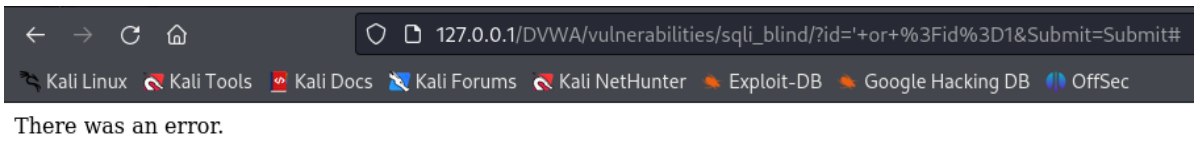
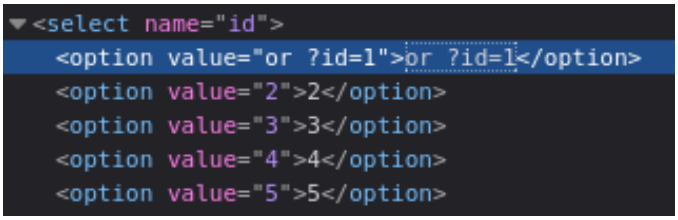
Blind SQL Injection

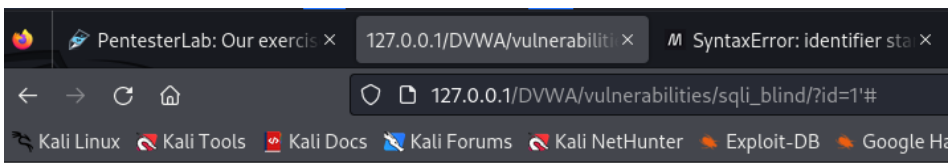
- Blind SQL (Structured Query Language) injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the applications response
- This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection
- Type of blind SQL Injection
  - Content-based: Using a simple page, which displays an article with given ID as the parameter, the attacker may perform a couple of simple tests to determine if the page is vulnerable to SQL Injection attacks
  - Low level



There was an error.

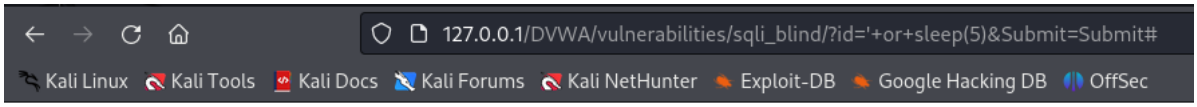
  - Medium level
    - Using inspector to config the userID





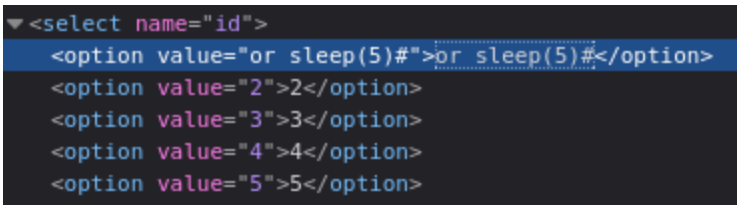
There was an error.

- Time-based: Rely on the database pausing for a specified amount of time, then returning the results, indicating successful SQL query executing. Using this method, an attacker enumerates each letter of the desired piece of data using the following logic
- Low level

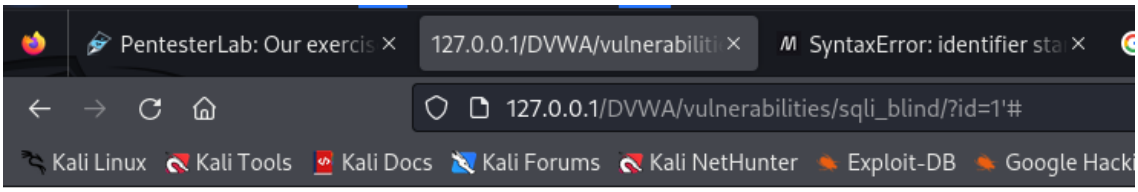


There was an error.

- Medium level
  - Using inspector to config the userID

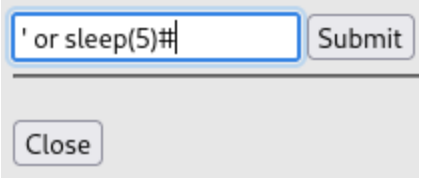


  - The server throw an error



There was an error.

- In high level is similar to the low level



- We inject the code and the website respone very low. Maybe the query I inject was executed