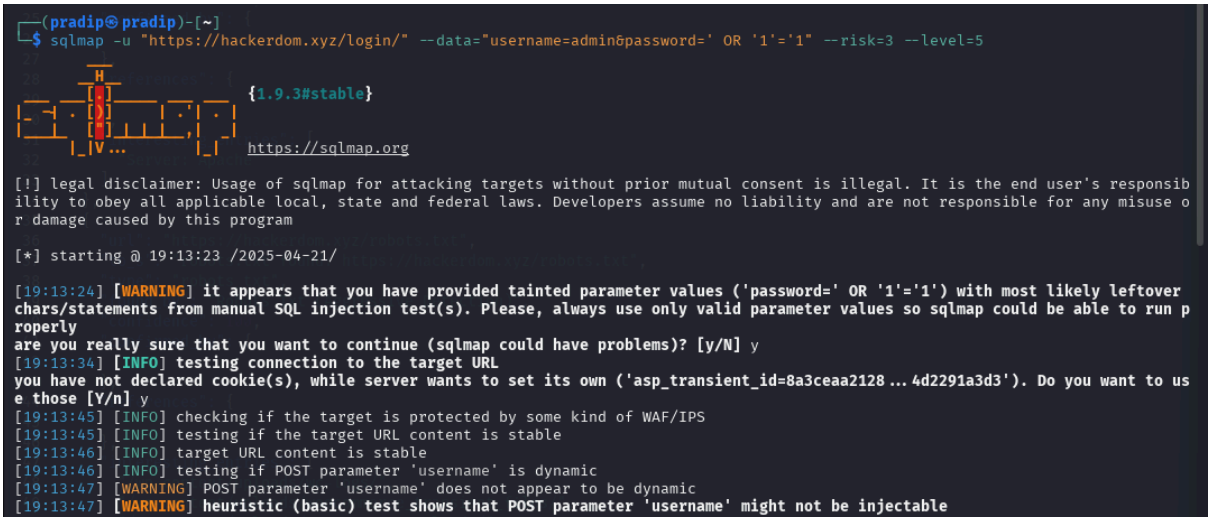
SQLMap Findings

Target URL: https://hackerdom.xyz/login/

Tool Used: SQLMap

Objective: Test the login form for SQL injection vulnerabilities using both automated and manual payloads.



Test Configuration:

- Method: POST
- Parameters: `username=admin&password=' OR '1'='1`
- Risk: 3
- Level: 5
- User consent: Yes (self-hosted test site)
- Cookies accepted dynamically

Findings:

- SQLMap initially flagged a potential **time-based blind SQL injection** vector in the `username` parameter.
- Extensive tests were performed across Boolean-based, error-based, stacked queries, and inline queries.
- After confirming injection behavior, SQLMap flagged the payload as a **false positive or unexploitable**.
- The `password`, `User-Agent`, `Referer`, and `Host` parameters were also tested but showed no signs of injection.

Conclusion:

- While SQLMap detected potential behavior similar to time-based injection, the injection was not exploitable.
- This suggests the site uses secure input handling or WAF filtering that prevents SQL exploitation.
- No actual data leakage or database interaction was observed.

Manually tested:

SQL Injection on the wordpress and web login page

Username: ' OR '1'='1
Password: ' OR '1'='1

USername: admin' –
Password: test

USername: ' OR 1=1 –\
Pass: anything