

Html Injection Reflected in Login Page in froxlor/froxlor

0

✓ Valid

Reported on Nov 4th 2022

Description

HTML Injection is a vulnerability in which the attacker can inject malicious html content in the login webpage.

Proof of Concept

#Navigate to:

[https://demo.froxlor.org/index.php?showmessage=4&customermail=%22%3Cmarquee%3E%3Cscript%3Ealert\('XSS'\)%3C/script%3E%3C/a%3E](https://demo.froxlor.org/index.php?showmessage=4&customermail=%22%3Cmarquee%3E%3Cscript%3Ealert('XSS')%3C/script%3E%3C/a%3E)

Impact

They can manipulate a trustful but vulnerable website against HTML Injection. They can create a fake webpage by using stored HTML Injection or they achieve XSS. After achieving XSS threat actors can steal cookies, hijack accounts, steal credentials and other sensitive information. Or an attacker can use tag `click here to get gift` it attack phishing to redirect the victim to another website.

References

- <https://huntr.dev/bounties/a3c506f0-5f8a-4eaa-b8cc-46fb9e35cf7a/>

CVE

CVE-2022-3869

(Published)

Vulnerability Type

CWE-94: Code Injection

Severity

Medium (6.5)

Chat with us

Medium (6.5)

Registry

Other

Affected Version

latest

Visibility

Public

Status

Fixed

Found by



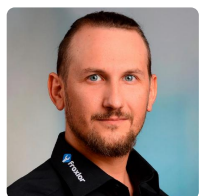
Hakiduck

@mike993

pro



Fixed by



Michael Kaufmann

@d00p

maintainer

This report was seen 598 times.

We are processing your report and will contact the **froxlor** team within 24 hours. 22 days ago

Hakiduck modified the report 22 days ago

We have contacted a member of the **froxlor** team and are waiting to hear back 21 days ago

Michael Kaufmann validated this vulnerability 21 days ago

I've patched the referenced report 9 days ago, yesterday was the release, why report this today?

Hakiduck has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Chat with us

the researcher's credibility has increased. 7/

Michael Kaufmann marked this as fixed in 0.10.38.2 with commit 3f10a4 21 days ago

Michael Kaufmann has been awarded the fix bounty ✓

This vulnerability has been assigned a CVE ✓

Michael Kaufmann published this vulnerability 21 days ago

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us