SQL INJECTION LABS

Install and open the XAMPP Control Panel and start the Tomcat service. Access the e-Store through the URL: http://localhost:8080/estore/

Because Tomcat uses port 8080, you may want to set the port for Burp to some other value, for example 8082. Consequently, to use Burp alongside your browser, your browser's proxy should be set to use 127.0.0.1 with port 8082.

You do not need to start Apache and MySQL in this coursework.

Note: you can work on this coursework using your own laptop (provided you have xampp installed). Simply download the estore.zip file from Moodle and unzip it under c:\xampp\tomcat\webapps

The website has a score board that contains a list of 12 challenges. The score board can be accessed by browsing to the "About Us" page then clicking on the "Scoring Page" link or by directly accessing: http://localhost:8080/estore/score.jsp

Challenges will be shown as green once solved as shown below:

Challenge	Done?
Login as test@e-store.com	
Login as user1@e-store.com	
Login as admin@e-store.com	
Find hidden content as a non admin user	
Find diagnostic data	
Level 1: Display a popup using: <script>alert("XSS")</script>.	
Level 2: Display a popup using: <script>alert("XSS")</script>	
Access someone elses basket	
Get the store to owe you money	
Change your password via a GET request	
Conquer AES encryption, and display a popup using: <script>alert("H@cked A3S")</script>	
Conquer AES encryption and append a list of table names to the normal results.	

Note: When you stop the Tomcat service and access the e-Store again, the score board will be reset and will show red against all challenges. This is normal and is nothing to worry about as you do not need to provide a screenshot of the score board with all the challenges solved in one go.

You do not need to attempt the challenges in the order specified in the score board. And, you do not need to solve challenge 2 (login as user1) nor challenge 3 (login as admin) because they are similar to challenge 1.

Also, I will provide you with the solution to challenge 5 (Find diagnostic data) because it will help you with other challenges. The e-Store uses a parameter called debug to display error messages. For example, visiting the following page will solve challenge 5: http://localhost:8080/estore/login.jsp?debug=true

To complete the 9 remaining challenges, you mainly need a browser, the browser's web development tools, and Burp Suite. But feel free to use any other tool you deem appropriate (including those in the Kali VM).

To help you with this, here are hints for each of the challenges:

Challenge	Hint
Challenge 1: Login as test…	SQL-injection. Your injected code needs to terminate the closing bracket shown in the error code. Remember to add the ?debug=true to the URL.
Challenge 4: Find hidden content	View Page Source
Challenge 6: Level 1 XSS	Reflective XSS.
Challenge 7: Level 2 XSS	Stored XSS.
Challenge 8: Access someone…	Cookie.
Challenge 9: Get the store…	Time for a bit of shopping and some simple arithmetic.
Challenge 10: Change your password…	From POST to GET.
Challenge 11: Conquer AES encryption, and display a popup	Inject script in the "Type" input box of "Advance Search". The form has a validate Form JavaScript function that calls another function encrypt Form which replaces special characters with their URL encoding. Try to bypass it.
Challenge 12: Conquer AES encryption and append a list of the table names	Combine the bypassing of validation from the previous challenge with SQL injection. Remember to use ?debug=true to get the website to display errors.