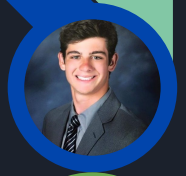
Pentest a Payment Provider

- Team: sdmay21-06
- Email: sdmay21-06@iastate.edu
- Client: Dwolla
- Advisor: Benjamin Blakely

The Team



Chief Pentester

Max Solaro — Cybersecurity Engineering • 2021

Testing Engineer

Matthew Maiman — Cybersecurity Engineering • 2021

Lead Reporter

Ryan Anderson — Cybersecurity Engineering • 2021

Facilitator & Scribe

Priyanka Kadaganchi — Computer Engineering • 2021

Editor

Nathan Key — Cybersecurity Engineering • 2021

Jacob Conn
CPR E • 2021

Web Pentester

KayAnne Bryant
CPR E • 2021

API Pentester

NDA

Permitted

- Team and Project progress on a general, ambiguous scale
- General testing techniques
- Tools utilized
- Project deliverables and overarching goals

Not Permitted

- Specific vulnerabilities
- Infrastructure details and endpoint technicalities
- Vulnerability impact and severity
- Specific exploits applicable to the discovered issues

Overview

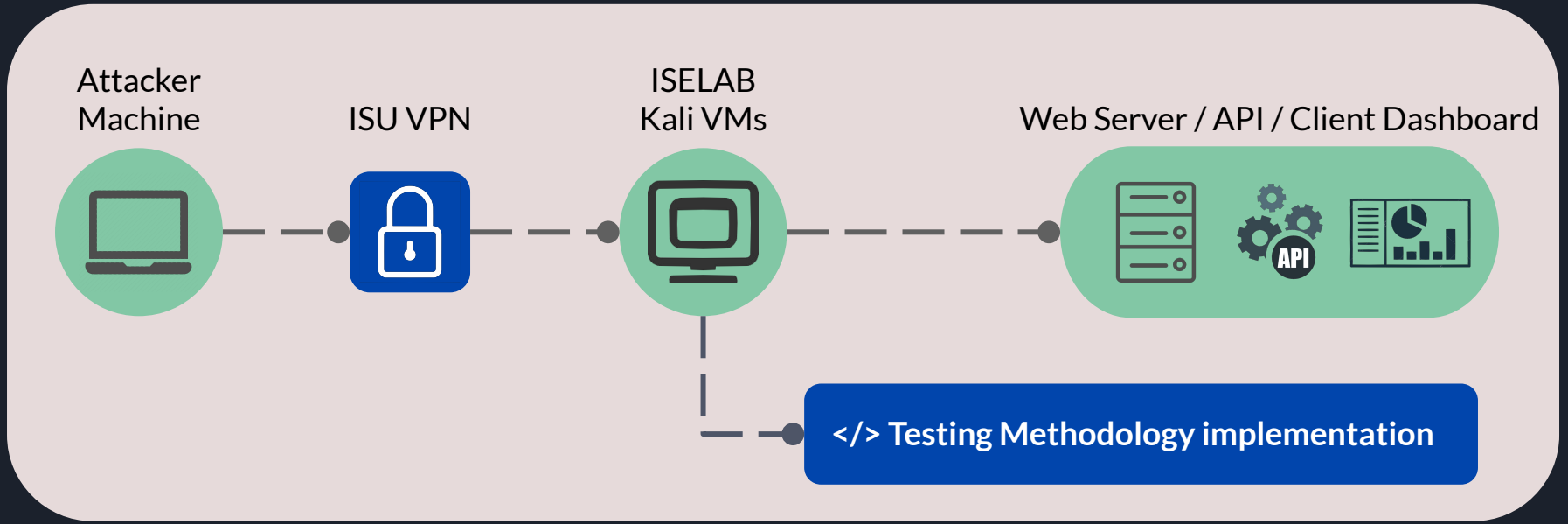
What is pentesting?

- Deep coverage of application/network to find high-risk vulnerabilities that are confirmed exploitable vulnerabilities. Typical PenTest stages are - Scoping, Testing/Validation, Reporting/Reposting.

Who is Dwolla?

- Dwolla is a cloud-first company, residing in AWS and utilizing Cloudflare. Since 2008, the company's infrastructure has powered billions of payments for millions of end users.

Penetration Testing Flowchart



Open-source Tools Used

OWASP Zap	A web application security scanner and is a useful way to perform an initial assessment of an application.
Postman	Postman is also an option to interface with and test API intended use cases.
Dwolla SDK	The Dwolla SDK will allow us to construct custom API requests to test for expected output
Burp Suite	It is one of the most popular penetration testing and vulnerability finder tools, and is often used for checking web application security.
Kali VM	The Kali Linux VM will allow us to utilize all of the tools we need to perform our testing

Project Goals

API	Explore and experiment with the API interface as much as possible. Map the environment and determine proper access control, authentication, data exposure, and injection practices are followed. Discover any weaknesses or possible violations.
Web App	Attack and test vulnerable elements on given webpages. Compile possible exploits or security misconfigurations associated with uncovered issues. Specifically target dashboard internal logic to find weaknesses in handling of sensitive information.
Client	Ensure client satisfaction is met and maintained. Provide a detailed and comprehensive report for review. Follow up with client following deliverables to affirm quality and perform any requested retesting

Web Technical Challenges

Cloudflare/Anti Automation

- Protects against general web-app vulnerabilities in attacks and headers
- Provides anti-bot protection, slows testing

External Penetration Test

- Treated like any other user on the internet
- Special treatment could allow for ease of testing

Paywalled Tools

- Advanced tools provide multiple libraries for better testing
- Throttled execution lengthens time of testing

Minor VM issues

- Connectivity Issues prevented access briefly
- Kali box has difficulty supporting multiple users testing at one time

API Technical Challenges

Tools

Both the SDK and Postman have flaws regarding automation and content
Other tools are blocked/interfered with by cloudflare

Experience

Overall inexperience with API testing and JSON formats

Documentation

Dwolla Docs contain a large collection of data/variables to track resulting in complex relationships

Deliverables

Executive Summary

Serves to provide a high level overview of the penetration test

Information covered:

- Purpose of penetration test
- General findings
- Vulnerability risk assessment
- Plans to remedy vulnerabilities

Aimed to give non-technical staff at Dwolla insight regarding security concerns from a business-oriented standpoint

Technical Report

Serves to provide technical details from the penetration test

Information Covered:

- Vulnerability risk assessment
- Confirmation of exploitation
- Tools and techniques used
- Technical impact on systems

Provides Dwolla's technical staff in-depth technical details, making understanding and patching vulnerabilities easier.

Thank you

Questions?