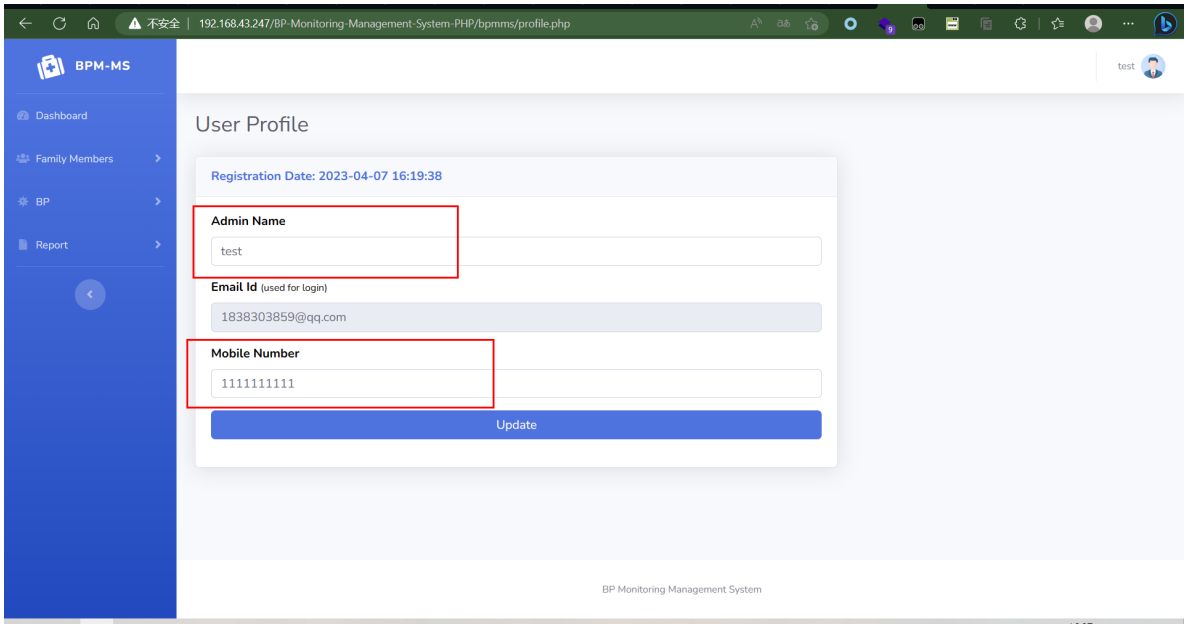
BP Monitoring Management System v1.0 Background Modification of Personal Information SQL Injection

Vulnerability Details

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



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 connection
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">
```

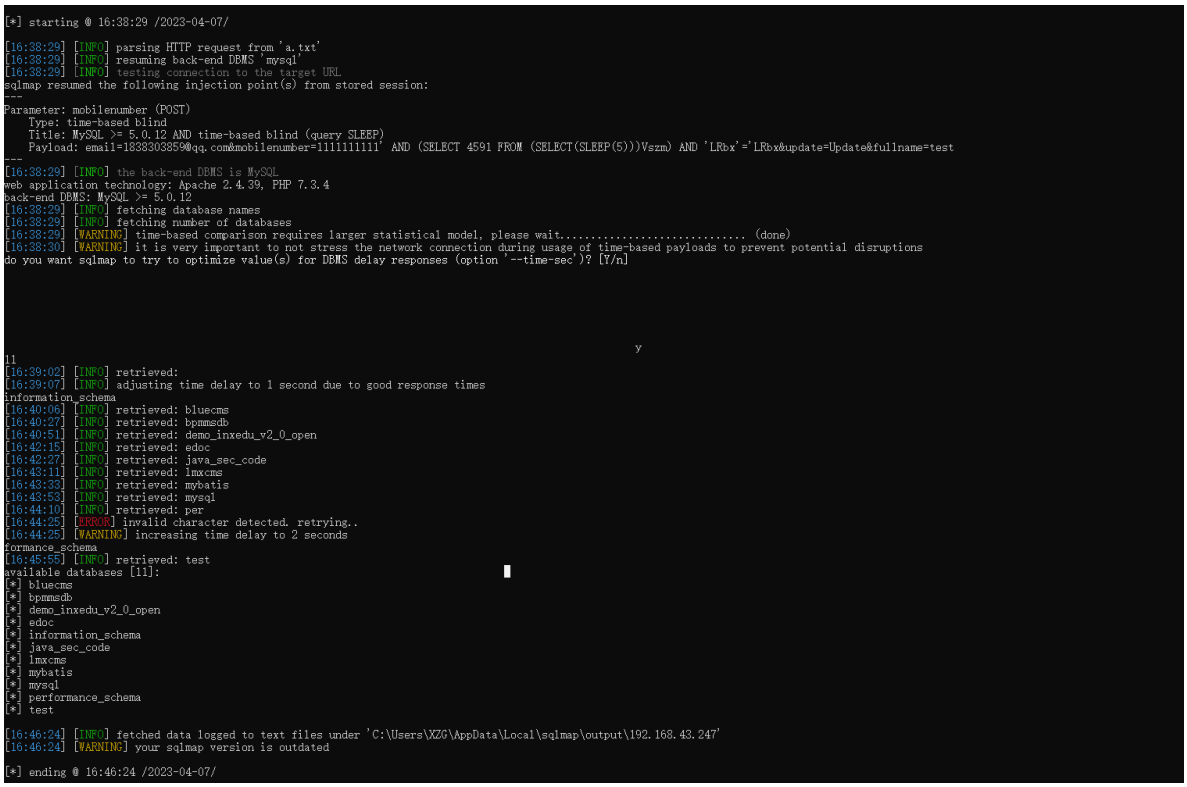
POST packet

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,application/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



The value of mobileNumber in the database has been uniformly modified to 1111111111 by maliciously injected SQL statements