Chamilo LMS - Bug #7269

Security issue Who Is Online

15/09/2014 21:13 - Jan Derriks

Status:	Bug resolved	**Start date:**	15/09/2014
Priority:	High	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Global / Others / Misc	**Estimated time:**	0.00 hour
Target version:	1.9.10	**Spent time:**	3.50 hours
Complexity:	Normal	**SCRUM pts - complexity:**	?

Description

When "show users online" is enabled, any user can easily harvest all the users on the platform by enumerating the URL:
https://campus.chamilo.org/main/social/profile.php?u=3
https://campus.chamilo.org/main/social/profile.php?u=372307

Where u=1 to 350000 (or more)

Then you will have the names, pictures and login-id's of all the users on the platform to start a dictionary attack (begin with password==userid).

This was not the intention of the "who is online" feature I hope.

Associated revisions

Revision 8b650bf9 - 17/09/2014 23:42 - Daniel Barreto

Remove username from profile except to platform admin or self user - refs #7269

Revision 03b4435c - 19/09/2014 18:53 - Daniel Barreto

Hide offline user image from profile - refs #7269

History

#1 - 17/09/2014 22:49 - Daniel Barreto

- Status changed from New to Assigned

- Assignee set to Daniel Barreto

I will modify social profile to only show username to admin users. Username data should not be public.

#2 - 17/09/2014 23:42 - Jan Derriks

Downloading 300000 user pictures with their names should also not be possible.
Extra fix:
1. only allow viewing of "Currently Online users"
2. encrypt the "u=1234" parameter with a simple base64 encoding after multiply by some secret number (or some other easy decodable algoritm) or use a session variable to remember what the user id was.

#3 - 18/09/2014 17:18 - Yannick Warnier

Technically, we can remove the possibility to view the profile.php page if not logged in. If you are logged in, then you should be able to view the pictures of your peers and minimal information.

I cannot see how the "viewing pictures only of online users" is a security improvement, though. Because the only solution to not show my picture would be to never connect :-)

#4 - 18/09/2014 17:29 - Jan Derriks

"viewing pictures only of online users" is not the issue here.
Downloading pictures, uid's and names of ALL users on the system by ANY logged-in user was considered a privacy issue here. Normal users should not be able to do that.

#5 - 18/09/2014 17:53 - Daniel Barreto

And what about to only see profiles of classmates (user with at least one same course)?
This could be for user students and teachers.
Admin could see all profiles and any user, could see self profile.

#6 - 18/09/2014 18:44 - Julio Montoya

- Status changed from Assigned to Needs more info

- Assignee deleted (Daniel Barreto)

Changing social/profile.php?u=3 with social/profile.php?u=ywarnier doesn't fix this issue?

In order to get the picture you must contain a little bit more of information:

Like the user_id, a unique key and the user picture name:

https://campus.chamilo.org/main/upload/users/3/3/3_4df1637863f89_yannick.warnier.64x64.jpg?541b096a8e2c7

So is not that easy to get the picture ...

Other solution is to create the option of "visibility" in profiles:

I mean the user can change from:

- public (all registered users),
- friends (my friends from the social tool)
- private (only me)

#7 - 19/09/2014 19:35 - Daniel Barreto

- Status changed from Needs more info to Assigned

- Assignee set to Daniel Barreto

Send Pull request 364 to add next chamges:

1. Hide username from social profile except Admin and user self
2. Hide official code from social profile except Admin and user self
3. Show unknown picture as user image when user is offline.

Pull request:
https://github.com/chamilo/chamilo-lms/pull/364

#8 - 12/10/2014 08:34 - Yannick Warnier

- Category set to Global / Others / Misc

- Status changed from Assigned to Needs testing

- Assignee deleted (Daniel Barreto)

- % Done changed from 0 to 80

I have included Daniel's changes into Chamilo. You should be able to see it on https://stable.chamilo.org

I believe this is enough (for now) to cover the main issue of information divulgation. If you believe we should provide **options** for some admins to enable if they feel this is too weak, please let us know. Otherwise, I will close this task in about a week.

#9 - 19/10/2014 18:25 - Yannick Warnier

- Status changed from Needs testing to Bug resolved

- % Done changed from 80 to 100