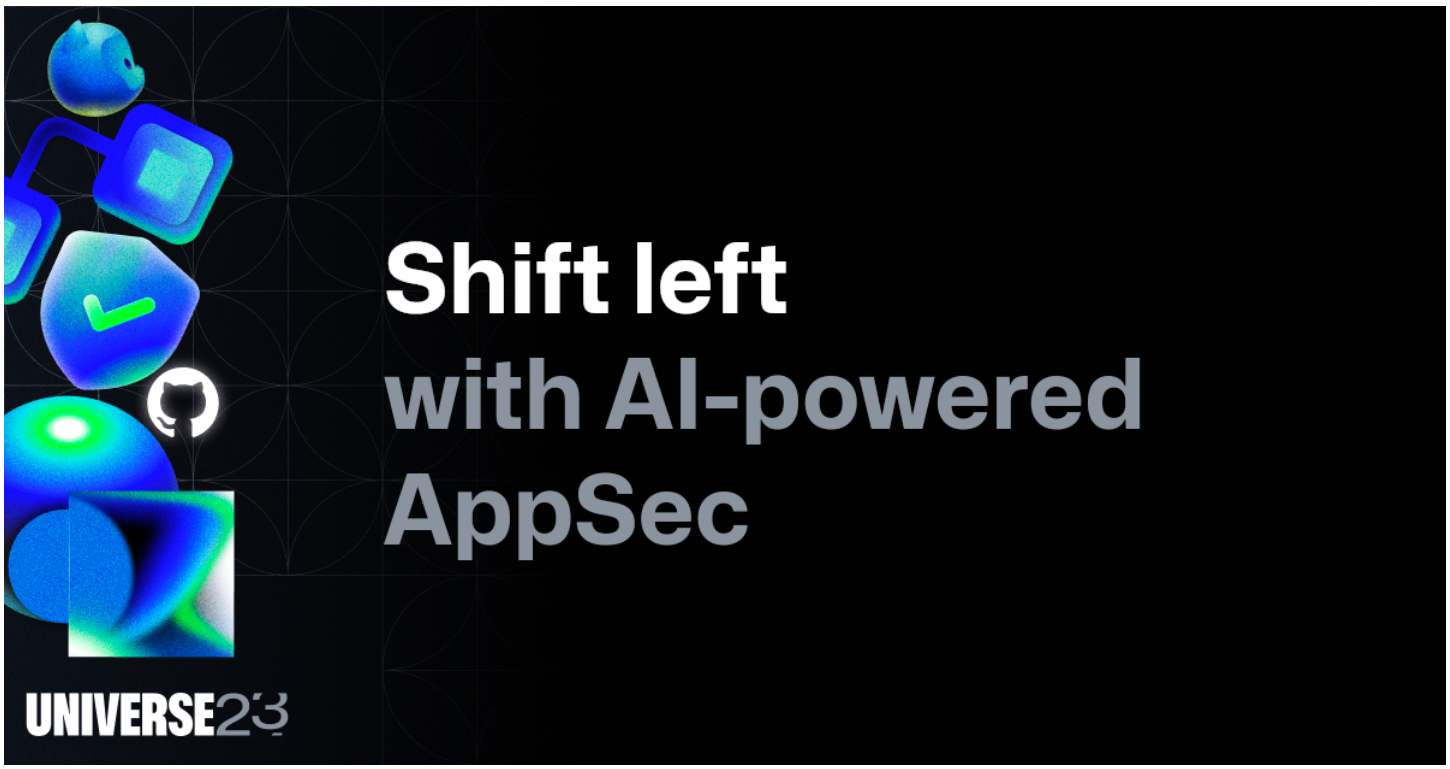
GitHub

NEWS RELEASE

2023年11月17日
ギットハブ・ジャパン合同会社

GitHub Advanced Securityの新機能、AIを駆使したアプリケーションセキュリティテストを発表
～これまで以上に効率的にソースコードの保護を実現～



安全なソフトウェアを開発、拡張、提供するためにAIを搭載した世界最大の開発者プラットフォームを提供するGitHub, Inc.（本社：米国サンフランシスコ）は2023年11月8日(米国時間)、GitHub Advanced Securityの新たな機能として、AIを駆使したアプリケーションセキュリティテストを発表しました。

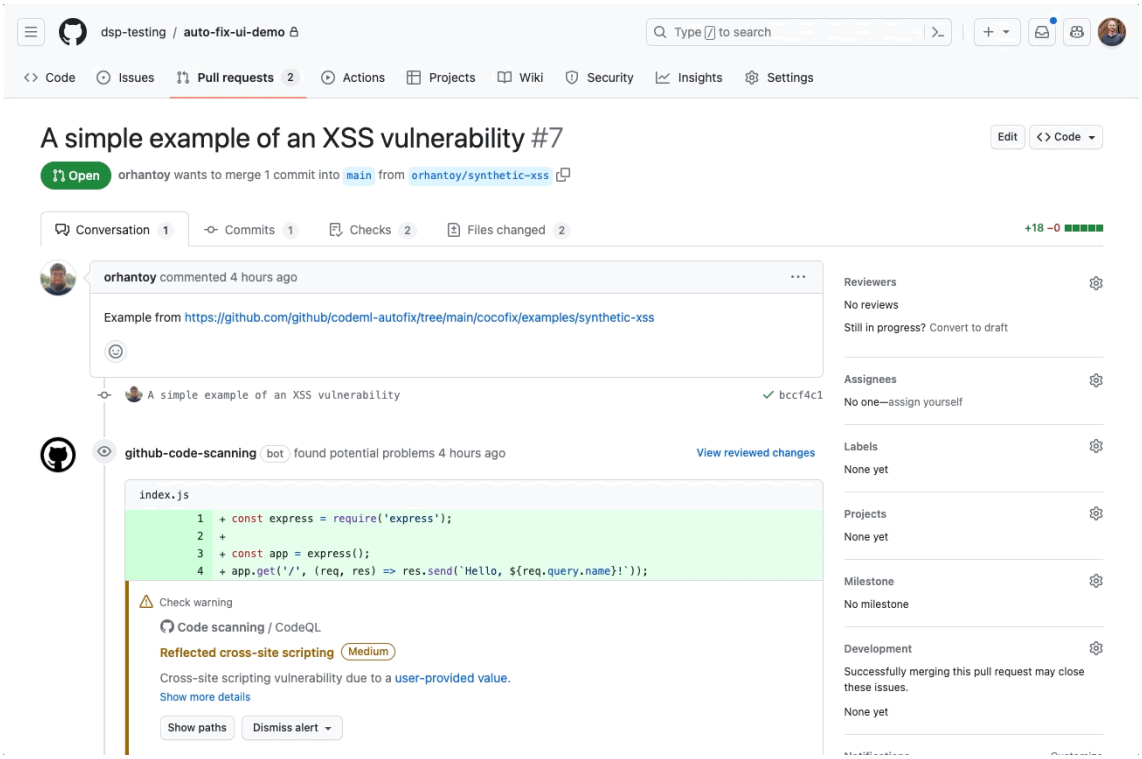
GitHubでは、ソフトウェア開発におけるワークフローの不協和を減らすことに注力しています。セキュリティの観点において、これは非常に重要であるためです。開発者は、問題が起きてから脆弱性をテスト、修正するのではなく、コードを作成したその場で直ぐに保護できる体制を必要としています。安全なアプリケーションを提供するには、組み込みのセキュリティが欠かせません。

この1年間にGitHub Advanced Securityは、アプリケーションセキュリティテストとソフトウェアサプライチェーン機能を向上させる70以上の機能をリリースしてきました。Dependabotでは1つのPull Requestで複数のバージョンアップデートをグループ化できるようになり、Code Scanningでは1つのクエリで最大1,000件のリポジトリのバリアント解析を実行できるように

なりました。また、Secret　Scanningはすべてのパブリックリポジトリで無料で利用できるだけでなく、有効性チェックが可能になりました。

さらには、AIを駆使することで、最初から安全なアプリケーションを開発する手法に変革が起こり、従来の「シフトレフト」の定義が根本的に変わる可能性もあります。今回GitHubは、AIを活用した、GitHub　Advanced　Security内の3つの機能のプレビュー版とSecurity Overview機能の改善を確実に終えました。

Code Scanningによる自動修正で問題を迅速に解決



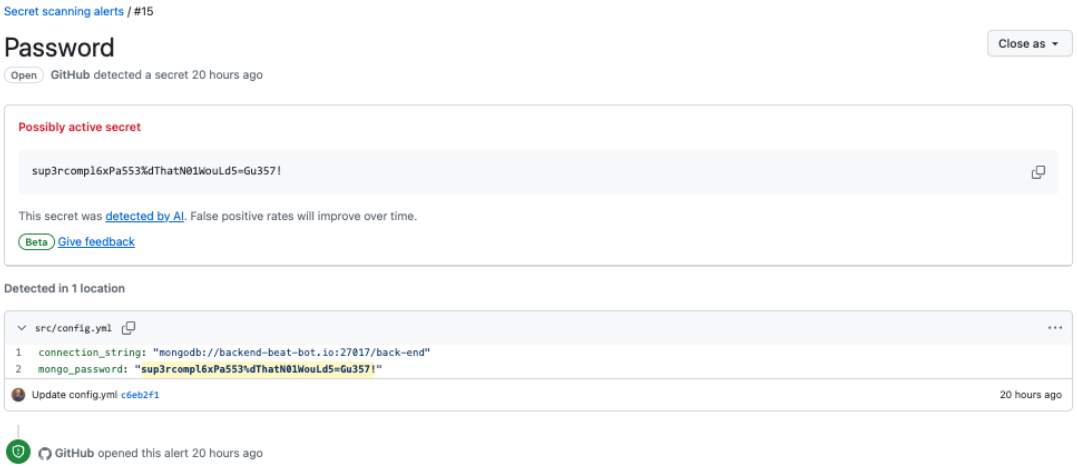
GitHubの静的分析エンジンであるCodeQLを利用したCode　Scanningに自動修正機能が追加され、修正時間の短縮、生産性の向上、技術的なセキュリティ負債の削減することで、より安全なコードを実現できるようになりました。

この新機能により、AIが生成したCodeQL、JavaScript、TypeScriptのアラートの修正をPull Requestで受け取れるようになります。これらはただの修正ではなく、すぐに使える正確な提案であり、脆弱性の内容とその修正方法を短時間で把握できます。これらの修正を即座にコードにコミットすることで、問題を速やかに解決し、コードベースの新たな脆弱性を防止できます。

CodeQL分析の後、GitHubは新しいアラートに対する修正を高度なLLMにシームレスに問い合わせます。AIが生成したこれらの修正提案は、Pull　Requestの[Conversation]タブと[Files　Changed]タブにコード提案として表示されます。その後、推奨された変更を確認して受け入れるだけでなく、コードベースにマージする前に提案された修正を編集することもできます。

この機能の優れている点は、ユーザーがコードを書きながら迅速に脆弱性を修正できるため、修正にかかる時間がさらに短縮され、不協和を生じさせることなく修正を行えることです。さらに、Code Scanningを利用した場合と同じ精度ですべてを実行できます。

漏洩したパスワードを**Secret Scanning**で検出

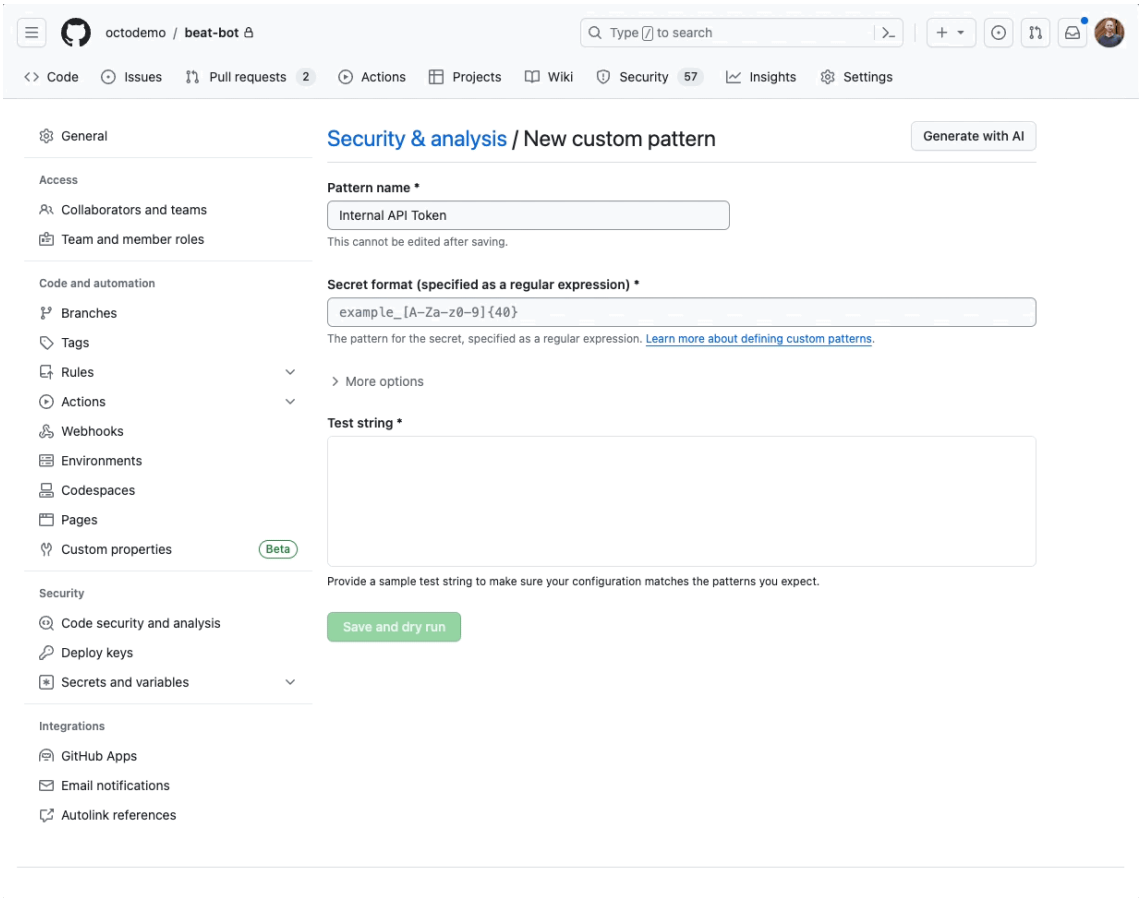


シークレット検出の中でも難しいカテゴリーがパスワードです。パスワードは一般的に漏洩しやすく、その結果、不正アクセスを狙う悪意のある攻撃者の格好の標的となっています。残念ながら、パスワードは特定のパターンに従うものではないため、シークレット検出ソリューションで検知することは困難ですが、最新世代のLLMでは従来の方法よりも少ない誤検出で、このようなパスワードを検出できるようになりました。

現在、限定的なパブリックベータ版として提供しているSecret　Scanningでは、AIの力を活用して、コード内の一般的なシークレットや構造化されていないシークレットを検出します。

スキャンの結果は、[Other]という別のタブに、信頼度の低いその他のパターンと共に表示されます。セキュリティマネージャーやリポジトリオーナーは、既存のUXで最も信頼性の高い、検出された問題の修正にも引き続き注力しながら、漏洩した可能性のある有効なパスワードに関するアラートをここで確認できます。アラートが妥当なものだと判断した場合は、開発者と協力して問題を解決できます。

カスタムパターンの正規表現ジェネレーターで時間を節約

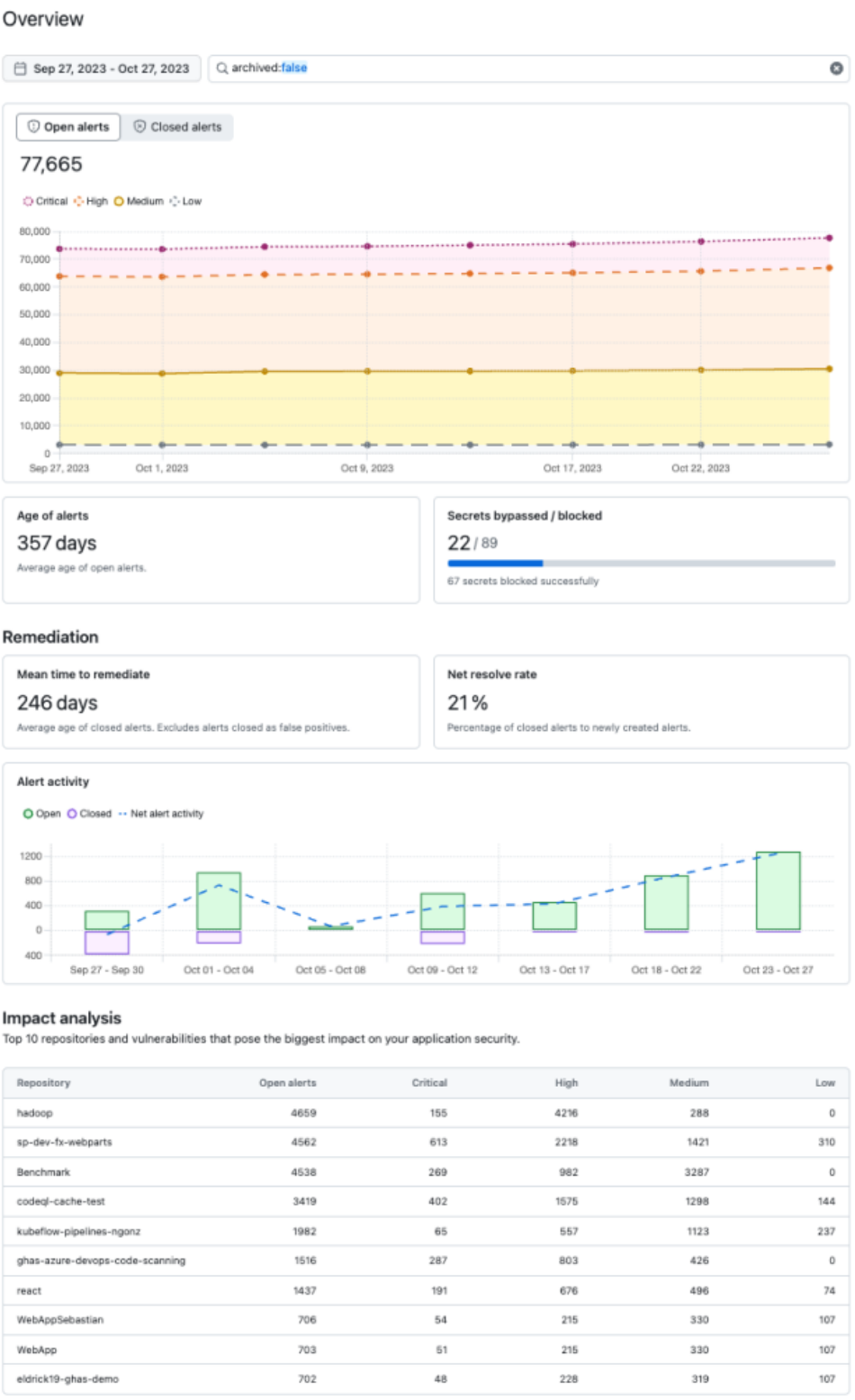


GitHubのSecret　Scanningパートナープログラムは180社のパートナーと225種以上のサポートパターンを誇る強固なものですが、ユーザーは組織独自のシークレットタイプを検出するために、さらにカスタムパターンを作成しなければならない場合があります。ミニコーディング言語の習得と同様に、正規表現の記述には多くのパラメーターや微妙な差異が含まれるため、習得には大変な労力を必要とします。

カスタムパターンの作成と更新をより容易かつ迅速にするため、GitHubはAIを利用したカスタムパターンのオーサリング機能を追加しました。このフォームベースの新機能では、いくつかの簡単な質問に答えるだけで、カスタムパターンが正規表現の形で自動生成されます。この新機能により、新たに作成したパターンを保存する前に、リアルタイムでドライランを実行してスキャンが適切であることを確認できます。

これらのアップデートは、時間の節約に非常に有効であるだけでなく、最終的にはシークレットの確実な保護に必要となる保障の獲得につながります。

新しいSecurity Overviewダッシュボードでより重要なデータを表示



Impact analysis

Top 10 repositories and vulnerabilities that pose the biggest impact on your application security.

Repository	Open alerts	Critical	High	Medium	Low
hadoop	4659	155	4216	288	0
sp-dev-fx-webparts	4562	613	2218	1421	310
Benchmark	4538	269	982	3287	0
codeql-cache-test	3419	402	1575	1298	144
kubeflow-pipelines-ngonz	1982	65	557	1123	237
ghas-azure-devops-code-scanning	1516	287	803	426	0
react	1437	191	676	496	74
WebAppSebastian	706	54	215	330	107
WebApp	703	51	215	330	107
eldrick19-ghas-demo	702	48	228	319	107

GitHub Advanced Securityは開発者を対象に作られていますが、成功を収めているセキュリティプログラムはいずれも、開発者とセキュリティチームが共同で作業しています。今回、Security Overviewダッシュボードが新しくなったことで、セキュリティマネージャーや管理者は、GitHub上のセキュリティアラートに過去のトレンド分析を加えて使用できるようになりました。

このダッシュボードを使用すると、リスク、修正策、防止策を通じて、組織の全体的なセキュリティの状況を把握できます。

- リスク:リポジトリ全体で検出されたセキュリティ上の問題に加えて、検出された問題が増減した箇所や検出された問題のカテゴリーも示します。
- 修正策: 現在の修正策の有効性を把握するのに役立ちます。例えば、検出されたセキュリティ上の問題の何件が修正されたのか、組織全体の平均修正時間はどれくらいかなどを把握できます。
- 防止策: プッシュ保護などの機能でセキュリティ上の問題が防止された箇所を明確に把握できます。

これらのタイルは、日付範囲やリポジトリなどの基準でデータをフィルタリングすると動的に変化するだけではなく、AppSecプログラムに関する差し迫った問題への対応策を、これまで以上に迅速に取得することができます。

より良いセキュリティが、開発者をより幸せにする

アプリケーションセキュリティテストを使用することで、開発者とセキュリティチームは、GitHub内ですでに作業しているセキュリティ問題に対して、より効果的に協力して検出、修正で対応できるようになります。GitHubは、AIの力を活用してアラートの関連性を高め、修正をよりスピーディーに行い、管理者エクスペリエンスを向上できることに期待を寄せています。チームの幸福度と生産性、さらにはコードの安全性が高まることが、GitHubの最終目標です。

AIを活用したセキュリティの可能性を体験するには、ウェイティングリストにお申し込みください。

本リリースの詳細については下記ブログもご覧ください。
GitHub Blog
英語:
https://github.blog/2023-11-08-ai-powered-appsec/

日本語:
https://github.blog/jp/2023-11-17-ai-powered-appsec/

GitHubに関する情報は、こちらからもご覧いただけます。
Blog: (英語) https://github.blog (日本語) https://github.blog/jp
X: (英語) @github(https://twitter.com/github)
(日本語) @GitHubJapan(https://twitter.com/githubjapan)

【GitHub について】https://github.co.jp
GitHubは、すべての開発者のためのグローバルホームとして、安全なソフトウェアの開発拡張、提供するための統合開発者プラットフォームです。フォーチュン100に名を連ねる企業のうち90社に所属する開発者を含む1億人以上がGitHubを利用し、3億3千万以上のリポジトリから、社会に素晴らしいものを創造し送り出しています。GitHubが提供するすべてのコラボレーション機能は、個人やチームがこれまでよりも迅速に、さらに高品質なコーディングをかつてないほどに容易にしています。

【製品／サービスに関するお問い合わせ先】
ギットハブ・ジャパン営業およびサポート窓口
Email: jp-sales@github.com