SIT 218/738: Secure coding

**Pass task 4.1P: Injection attack preventions using hibernate validator**

**Overview**

In 05-coachwebapp-spring web app we implemented the regex pattern to prevent users from entering the scripts or tagged input values in the format ‘<>’. This prevented many of the XSS attack input patterns. Even though sometimes these filters can be bypassed using more clever inputs that do not get caught in the filters like try to enter the below value in the name field.

1. name "<script>alert("XSS"); </script>"
2. <a aa aaa aaaa aaaaa aaaaaa aaaaaaa aaaaaaaa aaaaaaaaa aaaaaaaaaa href=j&#97v&#97script:&#97lert(1)>ClickMe
3. <script x> alert(1) </script 1=2

Discuss why these are getting bypassed.

Correct the regex expression that can block these patterns as well.

Now add two fields to the web app that asks user to enter their email address and a text area that allows users to send a custom request to the coach. Add the correct input validations to prevent any XSS both at the client level and at server level. The email address should contain appropriate characters such as ‘@’ and ‘.com’. The text area should contain only maximum 200 characters.

Use this <https://www.geeksforgeeks.org/spring-mvc-textarea/> as reference for adding the textarea to the spring app. Use this for client side html validations <https://developer.mozilla.org/en-US/docs/Learn/Forms/Form_validation>

**Submission Requirements:**

Submit one PDF file containing the following information:

1. The correct regex pattern that blocks these injected data in all the fields
2. Screenshot of the updated app
3. Updated Client.java code added to the submission document.
4. Updated CoachController.java code added to the submission.
5. Updated HTML pages added to the submission document.

**Submission Due**

The due for each task has been stated via its OnTrack task information dashboard.