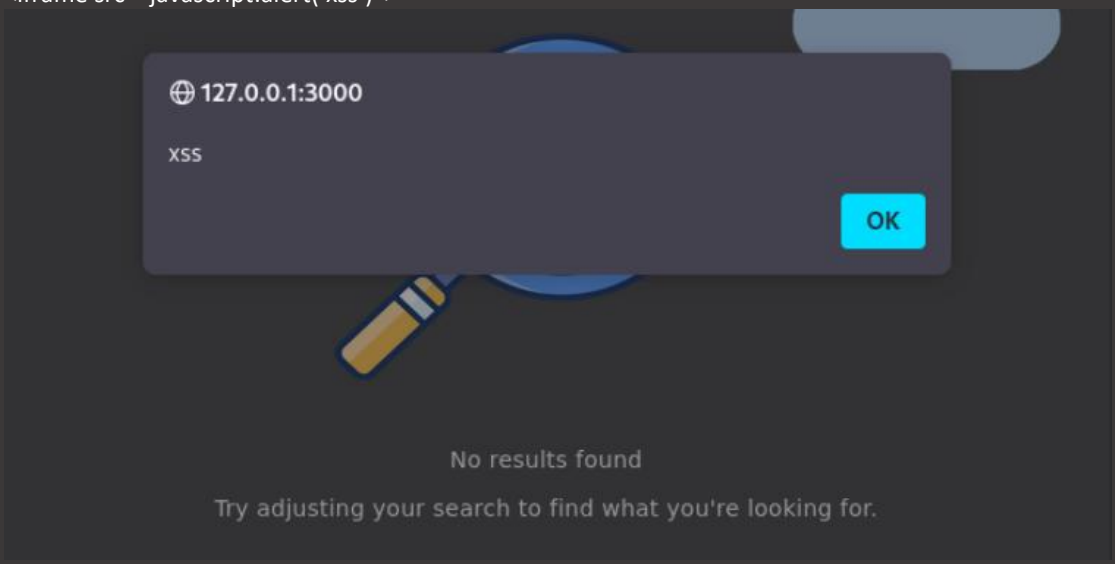
Juice-Shop exploring Report

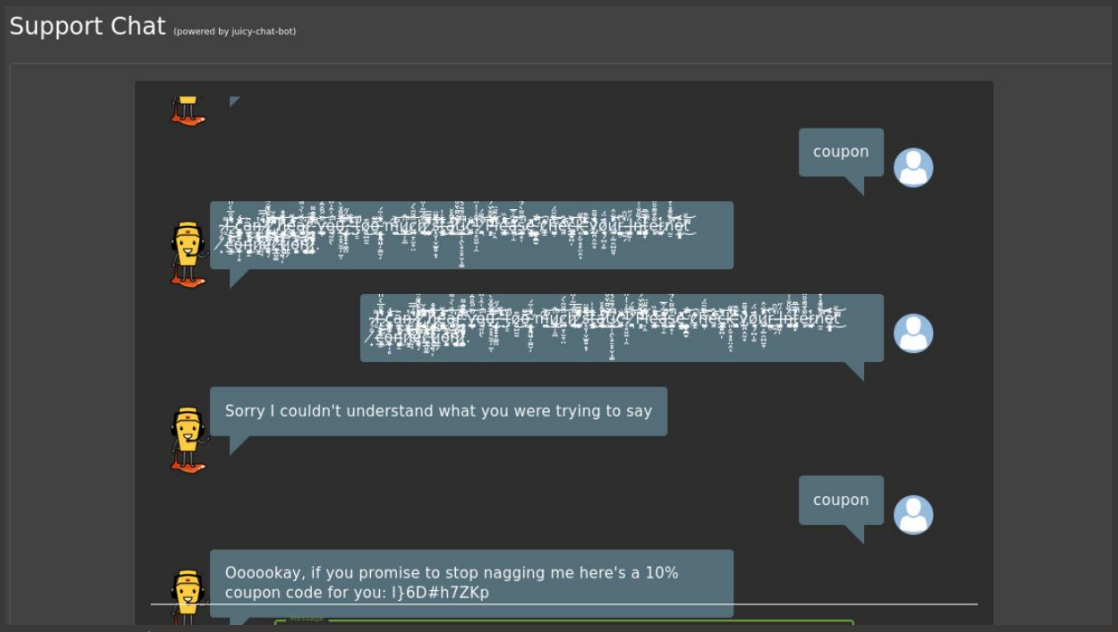
Juice-shop - interactive vulnerable platform, where entry-level pentesters can apply their skills and knowledge, put teory to practice.

First that we need to do - install npm server. This will allow us to have access to site every time when we need it. There are several steps to achieve this.
1. Install nodejs through terminal
Sudo nodejs install
2. Instal npm
Sudo npm install
3. Install juice-shop from github
Git clone https://github.con/juice-shop/juice-shop.git
4. Enter to the fold Juice-shop
Cd juice-shop
5. Start npm-server
Npm start
6. Open site with browser on the port 3000.
127.0.0.1:3000/

Tasks level EASY
1. XSS-injection.
This term means a web-security vulnerability where an attacker can inject malicious scripts into trusted web-sites.
For our understanding if site vulnerable to XSS-injection or not we can use search-field. For this we can enter <h1>owasp. We can see that site do not resist. So we can use next script:
<iframe src=”javascript:alert(‘xss’)”>



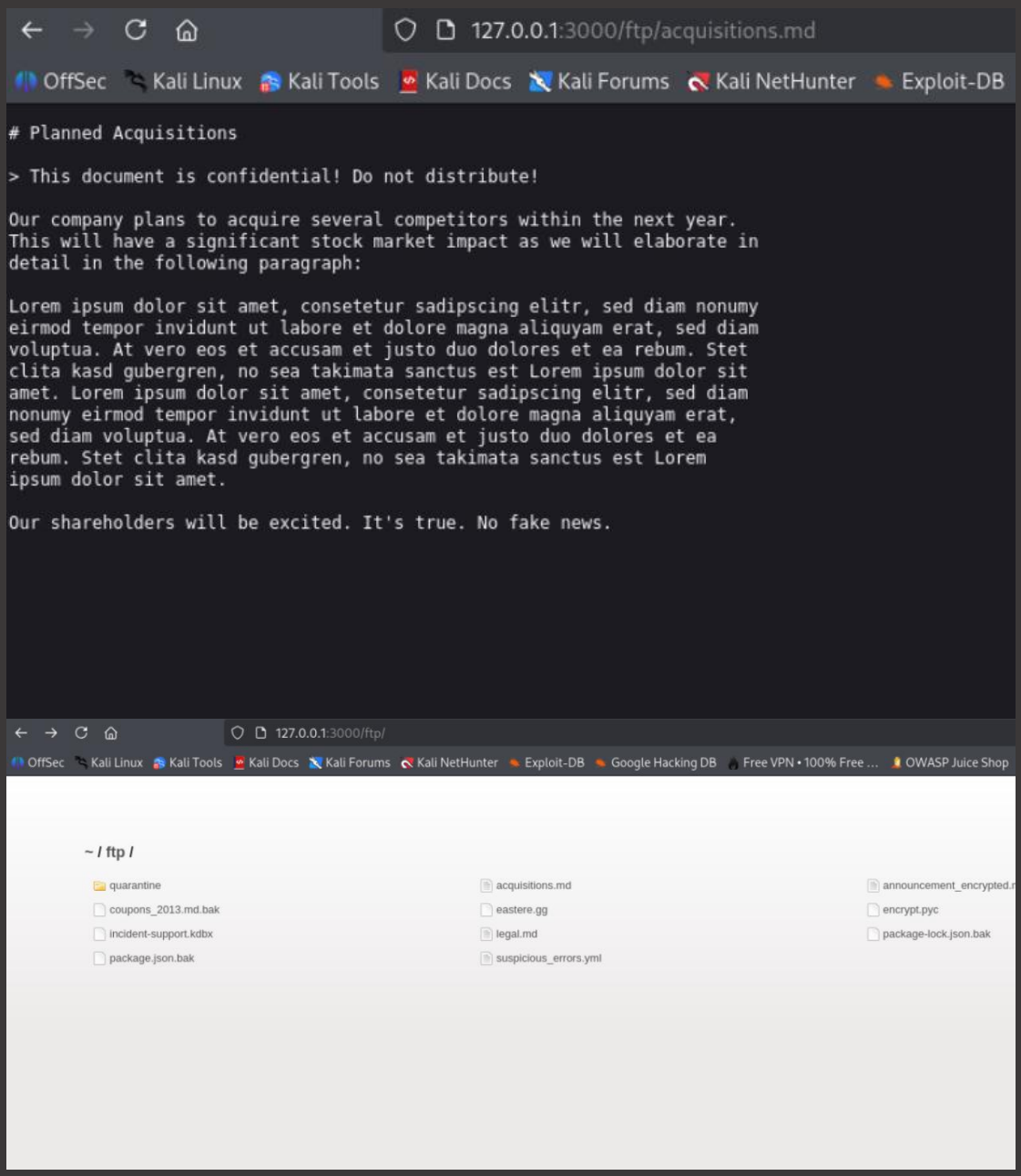
As result we can see next changes in the address field: 127.0.0.1:3000/#/search?q=<iframe src%3D”javascript:alert(‘xss)”>
2. Brutforce chat-bot
Bruteforce this is trial-or-error method, that implies repetitive tries with every possible combinations. Using this method while talking with site’s bot, we can reach next results:



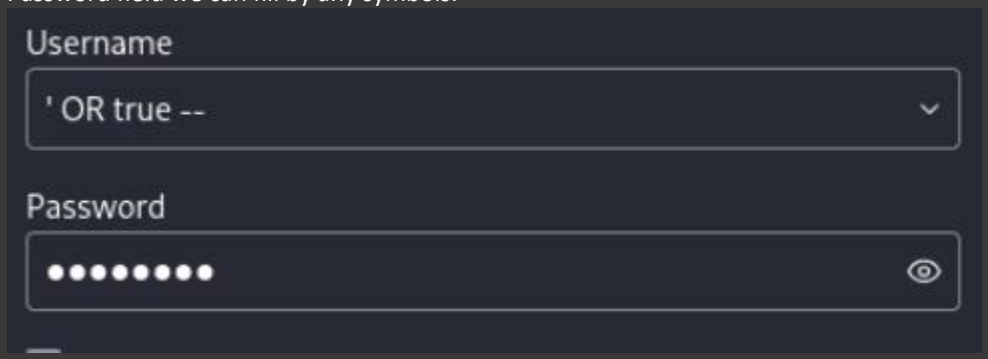
3. Searching for a hidden directories.
For this purpose we can use powerful utilita dirb.
Dirb http://127.0.0.1:3000 -f

```
┌──(vbox㉿vbox)-[~/Downloads/juice-shop]
└─$ dirb http://127.0.0.1:3000 -f

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Dec  4 16:45:22 2025
URL_BASE: http://127.0.0.1:3000/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Fine tunning of NOT_FOUND detection

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://127.0.0.1:3000/ ----
+ http://127.0.0.1:3000/assets (CODE:301|SIZE:156)
+ http://127.0.0.1:3000/ftp (CODE:200|SIZE:941)
+ http://127.0.0.1:3000/profile (CODE:500|SIZE:1061)
+ http://127.0.0.1:3000/promotion (CODE:200|SIZE:692)
+ http://127.0.0.1:3000/redirect (CODE:500|SIZE:3559)
+ http://127.0.0.1:3000/robots.txt (CODE:200|SIZE:3)
+ http://127.0.0.1:3000/video (CODE:200|SIZE:263788)
+ http://127.0.0.1:3000/Video (CODE:200|SIZE:263788)

(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT CONNECT)

-----------------
END_TIME: Thu Dec  4 16:47:48 2025
DOWNLOADED: 4589 - FOUND: 8
```

Code 200 allows us to see which directories are active and exists in the access zone.
One of them is directory /ftp, where we can find a document acquisitions.md, that suppose to be confidential.



4. SQL-injection for password bypassing
We can start our penetration in the registration form. For this we can put next to the username field:
- ‘
- ‘ or true
- ‘ or true --
Password field we can fill by any symbols.



As result, we can login as an adiministrator.