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

Web - Team Lead

Ryan Anderson — Cybersecurity Engineering • 2021

API - Team Lead

Matthew Maiman — Cybersecurity Engineering • 2021

Facilitator & Scribe

Priyanka Kadaganchi — Computer Engineering • 2021

Editor

Nathan Key — Cybersecurity Engineering • 2021

Jacob Conn
CPR E • 2021

Web Testing Eng

KayAnne Bryant
CPR E • 2021

API Testing Eng

Overview

What is pentesting?

- Detailed exploration of client’s network and services
- Discover potential vulnerabilities and weaknesses
- Evaluate risk and provide feedback to client

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.

NDA

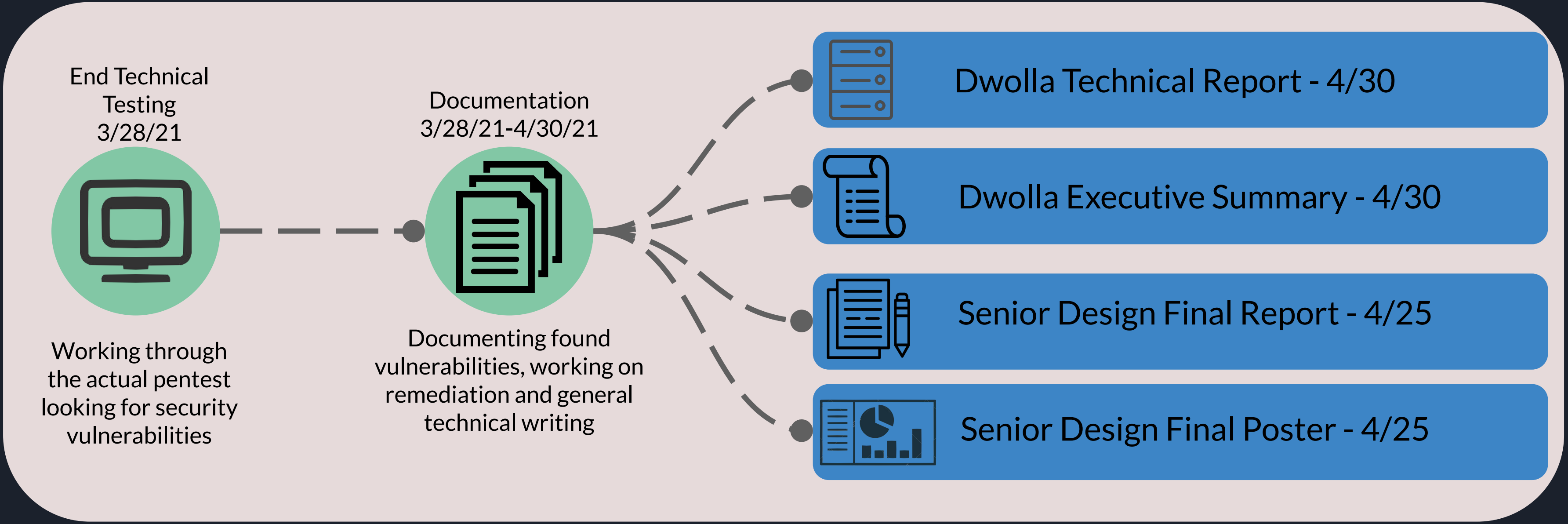
Permitted

- 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

Timeline



End Technical Testing 3/28/21

Working through the actual pentest looking for security vulnerabilities

Documentation 3/28/21-4/30/21

Documenting found vulnerabilities, working on remediation and general technical writing

Dwolla Technical Report - 4/30

Dwolla Executive Summary - 4/30

Senior Design Final Report - 4/25

Senior Design Final Poster - 4/25

Current Progress

Testing Wrapup

- Completed practical testing phase within last two weeks
- Finished rounding off tests on web app and API, covering OWASP Top-10
- Gathered screenshot or video evidence and reproduction steps for found vulns

Deliverables

- Compiled and organized vulnerabilities and performed risk audits for technical report
- Drafted outlines and details on findings for executive summary with predicted operations impacts

492

- Finishing details on Poster and Final Report, including info discussed here
- Preparing for faculty presentation next week, beginning work on presentation and discussion

Challenges

Challenge 1: Vulnerability Assessment

- Assessing the risk of each of the vulnerabilities found according to clients systems
- Ensuring all vulnerabilities reported will provide value
- Confirming which vulnerabilities will be protected under the NDA

Challenge 2: Confirmation and Remedy Reporting

- Creating useful guide for both Dwolla technical and non-technical oriented staff
- Making sure vulnerabilities found can be easily reproduced, and steps are clear and concise

Standards

OWASP API Top-10

Utilizing the API Security Top 10, the API team was able to target specific areas depending on the most likely vulnerabilities as described in this list.

OWASP Web Top-10

Utilizing the Web Application Security Top 10, the Web team was able to target specific areas depending on the most likely vulnerabilities as described in this list.

NIST

"Technical Guide to Information Security Testing and Assessment."

This standard deals with the more general process of pentesting, risk assessment, and mitigation.

In regards to the project, this was a great starting point due to its more broad approach.

Standards Continued

PTES

This standard also deals with a broader approach, and is broken down into 7 main sections.

Pre-engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post Exploitation, and Reporting.

OISSG

"Information Systems Security Assessment Framework."

Richard R. Linde

"Operating System Penetration."

Referred to by experts as "The First Pentesting Paper."

Many points made in this standard were built upon by later standards.

Constraints

- Sandbox environment
  - https://api-sandbox.dwolla.com
  - https://accounts-sandbox.dwolla.com
  - https://dashboard-sandbox.dwolla.com
- Public Sandbox API
- Certain attacks not allowed
  - Denial of service, crawling, spidering, accessibility interference/interruption, resource limitations, resource allocation
- Test only within Dwolla sandbox account
- Non-disclosure agreement
  - Course document redactions

Requirements

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?