## OWASP 07 – Cross-site scripting

### Walkthrough – Bank App

1. The application does not sanitize user input to escape from XSS input
2. Create a new account and give it the First name of <script>alert(1)</script>
3. When you log in to this account and it displays reach a menu that displays the first name of the account it will trigger alert with the value of 1
   1. If you try and put the alert into the username, last name, or address section instead, it will not trigger any alerts unless we can get to the admin page



### Exercises – Bank 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 Bank app to escape XSS input
2. Optional: create a function that takes the input values and filters out potential cross-site scripting characters