

Web shell via File upload functionality in Home owners collection management system

0 stars 0 forks

Star

Notifications

<> Code

Issues

Pull requests

Actions

Projects

Security

Insights

main

Go to file



lohyt Update README.md ...

on Mar 26 6

[View code](#)

README.md

CVE-2022-25016

Web-shell-via-file-upload-in-hocms

Web shell via File upload functionality in Home owners collection management system

Description: Web shell via file upload functionality in Home Owners Collection Management System from Sourcecodester website.

[Vulnerability Type] Web shell via file upload functionality.

[Vendor of Product] <https://www.sourcecodester.com/>

[Affected Product Code Base] Student Attendance Management System

[Affected Component] http://localhost/student_attendance/index.php?page=site_settings

[Attack Type] Remote

[Impact Information Disclosure] true

[Attack Vectors] Steps to reproduce: Navigate to the url http://localhost/hocms/admin/?page=system_info Download the webshell from <https://raw.githubusercontent.com/artyuum/Simple-PHP-Web-Shell/master/index.php> and save it with php extension. Upload the php file that has been saved in the above step and click on update. Right click on the broken image and click on "Open link in new tab" The web shell gets executed and attacker can run arbitrary os commands on the server.

[Discoverer] M Lohith

Releases

No releases published

Packages

No packages published