```
In [ ]: Training Day 9 Report– 1 July 2025
         Introduction
         Day 9 focused on Cross-Site Request Forgery (CSRF), where an attacker tricks
         browser into performing unintended actions on a site where the victim is auth
         Key Concepts Discussed
         Weexplained the mechanics of CSRF, why state-changing HTTP requests are vulne
         and how anti-CSRF tokens, SameSite cookie attributes, and referer checks help
         the risk.
         Lab Preparation in Theory
         The safe plan included designing proof-of-concept pages in an isolated enviro
         understand token validation flows without interacting with production systems
         Practical Understanding (Theory)
         We discussed server-side validation strategies and how to design APIs to be l
         to CSRF by avoiding cookie-based auth for unsafe actions or by enforcing expl
         use for state changes.
         Key Takeaways
         Preventative design and explicit server-side checks are essential. CSRF is mi
         effectively with correctly applied tokens and cookie attributes.
         Conclusion
         Next sessions will investigate insecure file handling and inclusion issues th
         to remote code access.
```