

POSTMANを用いたAPI開発の品質保証の向上 認証から機能、非機能テスト、そしてチーム連携

氏名 菅谷 佑司
所属 株式会社マネーフォワード

はじめに・背景

私は会計システムに関するAPI開発を行う5名ほどのプロジェクトに途中から最初のQAエンジニアとして参画した。プロジェクトではPOSTMANを使用していたが、テスト実施の際にAPIの振る舞いを確認するレベルに留まっていた。POSTMANの機能を深く理解し活用すれば、効率よくAPI開発の品質を向上させられるのではないかと考え、POSTMANについて学ぶことを決め、学んだ内容を実際にどのように活用したのか、活用した結果について紹介する。

概要

本事例紹介では、API開発における品質保証の向上を目指し、POSTMANを活用した実践的なアプローチについて紹介する。私が所属しているAPI開発プロジェクトでは、認証プロセスの煩雑さや手動テストの時間がかかり、迅速なテストが難しいという問題があった。また、性能テストでは別ツールの使用によりデータの再利用ができず、セキュリティテストではチーム内で実施実績がなく、外部専門会社に依頼する際に調整コストがかかることが課題だった。さらに、API利用方法がプロジェクト外のメンバーに共有されず、知識が特定のメンバーに依存していた。

これらの問題に対して、POSTMANが提供している機能を取り入れることにより、認証プロセスの自動化、自動テストの導入をし、テスト実施にかけていた工数の短縮させた。また、POSTMANを利用して性能テストやセキュリティテストを実施し効率よく非機能面での品質保証を行った。APIの利用連携に関しては、有料プランに加入が必要なため、POSTMANのテストコレクションをドライブ上で管理することによりチームを超えた連携を可能にした。

問題提起

- アクセストークンの取得および更新のプロセスが複雑で煩雑なため、テストの継続性が損なわれている(60分おきに手動で更新が必要)。
- テストスクリプトが用意されておらず、テストを実施するたびに手動でAPIの振る舞いを確認している。
- 機能テストと性能テストで異なるツールを使用しており、認証やリクエストの設定を毎回行う必要がある。
- セキュリティテストをチームで実施した実績がなく、外部の専門会社に依頼する必要があり、依頼する際のコミュニケーションコストやスケジュールに依存する問題がある。
- 認証が複雑であり、開発メンバー以外がAPIを利用するのが難しい。APIドキュメントを見て自分でリクエストを一から作成しなければならないため、利用に対するハードルが高い。

課題

- アクセストークンの自動取得と更新が必要。
- リグレッションテストの自動化が必要。
- 認証や性能テストのスクリプトを一度に準備し、再利用可能な形で管理する必要がある。
- セキュリティテストのスムーズな実施が必要。
- 開発チーム以外でもAPIへのアクセスと共有が容易になる環境の整備が必要。

対策および評価(メリット、デメリット)

- PostmanのOAuth2.0自動トークン・リフレッシュ機能を活用し、認証プロセスを自動化する。

・メリット

テスト実施中にトークンが失効せず、テストの継続性が保たれる。

・デメリット

特になし

- POSTMANでテストスクリプトを作成し、構築したテストをCIに組み込みテストを自動化する。

・メリット

テスト実施にかかる工数を大幅に短縮する。常にテストされている状態を保てる。

・デメリット

認証プロセスが原因で自動化できない可能性がある。一からテストスクリプトを作成するため自動化の土台を作るまでのコストがかかり、仕様が更新するたびにテストのメンテナンスタスクが発生する。

3. 認証設定と作成済みのリクエストを組み合わせるPOSTMAN内で性能テストを実施する。
 - ・メリット
認証設定や既存のリクエストを再利用できる。機能テストと性能テストでツールの統一が可能。
 - ・デメリット
無料プランでは仮想ユーザー数の制限があり、設計した一部のテストができない可能性がある。
4. 脆弱性診断ツールであるOWASP ZAPとPOSTMANを組み合わせる脆弱性診断を実施する。
 - ・メリット
専門会社を利用しないため、外部環境に依存せず、セキュリティテストの実施が可能。
 - ・デメリット
専門会社のセキュリティ診断と同等のテストが担保できるとは限らないため、社内のセキュリティ部門を巻き込み相談する必要がある。
5. POSTMANのコラボレーション機能を活用し、関係者にワークスペースの共有を行う
 - ・メリット
誰もが事前設定不要でAPIの利用を可能にし、開発者以外の視点を持つ関係者にAPIに触ってもらいやすくなることにより、よりユーザー観の不具合や改善要望を検知しやすくなる。
 - ・デメリット
無料プランではワークスペース共有の人数制限があり、有料プランの加入が必須になる。

結果・まとめ

対策を講じた結果、認証プロセスの自動化や3-4時間かけていた手動テストの短縮が実現し、数分で完了するようになった。非機能面では、データの再利用により、性能やセキュリティテストの効率的な実施が可能となり、API開発プロジェクトの品質を機能面、非機能面の両面から保証することができた一方で、いくつかの新たな問題に直面した。

新たな問題

1. CLIツールを使用した場合、認証の自動更新に対応しておらず、CIに組み込めなかった。
2. 複数人でのワークスペースの共有は有償機能であり、有料プラン加入のハードルが高かった。

解決策

1. スケジュール機能などCI以外でPOSTMANが提供している自動化機能を活用する。または他のツール導入を検討する。
2. テストコレクションをJSON形式で出力し、共用ドライブで管理をする。利用方法についての一連の流れを資料にまとめてAPI利用ガイドラインとして関係者に展開する。

苦労した点

社内でAPIの品質保証やPOSTMANの活用事例などの情報があまり蓄積されていなかったため、活用できそうな機能の調査や自動テストの書き方を学ぶのに時間や学習コストがかかってしまった。実際にプロジェクトに活用するまでのプロセスが困難だった。

気をつけた方が良い点

OWASP ZAPを用いた脆弱性診断については、専門のセキュリティ会社と同等の診断ができるとは限らないため、セキュリティテストを外部に依頼するべきかどうかは根拠やデータを集めた上で判断する必要がある。本プロジェクトでは新規公開時には専門のセキュリティ会社の診断を受け、その後のリリースについては基盤等の大きな変更がない限りOWASP ZAPでの診断を行なっている。

またPOSTMANの導入について、今回は既にプロジェクトで導入されていたため活用方法を考えて計画を立てたが、未導入の場合、プランごとの機能制限や無料プランでの代替策を事前に調査し、導入の可否を検討する必要がある。

参考文献

Web

認証関連

- ・POSTMAN official website

- ・<https://learning.postman.com/docs/sending-requests/authorization/oauth-20/>

- ・安心してください。PostmanはOAuth2.0の自動トークンリフレッシュをサポートしてますよ

<https://qiita.com/yokawasa/items/b4d89d983bfd23792788>

2023年07月06日

@yokawasa(Yoichi Kawasaki)

機能テスト関連

- ・POSTMAN official website

- ・<https://www.postman.com/product/postbot/>

- ・<https://learning.postman.com/docs/sending-requests/variables/managing-environments/>

- ・<https://learning.postman.com/docs/collections/using-newman-cli/command-line-integration-with-newman/>

- ・Postmanで使えるAIテスト生成機能「Postbot」がリリース

<https://qiita.com/nagix/items/4ae601117b39b05458ec>

2023年07月19日

@nagix(草薙 昭彦)

セキュリティテスト関連

- ・API Security Testing With Postman and OWASP Zap

<https://thetesttherapist.com/2022/02/13/api-security-testing-with-postman-and-owasp-zap/comment-page-1/>

2022年2月13日

Mohamed

性能テスト関連

- ・POSTMAN official website

- ・<https://learning.postman.com/docs/collections/performance-testing/performance-test-configuration/>

- ・超便利！PostmanのAPIパフォーマンステストで簡単かつ素早く性能フィードバックを手に入れよう

<https://qiita.com/yokawasa/items/c172f1765026bf90d3ac>

2023年06月20日

@yokawasa(Yoichi Kawasaki)

チームコラボレーション関連

- ・POSTMAN official website

- ・<https://learning.postman.com/docs/collaborating-in-postman/working-with-your-team/collaboration-overview/>

- ・Postmanでチームコラボレーション！

<https://speakerdeck.com/nagix/postmandetimukoraboresiyon>

2024年02月26日

草薙 昭彦