Broken Authentication and session management OWASP A2 #2314

Closed Songohan22 opened this issue on May 11, 2020 · 10 comments

Songohan22 commented on May 11, 2020 • edited

Describe the bug
Hello every one, I have found a small vulnerbility your PHP Fusion.

Here is the error details.(Broken Authentication and session management PHP Fusionon)
Cookies are used to maintain session of the particular user and they should expire once the user logs out of his PHP Fusion account.In secure web application,Cookies immediately expire once the user logs out of his account.
But this is not happening in the case of HP Fusion same cookies can be used again and again to open the session of the victim.
In this Loop Hole The Application does not destroy session after logout.. means the cookies are working to login to user account & change account Information, The Cookies are usable i'm able to access the account & edit info.

If anything is wrong please reponse to me. Thank you.

To Reproduce
Steps to reproduce the behavior:

1. Login to your account.......
2. Get the cookies using " Brub Suite" or "EditThisCookie"
3. Logout from the account...
4. Clear all the cookies related to PHP Fusion
5. Save the cookies you copied in a text file...
6. Now Injact/Import Old Cookies to the PHP Fusion by "EditThisCookie"...
7. As u can see.. you will be again logged In to PHP Fusion .. using old session cookies..

For More Information about This Vulnerability You can check OWASP Guide
https://www.owasp.org/index.php?title=Broken_Authentication_and_Session_Management&setlang=en

Here is a Video POC: https://drive.google.com/file/d/14IIln0HcVyBk_kfcUJsZdpYgx72xdBZa/view

Songohan22 commented on May 12, 2020 Author

I look forward to listening your reply.

Songohan22 commented on May 12, 2020 Author

More information POC link: https://drive.google.com/open?id=1c_wN77CkS5nEK_tAUaRDwMo5g-Zx55K4
Impact: Means the cookies are working to login to user account & change account Information, The Cookies are usable i'm able to access the account & edit info, use all function user.

FrederickChan commented on May 13, 2020 • edited Member

The current cookie is built using the user salt which was probably never updated during logout. I will make the amends tomorrow. If we generate a new one, it will fix the issue.

Thank you for the report.

👍 2 😄 1

FrederickChan added a commit that referenced this issue on May 13, 2020

#2314 - Proposed solution 0f80a68

FrederickChan commented on May 13, 2020 Member

While we need to have a raw password input to create a new hash, it is quite absurd to ask for one during logout. My solution is to use $_SESSION storage to store future data which we will use during Logout. Please verify that you cannot access $_SESSION storage throughout the whole login session. The $_SESSION is "logout_hash" before we close this issue. If your tool can access this session, the storage medium must be SQL, and we will need to impose on the upgrade of this fix as a **major** instead of **minor**.

So please advice if anyone can tell me "Yes, I can access these variables with my superman tool", with proof, then we will fix this as a major with 3 new table columns in DB_USERS.

FrederickChan commented on May 13, 2020 Member

@JoakimFalk @RobiNN1 , please do not let this issue hinder the new release timeline since it is quite critical that one whether this patch is good enough or not. See my comments above.

Regardless, the patch is done, and IF the patch is not good enough, it could be a major here. We will probably be looking at an upgrade release.

Songohan22 commented on May 13, 2020 Author

Hello **@FrederickChan**
Solutions fix issue:

- User session should be destroyed when logged out.

- Also add a csrf token into the cookie.
  Thank you.

FrederickChan commented on May 14, 2020 • edited Member

`User session should be destroyed when logged out. Also add a csrf token into the cookie.`
We did that both over a century ago. 👍 During a point of time, OWASP techniques were not founded yet. Credits to previous lead developers on this.

What we didn't to do was to invalidate it by creating a new one. Implement Round Robin method on the CSRF Token itself. My patch did that, but the method employed is utilizing server $_SESSION as medium for storage.

The current patch is fit for minor release updates as changes are made on codes and file based only. User can just download and patch file, and get it done.

Another method will be database structure adjustments. This will require user to run install/upgrade script, and many will be reluctant to do it and therefore, equals less effective measure in a major patch.

I'm thinking a minor is fast, and more effective, even though it uses $_SESSION.

FrederickChan closed this as completed on May 14, 2020

Songohan22 commented on May 14, 2020 Author

I just want to give your suggestions for the best service to your customers.

A system can have many or one admin, not necessarily just one, so your idea of saying it doesn't matter is not very true.
Ideally, you should build a SESSION management driver, it will automatically check the value of the SESSION generated in your system has been disabled or not and etc. I think that the way you generate a new session value is not optimal, the more sessions that are created, the harder it will be to manage and be easy exploited, and we don't need to generate a new SESSION code when logging out?

FrederickChan commented on May 15, 2020 Member

Maybe we are on the wrong page. I did not say anything regarding Admin or Admin Panel.
From your reply, I assume that you aren't reading my commit. php-fusion/php-fusion@ `0f80a68`

Well, I have redid the test, and this can be simply be overridden if the user closes his browser. It's not effective solution.

FrederickChan reopened this on May 15, 2020

Songohan22 commented on May 15, 2020 Author

It is only my opinion to comment on this matter.
Thank you for reply.

FrederickChan added a commit that referenced this issue on May 15, 2020

`#2314 Closed` 6447836

FrederickChan added a commit that referenced this issue on May 15, 2020

`#2314 - Logouts a user if session doesn't exist.` 450d47a

FrederickChan closed this as completed on May 15, 2020

FrederickChan added a commit that referenced this issue on May 15, 2020

`Upgrade required for #2314` … 6a659a7

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants