# Pentest a Payment Provider

Design Document

**sdmay21-06**

Dwolla - Ben Blakely

**The team:**
Max Solaro - Chief Pentester
Matt Maiman - Testing Engineer
Ryan Anderson - Lead Reporter
Priyanka Kadaganchi - Facilitator & Scribe
Nathan Key - Editor

sdmay21-06@iastate.edu
[TEAM WEBSITE]

*Last revision - 9/18/20*

# Executive Summary

## Development Standards & Practices Used

**Standards practices**

- National Institute for Standards in Technology 800-115
- Payment Card Industry Data Security Standard
- Certified Ethical Hacker Training

## Summary of Requirements

- Develop and execute a penetration testing methodology for Dwolla's Sandbox API
- Do not perform any Denial of Service or other malicious attacks that would harm Dwolla's clients

## Applicable Courses from Iowa State University Curriculum

- CprE/CybE 230 / 231 / 234 / 331

## New Skills/Knowledge acquired that was not taught in courses

*List all new skills/knowledge that your team acquired which was not part of your Iowa State curriculum in order to complete this project.*

- WIP

## Tables, Graphs, Images

# Table of Contents

# 1 Introduction

## 1.1 Acknowledgement

Benjamin Blakely -- Professional advisor, client. Contributed significant technical advice, assistance, tools, and references.

## 1.2 Problem and Solution Statement

### Problem Statement

The payment provider Dwolla is contracting a team of cybersecurity professionals to perform a thorough penetration test against the Sandbox API provided by Dwolla for their clients. The contracted cybersecurity actors will perform as Red Team to assess the API, Sandbox dashboard, and Sandbox accounts login for known security vulnerabilities. Because the Sandbox API is public, found vulnerabilities must be validated and risk assessed. It is critical that Dwolla receive every security perspective possible to flush out any security issues and risk present on a public-facing service.

### Solution Statement

Properly executing a penetration test requires cohesion between both actors and client. A clearly defined Scope and Rules of Engagement must both be drafted before any intrusion into the problem area. These two items will be well stated further below in this documentation. Requirements and limitations keep the actors focused on the problem area assigned by Dwolla and prevent unauthorized security events. During the test, Red Team is expected to discover, validate, and appraise severity of common security vulnerabilities within the defined scope. The goal therefore is to identify these potential vulnerabilities within the API and determine their exploitability. To accomplish this, an evaluation and exploitation methodology will be devised by Red Team as agreed upon with Dwolla. This methodology and all discovered vulnerabilities with their associated risk audits will be compiled into a final report for the client. Potential remediation approaches will be discussed with Dwolla following completion of the penetration test. Re-testing may be done at a later date if deemed necessary.

## 1.3 Operational Environment

### Scope

We have a very well defined scope for this project that we must work in. We have three URLs which we are to stay within: https://api-sandbox.dwolla.com, https://accounts-sandbox.dwolla.com, and https://dashboard-sandbox.dwolla.com. All of these networks live within a sandbox environment, not a live production. We will be performing these tests from our personal computers and from Kali Linux VM's. While pentesting the web api, we will go through OWASP top ten web application security vulnerabilities. Looking at the dashboard and accounts sandbox, we will focus more on application vulnerabilities.

While testing the sandbox environment, we must ensure that we do not interfere with other users as the sandbox is an open environment. In addition, we mustn't utilize any attacks that would stress the server or perform a denial of service. This includes, crawling, fuzzing, and intentional DOS's. Furthermore, any vulnerabilities found should be responsibly and ethically disclosed to Dwolla.

### 1.4 Requirements

- A team member is required to stay within the rules of engagement and scope of this project.
- A dwolla sandbox account: This account will be used by all the team members for penetration testing against the dwolla network.
- A detailed documentation of any components within the scope should be made available to testers for them to implement pentesting smoothly.
- A detailed documentation for the client as well for them to know the details and implementation guidelines.
- Security controls that would detect or prevent testing. Consider whether these should be disabled or configured to not interfere during testing.

### 1.5 Intended Users and Uses

The intended audience for the pen test deliverable is Dwolla and their clients. Dwolla is the primary recipient, and audience of the final report deliverables, and would receive these deliverables and utilize them directly. Dwolla's clients benefit from the project indirectly from security fixes implemented as a result of the test.

### 1.6 Assumptions and Limitations

**Assumptions**

- Team members are authorized to, and have been given permission to complete the pentest within the agreed upon rules and scope, and shall not be penalized in any way for carrying out any tasks associated with the test.
- All team members(5 members) will have access to the testing environment, and have the ability to create an account.
- Team members will have access to all necessary equipment when needed.
- Team members should not be required to purchase equipment or software for the test.
- Team members will be available for scheduled meetings unless specified in advance.
- Team members will be allowed to ask questions and inquire about network and software details.
- If no vulnerabilities can be located by the team, a separate, vulnerable system will be set up to allow the team to complete the test.
- The requirements for successfully completing a senior project will be adapted to meet the expectations of a pentest.

**Limitations**

- Team members shall not interfere with the standard operations of Dwolla.
- Team members must remain within the defined scope and adhere to the agreed upon rules of engagement.
- Team members shall document all of their findings and procedures for use in final deliverables
- Team members must adhere to the signed non disclosure agreement for information gathered during the course of the test.
- Team members are to disclose any potential vulnerabilities responsibly through the executive summary and technical report.

## 1.7 Expected End Product and Deliverables

### Objective

The development and execution of a penetration testing methodology. This pentest will provide Dwolla with valuable new perspectives on the security of their API.

### Deliverables

- **Scope and Rules of engagement during the pentest**

  These documents will ensure that the penetration test against Dwolla is performed to the client's specifications. The scope will make certain, guarantee, certify that the penetration test is only against the systems designated by the client. The rules of engagement will outline how the penetration test is to be conducted, such as the type of tests performed.

  *Delivery Date: 10/20/2020*

- **Methodology used during the pentest**

  After finalizing the scope and rules of engagement, the methodology for the penetration test will be developed around them. The methodology will lay out the methods and tools that will be used by the team. The methods outlined in the document will cover how the team will collect information, analyze vulnerabilities, proceed with exploitation, handle information post-exploitation, and report results. The tools outlined in the methodology will be centered around the constraints of the scope and rules of engagement. The tools used during the pentest will consist of open source linux software. Both the methods and tools will be based on most common vulnerabilities affecting API software.

  *Delivery Date: 11/20/2020*

- **Executive Summary of the Pentest**

  The executive summary is one of the major documents of the final report to the client. This document will cover the results of the penetration test from a high level. This document will include details such as the purpose of the penetration test, general findings, risk ranking for each of the vulnerabilities, and plans to remedy each one of those vulnerabilities. This report will provide Dwolla's non-technical staff an insight into the security concerns from a business-oriented standpoint.

  *Delivery Date: 3/28/2021*

- **Technical Report of the Pentest**

  The technical report is the second major document for the final report to the client. This document will cover the result of the penetration test from a more technical level. This document will include details such as the vulnerability assessment, confirmation of the exploited vulnerabilities, techniques and accessed systems post-exploitation, and the impact that the vulnerabilities had on the system. Dwolla's technical staff will use this report to understand vulnerabilities that were exploited in their API, and consider how they will remedy the issues based on vulnerability impact.

  *Delivery Date: 4/30/2021*

# 2 Project Plan - WIP

## 2.1 Task Decomposition

**Develop testing methodology**

- Familiarize ourselves with the software that we will be testing
- Perform reconnaissance and gather information on Dwolla's API and Web App
- Research common vulnerabilities and techniques against API's
- Develop list of attacks we will perform on the software

**Execute practical penetration test**

- Divide work among team to execute different parts of the pentest based on personal research
- Perform planned attacks on Dwolla's client API
- Record and validate vulnerabilities found during the testing
- Attempt further escalation into the software after initial vulnerability
- Record, but do not exfiltrate, sensitive information found during the test

**Draft final report**

- Gather vulnerabilities and sensitive information found from each group member
- Create high-level report for clients covering general findings and remediation plans
- Create technical report proving vulnerabilities and providing technical details
- Present both documents, as well as presentation, to the client

## 2.2 Risks And Risk Management/Mitigation

| Potential Risk | Risk Factor | Mitigation Plan |
|---|---|---|
| During the execution of our pentest, a risk exists that we will not be able to find any vulnerabilities significant enough in Dwolla's API . | Likelihood = 3<br>Impact = 5<br><br>Risk Factor = .6 | Our team will first search new tools and develop additional strategies for testing Dwolla's API. If that fails, we will test our methodology against vulnerable API's popular for testing common vulnerabilities. |
| The team may expose a vulnerability that could cause major damage to Dwolla. | Likelihood = 1<br>Impact = 5<br><br>Risk factor = .5 | Our team will notify Dwolla immediately and provide help to patch this vulnerability, rather than waiting until the reports are written |
| Team members' personal IP addresses could become blocked by Dwolla's attack prevention systems. | Likelihood = 2<br>Impact = 2<br><br>Risk factor = .16 | N/A |
| Team members lose computers / are unable to connect to the world wide web. | Likelihood = 2<br>Impact = 4<br><br>Risk factor = .32 | N/A |

## 2.3 Project Proposed Milestones, Metrics, and Evaluation Criteria

**Develop testing methodology (11/20/20)**

- Familiarize ourselves with the software that we will be testing. This will be done by reviewing the Dwolla provided SDK. Additionally this can be considered completed after an account is created within the Dwolla Sandbox environment and fund transfers are simulated correctly.
- Perform reconnaissance and gather information on Dwolla's API and Web App. This can be considered completed after we have successfully simulated requests against Dwolla's API using Postman or a similar tool.
- Research common vulnerabilities and techniques against API's. This can be considered completed after reading through OWASP's top ten web vulnerabilities.
- Develop list of attacks we will perform on the software. This can be considered completed after a list of vulnerabilities is composed. The list should contain more than 15 potential vulnerabilities.

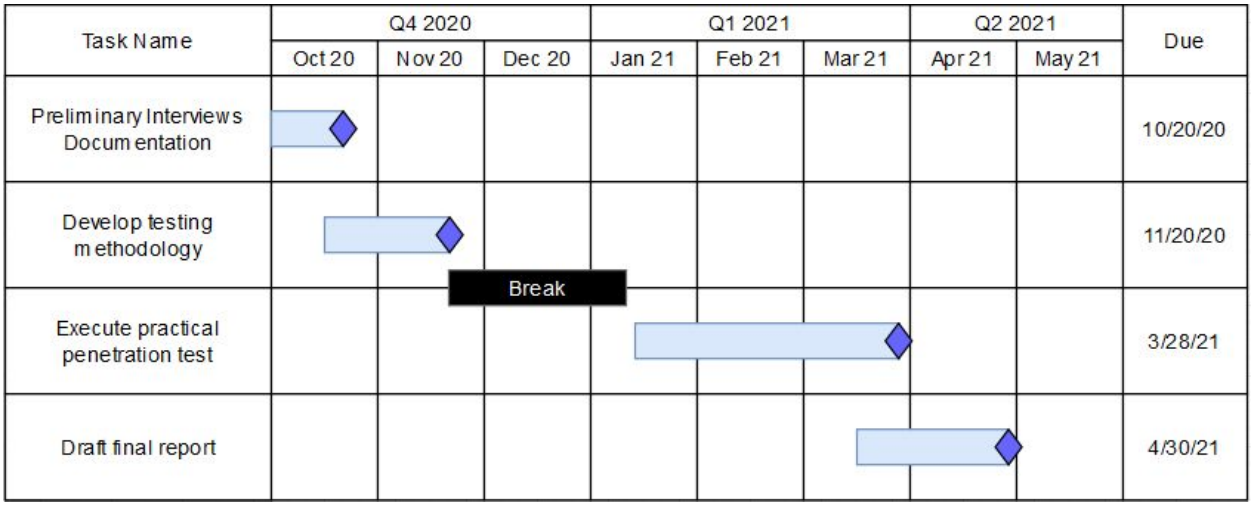
**Execute practical penetration test (3/28/21)**

While executing the practical pentest, we will use the list of potential vulnerabilities previously identified. Progress can easily be tracked as each vulnerability is evaluated. If no exploits are found for a vulnerability, said vulnerability can be marked as tested for and we will continue moving down the list. In the event a vulnerability with a live exploit is found, we will document it and potentially attempt to escalate privileges.

**Draft final report (4/30/21)**

All reporting will follow the standards laid out by PTES or the Penetration Testing Execution Standards. This includes assessing the risk for each vulnerability that is found. Risk assessments are on a predetermined scale of 1-15. In addition to risk assessments, there will be general findings, recommendations and a strategic roadmap documenting any issues found along with solutions. The report will also include our entire testing methodology, including general vulnerability assessment and post exploitation findings.

## 2.4 Project Timeline/Schedule (Tentative)



**Preliminary Interviews (10/20/20)**

Initial interviews and questions regarding the scope, rules of engagement, timeline, and expected deliverables shall be completed by this date. First drafts of the design document will be completed with details concerning the limitations and expectations of the project. Furthermore, initial research into the OWASP common vulnerabilities and early probing of the given scope will be conducted.

**Develop testing methodology (11/20/20)**

As described above in the task decomposition, the team is expected to have developed a common list of vulnerabilities, attacks, and methods on how the problem area will be addressed. A clear understanding of the tools we will be using, how they will be used, and the steps we will take to complete the pentest is expected by this deadline.

**Execute practical penetration test (3/28/21)**

At the lastest, by this date the practical penetration test will have wrapped, with details outlining discovered issues, known exploits, and reproduction steps recorded. In addition to these items, a full breakdown of the workload assigned and performed by each team member will be recorded. Lastly, a full risk audit for each exploit discovered must be completed by this date.

**Draft final report (4/30/21)**

Finally, with the practical test completed, all information and data recorded during the test will be organized and compiled into a final report for the client. This deliverable will be expected by the end of the semester, however earlier is preferable to leave time to discuss the found issues, remedies, and possibilities of re-testing to affirm patches. Therefore, a meeting to discuss the final report is expected to happen by the end of April.

## 2.5 Project Tracking Procedures

-Our group will use Trello which is a list-making application and each card can be appointed to a team member. Which will help us track information regarding vulnerabilities. Google docs will be used to track progress on developing the pentest throughout the course of this and next semester and this will help our team make sure we are not duplicating work.

-For normal communication with the project members we have decided to use discord. Discord is an instant messaging application.

-To communicate with our Client (Ben Blakely) we will do it through email.

## 2.6 Personnel Effort Requirements

As this is a 3 credit class it means that about 9 hours should be given by each individual.

| Name | Work/ Role | Number of hours per week | Total number of months for this project |
|---|---|---|---|
| Matthew Maiman | Testing Engineer | 9- 12 hours | 8 months |
| Ryan Anderson | Lead Reporter | 9 - 12 hours | 8 months |
| Max Solaro | Chief Pentester | 9 - 12 hours | 8 months |

| | | | |
|---|---|---|---|
| Nathan Key | Editor | 9 - 12 hours | 8 months |
| Priyanka Kadaganchi | Facilitator/ Scribe | 9 - 12 hours | 8 months |

**Tasks time distribution:**

| Task | Time |
|---|---|
| **Develop testing methodology** | **3 months** |
| **Execute practical penetration test** | **3 months** |
| **Draft final report** | **½ month** |

### 2.7 Other Resource Requirements

Identify the other resources aside from financial (such as parts and materials) required to complete the project.

- A Computer or some device capable of connecting to the testing environment.
- Virtual machine or Some Linux Operating system that can access the necessary tools.
- Open source cyber security penetration testing tools.
- Access to document and project management software such as Google docs and Trello.
- A suitable Network connection.

### 2.8 Financial Requirements

This project will be utilizing open-source and free software to fully perform the required tasks. No fees or costs will be incurred.

# 3 Design

## 3.1 Previous Work And Literature

Include relevant background/literature review for the project

– If similar products exist in the market, describe what has already been done

– If you are following previous work, cite that and discuss the advantages/shortcomings

– Note that while you are not expected to "compete" with other existing products / research groups, you should be able to differentiate your project from what is available

Detail any similar products or research done on this topic previously. Please cite your sources and include them in your references. All figures must be captioned and referenced in your text.

## 3.2 Design Thinking

Detail any design thinking driven design "define" aspects that shape your design. Enumerate some of the other design choices that came up in your design thinking "ideate" phase.

## 3.3 Proposed Design

Include any/all possible methods of approach to solving the problem:

- Discuss what you have done so far – what have you tried/implemented/tested?
- Some discussion of how this design satisfies the **functional and non-functional requirements** of the project.
- If any **standards** are relevant to your project (e.g. IEEE standards, NIST standards) discuss the applicability of those standards here
- This design description should be in **sufficient detail** that another team of engineers can look through it and implement it.

## 3.4 Technology Considerations

Highlight the strengths, weakness, and trade-offs made in technology available.

Discuss possible solutions and design alternatives

## 3.5 Design Analysis

– Did your proposed design from 3.3 work? Why or why not?

– What are your observations, thoughts, and ideas to modify or iterate over the design?

### 3.6 Development Process

Discuss what development process you are following with a rationale for it – Waterfall, TDD, Agile. Note that this is not necessarily only for software projects. Development processes are applicable for all design projects.

### 3.7 Design Plan

Describe a design plan with respect to use-cases within the context of requirements, modules in your design (dependency/concurrency of modules through a module diagram, interfaces, architectural overview), module constraints tied to requirements.

# 4 Testing

Testing is an extremely important component of most projects, whether it involves a circuit, a process, or software.

1. Define the needed types of tests (unit testing for modules, integrity testing for interfaces, user-study or acceptance testing for functional and non-functional requirements).
2. Define/identify the individual items/units and interfaces to be tested.
3. Define, design, and develop the actual test cases.
4. Determine the anticipated test results for each test case
5. Perform the actual tests.
6. Evaluate the actual test results.
7. Make the necessary changes to the product being tested
8. Perform any necessary retesting
9. Document the entire testing process and its results

Include Functional and Non-Functional Testing, Modeling and Simulations, challenges you have determined.

## 4.1 Unit Testing

– Discuss any hardware/software units being tested in isolation

## 4.2 Interface Testing

– Discuss how the composition of two or more units (interfaces) are to be tested. Enumerate all the relevant interfaces in your design.

## 4.3 Acceptance Testing

How will you demonstrate that the design requirements, both functional and non-functional are being met? How would you involve your client in the acceptance testing?

## 4.4 Results

– List and explain any and all results obtained so far during the testing phase

- Include failures and successes
- Explain what you learned and how you are planning to change the design iteratively as you progress with your project
- If you are including figures, please include captions and cite it in the text

# 5 Implementation

Describe any (preliminary) implementation plan for the next semester for your proposed design in 3.3.

# 6 Closing Material

## 6.1 Conclusion

Summarize the work you have done so far. Briefly reiterate your goals. Then, reiterate the best plan of action (or solution) to achieving your goals and indicate why this surpasses all other possible solutions tested.

## 6.2 References

List technical references and related work / market survey references. Do professional citation style (ex. IEEE).

## 6.3 Appendices

Any additional information that would be helpful to the evaluation of your design document.

If you have any large graphs, tables, or similar data that does not directly pertain to the problem but helps support it, include it here. This would also be a good area to include hardware/software manuals used. May include CAD files, circuit schematics, layout etc,. PCB testing issues etc., Software bugs etc.