****

Penetration Testing Report for Pied Piper

**November 3, 2021 ⠂CONFIDENTIAL**

**Description**

This document details the process and result of a penetration test performed by Allsafe Cybersecurity from October 1, 2021 to November 1, 2021.

**Author**

AJ Dumanhug, CEH, ECSA, CRTP, CRTE, OSCP, OSWE, PNPT, eCDFP  
Lead Penetration Tester  
Allsafe Cybersecurity

***Date Published: November 3, 2021  
Version: 1.0***

# Table of Contents

[**Table of Contents**](#_qwrpwdk16i1i) **2**

[**Confidentiality Statement**](#_x542ipozr7l0) **3**

[**Disclaimer**](#_5oolloqwxx00) **3**

[**Contact Information**](#_338g0f57bzx7) **3**

[**Severity Ratings**](#_vvo4742ln7qi) **4**

**Penetration Testing Methodology 5**

[**Scope**](#_eer12jpqsvg3) **6**

[**Scope Exclusions**](#_68tlejrv4a8p) **6**

[**Executive Summary**](#_tbf6skxk2gb) **7**

[**Technical Findings**](#_rj93hvith4ld) **8**

[Improper Restriction of Excessive Authentication Attempts in /admin (Critical)](#_i2kc93mqaag3) 8

[**Last Page**](#_5r0olhbdmnuu) **11**

# 

# 

# 

# 

# 

# 

# Confidentiality Statement

This document contains information that is proprietary and confidential. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Pied Piper and Allsafe Cybersecurity.

Pied Piper may share this document with auditors under non-disclosure agreements (NDAs) in order to demonstrate compliance with penetration test requirements.

# Disclaimer

Penetration Testing is considered as a snapshot in time. The technical findings and general recommendations are based on the information gathered during the penetration testing and do not include any changes or modifications made outside of the time frame.

# Contact Information

The following are the point of contact (POC) of respective teams.

| **Full name** | **Title** | **Contact Information** |
| --- | --- | --- |
| **Pied Piper** | | |
| Dinesh Chugtai | Chief Technology Officer | dinesh@piedpier.com |
| **Allsafe Cybersecurity** | | |
| Allan Jay Dumanhug | Lead Penetration Tester | aj@allsafe.xyz |

# Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

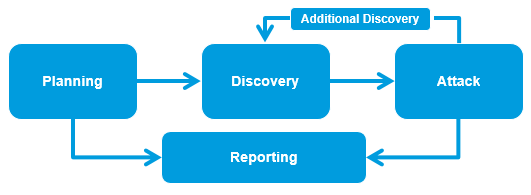
| **Severity** | **CVSS 3.1 Score Range** | **Definition** |
| --- | --- | --- |
| **Critical** | 9.0 - 10.0 | Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately. |
| **High** | 7.0 - 8.9 | Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible |
| **Moderate** | 4.0 - 6.9 | Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved. |
| **Low** | 0.1 - 3.9 | Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window. |
| **None** | 0 | No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation. |

# 

# 

# Penetration Testing Methodology

Allsafe Cybersecurity followed the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment. *(Note that the methodology really depends on your team)*



Phases of penetration testing activities include the following:

* Planning - Customer goals are gathered and rules of engagement obtained.
* Discovery - Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
* Attack - Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
* Reporting - Document all found vulnerabilities and exploits.

# Scope

| Asset Type | Details |
| --- | --- |
| Website Application | https://piedpiper.com |
| API | https://api.piedpiper.com |

# Scope Exclusions

As per client request, Allsafe Cybersecurity did not perform any of the following attacks during testing:

* Denial of Service (DoS) attacks against production infrastructure
* Phishing / Social Engineering attacks

# Executive Summary

Pied Piper engaged with Allsafe Cybersecurity to conduct an extensive penetration testing from October 1, 2021 to November 1, 2021 in order to determine its exposure to a targeted attack. All activities were conducted in a manner that simulated an external user or malicious actor.

The following are the goals of the penetration test as request by Pied Piper are:

* Identify if an external user or malicious actor could penetrate Pied Piper’s defenses.
* Determine if there are any information exposure
* Assess the current security posture of the website application

All the testing performed is based on the [OWASP Web Security Testing Guide (v4.1)](https://owasp.org/www-project-web-security-testing-guide/v41/) with prioritization to OWASP’s [Top 10 Web Application Security Risks](https://owasp.org/www-project-top-ten/) and [API Security Top 10 2019](https://owasp.org/www-project-api-security/).

Allsafe Cybersecurity team discovered 1 vulnerability that had a CVSS score of 7.0 or higher, rangking either high or critical. These security vulnerabilities should be prioritized by Pied Piper for fixing as it represents the greatest immediate risk to Pied Piper.

The following tables illustrate the vulnerabilities found by severity per asset.

| **Asset** | **None** | **Low** | **Medium** | **High** | **Critical** | **Total** |
| --- | --- | --- | --- | --- | --- | --- |
| https://piedpiper.com | 0 | 0 | 0 | 0 | 0 | 0 |
| https://api.piedpiper.com | 0 | 0 | 0 | 0 | 1 | 1 |

# Technical Findings

### Improper Restriction of Excessive Authentication Attempts in /admin (Critical)

| Severity | Critical (9.8) - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| --- | --- |
| Affected Scope | https://api.piedpiper.com/admin |
| Weakness Type | [CWE-307](https://cwe.mitre.org/data/definitions/307.html) |
| Tools Used | Ffuf and BurpSuite Intruder |
| **Details**  PiedPiper’s admin panel is accessible publicly to any user. This panel does not have any rate limit or account lockout protection to prevent brute force attacks.  **Proof of Concept**  We initially performed directory enumeration to identify accessible pages or directories on the website application. Screenshot below shows that tool discovered an accessible admin panel.    Upon accessing the admin panel, we noticed that Pied Piper uses ‘admin’ as a username after performing fingerprinting.    We then fired up BurpSuite to brute force the login form using the Intruder tool. After a few seconds, we already found the password.    The Admin credential is the following:  Username: admin Password: Admin123  **Impact**  This could allow attackers to compromise the admin account by performing a simple brute force attack.  **Recommendation**   1. Have a security policy that will require employees to come up with a strong password by following the password requirement set forth by the company. 2. Do not allow users to use ‘admin’ username. 3. Implement account lockout to prevent attackers from continuously performing brute-force attack and/or password spraying. 4. If possible, implement and enforce Two-Factor Authentication (2FA) to prevent full access to the account.   **References**   * https://cwe.mitre.org/data/definitions/307.html | |



# Last Page