

New issue

[Jump to bottom](#)

# Security Issue -Stored XSS (markdown) #35

✓ Closed alestorm980 opened this issue on Feb 7 · 1 comment

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** allows an authenticated admin user to inject persistent javascript code inside the markdown descriptions while creating a product, report or finding.

### 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

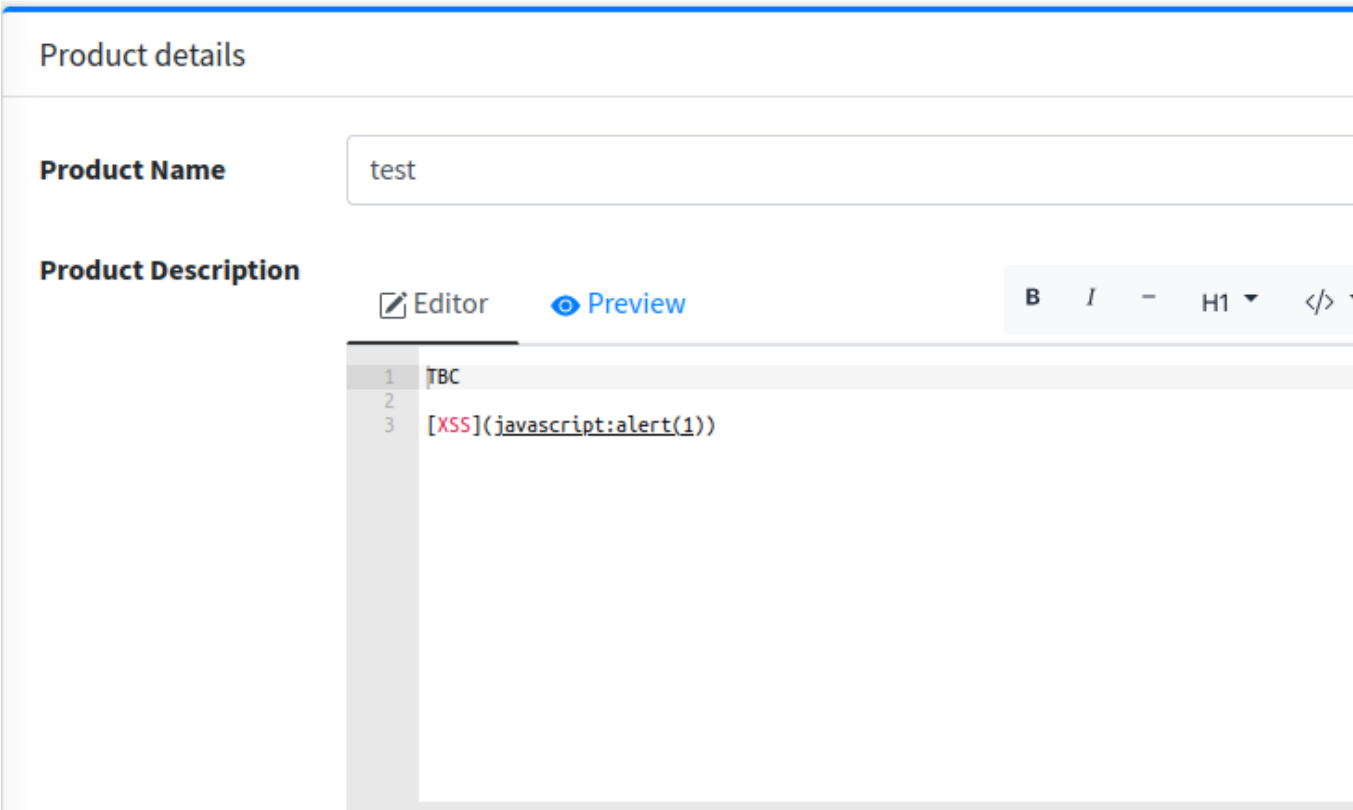
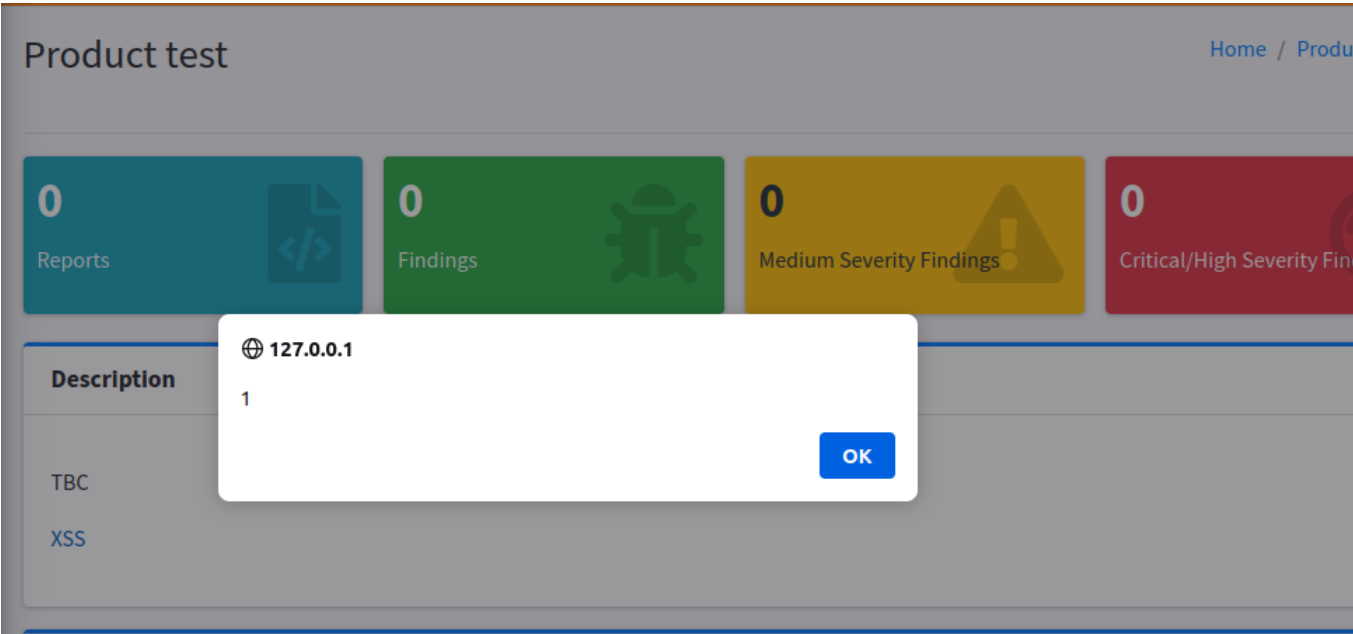
## Steps to reproduce

1. Click on 'Add Product'.
2. Insert the following PoC inside the product description.

```
[XSS](javascript:alert(1))
```

- 3. Click on 'Save Product'
- 4. If a user visits the product and click on the link in the description the Javascript code will be rendered.

## Screenshots and files




## 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, that happen to me to trust in markdown  . 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

