SafeBank

Steven.Tester@STechSolutions.com

Table of Contents

Executive Summary

Executive Summary

S'Tech Solutions was engaged by Safe Bank to perform an application Penetration test on the Safe Bank Web application. This report aims to outline the investigation and highlight the overall security posture of the Safe Banks application.

This executive summary presents the outcomes of a recent penetration test conducted on the web application, focusing on identifying vulnerabilities that could compromise its security. The findings are categorized based on the application's security posture, compliance with standards, and areas requiring additional scrutiny.

FINDINGS

1. **No Detected Vulnerabilities:** The examination concluded that, within the allocated timeframe, no vulnerabilities were detected, highlighting the efficacy of existing security measures.
2. **Strong Security Posture:** The application demonstrated robust security practices, indicative of proactive efforts to maintain a secure environment.
3. **Compliance with Cyber Essentials:** Initial assessments suggest compliance with Cyber Essentials standards, although further evaluation is recommended for thorough confirmation.

OBJECTIVE

The primary goal was to identify potential security vulnerabilities and compliance issues from an external perspective, simulating a real-world attack scenario without prior internal knowledge of the application.

Methodology and Scope

Scope

The following scope was provided by the client before testing commenced.

Internet access is provided so you can download your preferred tools, please refrain from using the labs to conduct any other activity other than its intended use. The infrastructure includes 3 networks. The only "publicly accessible" (within the confines of the lab) is the firewall and the Safebank website which you will find on

- 10.0.0.3.

Testing was performed from a Black box perspective and included areas included in the OWASP v.4 testing guide.

The credentials provided below were to enable the tester to access the testing environment.

- Kali Linux - kali:kali
- Windows 10 - Student:password

No credentials were provided to access the application its self.

Methodology

Over a concise 24-hour period, STech Solutions employed the following methodologies:

Automated Scanning: Utilizing state-of-the-art tools for rapid identification of common vulnerabilities. Expert Analysis: Involving experienced cybersecurity professionals in assessing the automated scan results. Compliance Verification: Checking adherence to the Cyber Essentials framework.

Vulnerability Overview

In the course of this penetration test **1 Info** vulnerabilities were identified:

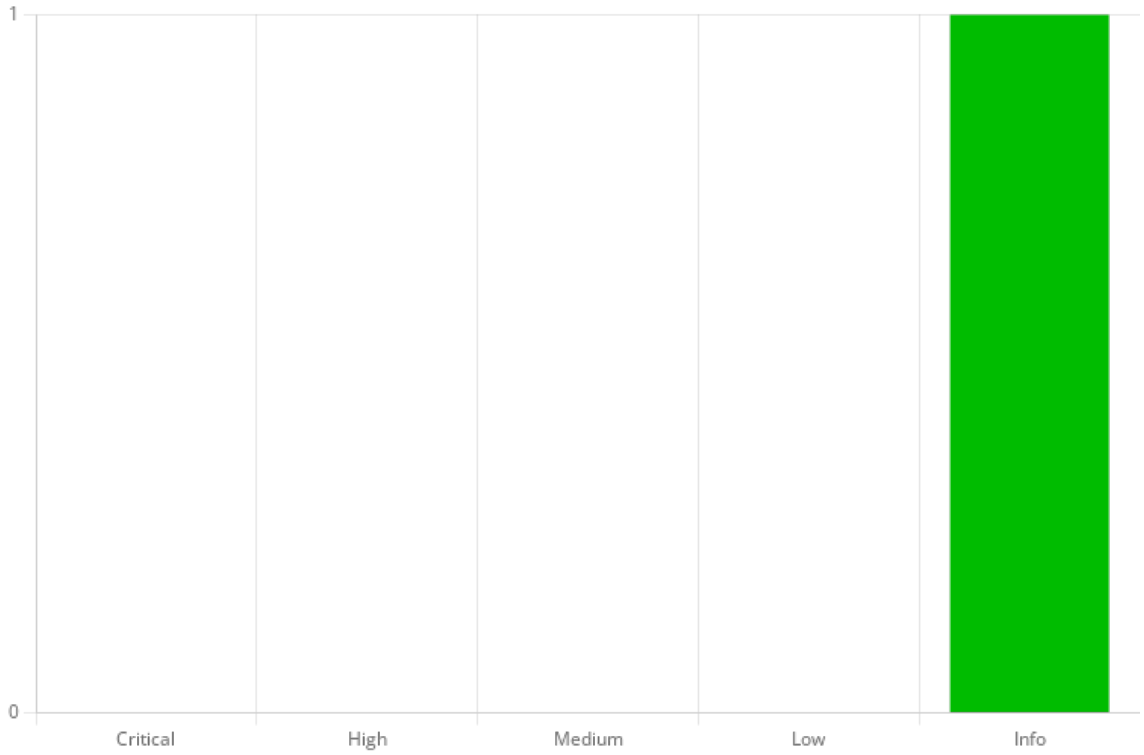

Figure 1 - Distribution of identified vulnerabilities

A tabular overview of all vulnerabilities identified:

Vulnerability	Criticality
Informational only - WordPress Contact Form 7 5.3.1 Shell Upload	**Info**

A list of all vulnerabilities including a brief description:

1. Informational only - WordPress Contact Form 7 5.3.1 Shell Upload (Info: 0.0)

Affects: CV upload functionality
The Information contained within the summary is intended for use only on a retest to aid the testers in assessing if there is a workaround for the Contact Form 7 vulnerability.

Vulnerability Details

1. Informational only - WordPress Contact Form 7 5.3.1 Shell Upload

Remediation Status:
Criticality: Info
CVSS-Score: 0.0
Affects: CV upload functionality

Overview

The Information contained within the summary is intended for use only on a retest to aid the testers in assessing if there is a workaround for the Contact Form 7 vulnerability.

Description

Technical Description of WordPress Contact Form 7 5.3.1 Shell Upload Vulnerability

The WordPress Contact Form 7 plugin is a widely used tool for creating and managing contact forms on WordPress websites. However, version 5.3.1 of the plugin was found to be vulnerable to a critical security issue known as a "Shell Upload" vulnerability.

Vulnerability Overview:

The Shell Upload vulnerability in Contact Form 7 version 5.3.1 allows an attacker to upload and execute malicious PHP files on the server. This vulnerability arises due to insufficient input validation and sanitization in the file upload functionality of the plugin.

Exploitation Process:

1. **File Upload Functionality:** The Contact Form 7 plugin includes a feature that allows users to upload files through contact forms. This functionality is intended for legitimate use cases such as uploading images or documents.
2. **Lack of Validation:** However, version 5.3.1 fails to adequately validate the file types being uploaded. As a result, an attacker can upload a file with a malicious PHP payload, disguised as an image or other benign file type.
3. **Execution of Arbitrary Code:** Once the malicious file is uploaded to the server, the attacker can then trigger its execution by accessing the file through its URL. This allows the attacker to execute arbitrary code within the context of the web server, potentially leading to complete compromise of the WordPress installation.

Impact:

The impact of this vulnerability is severe, as it grants attackers the ability to execute arbitrary code on the server. Depending on the server's configuration and permissions, an attacker could achieve various malicious objectives, including:

- **Server Compromise:** By uploading and executing a web shell, an attacker can gain unauthorized access to the server, allowing for further exploitation and data exfiltration.

ttackers may deface the website by modifying or replacing existing files with malicious content.
- **Data Theft:** Access to the server could enable attackers to steal sensitive data, such as user credentials, personal information, or proprietary business data.

Recommendation

Additional Information

- https://secure.wphackedhelp.com/blog/contact-form-7-plugin-vulnerability-exploit/

List of Changes

Version	Date	Description	Author

Disclaimer

DISCLAIMER:

STech Solutions provides penetration testing services with the utmost professionalism and expertise. Our team of skilled professionals conducts comprehensive assessments to identify vulnerabilities within your systems, networks, and applications. However, it is essential to understand the following disclaimers and terms of service (TOS) before engaging our services:

1. **Limitations of Testing:** Penetration testing is a simulated attack on your systems and networks to identify potential vulnerabilities. While we strive to conduct thorough assessments, it is impossible to guarantee that all vulnerabilities will be discovered or that our findings encompass every potential risk.
2. **Scope Limitations:** Our penetration testing services are conducted within the agreed-upon scope, as defined in the engagement contract. Any systems, networks, or applications outside of this scope may not be assessed or included in our findings.
3. **Third-Party Systems:** STech Solutions is not responsible for third-party systems, services, or applications that may interact with or be integrated into your infrastructure. Any vulnerabilities or risks associated with third-party components are outside the scope of our assessments.
4. **False Positives and Negatives:** While we employ advanced tools and methodologies, our findings may include false positives or false negatives. It is essential to verify and validate all identified vulnerabilities to prioritize remediation efforts effectively.
5. **No Warranty:** STech Solutions provides penetration testing services "as is" without any warranty, express or implied. We do not guarantee the security or invulnerability of your systems, networks, or applications, nor do we accept liability for any damages resulting from our services.
6. **Client Responsibilities:** Clients are responsible for implementing recommended remediation measures based on our findings. Failure to address identified vulnerabilities may expose your organization to security risks and potential breaches.
7. **Confidentiality:** We treat all information obtained during penetration testing engagements with the utmost confidentiality. However, clients should ensure that appropriate measures are in place to protect sensitive data and intellectual property.

TERMS OF SERVICE (TOS):

1. **Engagement Agreement:** The engagement agreement outlines the scope, objectives, and terms of the penetration testing engagement. Clients must review and agree to the terms before commencement of testing.

s are outlined in the engagement agreement and must be adhered to by the client. Failure to fulfill payment obligations may result in suspension or termination of services.
3. **Access and Permissions:** Clients must provide necessary access permissions, credentials, and authorization for STech Solutions to conduct penetration testing. Failure to provide adequate access may hinder the effectiveness of our assessments.
4. **Reporting:** Upon completion of testing, STech Solutions provides a detailed report outlining findings, recommendations, and remediation strategies. Clients are responsible for reviewing and acting upon the contents of the report in a timely manner.
5. **Intellectual Property:** All intellectual property rights associated with our penetration testing reports and findings remain with STech Solutions unless otherwise agreed upon in writing.
6. **Indemnification:** Clients agree to indemnify and hold harmless STech Solutions from any claims, damages, or liabilities arising from the use of our penetration testing services or reliance on our findings.

By engaging STech Solutions for penetration testing services, clients acknowledge that they have read, understood, and agreed to the terms and disclaimers outlined herein. For further clarification or inquiries regarding our services, please contact our team.

Imprint

STech Solutions
Main Street 1337 | Tester Row
London | UK