

Annual pentest finding (2021) - Autocomplete Enabled

Location

- <https://gitlab.com/users/password/new> (user_email)
- https://gitlab.com/users/sign_in (user_login)
- https://gitlab.com/users/sign_in (user_password)
- https://gitlab.com/users/sign_up (new_user_first_name)
- https://gitlab.com/users/sign_up (new_user_last_name)
- https://gitlab.com/users/sign_up (new_user_username)
- https://gitlab.com/users/sign_up (new_user_email)
- https://gitlab.com/users/sign_up (new_user_password)
- <https://gitlab.com/users/confirmation/new> (user_email)
- <https://gitlab.com/groups/new#import-group-pane> (bulk_import_gitlab_access_token)

Impact

Sensitive data such as usernames, passwords, and access tokens could be retrieved locally via the browser's history if the local user's system is compromised.

Description

The autocomplete function, implemented by many popular browsers, allows a user the option of storing form field values so that the browser can automatically populate the same fields of a form later. Although this feature can be a convenience for users of the application, it creates a security risk, as sensitive user data such as username, password, and access tokens were stored locally and may be recovered if an attacker is able to gain access to the workstation, or through exploitation of a cross-site scripting vulnerability. Gitlab.com did not set the autocomplete attribute to OFF on form fields containing sensitive data.


Recommendation

Forms containing sensitive information should have the autocomplete option disabled on both the form and the sensitive fields.^{16, 17} For example:

```
<form autocomplete="off">
...
<input type="text" name="user_email" autocomplete="off">
<input type="text" name="user_login" autocomplete="off">
...
</form>
```

Although the recent versions of most of modern browsers do not respect the autocomplete attribute for the fields of type "password", it is still recommended that this practice should be followed as users could have changed their browsers' policies to respect this attribute.

Edited 1 year ago by [James Ritchey](#)

 Drag your designs here or [click to upload](#).

Tasks  0



































No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items  0

Link issues together to show that they're related or that one is blocking others. [Learn more](#).

Activity



-  **James Ritchey** added `priority: 4` `severity: 4` scoped labels [1 year ago](#)
-  **James Ritchey** changed the description [1 year ago](#)
-  **James Ritchey** added `security` label [1 year ago](#)
-  **GitLab SecurityBot** added `security-group-missing` `security-triage-appsec` labels [1 year ago](#)
-  **GitLab Bot**  **@gitlab-bot** · [1 year ago](#) Maintainer
👉, please can you add a [type label](#) to this issue to help with [issue discovery in issue reports](#).
-   **GitLab Bot**  added `auto updated` label [1 year ago](#)
-  **Nikhil George** **@ngeorge1** · [1 year ago](#) Developer
Dup of [#27125 \(closed\)](#)
-  **Nikhil George** added `group authentication and authorization` `devops manage` scoped labels [1 year ago](#)
-  **Nikhil George** removed `security-group-missing` label [1 year ago](#)
-  **Nikhil George** removed `security-triage-appsec` label [1 year ago](#)
-  **GitLab Bot**  **@gitlab-bot** · [1 year ago](#) Maintainer
Setting label(s) `Category:Authentication and Authorization` `section dev` based on ~"group::access".
-   **GitLab Bot**  added `Category:Authentication and Authorization` label [1 year ago](#)
-   **GitLab Bot**  added `section dev` scoped label [1 year ago](#)
-  **Michelle Gill** added `FY22 Q3` scoped label [1 year ago](#)
-  **Rohit Shambhuni** **@rshambhuni** · [1 year ago](#) Developer
This can be fixed on canonical.
-  **Rohit Shambhuni** changed due date to October 06, 2021 [1 year ago](#)
-  **Rohit Shambhuni** added `security-backlog` `review-complete` scoped label [1 year ago](#)
-  **Rohit Shambhuni** changed due date to February 24, 2022 [1 year ago](#)
-  **Liam McAndrew** added `bug vulnerability` scoped label [1 year ago](#)
-  **Gary Holtz** assigned to [@garyh](#) [11 months ago](#)
-  **Liam McAndrew** added `frontend` label [11 months ago](#)
-  **Hannah Sutor** mentioned in issue [gitlab-org/manage/general-discussion#17440 \(closed\)](#) [10 months ago](#)
-  **Matt Nohr** added `workflow` `awaiting security release` scoped label [10 months ago](#)
-  **Hannah Sutor** mentioned in issue [gitlab-org/manage/general-discussion#17455 \(closed\)](#) [9 months ago](#)
-  **Dominic Couture** added `type bug` scoped label [9 months ago](#)
-  **Hannah Sutor** mentioned in issue [gitlab-org/manage/general-discussion#17462 \(closed\)](#) [9 months ago](#)



Andrew Kelly [@ankelly](#) · 9 months ago

Developer

This was fixed in 14.7.1 and assigned CVE-2022-0167

Edited by [Andrew Kelly](#) 9 months ago



Andrew Kelly closed 9 months ago



Hannah Sutor changed milestone to [%14.7](#) 9 months ago



Vitor Meireles De Sousa made the issue visible to everyone 5 months ago

Please [register](#) or [sign in](#) to reply