Redama LLC

Standard Pen Test Report

Standard Pen Test Penetration Test Report Results

Report creation date: **May 23, 2024**

Testing period: **March 22, 2022** to **March 31, 2023**

Prepared by: **William Keeling, ase@bugcrowd.com**

bugcrowd

Table of contents

Executive Summary

Redama LLC engaged Bugcrowd, Inc. to perform a Standard Pen Test which took place from March 22nd, 2022, through March 31st, 2023.

The purpose of this engagement was to identify security vulnerabilities in the assets listed under the Targets and Scope section of the report. Once identified, each vulnerability was rated for technical impact defined in the Findings Summary section of the report.

To perform this test, our researcher leveraged several common tools to help identify and exploit vulnerable findings in the environment. Manual testing of the scope was performed, evaluating the assets for weaknesses as per the Bugcrowd methodology. In support of this, active scanners and scripts were used in an attempt to identify any commonly found, known vulnerabilities.

At the time of this report, **3 vulnerabilities** were identified, including:

- **3 critical**
- **0 severe**
- **0 moderate**
- **0 low**
- **0 informational**

At this time, **Bugcrowd has rated the overall risk to Redama LLC as Critical** based on the observed vulnerabilities. Our rating is based on the severity of the findings disclosed within this report.

It is recommended that Redama LLC focus on critical and severe issues first, with moderate, low, and informational findings being fixed once all severe and critical issues are remediated.

Bugcrowd recommends that all critical, severe, and moderate severity findings are retested once remediation activities are completed.

If not already implemented, Bugcrowd recommends taking the following high-level actions to further improve the overall security posture of the organization:

- Implement a secure development lifecycle such as Microsoft Secure Development Lifecycle (MSDL).
- Implement a static code analysis (SAST) tool into the development lifecycle to minimize the introduction of vulnerabilities in code.
- Provide regular secure development training to developers to ensure that they are aware of secure development practices and emerging threats.

The continuation of this report contains technical details of the specific vulnerabilities that were discovered throughout the Standard Pen Test Pen Test engagement. It should be noted that many of the details, including comments, up-to-date remediation.

This report is just a summary of the information available and is a 'snapshot' in time of the state for the tested environment.

All details of the engagement's findings — comments, code, and any researcher provided remediation information — can be found in the Bugcrowd Platform: https://tracker.bugcrowd.com

Engagement details

Scope of testing

Prior to penetration test launching, Bugcrowd worked with Redama LLC. to define the rules of the engagement, commonly known as the engagement brief, which includes the scope of work.

The following targets were considered explicitly in-scope for testing:

- api: http://*.macgyverhuel.co
- api: www.newtarget1.com
- website: http://*.mayert.net
- network: example.com/testing12345
- website: http://*.secrettarget.com
- ios: http://bharat.com

The following items are explicitly out-of-scope:

- website: Webpacker
- api: http://*.macgyverhuel.co

All details of the engagement scope and full brief can be reviewed in each of the respective Engagement Settings pages found on the Bugcrowd Platform.

Findings table

The following table lists all validated findings identified through manual testing grouped by Vulnerability Rating Taxonomy (VRT):

Vulnerability Rating Taxonomy (VRT)	Title	Priority
Broken Access Control (BAC)	F001 - IDOR in example.com	P1
Broken Authentication and Session Management	F002 - New submission	P1
Server Security Misconfiguration	F003 - UAT to check for submission	P1

Broken Access Control (BAC)

P1

F001 - IDOR in example.com

Bug URL:
www.example.com

Description:
This is an emergency

Vulnerability Rating Taxonomy (VRT):
Broken Access Control (BAC) > Insecure Direct Object References (IDOR)

CVSS rating (v3):
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N [7.5]

Submission ID:
bfae643c-ed4c-423b-b033-178577fee7cf

Broken Authentication and Session Management

P1

F002 - New submission

Bug URL:
xyz.com

Description:
Description

Vulnerability Rating Taxonomy (VRT):
Broken Authentication and Session Management > Second Factor Authentication (2FA) Bypass

CVSS rating (v3):
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N [6.5]

Submission ID:
3036cda6-4b7b-477f-aa6d-806fdac0dd2e

Server Security Misconfiguration

P1

F003 - UAT to check for submission

Description:
Overview of the Vulnerability:

Default credentials are credentials that are set as default by the manufacturer or supplier of hardware and software products. These credentials often have Administrator privileges. An attacker can take advantage of default credentials and login to administrative accounts using wordlists of usernames and passwords found online, which may give them the authority to change the state of the application or users' accounts.

Business Impact:

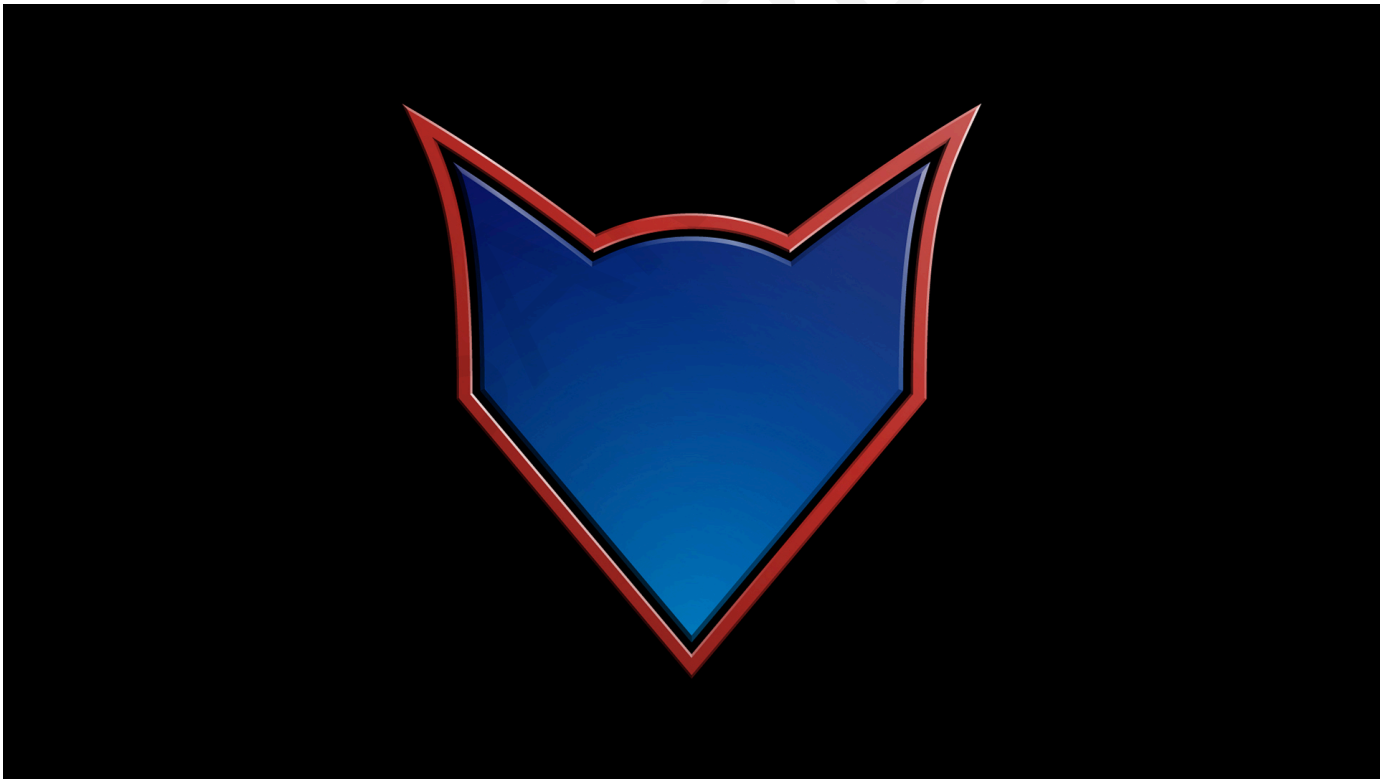
Default credentials can result in repetitional damage and indirect financial loss for the business through the impact to customers' trust in the application's security of user accounts. If an attacker successfully guesses default credentials it can lead to user account compromise and data exfiltration.

Steps to Reproduce:

- Use a browser to navigate to: {{URL}}
- Enter the username and password combination {{Username:DefaultPassword}}
- Observe the successful login to an Admin account

Proof of Concept (PoC):

The screenshot(s) below demonstrates the default credentials:



Screen%20Recording%202022-11-28%20at%202.10.57%20PM.mov

Vulnerability Rating Taxonomy (VRT):

Server Security Misconfiguration > Using Default Credentials

CVSS rating (v3):

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L [9.4]

Submission ID:
ebe14822-64a2-47e9-9340-1ba250ab3b66

Reporting and Methodology

By leading with a best-in-class testing approach, Bugcrowd's methodology provides enhanced risk reduction while supporting critical compliance initiatives. A review of these standards follows.

Reviewed Organizational Methodology Standards:

- PCI DSS Requirement 11.2, 11.3.1, 11.3.3, 11.3.4
- NIST 800-115 - Technical Guide to Information Security Testing and Assessment 2.1 "Information Security Assessment Methodology"
- Open Source Security Testing Methodology Manual (OSSTMM)
- Penetration Testing Execution Standard (PTES)

In order to create a complete testing methodology, Bugcrowd has pulled from the following industry standard operational methodologies:

- OWASP Testing Guide (OTG)
- Web Application Hacker Handbook Methodology (WAHHM)
- Others where applicable (SANS Top 25, CREST, WASC, PTES)

Appendix A - Risk and priority key

The following key is used to explain how Bugcrowd rates valid vulnerability submissions and their technical severity. As a trusted advisor Bugcrowd also provides common "next steps" for program owners per severity category.

Technical severity	Example vulnerability types
P1 **Critical** Critical severity submissions (also known as "P1" or "Priority 1") are submissions that are escalated to Bugcrowd as soon as they are validated. These issues warrant the highest security consideration and should be addressed immediately. Commonly, submissions marked as Critical can cause financial theft, unavailability of services, large-scale account compromise, etc.	• Remote Code Execution • Vertical Authentication Bypass • XML External Entities Injection • SQL Injection • Insecure Direct Object Reference for a critical function
P2 **Severe** Severe severity submissions (also known as "P2" or "Priority 2") are vulnerability submissions that should be slated for fix in the very near future. These issues still warrant prudent consideration but are often not availability or "breach level" submissions. Commonly, submissions marked as Severe can cause account compromise (with user interaction), sensitive information leakage, etc.	• Lateral authentication bypass • Stored Cross-Site Scripting • Cross-Site Request Forgery for a critical function • Insecure Direct Object Reference for an important function • Internal Server-Side Request Forgery
P3 **Moderate** Moderate severity submissions (also known as "P3" or "Priority 3") are vulnerability submissions that should be slated for fix in the major release cycle. These vulnerabilities can commonly impact single users but require user interaction to trigger or only disclose moderately sensitive information.	• Reflected Cross-Site Scripting with limited impact • Cross-Site Request Forgery for an important function • Insecure Direct Object Reference for an unimportant function
P4 **Low** Low severity submissions (also known as "P4" or "Priority 4") are vulnerability submissions that should be considered for fix within the next six months. These vulnerabilities represent the least danger to confidentiality, integrity, and availability.	• Cross-Site Scripting with limited impact • Cross-Site Request Forgery for an unimportant function • External Server-Side Request Forgery
P5 **Informational** Informational submissions (also known as "P5" or "Priority 5") are vulnerability submissions that are valid but out-of-scope or are "won't fix" issues, such as best practices.	• Lack of code obfuscation • Autocomplete enabled • Non-exploitable SSL issues

VRT

Bugcrowd's Vulnerability Rating Taxonomy

More detailed information regarding our vulnerability classification can be found at: https://bugcrowd.com/vrt

Appendix B - Vulnerability details

This section outlines the full submission data for each valid finding. These findings are unaltered from their original state from the researcher. Due to the competitive nature and gamification of crowd-sourced security assessments, some typos or grammar errors may occur. Each finding is headlined with the submission title and priority followed by more detailed vulnerability information based on the type of finding submitted. Several other fields may appear based on the context and VRT classification selected by a researcher.

Such details may include the following:

Title

A brief summary of the vulnerability.

Bug URL

This is the full URL/URI of where the vulnerability took place

Description

This section appears above the "Reference Number" as a free form area for the researcher to describe the context of the submission. The full HTTP(S) request that triggered the vulnerability is normally in this field, including all its associated headers and cookie information.

Target

The target that is vulnerable.

Vulnerability Rating Taxonomy (VRT)

The Vulnerability Rating Taxonomy (https://bugcrowd.com/vrt) is the baseline guide used for classifying technical severity.

CVSS rating(v3)

The CVSS vector string for this submission, if provided, and the score calculated from that vector string

Jira ID

This is the ID to a customer Jira ticket associated with a vulnerability submission.

Custom fields

Some customers add extra attributes to vulnerability submissions, for example, "Product Start Version" or "Product End Version".

Submission ID

Submission ID is visible to customers and researchers.

bugcrowd

Bugcrowd Inc.
300 California St
Suite 220
San Francisco, CA 94104
(888)361-9734

May 23 2024

Closing Statement

Introduction

This report reflects testing of Redama LLC's targets between the dates of **March 22nd, 2022** to **March 31st, 2023** . The purpose of this assessment was to identify security issues that could adversely affect the integrity of Redama LLC. The assessment was performed under the guidelines provided in the statement of work between Redama LLC and Bugcrowd. This document provides a high-level overview of the testing performed and the test results.

Pen Test Portfolio Overview

The Bugcrowd Pen Test portfolio provides organizations with the power of the Crowd, through two unique engagement styles designed to fit a range of security workflows and objectives. Max Pen Test (MPT), Plus Pen Test (PPT), Standard Pen Test (SPT), and Basic Pen Test (BPT) are all powered by the Bugcrowd Platform, enabling rapid setup, launch, and real-time results.

While Bugcrowd offers both continuous and on-demand penetration testing options, it is important to note that this document represents a point-in-time evaluation of security posture. Security threats and attacker techniques evolve rapidly, and the results of this assessment are not intended to represent an endorsement of the adequacy of current security measures against future threats. This document contains information in summary form and is therefore intended for general guidance only; it is not intended as a substitute for detailed research or the exercise of professional judgment. The information presented here should not be construed as professional advice or service.

Testing Methods

This security assessment leveraged researchers that used a combination of proprietary, public, automated, and manual test techniques throughout the assessment. Commonly tested vulnerabilities include code injection, cross-site request forgery, cross-site scripting, insecure storage of sensitive data, authorization/authentication vulnerabilities, business logic vulnerabilities, and more.

Summary of Findings

The summary of Bugcrowd's findings are as follows:

Severity	Number of findings
Critical	3
Severe	0
Moderate	0
Low	0
Informational	0