```
In [ ]: Training Day 7 Report– 29 June 2025
         Introduction
         Day 7 concentrated on SQL Injection (SQLi) – one of the most severe classes c
         vulnerabilities that allow attackers to manipulate backend database queries.
         Key Concepts Discussed
         We learned about different SQLi types: error-based, union-based, and blind SQ
         discussion included how unsanitized input can alter SQL statements and the ri
        ciated with exposing database contents, authentication bypass, or altering dat
         Lab Preparation in Theory
         The class planned a safe exercise framework to identify SQLi vectors, emphasi
        destructive testing. Techniques to validate vulnerabilities without data loss
        scribed conceptually.
         Practical Understanding (Theory)
         We discussed defensive coding practices including parameterized queries, stor
        dures, and least-privilege database accounts. The role of input validation anc
         encoding in mitigating SQLi was explained.
         Key Takeaways
         SQLi remains prevalent where input is trusted. Developers and testers must ap
         defenses to prevent successful exploitation.
         Conclusion
         The next lessons will extend to client-side attacks like XSS that affect brow
```