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

Report Period: 2/22/21-3/1/21
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:

Over this last week we worked on investigating a few specific vulnerabilities including broken authentication, excessive data exposure, and injection. In order to efficiently run these tests, we continued working on familiarizing ourselves with the Dwolla API variables and endpoints and with the DwollaSDK. We will continue to write custom requests in order to further test the API.

Past Week Accomplishments:

- Dwolla API testing- Max, Matt, Priyanka, KayAnne
    - Began more comprehensive API endpoint testing. Mapped out API environment variables for a better understanding of how they interact in the hopes of uncovering Excessive Data Exposure.
    - Broken User Authentication: Looked into accessing resources meant for other users without proper authentication. Tested 2 different endpoints, both properly handled our improper access attempts.
- Dwolla WebApp testing - Ryan, Nathan, Jacob
    - Completed automated testing of common and known vulnerabilities against the Dwolla dashboard and accounts page. Recorded vulnerabilities tested and forwarded results to our client.
    - Laid out objectives for the upcoming tests, with testing dwolla dashboard http headers are up to current security standards, and began enumerating internal logic processes within the dashboard for further testing.Ensuring that http headers are up to current security standards

Pending Issues:

No pending issues

Individual Contributions:

Name	Contributions	Hours last week	Cumulative Hours
Max Solaro	Worked on scripts for API testing. Began testing for injection by attempting to write misconfigured POST requests (WIP). Looked into broken user authentication by attempting to access resources from other accounts.	5	18
Matthew Maiman	Worked with API team to further explore the Python SDK, Postman, and the API functionalities. Began early testing of OWASP Top-10. Contacted client for further guidance moving forward with testing. Started configuring ZAP	6	17
Ryan Anderson	Forwarded testing results to client, and began enumerating new vulnerabilities to test in terms of internal logic and header security.	5	25
Nathan Key	Continued with preliminary investigation of vulnerabilities and transitioned to investigating header security of clients web application.	4	12
Priyanka Kadaganchi	Conducting preliminary tests and writing scripts on the Python SDK.Played around with the Postman functionalities and started planning with the team to work with OWASP-ZAP.	4	12
Jacob Conn	Investigating header security as we wrapped up preliminary scans. Approaching our vulnerability assessments with a more refined focus.	4	14
KayAnne Bryant	Worked with API further and explored the Python SDK, Postman, and the API functionalities. Began early testing of OWASP Top-10. Started configuring ZAP scanner	4	15

Plans For Upcoming Week:

- API Team (Max, Matt, Priyanka, KayAnne):
    - Parse through the client email containing further guidance and information on moving forward with the API testing.

    - Expand testing horizon in combing the API for authentication bypasses or authorization elevation. Client suggested creating a secondary account to assess the possibility of cross-accessing data between accounts.
    - Move forward with OWASP-Zap and begin automated tests with manual proxy.
    - Continue playing with the SDK to poke around the endpoints and attempt to find any issues pertaining to the OWASP Top-10 and data leakage.
- WebApp Team (Ryan, Nathan, Jacob):
    - Test returned HTTP headers for security misconverations, and deviations from best practices
    - Explore the Dwolla dashboard for internal logic operations which could be vulnerable to various sorts of attacks.
    - Continue to list vulnerabilities found within the dashboard and accounts web applications.

Advisor Meeting Summary:

No meeting during this reporting period.