

New issue

Jump to bottom

# Four CSRF vulnerabilities in pluck cms 4.7.9 #69

Closed China-Eugene opened this issue on Feb 18, 2019 · 12 comments

Labels invalid Password Required for exploit Security:low wontfix

China-Eugene commented on Feb 18, 2019

One: use CSRF vulnerability to delete pictures  
Vulnerability details:  
When the administrator logs in, opening the webpage will automatically delete the specified image.  
Vulnerability url: <http://127.0.0.1/pluck/admin.php?action=images>  
Vulnerability POC:  
  
<iframe src="http://127.0.0.1/pluck/admin.php?action=deleteimage&var1=test.jpg" >  
Two: use the CSRF vulnerability to delete the topic  
Vulnerability details:  
When the administrator logs in, opening the web page will automatically delete the specified topic.  
Vulnerability url: <http://127.0.0.1/pluck/admin.php?action=theme>  
Vulnerability POC:  
  
<iframe src="http://127.0.0.1/pluck/admin.php?action=theme\_delete&var1=oldstyl">  
Three: use CSRF vulnerability to remove the module  
Vulnerability details:  
When the administrator logs in, open the webpage and the specified module will be deleted automatically.  
Vulnerability url: <http://127.0.0.1/pluck/admin.php?action=modules>  
Vulnerability POC:  
  
<iframe src="http://127.0.0.1/pluck/admin.php?action=module\_delete&var1=albums" >  
Four: use CSRF vulnerability to delete pictures  
Vulnerability details:  
When the administrator logs in, opening the web page will automatically delete the specified article.  
Vulnerability url: <http://127.0.0.1/pluck/admin.php?action=page>  
Vulnerability POC:  
  
<iframe src="http://127.0.0.1/pluck/admin.php?action=deletepage&var1=aaaa">  
Vulnerability suggestions:  
One: Detect user submissions by referer, token, or verification code.  
Second: It is best to use the post operation for users to modify and delete.

China-Eugene commented on Feb 18, 2019

Author

The fourth is to use the CSRF vulnerability to delete articles

BSteeloooper commented on Feb 19, 2019

Contributor

Funny, even github is vulnerable.. it opened a new window for me :)  
How would you exploit this?  
Admins are instructed to go to the domain.tld/login.php to logon to Pluck.  
Than after this they randomly go to your constructed website in which you know which page/ image etc exists and delete this?  
Please explain an attack vector in which the admin is not willingly logged on to the admin page.

BSteeloooper added Password Required for exploit Security:low labels on Feb 19, 2019

BSteeloooper commented on Feb 19, 2019

Contributor

Dear Eugene,  
  
Thank you for the thumbs down emoji. You deleted your comment that I will never understand security, since you don't know me, you cannot state this fact. I am a Penetration Tester since 2008 and have successfully penetrated several applications and websites. You have several types of attack vectors. For this you need two, Social Engineering and Phishing.  
  
With a code audit (which is now possible as you stated that it is open source) you can maybe find exploits. Lots have been found and fixed. We are always open to learn about new exploits and bugs.  
Issues which require a login before being able to be exploited are very hard to exploit. The attack vector is so small and complicated that the risk is near zero. Since two attack vectors need to be combined and the type of end user for this product I cannot find any reason to believe that a hacker would invest that amount of effort and time into an exploit which than easily can be undone by recovering the item from the trash bin.  
  
If you see another attack vector which can be used at this moment please let me know and I will certainly fix this for you, until then it is rated LOW and I think it will be a won't fix.  
  
Waiting for you reply,  
  
Kind regards,  
Bas

China-Eugene commented on Feb 19, 2019

Author


Hi Bas Steelooper, I sent an email to your steelooper mailbox.

 BSteel00per added the **wontfix** label on Apr 2, 2019

BSteel00per commented on Apr 2, 2019

Contributor

I have tried several times to do this on websites with some kind of automation, but without access to the machine of the admin this is not possible to exploit.

 BSteel00per closed this as completed on Apr 2, 2019

 BSteel00per added the **invalid** label on May 15, 2019

BSteel00per commented on May 15, 2019

Contributor

This is an invalid report. With the password the complete website can be taken over. Without the password this is not exploitable.

attributionorg commented on May 15, 2019

With a CSRF attack, it does not require the attacker to know the password. It requires the attacker to trick an admin who is authenticated to the app, to click a malicious link, that will invoke an action with the admin's privileges. This is very different than the two authenticated file upload issues that were rejected as invalid.

BSteel00per commented on May 15, 2019 • edited

Contributor

Dear Jericho,

So how would this be exploitable for Pluck? Pluck is a CMS for small websites which have little updates.

You would have to know the person responsible for maintaining the website, and have them logon to the admin console and then trick them to a website which opens your iframes or have them click on links...

You have to have the correct website also, you would have the need to index the website and have all the items which you want to delete, all pages you want to delete etc.

Again, I don't see a valid exploit path for this.

Without an attack vector this report is invalid, the attack vector has been asked and not supplied, but the CVE has been marked HIGH and easy exploitable by the OP.

attributionorg commented on May 15, 2019

It would be a targeted attack, yes, and you would have to know the administrator of the site. But really that is all you need, and to trick them into clicking the link. That makes the complexity of attack higher than some attacks, but it is the same complexity as a reflected XSS attack. The idea is that they are already authenticated, as many apps allow an admin to stay authenticated for long periods of time without having to re-authenticate for convenience. If that isn't the case and the app terminates a session after X minutes, then the difficulty of exploitation is even higher. As far as knowledge past that, I am not familiar with Pluck. If Pluck uses sequential numeric designations for something, then the attacker doesn't need to know anything specific about the victim's installation, they can send the CSRF to delete a page and specify e.g. "page 1" (however that is translated to parameters in the request). If Pluck uses custom names instead of numbers e.g. 'mypage', then yes, the difficulty of attack goes up even higher and is not likely to happen at all.

That said, CSRF is a valid attack. Most CSRF reported (~ 222 this year that I have seen) rely on the software not having such custom naming elements. In most cases, the attacker could download the software, perform the requests themselves, capture the GET or POST request w/ parameters, and use that to form the attack. More information: [https://www.owasp.org/index.php/Cross-Site\\_Request\\_Forgery\\_\(CSRF\)](https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF))

Using CVSSv2, a CSRF attack is only rated as 4.3. Using CVSSv3, a CSRF attack is rated as 8.8, and 'High', which many people feel is absurd given the preconditions that exist. Personally, I would ignore the 'High' rating and focus on the requirements for attack and the capability for damage, and triage accordingly.

BSteel00per commented on May 15, 2019

Contributor

Dear Jericho,

Pluck uses custom naming. The names of the pages are derived from the name, and can be modified by the user. The display in the url is a seo optimized name, the edit and delete urls require the file name, which is in most cases the same, but this is not a guarantee.

Pluck has a session timeout from Apache/nginx with php, which defaults to 30 mins. When the session is expired the user is logged of. Returning to the page requires you to re-login.

The attack therefor needs the following steps:

- have the administrator logon to the admin page
- make sure the administrator does not logon or close the browser
- redirect the administrator to the constructed webpage which calls the crafted urls with the specific pages, items for that website.

As said before I don't see the attack vector for Pluck. We don't have a stay logged on option or something similar.

On a side note... nothing is deleted definitely. It is put in the trashcan and can be restored with 1 click.

attributionorg commented on May 15, 2019

With all of that in mind, the risk rating would go down further. Access complexity would be 'high' instead of 'medium', and the window for attack along with knowledge required would make this extremely difficult to perform I would assume. It sounds like Pluck has a great system for defense in depth here.

On an academic level, this is still a vulnerability. In reality, this is what we call a "and pigs may fly" attack scenario. =)

Thanks for taking the time to detail all of that. I really appreciate when project maintainers dig in a bit to figure out these details. It is always refreshing and encouraging to see.

attributionorg commented on May 15, 2019

BTW, changing the access complexity from 'medium' to 'high' changes the CVSSv2 score to 2.8 and CVSSv3 score to 5.3. I still think the v3 score is not a good representation of the severity of this issue.

Assignees

No one assigned

Labels

invalid Password Required for exploit Security:low wontfix

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

