Requester Inc

Application Scanning Report

July 20, 2023

Submitted by: User

Contents

Document Information....3
Contacts....4
Scope....4
Accounts Utilized....4
Executive Summary....5
Conclusions....5
Tools used....5
Sample of relevant vulnerabilities reported by Scanners.....6

Document Information

This document contains information retrieved by an independent contractor using the Hackybara platform. It is provided to Requester Inc in accordance with the terms of any agreement between the independent contractor and Requester Inc. Information within this document contains sensitive information related to Requester Inc and should not be released to another vendor, business partner or contractor without written approval from Requester Inc. Furthermore, this document may not be copied, distributed, reproduced, or retained by the independent contractor without approval from Requester Inc.

The contents of this document does not constitute legal advice. The independent contractor using Hackybara's platform offer of services or deliverables that relate to compliance, litigation, or other legal interests is not intended as legal counsel and should not be taken as such.

Contacts

Hackybara Platform Scanning Tester		
Name	**Role**	**Contact Information**
John Jacob	Hackybara Independent Contractor (HIC)	Johnjacob1899@gmail.com

Requester Inc		
Name	**Role**	**Contact Information**
Bob Cyber	Application Coordinator	bobcyber@gmail.com
Alice Cyber	Security Officer	Aliceccyber@gmail.com

Scope

The Scanning was performed against the following Requester Inc application:

Address/URL	Visibility
Requesterinc.com	Requester Inc external network

Accounts Utilized

The following accounts were used during the assessment:

Account	Account Type
BOBUSER	User
BOBADMIN	Administrator
ALICEREQUESTER	Business Account
ALICEBUILDER	Developer

Executive Summary

Requester Inc contacted Hackybara to perform vulnerability scans of its Blog application. A vulnerability scan is intended to identify security risks, vulnerabilities, needed best security practices, impact of vulnerabilities, and document all security findings. The assessment took place between July 1st and July 20th, 2023, and was conducted remotely.

During the assessment, HIC identified sixteen (16) findings, including four (4) high risk vulnerabilities. Please see a sample of discovered vulnerabilities below. **Examine the attached CSV/XML/HTML or Database file that was included with this report for more information and full scan results.**

Conclusions

Overall, vulnerability scanners utilized were able to discover multiple serious vulnerabilities. Further testing should be conducted to determine the severity of the discovered vulnerabilities and to test for false positives.

Tools used

- **BurpSuite Active Scanner**
- **Nessus**
- **Nikto**
- **Openvas**

Sample of relevant vulnerabilities reported by Scanners.

Finding Title	Scanner Discovered on	Severity Rating	Location	CVSS Score
1.SQL Injection	Nessus	HIGH	https://www.requesterinc.com/SQLexamplepage.php?	8.9
2. Reflected Cross-Site Scripting	Nessus/Burp	HIGH	https://www.requesterinc.com/crossexamplepage.php?	7.2
3. Unencrypted Communications	Nessus/Burp /Openvas	HIGH	https://www.requesterinc.com/Unexamplepage.php ?	7
4. Weak Authentication	Nesus/Burp /Openvas	HIGH	https://www.requesterinc.com/weakexamplepage.php?	7
5. Apache Tomcat XML Parser Vulnerability	Burp/ Openvas	MEDIUM	https://www.requesterinc.com/Tomcatexamplepage.php?	4.6
6. Insufficient Cache Control Headers	Nessus/Burp /Openvas/ Nikto	LOW	https://www.requesterinc.com/poodleexamplepage.php?	2.5

Please Examine the attached CSV/XML/HTML or Database file that was included with this report for more information and full scan results.