# Improper Restriction of Rendered UI Layers or Frames in getgrav/grav-plugin-admin

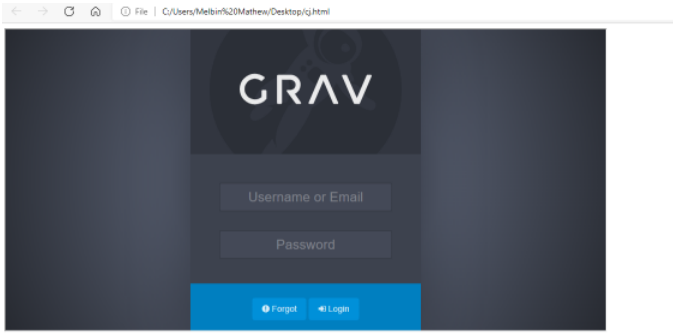
0

Valid Reported on Aug 23rd 2021

## ✍️ Description

It can be possible to perform a clickjacking attack due to the lack of frame restrictions. The application does not set the response header X-Frame-Options: DENY.

## 🦹 Proof of Concept




## 💥 Impact

According to PortSwigger references, it is possible for a page controlled by an attacker to load the website within an iframe. This will enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery and may result in unauthorized actions. 📍 Location index.php#L1 📝 References Clickjacking (UI redressing)

## References

- Clickjacking (UI redressing)

CVE
CVE-2021-3799
(Published)

Vulnerability Type
CWE-1021: Improper Restriction of Rendered UI Layers or Frames

Severity
Medium (5.4)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

Melbin Mathew Antony
@melbinkm
amateur

This report was seen 436 times.

We have contacted a member of the **getgrav/grav-plugin-admin** team and are waiting to hear back a year ago

**Melbin Mathew Antony** modified the report a year ago

Andy Miller a year ago

This was fixed in Admin v1.10.20

**Andy Miller** validated this vulnerability a year ago

**Melbin Mathew Antony** has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

**Andy Miller** a year ago

I can't set this to "Confirm Fix" because the issue was created against getgrav/grav but the problem/fix is actually in getgrav/grav-plugin-admin repository. Please change the repo.

https://github.com/getgrav/grav-plugin-admin/commit/853abfbbd3c14a0a601c941dcfaa3858b6283b69

**Jamie Slome** a year ago Admin

@andy - I have updated the repository for this report to reflect `grav-plugin-admin` .

Feel free to confirm the fix, and we can get a CVE published here for you.

Cheers! 🎉

A **getgrav/grav-plugin-admin** maintainer marked this as fixed with commit **853abf** a year ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

**Jamie Slome** a year ago Admin

CVE published! 🎉

Sign in to join this conversation