Vulnerability Name: Session Hijacking.

Affected URL: http://localhost/hospital/hms/admin/dashboard.php

Affected Project: PHPGurukul Hospital Management System In PHP

Official Website: https://phpgurukul.com/hospital-management-system-in-php/

Version: 4.0

Description: Session hijacking is an attack where an attacker takes over a user's session by stealing or predicting their session ID or token. This allows the attacker to impersonate the user and access their data or services. Common methods include sniffing network traffic, exploiting XSS vulnerabilities, or using man-in-the-middle attacks.

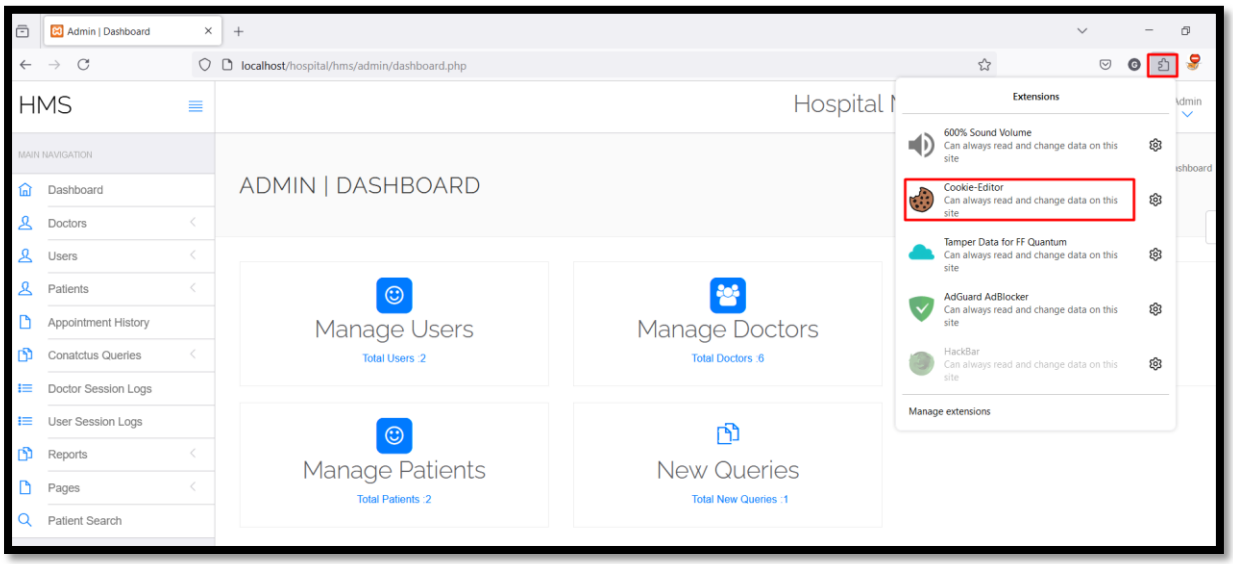
Impact: Session hijacking allows attackers to take over a user's session, leading to unauthorized access to sensitive information, identity theft, financial fraud, and potential privilege escalation. It can cause significant damage, including data breaches, service disruption, and reputational harm to business.

Remediation:

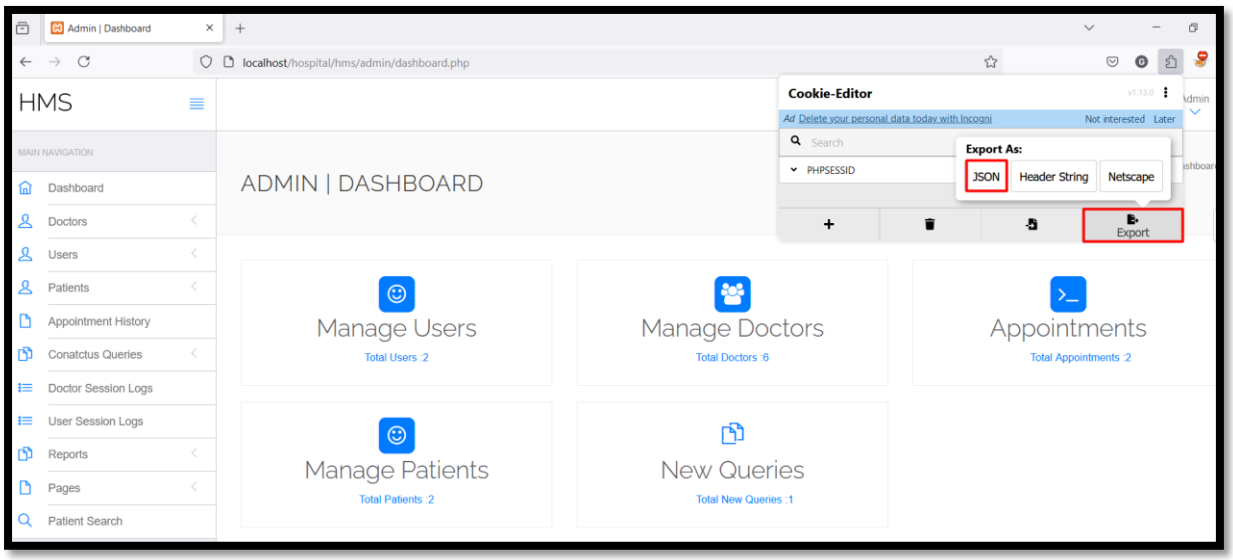
- Using HTTPS/SSL to encrypt data transmission and prevent session tokens from being intercepted.
- Applying secure session management practices, such as regenerating session tokens after login, setting appropriate expiration times, and tying tokens to IP addresses or user agents.
- Implementing multi-factor authentication (MFA) to add an additional layer of security beyond session tokens.

POC

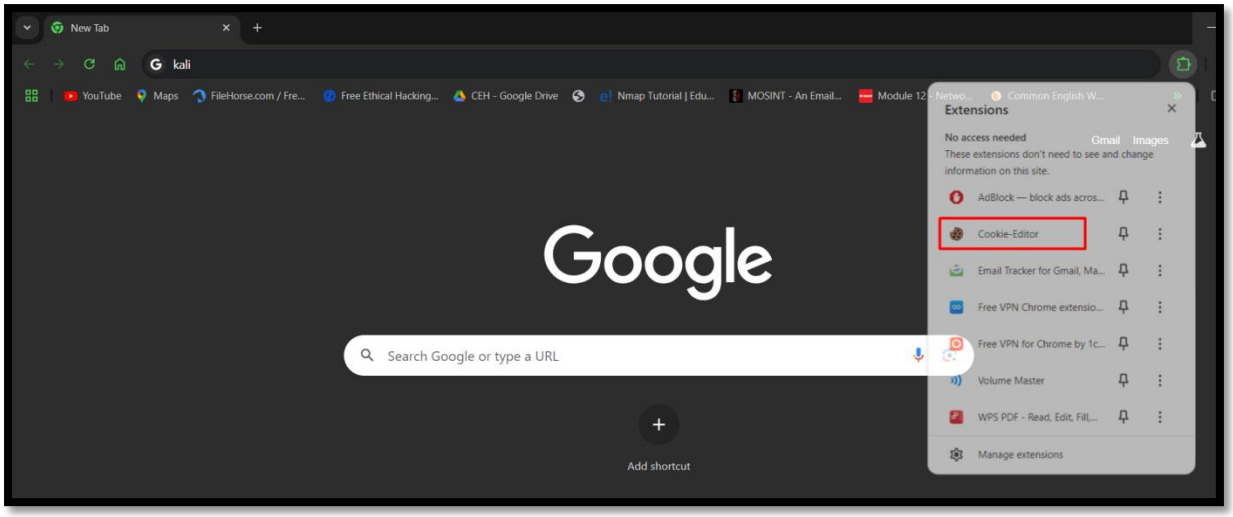
Step 1: Go to Extension and then click on Cookie-Editor.

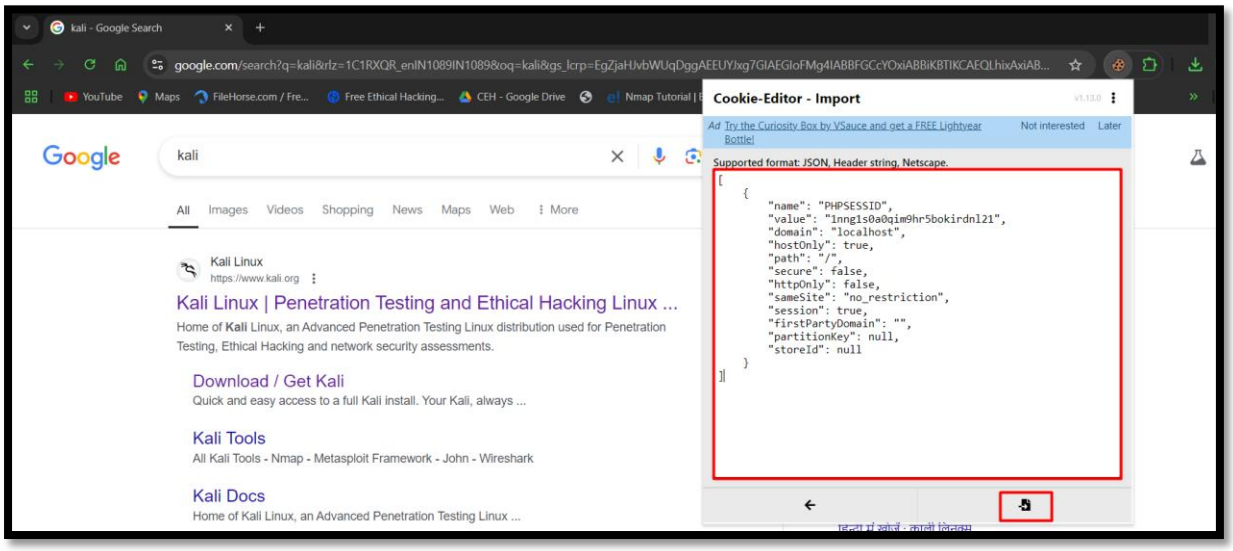


Step 2: Click here to export the cookie JSON.



Step 3: Open new browser, go to Cookie-Editor, and import the JSON cookie.





Step 4: Go to url: http://localhost/hospital/hms/admin/dashboard.php, account will be loged in.