Ashish Dhone Follow
Jan 6, 2021 · 3 min read · · Listen

Privilege Escalation — Unauthenticated access to Admin Portal (CVE-2020–35745)

Introduction

This article is a write up on how I found a Privilege Escalation Vulnerability where an attacker can access complete admin portal without authentication which gave me a new CVE-2020–35745.

What is Privilege Escalation?

Privilege escalation occurs when a user gets access to more resources or functionality than they are normally allowed, and such elevation or changes should have been prevented by the application. This is usually caused by a flaw in the application. The result is that the application performs actions with more privileges than those intended by the developer or system administrator.

Usually, people refer to vertical escalation when it is possible to access resources granted to more privileged accounts (e.g., acquiring administrative privileges for the application), and to horizontal escalation when it is possible to access resources granted to a similarly configured account (e.g., in an online banking application, accessing information related to a different user).

Vulnerability exploitation

I have found this vulnerability in Hospital Management System — 4.0 of PHPGURUKUL.

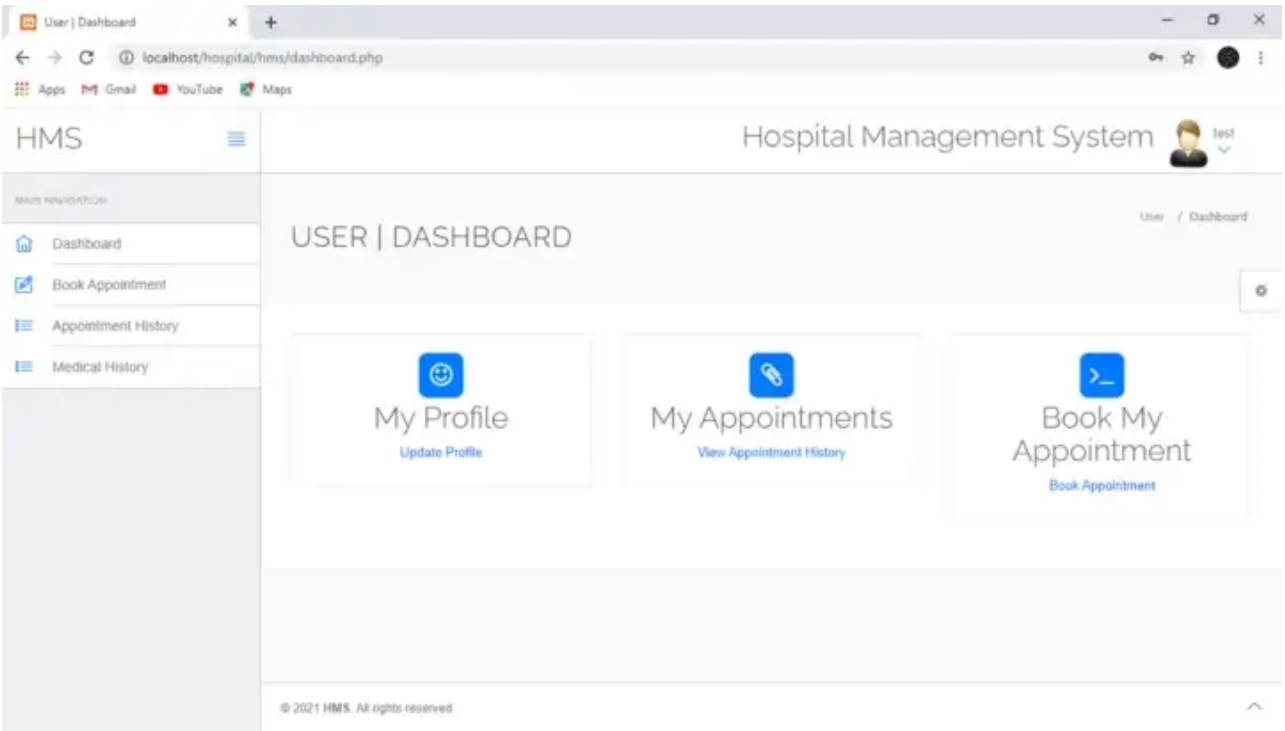
Hospital Management System is a web application for the hospital which manages doctors and patients. In this project, they use PHP and MySQL database.
The entire project mainly consists of 3 modules, which are

1. **Admin module**
2. **User module**
3. **Doctor module**

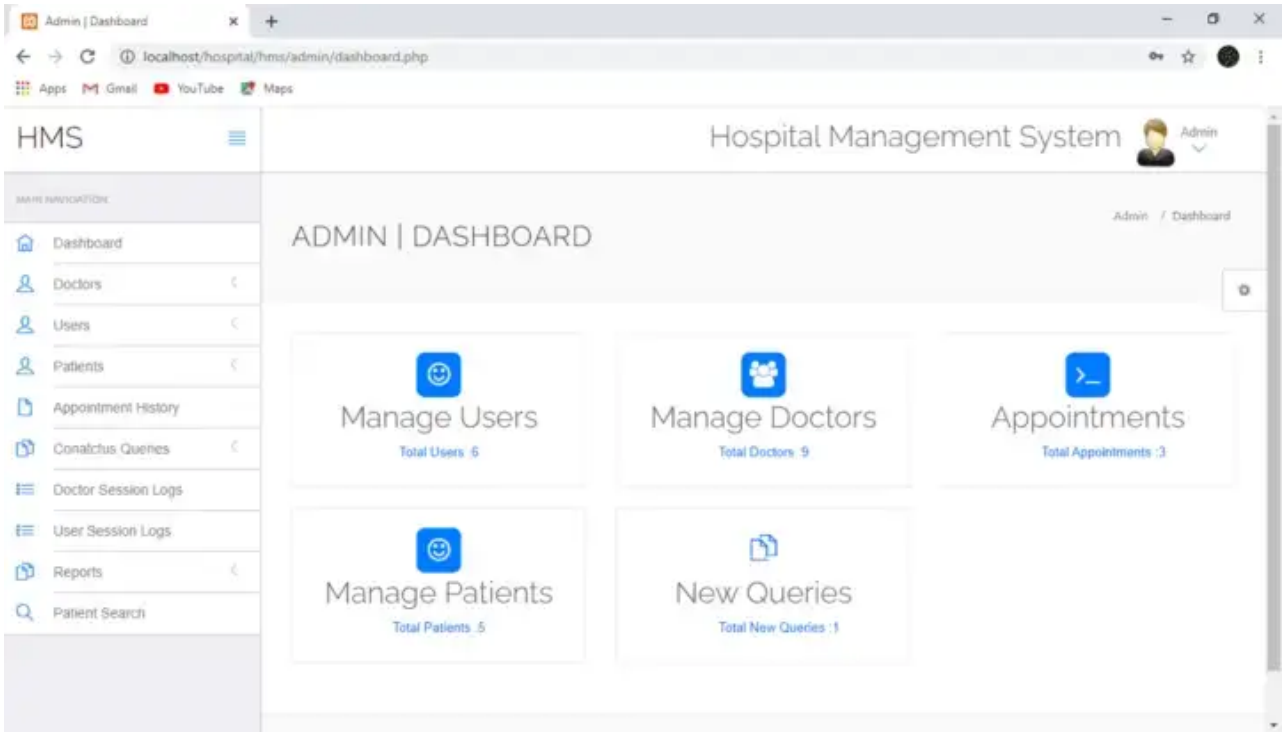
So we need installation process and source code to get started, we get complete details here.

Once we are done with the setup, we get portal to login for all modules.

So I Logged into **User Module** with provided credentials I was getting below dashboard.



Then logged in with **Admin Module** with provided credentials getting below admin dashboard, so till here everything was good.



Now when I looked at admin URL it was http://localhost/hospital/hms/admin/dashboard.php

and I was like only **/admin** endpoint is added to admin dashboard while in user we are getting URL without **/admin** endpoint i.e. http://localhost/hospital/hms/dashboard.php

Without wasting time I logged out from all dashboard checking whether session management is properly configured or not I visited http://localhost/hospital/hms/admin/dashboard.php and checked whether I am still logged in or not but everything was good and I was redirect to login portal.

Here comes the final part, I logged into USER Dashboard and I was redirected to http://localhost/hospital/hms/dashboard.php

Now I have just added **/admin** endpoint where I was still logged into USER account like this http://localhost/hospital/hms/admin/dashboard.php and BOOM I was logged into ADMIN dashboard as this was not properly restricting access to admin/dashboard.php, where I was able to access all data of users, doctors, patients, change admin password, get appointment history and access all session logs.

Happy to get a CVE-2020–35745.

POC Video: https://youtu.be/vnSsg6iwV9Y

If you need any help or want to connect, you can connect with me via LinkedIn at https://in.linkedin.com/in/ashish-dhone-640489135

I hope it will help you somewhere with your journey !!

Thanks for Reading !!

./Keep_Hacking