

VULNERABILITY ASSESMENT

SOJOSPECT

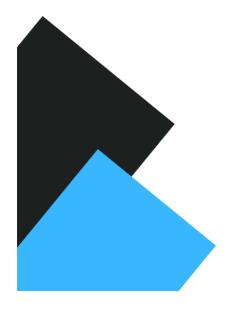
v1.0.0

Scanned by: admin

17/08/2023

Scanned on:

http://chmsdemo.greenfossil.com/



GREEN FOSSIL PTE LTD

Table of Contents

1. Executive Summary2
2. Scan Results2
3. Our Findings2
4. Risk Assessment2
Critical Severity Vulnerability2
High Severity Vulnerability3
Medium Severity Vulnerability3
Low Severity Vulnerability3
5. Recommendations
Remediation4

1. Executive Summary

This report provides an overview of the Vulnerability Test Assessment conducted for Green Fossils' Church Management System, addressing the OWASP Top 10 security risks. The assessment aims to identify and evaluate vulnerabilities in the company's web application and infrastructure which enables informed decision-making to enhance the overall security posture.

Scanned by: admin

Ommitted Scans:

unrestricted_file_upload, bruteforce, Forced_browsing, injection,

Each risk category was examined thoroughly and vulnerabilities were identified and classified based on their severity. The key findings and recommendations from the assessment are summarized below. The vulnerabilities identified in the Vulnerability Test Assessment Suite for Green Fossils' digital assets pose significant risks to the company's operations, reputation, and bottom line. Ignoring or delaying the remediation of these vulnerabilities can lead to a range of detrimental business impacts.

2. Scan Results

The raw scan results will be provided upon delivery.

3. Our Findings

The results from the credentialed patch audit are listed below.

4. Risk Assessment

This report identifies security risks that could have significant impact on mission-critical applications used for day-to-day business operations.

Critical Severity	Medium Severity	Low Severity
0	1	3

High Severity Vulnerability

0 were unique high severity vulnerabilities. High severity vulnerabilities are often harder to exploit and may not provide the same access to affected systems.

Severity Vulnerability Type Checked at

Medium Severity Vulnerability

1 were unique medium severity vulnerabilities. These vulnerabilities often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner but are not as urgent as the other vulnerabilities.

Vulnerability	Description	Solution
Session	User interactions on the website can be replayed by	Ensure that data transferred is
Replay	attackers.	encrypted.

Low Severity Vulnerability

3 were unique low severity vulnerabilities. These vulnerabilities are not as serious as other vulerabilities but might be used by attackers in rare cases.

Vulnerability	Description	Solution
No robots_txt	robots.txt is a necessary standard used by websites to communicate with	Add the
	web crawlers and other automated agents (like search engine bots) about	robots_txt in the
	which parts of the site should not be crawled or scraped.	website
		directory.
Overinformative	Error messages are present that might provide data for attackers to use:	Use less
error		informative error
		messages.
Cookie attribute	'secure' value on cookie is not set to True or 'httpOnly' value is not set to	Set cookie values
is not secure.	True.	to be secure
		and/or httpOnly.

5. Recommendations

Recommendations in this report are based on the available findings from the credentialed patch audit. Vulnerability scanning is only one tool to assess the security posture of a network. The results should not be interpreted as definitive measurement of the security posture of the network. Other elements used to assess the current security posture would include policy review, a review of internal security controls and procedures, or internal red teaming/penetration testing.

Additional Resources

External sources are listed below which can help fix issues:

OWASP Top Ten Software Testing Help

TALK TO US

(65) 67751133 contactus@sp.edu.sg