VONAHI SECURITY

External Web Application Pentest
EXECUTIVE SUMMARY

CloudRadial

May 02, 2023

Copyright

Confidentiality

This document contains company confidential information of a proprietary and sensitive nature. As such, this document should be afforded the security and handling precautions that a confidential document warrants. This document should have a controlled distribution to relevant parties only and should not be copied without written permission. Vonahi Security treats the contents of a security audit as company confidential material and will not disclose the contents of this document to anyone without written permission.

Assessment Project Team

Below is a list of contacts that were involved in this engagement. Should you have any questions pertaining to the content of this document or any project and non-project-related items, please feel free to reach out to the necessary project contacts.

Primary Point of Contact	
Name:	Prashant Khare
Title:	Director of Application Security
Office:	+91(837) 899-0772
Email:	prashant@vonahi.io

Executive Summary

CloudRadial has requested the assistance of Vonahi Security to perform a comprehensive security assessment to assist with evaluating the cyber risks presented within the tested environment(s). The objective of this engagement was to determine if any identified threats could be used to mount an attack against the organization that could lead to the disclosure of sensitive information or access to critical information systems.

Included in this Executive Summary report is a high-level overview of the results that were observed during this assessment. A copy of more specific information pertaining to technical findings and remediation details are documented within the Technical Report as well as the Vulnerability Tracking Report.

Engagement Scope of Work

Prior to beginning the assessment, Vonahi Security and CloudRadial agreed to a scope of work to define the specific assessment phases. The table below outlines the engagement scope of work and details entailed within each assessment phase that was conducted as part of this engagement.

Assessment Component	Assessment Phases
External Web Application Pentest	During this phase, an assessment is performed against the web application environment to attempt identifying security threats that could potentially lead to access to sensitive and/or confidential data or systems. These attacks include OWASP Top 10 checks as well as well as the use of automated and manual application scanning tools.

Engagement Statistics

The information below displays overall statistics that were recorded as part of this engagement. Following the statistics, Vonahi Security has summarized all of the threats identified.

External Web Application Pentest

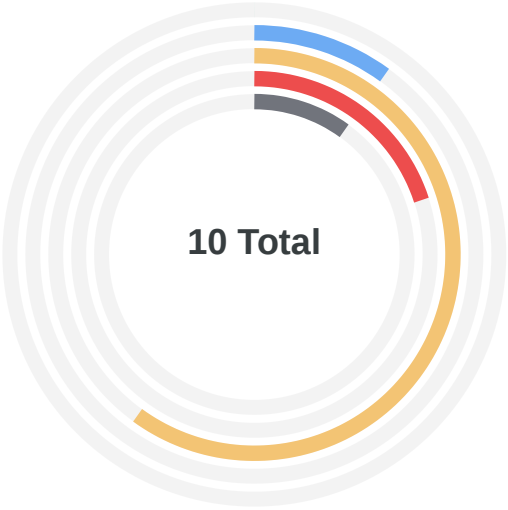
The information below provides a high-level overview of the assessment results recorded as part of this engagement. Following this section is a summary of all the threats identified and their potential risk to your organization.

Overall Severity Ranking	
	**ASSESSMENT SCHEDULE**  **Mon, May 01, 2023** 08:00 PM ET Immediate remediation or mitigation is required. Exploitation of identified vulnerabilities require minimal effort from an attacker and pose a significant threat. A successful attack could result in unauthorized access to systems and/or valuable data.

Engagement Results Charts

To help CloudRadial understand the severity of the threats identified during testing, Vonahi Security has included an over-all summary chart below that displays a comparison of the report findings as well as the vulnerabilities that were discovered.

External Web Application Pentest Results



PenTest Findings

The following chart displays the overall severity of the report findings that were documented as part of the penetration testing efforts.

1	CRITICAL	2	HIGH	6	MEDIUM
1	LOW	0	INFO		

Engagement Results Summary

To summarize the results, Vonahi Security has grouped all of the findings from the penetration test into rollup findings. These rollup findings can be used to quickly determine the root cause of the issues identified in the technical report. By implementing a remediation strategy for the findings based on the rollup issues identified below, CloudRadial's security posture would be greatly reduced.

External Web Application Pentest

Category	Summary
Configuration Deficiencies	Configuration weaknesses were identified that could potentially lead to a successful compromise of systems and/or data within the tested environment. Although some of the configuration weaknesses may be exploitable in limited circumstances, the potential impact of a successful attack could be relatively high.
Application	Configuration issues were identified within the tested application environment that could potentially lead to an attack against the application and/or its visitors. Application security issues typically stem from insecure coding practices or bugs that disclose sensitive or valuable information. By exploiting such security vulnerabilities, it may be possible for an attacker to gain unauthorized access to data and/or the underlying server hosting the application.

Remediation Roadmap

For each assessment conducted, Vonahi Security provided a remediation roadmap to help CloudRadial understand the issues within the respective environment and the overall remediation strategies that should be implemented to resolve the issues identified during the penetration test. It should be noted that the remediation strategies below apply to multiple issues identified within the technical report and can greatly reduce the overall attack surface once successfully implemented.

External Web Application Pentest

Issue	Remediation Strategy
Configuration Deficiencies	Implement or improve a security configuration baseline that adheres to security best practices and industry standards such as National Institute of Standards and Technology (NIST). This security configuration baseline should ensure that no services and/or systems are deployed within the environment until a thorough configuration review has been performed.
Application	Review the technical report for specific details pertaining to each application configuration issue. The organization should also consider adhering to web application security best practices documented by standards such as the OWASP Foundation.

Consultant Information

ALTON JOHNSON

Founder & Principal Security Consultant

Alton Johnson is the Founder and Principal Security Consultant for Vonahi Security where he focuses on building the future of offensive cybersecurity consulting services through automation. With over a decade of experience as a security consultant and over 10 industry-related certifications, Alton has helped CISOs at hundreds of small to Fortune 500 organizations requiring unique, modern-day approaches solve today's most complex security challenges. He regularly conducts research to identify ways to help organizations combat ever-changing cyber threats through efficient, cost effective, and non-traditional security assessments.

Prior to Vonahi Security, Alton has worked at several large and small cybersecurity consulting firms as a Principal Security Consultant. Throughout his professional career, he has performed hundreds of security assessments for organizations ranging from small businesses to Fortune 10 including: CVS HQ, Dollar General, Apple, Nintendo, NFL, Groupon, Charlotte Rouse, Chico's, and the Vitamin Shoppe. He is proficient with performing both traditional security assessments, such as network, physical, and application penetration testing, as well as advanced security assessments, such as red team engagements.

Notable Accomplishments

Alton has developed several penetration testing tools and scripts that are used widely within the information security industry. He has made some of these open-source tools available on GitHub, while others have been integrated in Kali Linux (formerly known as Backtrack Linux) and the Metasploit Framework. Kali Linux is a highly popular operating system specifically designed for penetration testers, while Metasploit is the industry's leading open-source penetration testing framework.

The penetration testing tools that were developed by Alton were written in multiple scripting languages, which provides him the ability to quickly and efficiently develop exploits and scripts that can be used for network traffic analysis, protocol/service fuzzing, exploitation, and quick completion of extremely time-consuming network-related tasks.

Certifications & Training

Alton successfully obtained some of the industry's most challenging and respected security certifications, including Offensive Security Certified Expert (OSCE), Offensive Security Certified Professional (OSCP), as well as eLearnSecurity's Certified Professional Penetration Tester (eCPPT). He also regularly attends information security conferences and has spoken at DerbyCon as well as local communities.

About Vonahi Security

WE AUTOMATE HACKING.

Vonahi Security is a cybersecurity company that developed vPenTest, a SaaS platform that automates network penetration testing, a valuable service that mimics the way a hacker would target an organization to obtain confidential information.

The penetration testing marketing is currently serviced by outsourced consultants providing manual testing. The high cost makes penetration testing primarily a once a year test that leaves major gaps in security. Through automation, our platform delivers continuous testing at a fraction of the cost of an outsourced consultant. We eliminate inefficiencies, increase the scope, free up budget for other cybersecurity initiatives, and ultimately make the organization more secure. Vonahi Security is headquartered in Atlanta, GA.

WHAT WE LOVE TO DO

- Network Penetration Testing
- Automated Penetration Testing
- Web Application Penetration Testing
- Mobile Application Penetration Testing
- Breach Simulation
- Social Engineering
- Phishing Assessments
- Red Team Operations

HELLO WORLD.
MEET MODERN
SECURITY.

CONTACT US

www.vonahi.io
info@vonahi.io
1.844.VONASEC (866-2732)
@vonahisec