Wacky Web Woes

In this tutorial, you will explore web app vulnerabilities. Use the `wackywebwoes.out` executable in a VM (that launches a web app) to access 7 rooms, each with clues, flags, and vulnerabilities.

Question 0

- What kind of server is the `wackywebwoes` program running?
- Explore Room 0 to get to Room 1. What is the flag hidden in Room 0?

Hint

- Remember to set the 'execute' permissions of `wackywebwoes`. Then run the program as follows:

```
$ ./wackywebwoes

 ▄▄▄▄▄▄▄ ▄▄▄▄ ▄▄▄▄▄
 ▀▀▀▄▀▀▀ ▄▀▄▀ ▀▀▀▄▀
    ▀ ▀  ▀▀▀▀    ▀

Running on http://0.0.0.0:5000
```

Question 1

- Read more about the `rockyou.txt` wordlist. When was this wordlist created?
- Room 1 can be solved with directory enumeration. What is the name of the hidden directory?
- What is a directory enumeration tool written in `Go`?

Hint

- For Room 1, it is sufficient to use `dirb` and the default wordlists.

```
$ dirb http://0.0.0.0:5000/ /usr/share/wordlists/dirb/common.txt
```

Question 2

- Room 2 deals with a cookie. What is the cookie encoded with?

Hint

- Like the other tutorial questions, CyberChef can help solve this one. You would also need to use the browser tools.

Question 3

- What is a commonly used pentesting tool for intercepting and modifying HTTP requests?

- What HTTP methods does Room 3 accept? What is the flag obtained from making this request?

Question 4

- What kind of XSS vulnerability is being demonstrated in Room 4?
- What is the flag returned in Room 4?

Hint

- Here's an example of a fetch request...

```
fetch('https://example.com/api', { method: 'POST', headers: {'Content-Type':
'application/json'}, body: JSON.stringify({ key1: 'value1', key2: 'value2'
}) })
```

Question 5

- What kind of SQL injection is being demonstrated in Room 5?
- What is the username used for the login form?
- How many columns are there in the SQLite database used?

Hint

- To solve this question, be sure to check the webpage source.
- Finding out the number of columns in the database will let you proceed to the next room...

Question 6

- What vulnerability is present in Room 6?
- What is the flag obtained from the `txt` file?

Hint

- The `/tmp` directory is a common target for penetration testing and security assessments...