VULNERABILITY ASSESSMENT

SOJOSPECT

v1.0.0

Scanned by: admin

23/08/2023

Scanned on: http://chmsdemo.greenfossil.com/

GREENFOSSIL PTE LTD

Table of Contents

1. Executive Summary

This report provides an overview of the Vulnerability Test Assessment conducted for Greenfossils' 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:
cookie_attribute_checking, 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 Greenfossils' 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 Replay	User interactions on the website can be replayed by attackers.	Ensure that data transferred is 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 web crawlers and other automated agents (like search engine bots) about which parts of the site should not be crawled or scraped.	Add the robots_txt in the website directory.
Login Page Overinformative error	Error messages are present that might provide data for attackers to use in the login page.	Use less informative error messages.
Overinformative error	Error messages are present that might provide data for attackers to use in these urls: ['http://chmsdemo.greenfossil.com//user/profile/28/contact/phone/new', 'http://chmsdemo.greenfossil.com//user/profile/28/contact/email/new', 'http://chmsdemo.greenfossil.com//user/profile/28/credential/new', 'http://chmsdemo.greenfossil.com//user/profile/28/language/new']	Use less informative error messages.

5. Recommendations

Recommendations in this report are based on the available findings from the credentialed patch audit. Vulnerability scanning is one of the many tools 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 - A standard awareness document for developers and web application security
Software Testing Help - A guide to OWASP Top 10 Security Vulnerabilities and mitigation strategies

TALK TO US

(65) 67751133

contactus@sp.edu.sg