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.

**Submission Requirements:**

Submit one PDF file containing the following information:

1. Screenshots showing the bypassing the of the filter for the three cases
2. A paragraph discussing why these are still getting bypassed.