```
In [ ]: Training Day 6 Report– 28 June 2025
         Introduction
         Day 6 began the web application security module, focusing on common applicati
        nerabilities and how they arise from insecure coding practices, design flaws,
        f
         igurations.
         Key Concepts Discussed
         The trainer introduced the OWASP Top Ten as a practical taxonomy for common w
         risks. We discussed input validation failures, broken authentication, sensiti
        sure, and insecure deserialization as examples of why web applications frequen
         exploitable issues.
         Lab Preparation in Theory
         The class discussed deploying intentionally vulnerable web apps in an isolate
         practice detection and safe exploitation. Concepts of web proxies, intercepti
         and secure logging were presented without performing live attacks.
         Practical Understanding (Theory)
         We emphasized understanding how web requests map to server-side logic and how
        controlled input can affect database queries, file handling, or control flow.
         of secure development practices to prevent such vulnerabilities was highlight
         Key Takeaways
         Adeveloper-centric view helps identify root causes. Reviewing OWASP categorie
         testing and remediation discussions effectively.
         Conclusion
         Following this overview, subsequent days will explore specific web vulnerabil
         injection and XSS in more depth.
```