ether / etherpad-lite Public

<> Code   Issues 122   Pull requests 30   Discussions   Actions   Projects   ···

New issue

Jump to bottom

plain text password in the database #3421

Closed   **ukcb** opened this issue on Jul 10, 2018 · 10 comments · Fixed by #4435

Assignees	
Labels	security
Milestone	1.9

ukcb commented on Jul 10, 2018

I can see my admin password in plain text in the database.

```
sessionstorage:-FWbiguBVxp1_VWLERNNheogwak9aewi {"cookie":
{"path":"/","_expires":null,"originalMaxAge":null,"httpOnly":true,"secure":false},
"passport":{},"user":{"password":"Here is a plain text password!",
"is_admin":true,"username":"admin"}}
```

That must not happen!

v1.6.6

muxator added the **security** label on Jul 13, 2018

muxator added this to the **1.8** milestone on Aug 8, 2018

muxator mentioned this issue on Aug 8, 2018

Etherpad lite stores admin/user password in plain-text in the log file and in the database #2216
Closed

muxator modified the milestones: **1.7.5**, **1.8** on Feb 5, 2019

muxator modified the milestones: **1.8.0**, **1.8.1** on Dec 7, 2019

JohnMcLear commented on Mar 29, 2020   Member

Steps to replicate

1. Uncomment password section
2. Visit /admin
3. Cat var/dirty.db | grep YOURPASS

JohnMcLear commented on Mar 29, 2020   Member

PR in to fix.
#3782

JohnMcLear added the **Waiting on Testing** label on Mar 31, 2020

muxator pushed a commit to JohnMcLear/etherpad-lite that referenced this issue on Mar 31, 2020

`SessionStore: replace password with PASSWORD_HIDDEN when storing in db` ···   `8a0ee23`

muxator closed this as completed in `53f1260` on Mar 31, 2020

muxator pushed a commit to anttiviljami/etherpad-lite that referenced this issue on Apr 2, 2020

`SessionStore: replace password with PASSWORD_HIDDEN when storing in db` ···   `5c5b99f`

alasserr commented on May 15, 2020 • edited

Hi, the 5c5b99f commit makes etherpad not usable (at least with the Docker version) :

- at first login, the admin password is the one one's set it up from Docker variables environment
- but then the login is changed to "PASSWORD_HIDDEN"
  I'm not sure it only concerns Docker versions but this is a HUGE problem.

Using etherpad/etherpad (1.8.4) with postgresQL DB. From Docker. But I tried modifying the password directly in settings.json => same issue (first login OK, second > PASSWORD_HIDDEN) so I'm not sure it is 100% Docker related.

Edit : I confirm that when I **remove** the code added by **@JohnMcLear** on file src/node/db/SessionStore.js from lines 40 to 45 the password is now kept between sessions.

alasserr mentioned this issue on May 15, 2020

Security regression on password (PASSWORD_HIDDEN) from commit 5c5b99fc9ad33054fb0291b92084e00ae1e634ef #4016

Closed

JohnMcLear commented on May 15, 2020 Member

Weird. I'm not sure how doesn't affect non docker deployed versions tho?

JohnMcLear commented on May 15, 2020 • edited

Member

I can't even get the password prompt. I changed password and I'm not re-prompted..

```
jose@server:~/develop$ cat settings.json | grep pass | grep derp
      "password": "derp",
```

What are you doing to get the re-prompt?

I went through every step and maybe it's related to just setting the password through the password environment variable? If you set the password with settings.json are things okay? I'm not suggestion you should I'm just trying to isolate the cause / scope of impact.

muxator commented on May 15, 2020 Contributor

The bug reported by @alasser is **confirmed** and it's **not** related to Docker.
I should have been more thorough in #3782 (comment), sorry.

Let's move the discussion on #4016.

rhansen added a commit to rhansen/etherpad-lite that referenced this issue on May 16, 2020

`Revert "SessionStore: replace password with PASSWORD_HIDDEN when stor…` … 87fa37b

rhansen mentioned this issue on May 16, 2020

Revert "SessionStore: replace password with PASSWORD_HIDDEN when storing in db" #4023

Merged

muxator pushed a commit that referenced this issue on May 17, 2020

`Revert "SessionStore: replace password with PASSWORD_HIDDEN when stor…` … ✗ 901a3f3

rhansen commented on May 17, 2020 Member

This issue should be repoened (the fix that closed this issue was reverted).

rhansen added a commit to rhansen/etherpad-lite that referenced this issue on May 17, 2020

`Revert "SessionStore: replace password with PASSWORD_HIDDEN when stor…` … af3f278

muxator pushed a commit that referenced this issue on May 22, 2020

`Revert "SessionStore: replace password with PASSWORD_HIDDEN when stor…` … ✗ 6a0f73d

JohnMcLear reopened this on Jul 19, 2020

JohnMcLear removed the **Waiting on Testing** label on Jul 20, 2020

JohnMcLear modified the milestones: **1.8.3**, **1.9** on Sep 9, 2020

JohnMcLear commented on Oct 24, 2020 Member

@rhansen can you think of a way to solve this issue? It's one of the most critical for 1.9

rhansen commented on Oct 24, 2020 Member

@JohnMcLear Wasn't this fixed by #4178?

rhansen commented on Oct 24, 2020 • edited Member

Oh, this is different.

Hmm... I think we can store a shallow copy of the `settings.users[username]` object as `req.session.user` and remove the password field from that copy. I'll toss together a PR.

rhansen self-assigned this on Oct 24, 2020

rhansen mentioned this issue on Oct 24, 2020

webaccess: Remove user's password from session info #4435

Merged

JohnMcLear closed this as completed in #4435 on Oct 27, 2020

Assignees

rhansen

Labels

security

Projects

None yet

Milestone

1.9

Development

Successfully merging a pull request may close this issue.

webaccess: Remove user's password from session info
ether/etherpad-lite

5 participants