

New issue

[Jump to bottom](#)

Security Issue - Stored XSS (Attack Tree) #36

Closed alestorm980 opened this issue on Feb 8 · 1 comment

Labels bug

alestorm980 commented on Feb 8 • edited

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

We will assign the cve id [CVE-2022-23051](#) to this issue but the information will be released after the vulnerability is patched. Attached below are the links to our responsible disclosure policy.

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

Bug description

PeteReport **Version 0.5** allows an authenticated admin user to inject persistent javascript code while adding an 'Attack Tree' by modifying the svg_file parameter.

CVSSv3 Vector:

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

CVSSv3 Base Score:

4.8

Steps to reproduce

1. Create a new Report.
2. Create a new Finding for the Report.

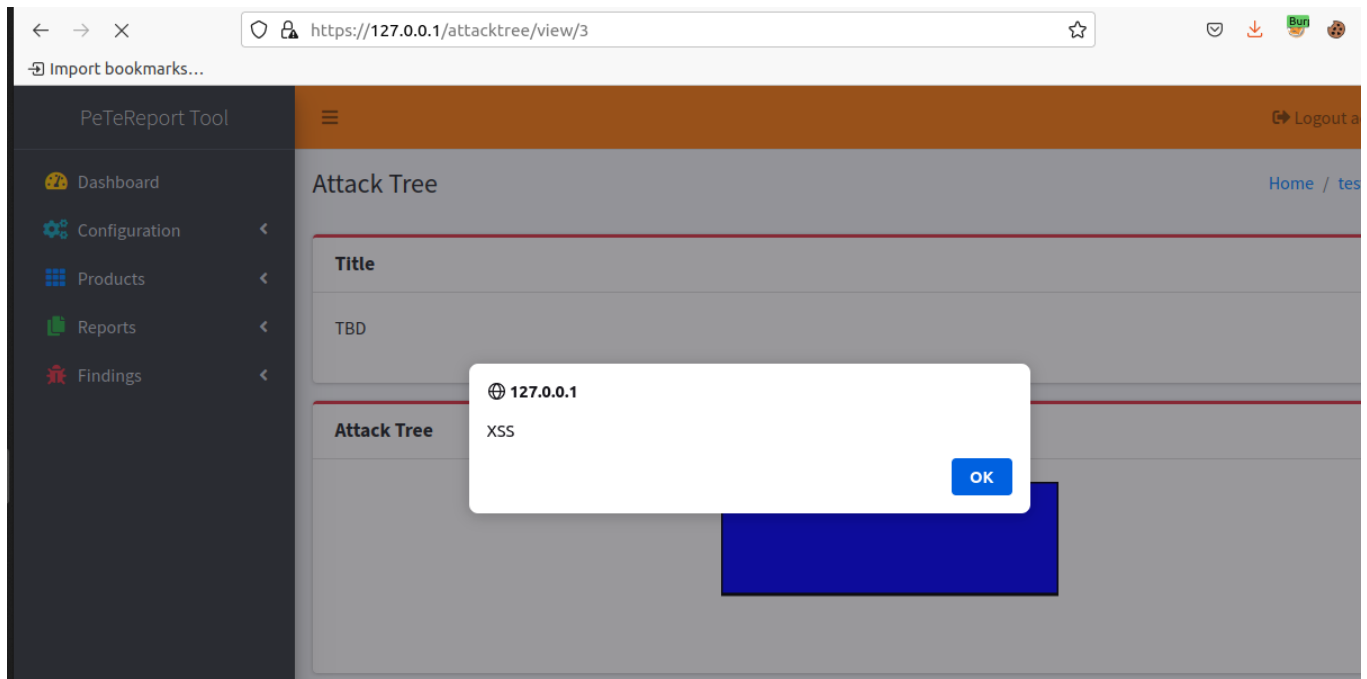
3. Go to 'Reports' > 'All Reports'.
4. Click on 'View' in the last created record.
5. Go to 'Attack Trees'.
6. Click on 'Add Attack Tree'.
7. Select your Finding and click on 'Save and Finish'.
8. Intercept the request and insert javascript code inside the svg_file parameter.

```
<script type="text/javascript">
  alert("XSS");
</script>
```

9. If a user visits the attack tree the javascript code will be rendered.


Screenshots and files

The screenshot displays the PeTeReport Tool web interface. The browser address bar shows the URL `https://127.0.0.1/report/attacktree/2`. The interface has a dark sidebar on the left with navigation links: Dashboard, Configuration, Products, Reports, and Findings. The main content area is titled 'hi Attack Trees' and includes a yellow 'Add Attack Tree' button. Below this, a table titled '0 Attack Tree' is shown, which is currently empty. The table has columns for 'Attack Tree', 'Finding', and 'Actions'. Above the table, there are options to 'Copy', 'CSV', 'Excel', 'PDF', 'Print', and 'Column visibility', along with a search bar. The table footer indicates 'Showing 0 to 0 of 0 entries' and includes 'Previous' and 'Next' navigation buttons. The footer of the page contains the copyright notice 'Copyright © 2021 PeTeReport. All rights reserved.' and the version number 'Version 0.5'.



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 Buen trabajo!

Should be fixed in the last commit, take a look and let me know if do you find more issues.

Muchas gracias :)

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

Assignees

No one assigned

Labels

`bug`

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

