In [ ]:

```
Training Day 8 Report– 30 June 2025
 Introduction
 Day 8 addressed Cross-Site Scripting (XSS), an attack that injects client-sid
 web pages viewed by other users, potentially enabling session hijacking, defa
 credential theft.
 Key Concepts Discussed
 We discussed stored, reflected, and DOM-based XSS, emphasizing how different
 points and output contexts change payloads and mitigation strategies. The imp
 of output encoding and content security policies was explained.
 Lab Preparation in Theory
 Safe techniques for discovering XSS were outlined, including how to model inp
 output flows and how to test without causing harm to user data or services.
 Practical Understanding (Theory)
 Thetrainer emphasized developer-side mitigations such as contextual encoding
works that auto-escape output. We also discussed the role of secure cookie att
 same-site policies in reducing browser-based attack impact.
 Key Takeaways
 XSS exploits client trust and thus requires both server-side and client-side
 Awareness and secure frameworks reduce exposure.
 Conclusion
 Following XSS, we will explore Cross-Site Request Forgery and other request-b
tacks.
```