

Gila CMS is an open source content management system and a website builder for your business. It is a content management system made in PHP and MySQL.

CVE-2021-37777

Problem Type: The application is vulnerable to Insecure Direct Object Reference.

The vulnerability was found in Gila CMS version 2.2.0.

Description: The Gila CMS website was found vulnerable to Insecure Direct Object Reference. Thumbnails uploaded by one site owner are visible by another site owner just by knowing the other site name and fuzzing for picture names. This leads to sensitive information disclosure.

Proof of Concept - [\[Link\]](#)

CVE-2021-39486

Problem Type: The application is vulnerable to cross site scripting attack. The vulnerability is a Stored XSS Using Unrestricted File Upload.

The vulnerability was found in Gila CMS version 2.2.0.

Description: A Stored XSS via Malicious File Upload exists in Gila CMS version 2.2.0. An attacker can use this to steal cookies, passwords or to run arbitrary code on a victim's browser.

Proof of Concept - [\[Link\]](#) [\[Link\]](#)



Contact
navidkagalwalla@hotmail.com



Created by Navid Kagalwalla ©2020