TryHackMe | SQL Injection Learning Path – Hands-On Experience

Recently, I completed the SQL Injection (SQLi) machine on TryHackMe, which provided a practical and in-depth understanding of one of the most critical web application vulnerabilities.

What I worked on:-

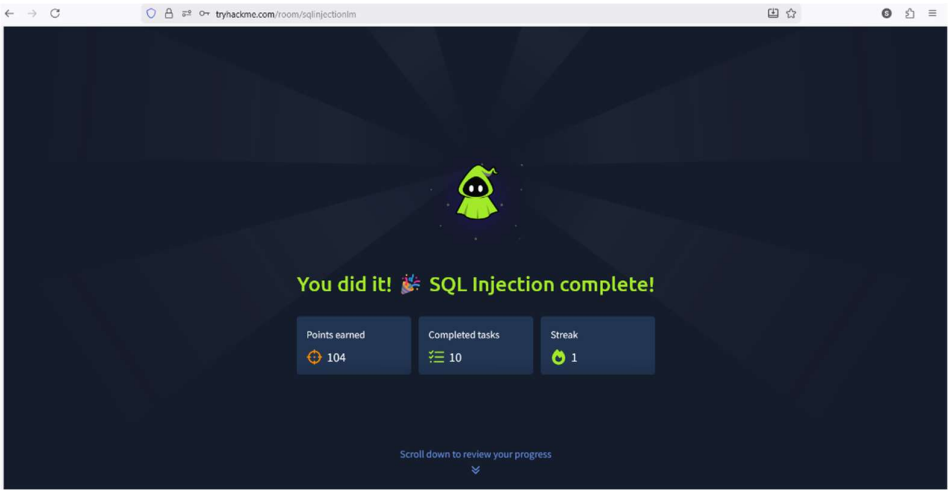
1) Understanding how SQL Injection vulnerabilities occur due to improper input validation
2) Performing manual SQL injection techniques to identify vulnerable parameters
3) Extracting database information such as:-
Database names
Tables and columns
Sensitive records
4) Learning how attackers bypass authentication mechanisms using SQLi
5) Exploring error-based and union-based SQL injection methods
6) Gaining insight into real-world exploitation scenarios

Key Takeaways:-

1) Importance of secure coding practices and input validation
2) How SQL Injection ranks in the OWASP Top 10 and its real-world impact
3) Defensive measures such as:-
Prepared statements
Parameterized queries
Proper error handling

💡 This hands-on lab strengthened my understanding of offensive testing techniques and the defensive mindset required to secure modern web applications.

📌 Platform: TryHackMe
📚 Topic: Web Application Security – SQL Injection


tryhackme.com/room/sqlinjectionlm
You did it! SQL Injection complete!
Points earned
104
Completed tasks
10
Streak
1
Scroll down to review your progress