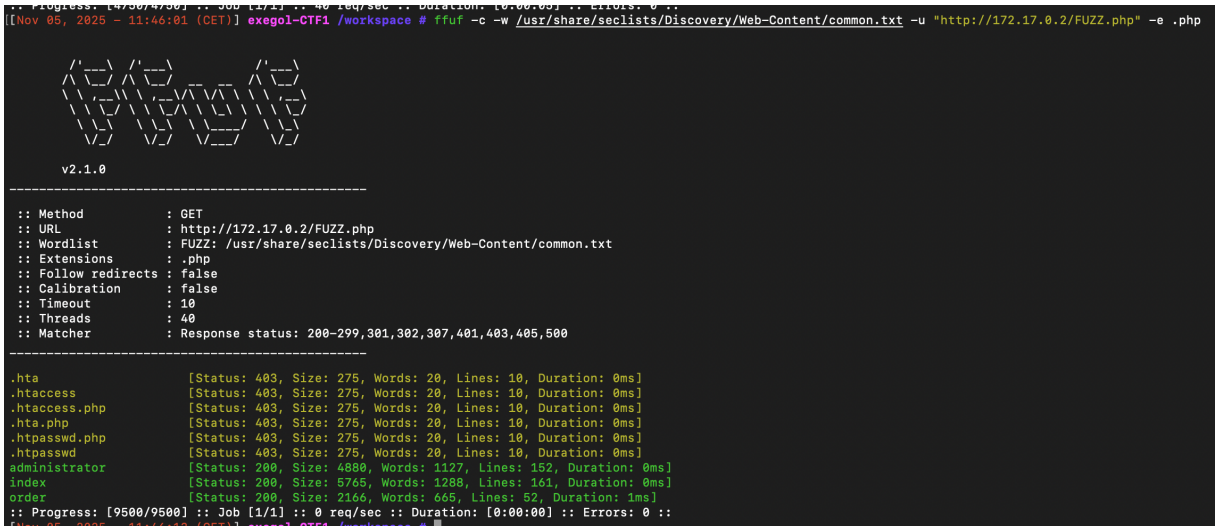
Quantum Cantina - Walkthrough

Web Fuzzing Strategy

First, the initial page presents no possibility of SQL injection, so it is necessary to proceed with web fuzzing to find pages not accessible from the homepage. To do this, we will use ffuf, which allows for the enumeration of pages on a website. We know the code is in PHP, so we can use .php to filter only for those pages. We can use the common.txt wordlist.

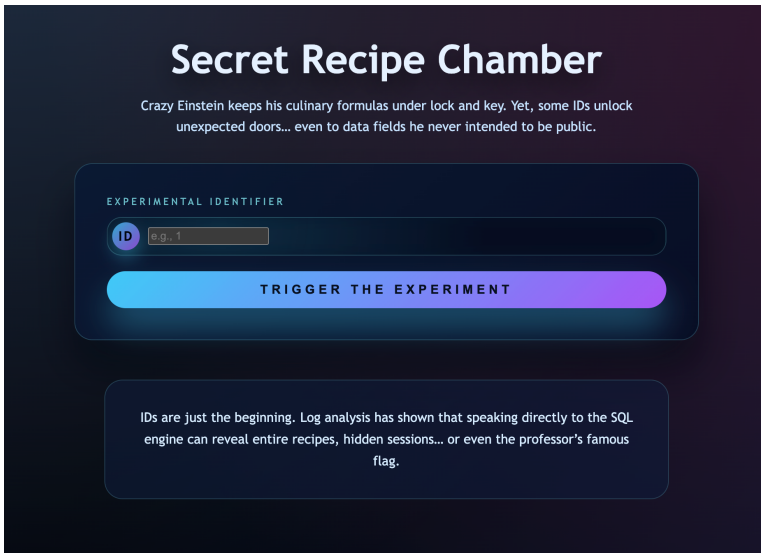
Here is the command that can be used:

```
ffuf -c -w /usr/share/seclists/Discovery/Web-Content/common.txt -u "http://172.17.0.2/FUZZ.php" -e .php
```

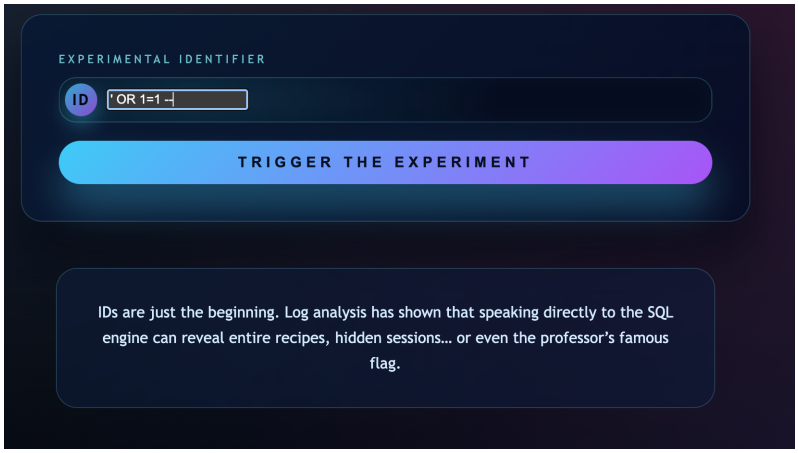


We notice that three pages are available: index.php (the homepage), and the pages order and administrator.

By navigating to http://localhost:8080/administrator.php, we encounter a form that appears to interact directly with the database.

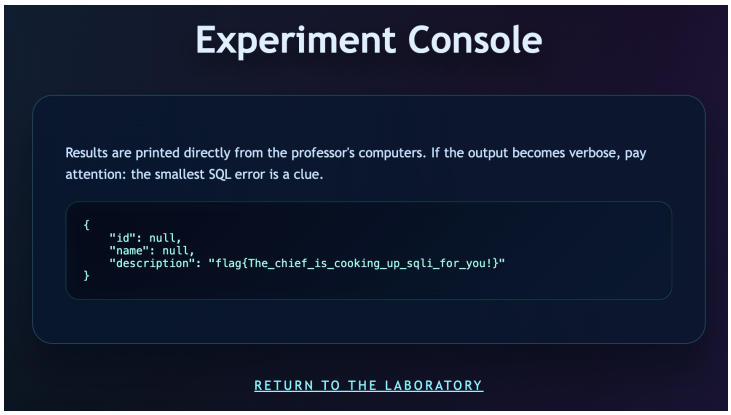


Known payloads for SQL injections can be tested, for example with the payload ' OR 1=1 --.



The flag is not present in the response. Let's try another payload; we can test with the payloads in UNION.

' UNION SELECT NULL,NULL,group_concat(password) FROM users –



We can retrieve the flag.