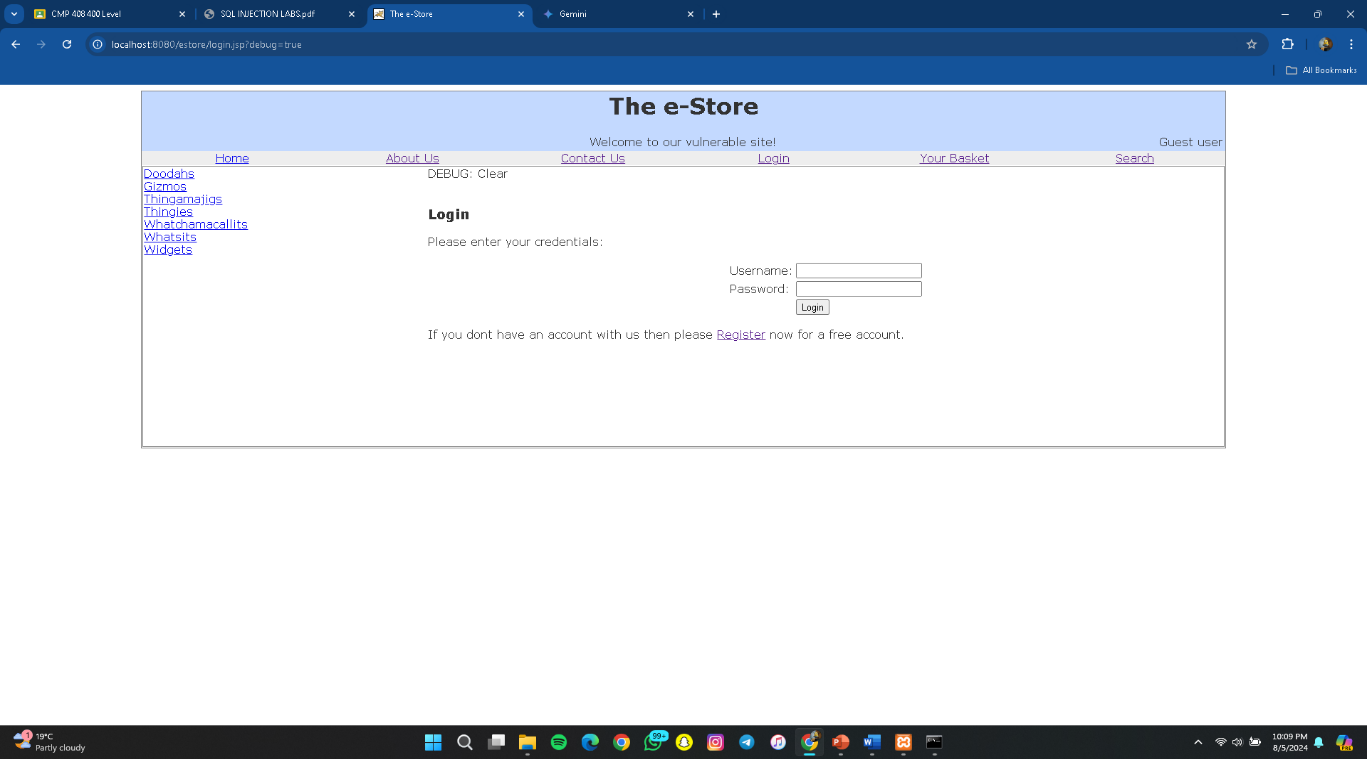
When logged in as a non-admin user the hyperlink to the admin panel is not available. To access the admin panel as a non admin user navigates to the admin panel using the browser URL tab and go to the URL of localhost8080/[estore.com/admin.jsp](http://estore.com/admin.jsp)



**Challenge 5**

Find diagnostic data

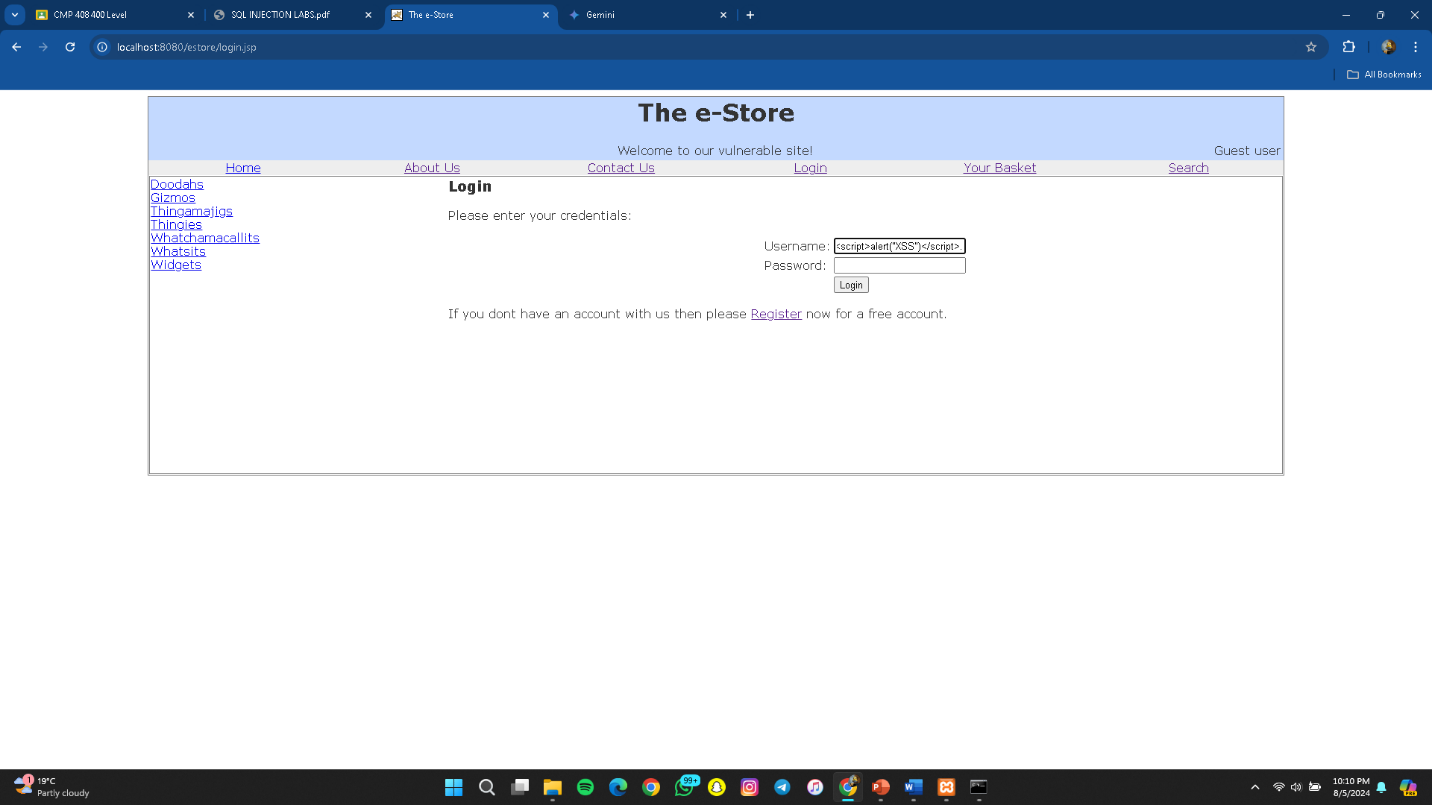
Diagnostic data can be found by adding the parameter ?debug=true to the URL as hinted in the lab guide.

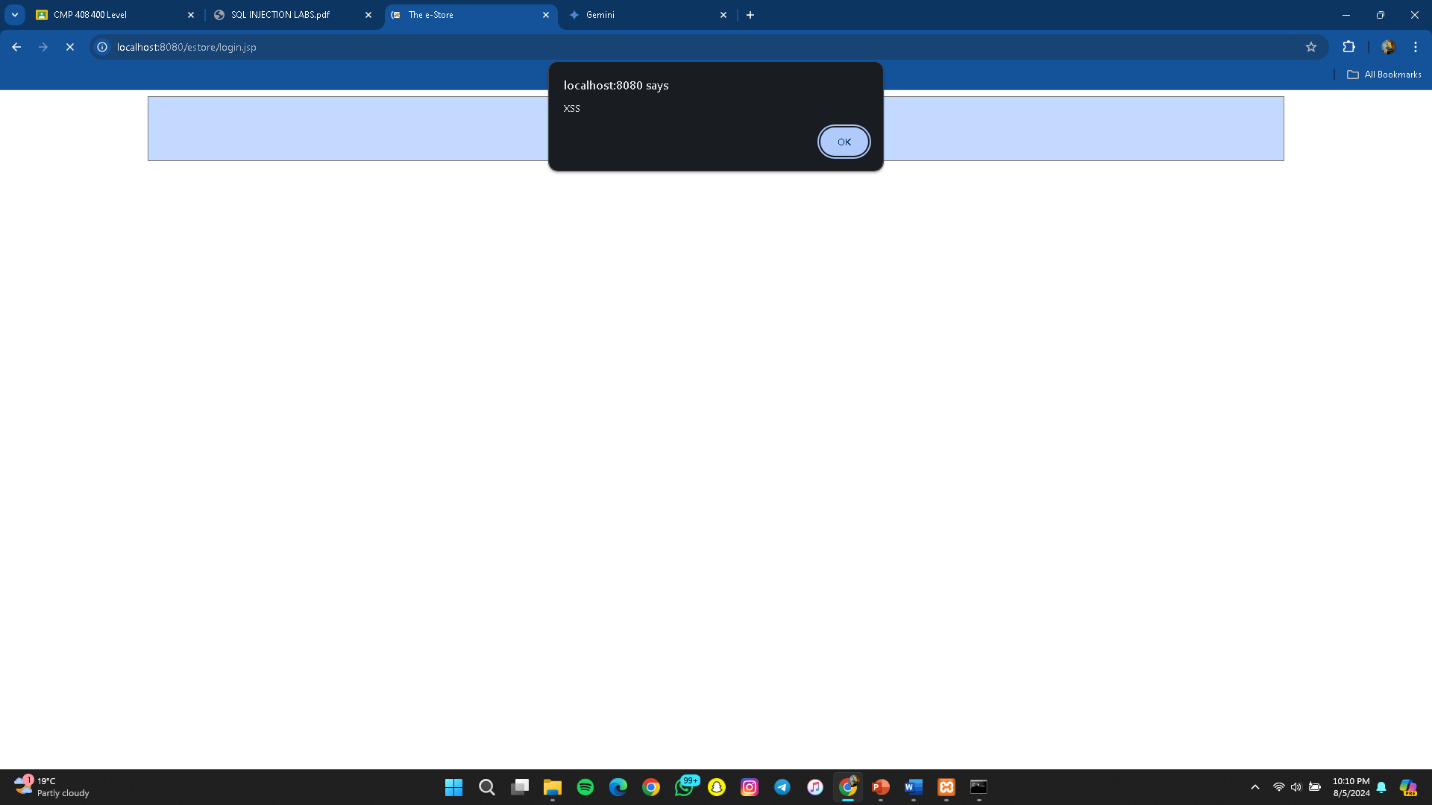


**Challenge 6**

Self XSS using <script>alert(“XSS”)</script>

A script can be input into an input box such as the search bar and the script is successfully executed in the browser as long as the website has no xss protection.  
The script alert(“XSS”) triggers the website to send an alert in the browser with the string XSS



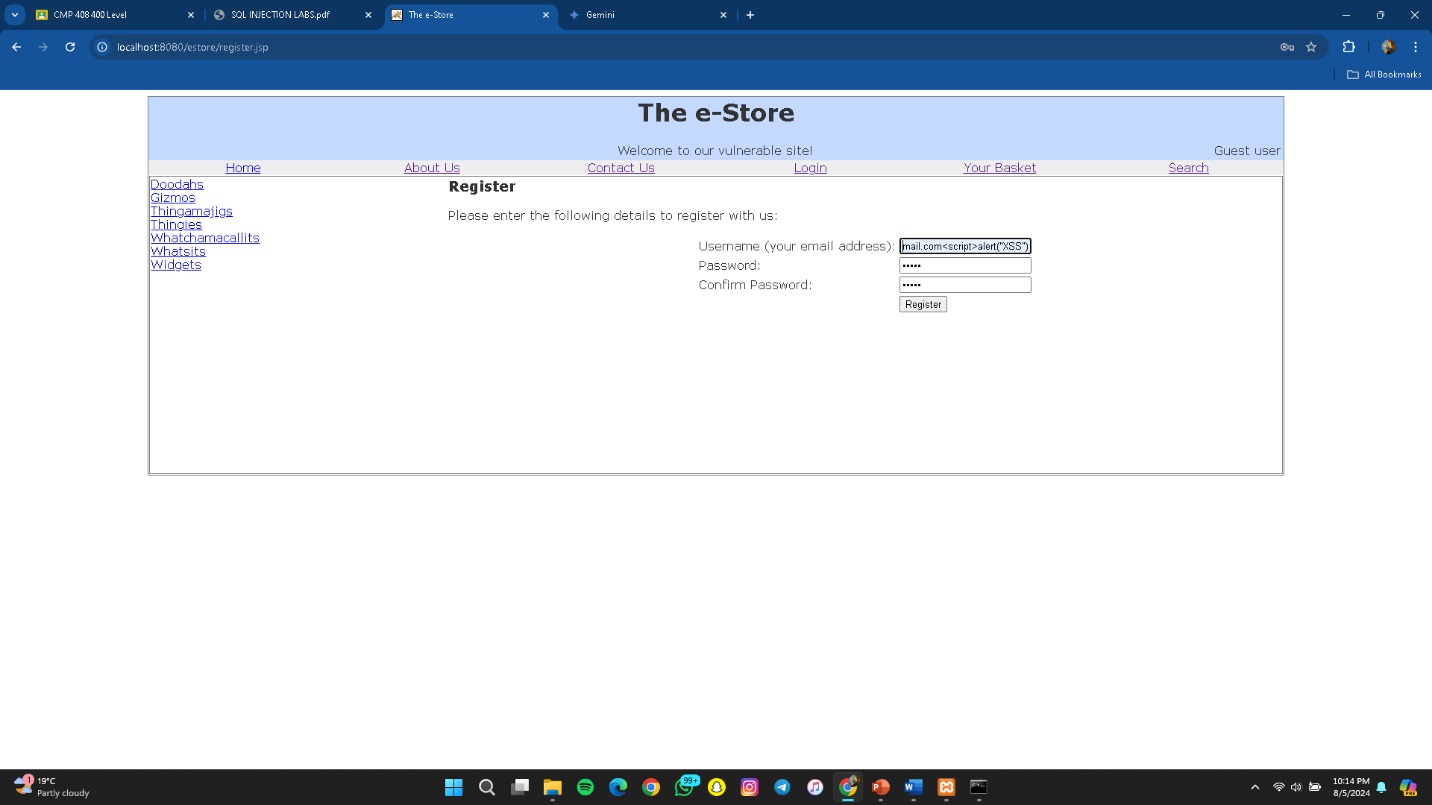


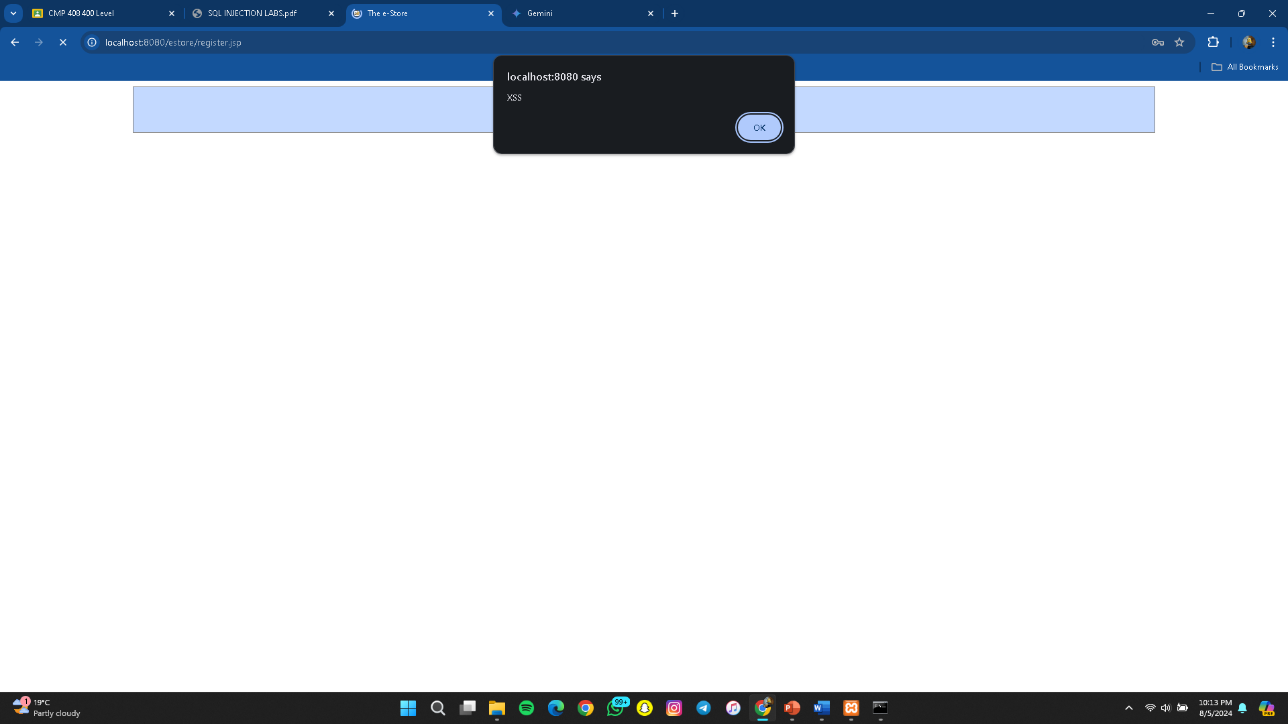
**Challenge 7**

Reflected XSS using <script>alert(“XSS”)</script>

A script can be input into an input box such as the search bar and the script is successfully executed in the browser as long as the website has no xss protection.  
The script alert(“XSS”) triggers the website to send an alert in the browser with the string XSS

The xss is a reflected xss when the malicious script affects the server.   
We can do this by using the registration form which sends input into the server when registering a new user.

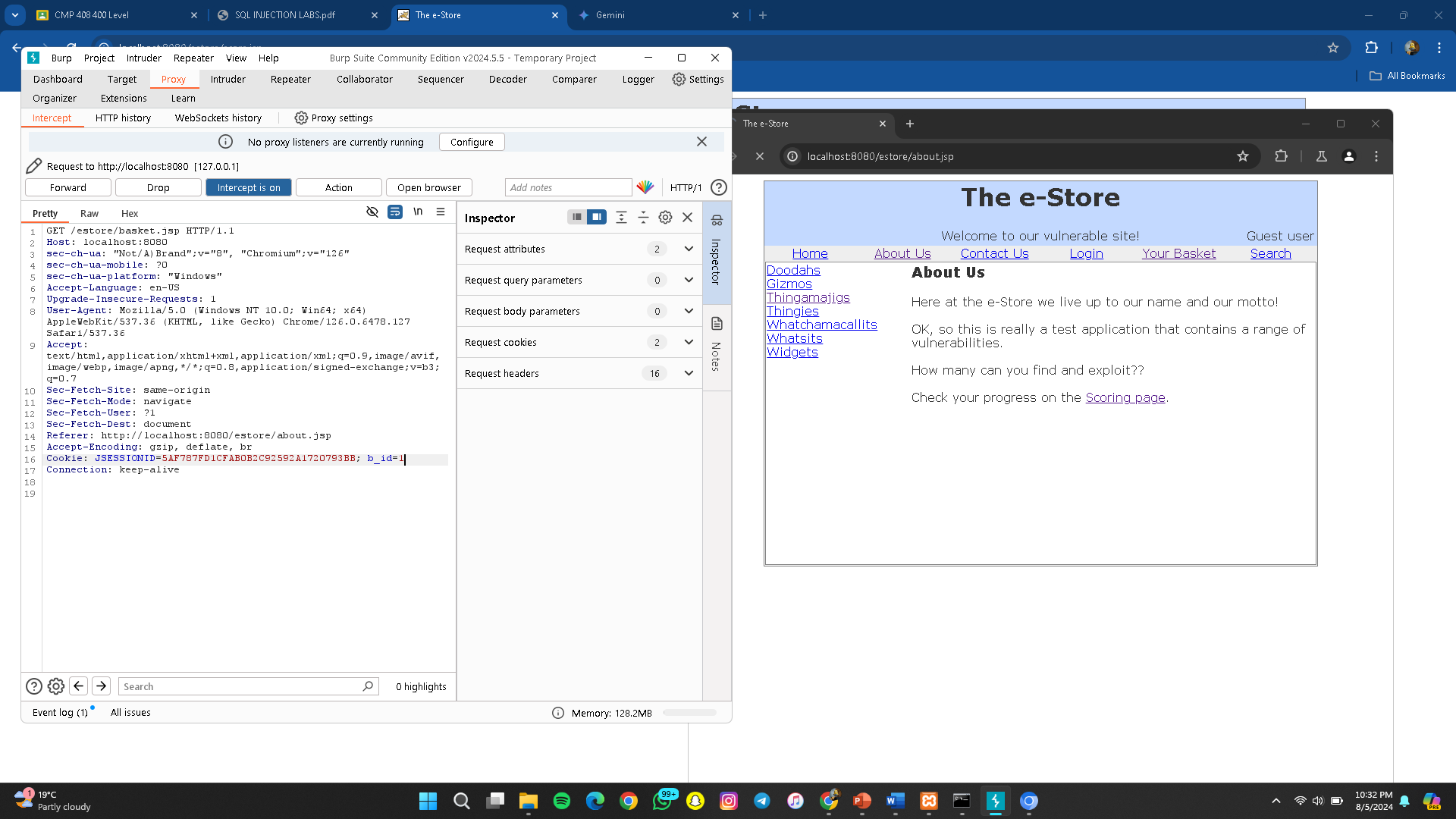




**Challenge 8**

Access someone else’s basket

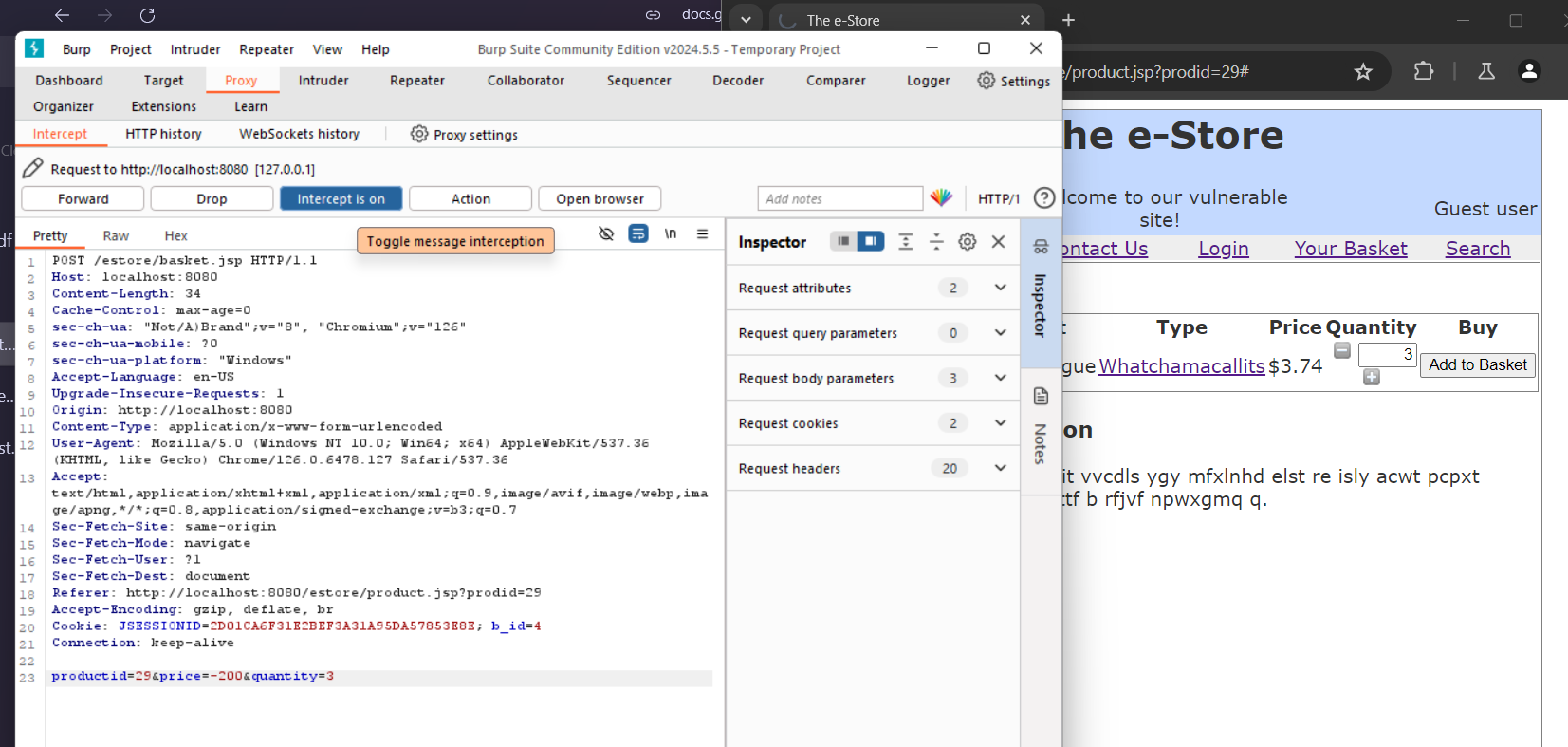
Making use of the intercept feature in burp suite’s proxy tab to intercept a request to get to a guest user basket. Modifying the cookies parameter to access a different b\_id leads to the website responding with a different user’s basket



The original request had a b\_id of 4 forwarding this leads to the user’s basket  
After changing the b\_id to 2 a different users basket page was gotten

**Challenge 9**

Get the store to owe you money

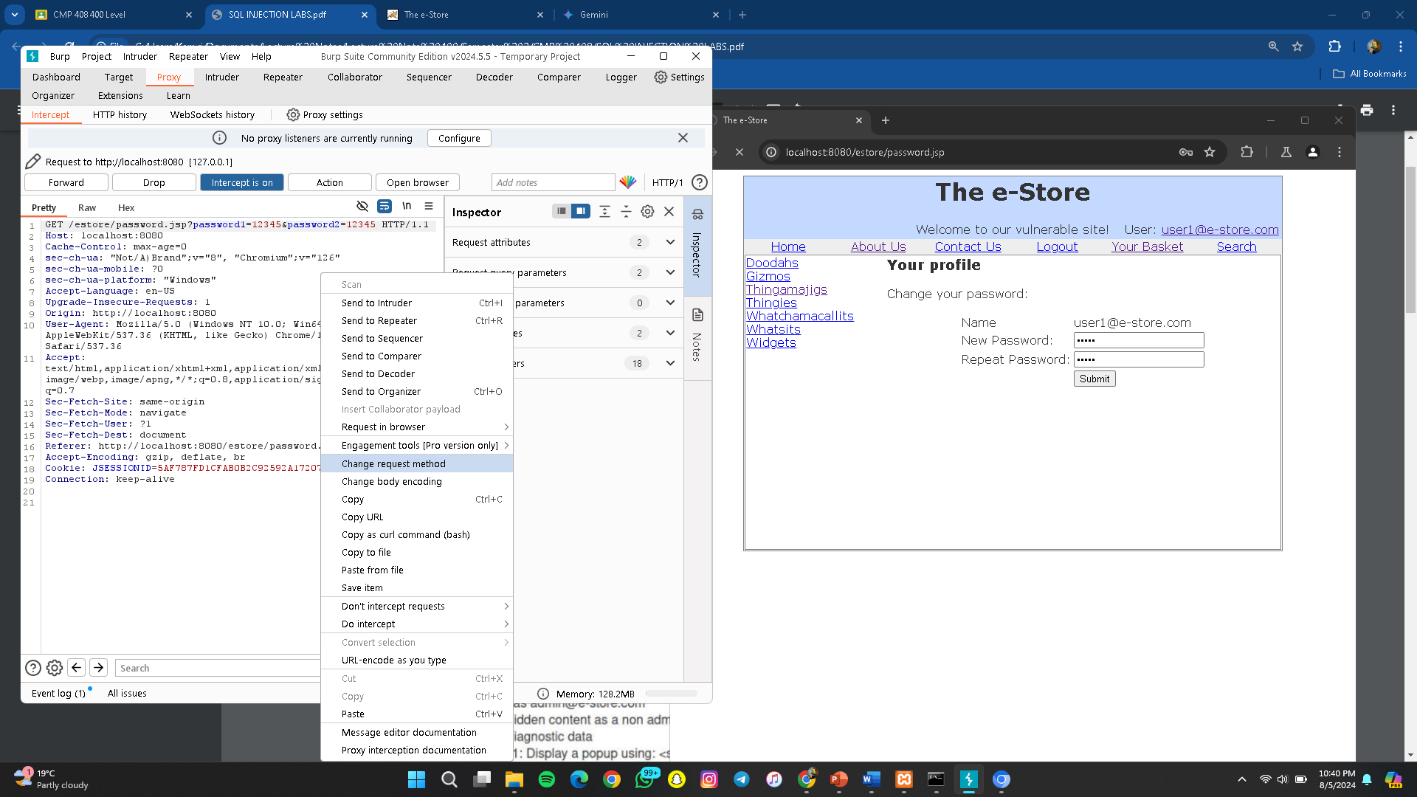
This is done by intercepting a purchase request to the server using burpsuite and modifying the request to cost a negative amount of money  


The original price of $3.74 has been changed to -200 in the proxy tab  
Forwarding this request to the server will cause the server to charge the user a negative amount and technically owe the user

**Challenge 10**

Change your password via a GET request

This can be done by using burpsuite to interrupt a a request to change the user’s pass word from localhost:8080/[estore.com/password.jsp](http://estore.com/password.jsp)



By interrupting the request and changing the request method we can change the user’s password using a GET request

**Challenge 11**

Conquer AES encryption, and display a popup using <script/>alert(“H@cked A3S“)</script/>

This can be done by intercepting a request to the site that makes use of AES encryption to validate queries and manipulation the response html

