PeTeReport 0.5 - Stored XSS (Attack Tree)

Summary

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

Affected versions	Version 0.5
Fixed versions	Version 0.7
State	Public
Release date	2022-02-23

Vulnerability

Kind	Stored cross-site scripting (XSS)
Rule	010. Stored cross-site scripting (XSS)
Remote	Yes
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
Exploit available	No
CVE ID(s)	CVE-2022-23051

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

Proof of Concept

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.

System Information

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

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

Mitigation

An updated version of PeteReport is available at the vendor page.

Credits

The vulnerability was discovered by Oscar Uribe from the Offensive Team of `Fluid Attacks.`

References

Vendor page https://github.com/1modm/petereport

Issue https://github.com/1modm/petereport/issues/36

Timeline

- 2022-02-08
  Vulnerability discovered.
- 2022-02-08
  Vendor contacted.
- 2022-02-09
  Vendor replied acknowledging the report.
- 2022-02-09
  Vulnerability patched.
- 2022-02-23
  Public Disclosure.

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

Services

Continuous Hacking

One-shot Hacking

Comparative

Solutions

DevSecOps

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Blog

Certifications

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

Documentation

Contact

Copyright © 2022 Fluid Attacks. We hack your software. All rights reserved.