New issue

Jump to bottom

[server/auth] ensure safe returnTo param #2879

Merged AlexTugarev merged 1 commit into `master` from `at/returnTo` on Jan 13, 2021

Conversation 4 Commits 1 Checks 0 Files changed 1

AlexTugarev commented on Jan 13, 2021 • edited — Member

This PR closes an open redirect issue. AFAIK this is problem if an attacker would fake a Gitpod-like website and make people use links with redirects to it. The fake website could potentially ask user to enter sensitive information.

Allowing for Gitpod homepage URLs comes in parallel via #2692. ✔

how to test

0. log in & log out without errors.
1. should login and start a workspace: http://at-returnto.staging.gitpod-dev.com/api/login?host=github.com&returnTo=http://at-returnto.staging.gitpod-dev.com/#https://github.com/gitpod-io/django-locallibrary-tutorial
2. log out.
3. should open the dashboard: http://at-returnto.staging.gitpod-dev.com/api/login?host=github.com&returnTo=https://github.com/gitpod-io/gitpod/pull/2879

`[server/auth] ensure safe returnTo param` ✓ 5212a82

AlexTugarev modified the milestones: **February 2021**, **January 2021** on Jan 13, 2021

AlexTugarev requested a review from **csweichel** 2 years ago

csweichel approved these changes on Jan 13, 2021

View changes

csweichel left a comment — Contributor

works as advertised. LGTM.

AlexTugarev merged commit `8ca431f` into `master` on Jan 13, 2021

3 checks passed

View details

AlexTugarev deleted the `at/returnTo` branch 2 years ago

AlexTugarev commented on Jun 22, 2021 • edited by werft-gitpod-dev-com bot — Member Author

Thanks for reporting, **@payloadartist**!

Just created an update #4567 to be picked up for https://www.gitpod.io/changelog soon.

👍 1

payloadartist commented on Jun 22, 2021 • edited by werft-gitpod-dev-com bot

> Thanks for reporting, **@payloadartist**!
>
> Just created an update #4567 to be picked up for https://www.gitpod.io/changelog soon.

FYI you can credit me with my Twitter handle - https://twitter.com/payloadartist in the changelog if you want

As I already see someone credited for a security vuln

> — #4118↗ - Fix Cross Origin Websocket Access (credit: **Joern Schneeweisz**↗ from the GitLab Security Research Team).

payloadartist commented on Jun 22, 2021

This was assigned **CVE-2021-35206** btw

Thanks

Reviewers

csweichel ✓

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

January 2021

Development

Successfully merging this pull request may close these issues.

None yet

3 participants