



attacks

[Home](#) / [Advisories](#) / [Money Transfer Management System 1.0 DOM-Based XSS](#)

Money Transfer Management System 1.0 – DOM-Based XSS

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 1.0
State	Public
Release date	2022-03-15

Vulnerability

Kind	DOM-Based Cross-Site Scripting (XSS)
Rule	<u>371. DOM-Based Cross-Site Scripting (XSS)</u>
Remote	Yes
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
Exploit available	No
CVE ID(s)	<u>CVE-2022-25221</u>



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. Send the following URL to a victim `http://127.0.0.1/mtms/admin/?page=xss';alert('XSS');//`
2. If a victim visits the link the JavaScript code will be triggered.

System Information

- Version: Money Transfer Management System version 1.0.
- Operating System: Linux.
- Web Server: Apache
- PHP Version: 7.4

- Database and version: MySQL

Exploit

There is no exploit for the vulnerability but can be manually exploited.

Mitigation

By 2022-03-15 there is not a patch resolving the issue.

Credits

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



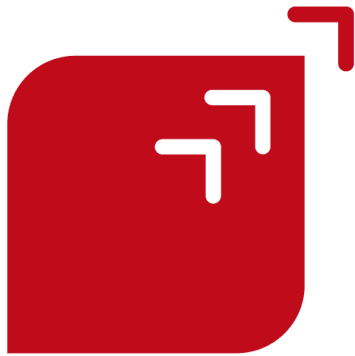
This website uses cookies

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

- ✓ 2022-02-15
Vulnerability discovered.
- ✓ 2022-02-15
Vendor contacted.
- ✓ 2022-03-15
Public Disclosure.



Services



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](#)

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Blog

Certifications

Partners

Careers

Advisories

FAQ

Documentation

Contact

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

[Service Status](#) - [Terms of Use](#) - [Privacy Policy](#) - [Cookie Policy](#)



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](#)