## OWASP 07 – Cross-site scripting

### Walkthrough – Shopping App

1. The application does not sanitize user input to escape from XSS input
2. Create a new account and give it the username of <body onload=alert("1")>;
3. When you log in to this account and it displays reach a menu that displays the username of the account it will trigger alert with the value of 1
4. From there figure out which inputs can trigger alerts and what cannot
   1. For this application its possible to trigger a XSS alert from the username, first name, last name, and address because they are shown on the view profile page

### Exercises – Shopping App

The application uses EJS which has the ability when writing the code to use methods to automatically escape cross-site scripting attacks

1. Modify the shopping app to escape XSS input
2. Optional: create a function that takes the input values and filters out potential cross-site scripting characters