EE/CPRE/SE 491 Bi-Weekly Report
sdmay21-06
Pentest a Payment Provider

Report Period: 3/2/21-3/15/21
Client & Advisor: Benjamin Blakely

Team Members & Roles:

Max Solaro - Chief Pentester
Matthew Maiman - Testing Engineer
Ryan Anderson - Lead Reporter
Nathan Key - Editor
Priyanka Kadaganchi - Facilitator & Scribe
Jacob Conn - Web Pentester
KayAnne Bryant - API Pentester

Weekly Summary:

For this week, both our API and WebApp team have continued to test their respective systems. With most of the common and very critical vulnerabilities tested, our teams work towards more specific testing to find weaknesses in Dwolla's internal logic, related to workflows, automation, and processing. As we continue to test Dwolla's system, we are listing areas of interest for further testing, and also pointing out systems which are unable to be tested due to anti-bot cloudflare protection.

Past Week Accomplishments:

- Dwolla API testing- Max, Matt, Priyanka, KayAnne
  - Continuing comprehensive API endpoint testing.
  - Researched and implemented new tools to further aid in testing.
  - Setup proxying through OWASP Zap to stage automated testing and intercept requests/responses
- Dwolla WebApp testing - Ryan, Nathan, Jacob
  - Continuing to test Dwolla dashboard internal logic and general web vulnerabilities.
  - Listing areas of the Dwolla dashboard that cannot be tested due to anti-bot protection.

Pending Issues:

No pending issues

Individual Contributions:

Name	Contributions	Hours last 2	Cumulative Hours

		weeks	
Max Solaro	Setup OwaspZap and began analyzing manual tests. Setup automated scans and evaluating results.	5	23
Matthew Maiman	Explored permission levels of different customer groups, setup Zap proxy and began automation. Manually evaluated automation for issues	8	25
Ryan Anderson	Testing of the dashboard continued, specifically focusing on internal logic. Began initial drafts for final report format/style.	9	34
Nathan Key	Continued Web dashboard testing and investigating potential vulnerabilities.	8	20
Priyanka Kadaganchi	Learning more and setting up of OWASP ZAP. Started the scans and analyzed the tests.	5	17
Jacob Conn	Continued testing dashboard. Focusing on automation.	6	20
KayAnne Bryant	Worked with setting up OWASP ZAP and starting scans and trying out different tests.	5	20

Plans For Upcoming Week:

- API Team (Max, Matt, Priyanka, KayAnne):
    - Continue researching new tools that could help provide new ideas/attack vectors.
    - Implement the advice given by Dr. Daniels and brainstorm ways to break dataflow.
    - Continue to expand on Zap, explore the tools possible there, and undertake further automation
- WebApp Team (Ryan, Nathan, Jacob):
    - Testing will continue for the dashboard, with emphasis on finding areas which can be tested, and aren't protected by cloudflare.
    - Begin formally reporting vulnerabilities found within the dashboard, which includes determining vulnerability impact score, and remediation plans.

Advisor Meeting Summary:

During this week's meeting with our advisor, we went over the vulnerabilities we have found within their systems, and discussed their severity and impact. We also presented our initial concerts about our testing methods being blocked by anti-bot protections, and layed out solutions if these problems continue.