New issue

Jump to bottom

# Pluck 4.7.15 - Session Fixation Vulnerability #99

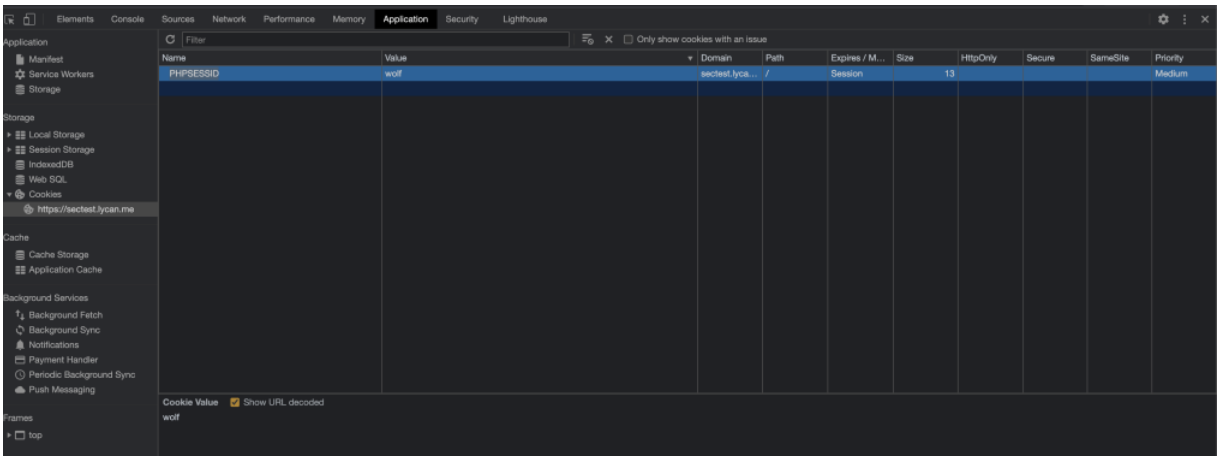
Closed naiagoesawoo opened this issue on Apr 20, 2021 · 4 comments

Labels Password Required for exploit Resolved Security:low

naiagoesawoo commented on Apr 20, 2021

**Issue Summary**
A session-fixation vulnerability exists within Pluck's administrative login system which can be abused to retain a valid login session even after an administrator has changed their password.

**Detailed Description**
It is possible to arbitrarily set the session ID of Pluck's "PHPSESSID" cookie. This cookie is used for maintaining administrative login sessions. This can be used in a session-fixation attack, for example, to sustain unauthorized access to the CMS after already gaining it through a primary vulnerability. Furthermore, Pluck does not expire sessions in a timely manner nor are sessions bound in any other way. This also allows an easier brute force attack, as it is possible to brute-force session IDs without rate-limits imposed by the normal login process.




**Reproduction Steps**

1. From Google Chrome, open the developer tools menu, navigate to: Application > Storage -> Cookies -> <PLUCK_DOMAIN>
2. Change the value of the "PHPSESSID" cookkie to an arbitrary value, such as "wolf".
3. Login to the pluck administrative panel, by visiting <PLUCK_DOMAIN>/login.php and login to the panel.
4. On a new browser, repeat steps 1 and 2.
5. On step 3, you will be given access without being prompted for administrative credentials.

**Impact**
After any primary exploit has occurred, the session fixation attack can be used in order to sustained unauthorized access. Because Pluck does not invalidate prior sessions after a password change, access can be sustained even after an administrator performs regular remediation attempts such as resetting their password.

BSteelooper added Password Required for exploit Security:low labels on Apr 21, 2021

BSteelooper added a commit that referenced this issue on Apr 26, 2021

fix for issue #99 2c3965d

BSteelooper commented on Apr 26, 2021 Contributor

Could you perform a retest with the latest dev version?

- Password change invalidates session
- logoff invalidates session
- no timer implemented yet

BSteelooper added the Resolved label on Apr 26, 2021

naiagoesawoo commented on Apr 26, 2021 Author

**Fixed**

1. I confirm that changing the admin password now properly invalidates an existing session.
2. I confirm that logging out properly validates an existing session

**Existing**

- It is still possible to arbitrarily set a session ID which Pluck will happily use -- eg. the original session fixation problem still exists.
- As you are already aware and stated, no timer has been implemented yet, so that is not something I checked for.

**BSteelooper** removed the Resolved label on Apr 26, 2021

**BSteelooper** added a commit that referenced this issue on Apr 29, 2021

`Fix for Session Fixation and Session expire #99` `33a6792`

**BSteelooper** commented on Apr 29, 2021 — Contributor

Could you perform a retest with the latest dev release?

Changes:

- fix for session fixation. every 30 minutes a new ID is generated
- fix for session not timing out. Session will timeout in 2 hours.

I might create a security options page where the session timeout is user manageble.

**BSteelooper** added the Resolved label on Apr 29, 2021

**naiagoesawoo** commented on Apr 30, 2021 — Author

Hello,

Your changes mitigate the possible damage done by exploiting the original session fixation vulnerability due to expiration of sessions. However, the vulnerability itself (the ability to set arbitrary session IDs) still exists. Your fix makes exploitation of this vastly more difficult as session IDs are regularly regenerated and sessions eventually expire.

Due to this, I consider the actual issue resolved as well :)

**naiagoesawoo** closed this as completed on Apr 30, 2021

Assignees

No one assigned

Labels

Password Required for exploit Resolved Security:low

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants