Pen-Testing a Payment Provider

sdmay21-06@iastate.edu
Client/Advisor: Ben Blakely
Priyanka Kadaganchi, Max Solaro, KayAnne Bryant, Matthew Maiman
Ryan Anderson, Jacob Conn, and Nathan Key

Motivation

Problem Statement

Dwolla, a payment systems provider, has requested a red team penetration test of their Sandbox web applications, as well as their publicly available API.

Solution

- Execute a penetration test against requested environments.
- Develop methodology for testing within the defined scope and rules of engagement.
- Report vulnerabilities found with a ranking of vulnerabilities based on risk to Dwolla's systems.

Relevant Standards

- OWASP Foundation. "API Security Top 10 2019."
- OWASP Foundation. "Web Application Security Top 10 2019."
- National Institute of Standards and Technology "Technical Guide to Information Security Testing and Assessment."
- PTES Team. "The Penetration Testing Execution Standard."

Main Deliverables

Executive Summary

- Give insight into vulnerabilities to non-technical staff
- Explain impact of vulnerabilities found from a business-oriented perspective
- Provide a problem-oriented solution guide

Technical Report

- Give in-depth technical explanation of vulnerabilities found
- Provide each vulnerability exploit path, risk rating, and remediation steps

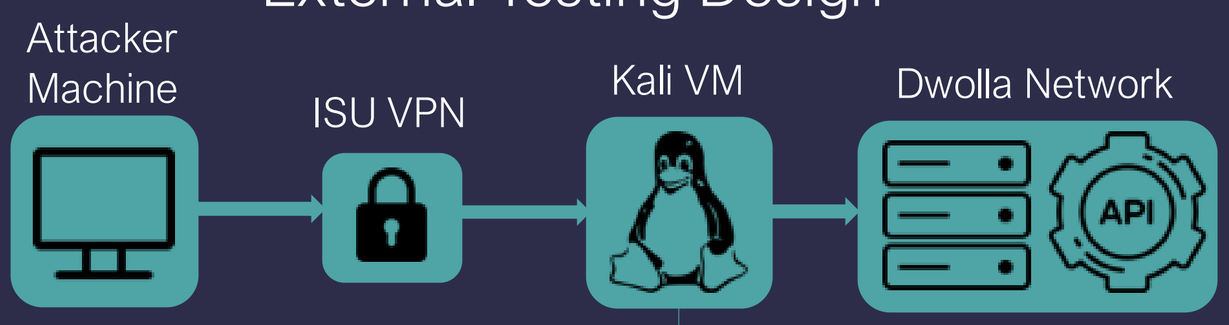
Technical Details

Open-Source Tools Used

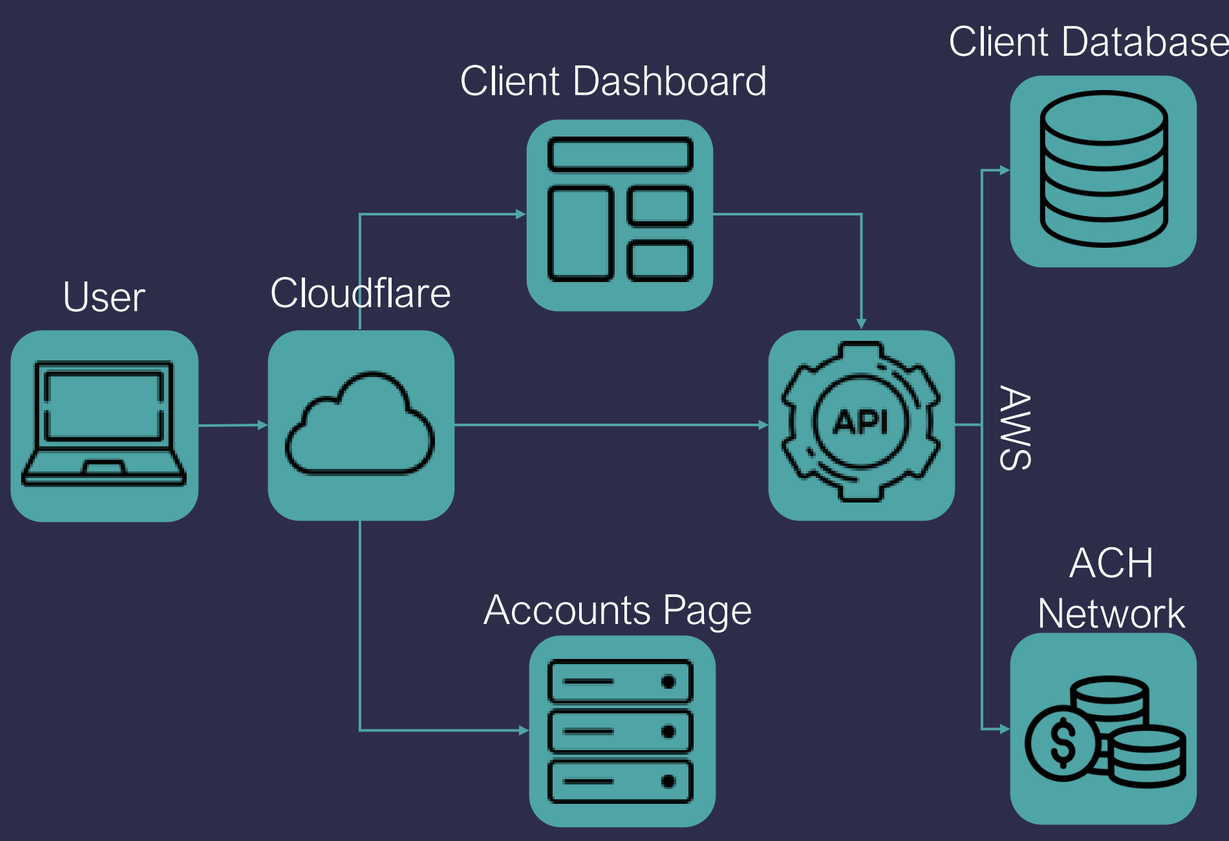
- Kali Linux
- OWASP-Zap
- BurpSuite Community Edition
- Dwolla SDK
- Postman
- Firefox
- Python

Conceptual Designs

External Testing Design



Dwolla Network Design



Operational Requirements

Scope

- Test only the sandbox dashboard and accounts page, and Dwolla API.
- Utilize Dwolla developed SDKs to interact with the Dwolla API.

Rules of Engagement

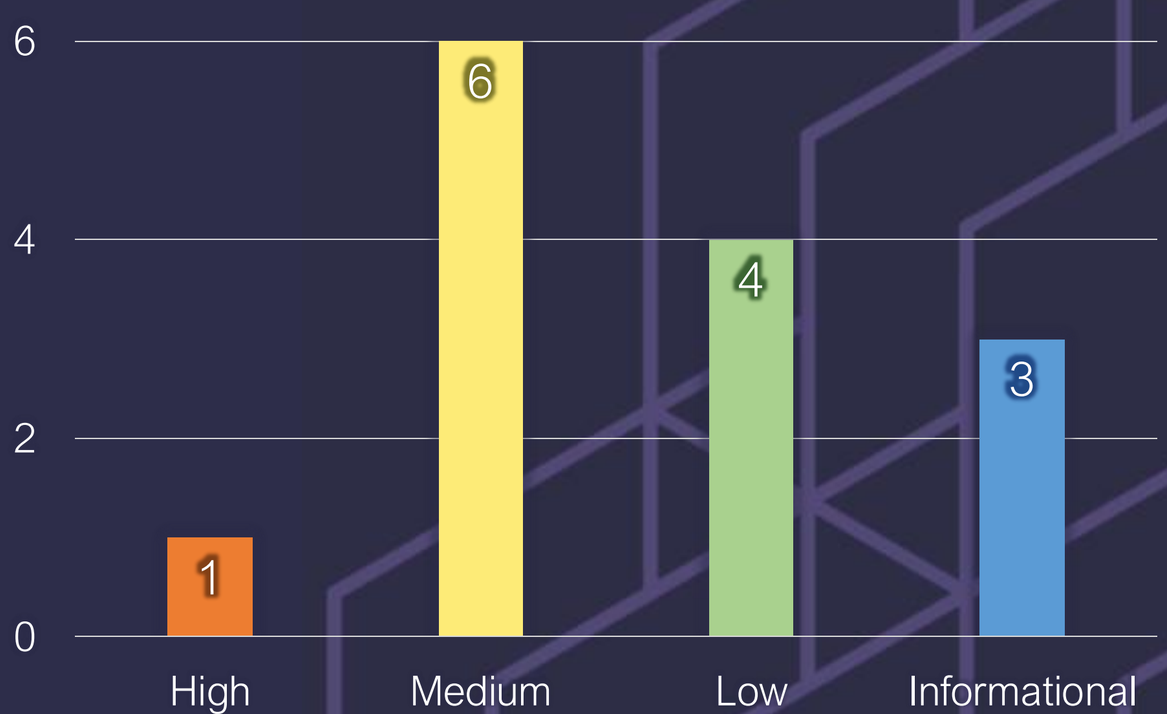
- Remain within scope
- Avoid stress testing through invasive attacks
- Protect Dwolla's clients through upholding the integrity of the Dwolla API or sandbox environment
- Utilize only open-source tools and resources

Testing Results

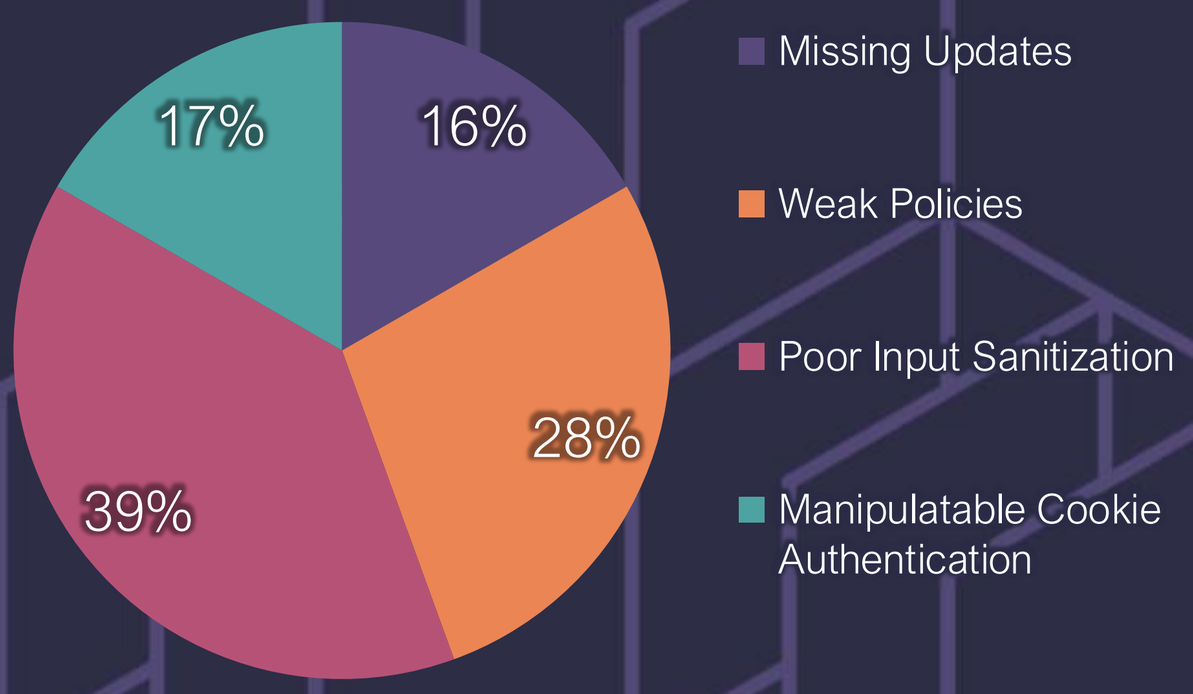
- Critical Vulnerability: Catastrophic Effects
- High Vulnerability: Significant Impact
- Medium Vulnerability: Moderate Threat
- Low Vulnerability: Minor Effects
- Informational Vulnerability: No Immediate Risks

(1)

Vulnerability Distribution (3)



Vulnerability Root Cause (2)



Results Summary

- (1): Rank of vulnerabilities
- (2): Distribution of found vulnerability root causes
- (3): Number of vulnerabilities found in each rank

* No critical vulnerabilities found