GitHub

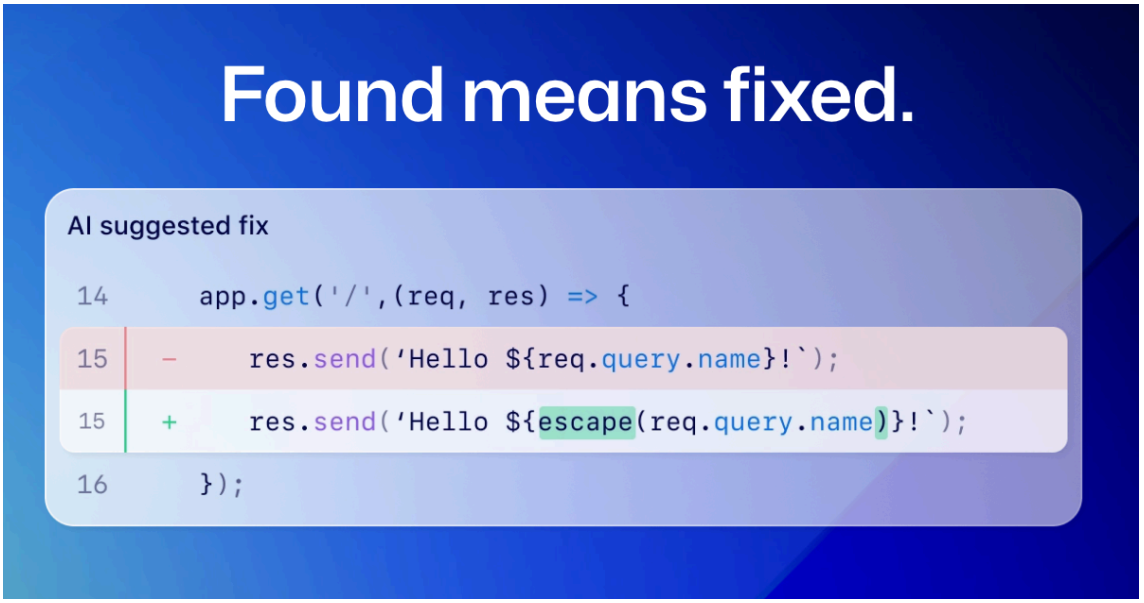
NEWS RELEASE

2024年3月28日
ギットハブ・ジャパン合同会社

GitHub、Code Scanningの自動修正機能のパブリックベータ版の提供を開始

GitHub CopilotとCodeQLと利用し、脆弱性の検出から修正提案に対応

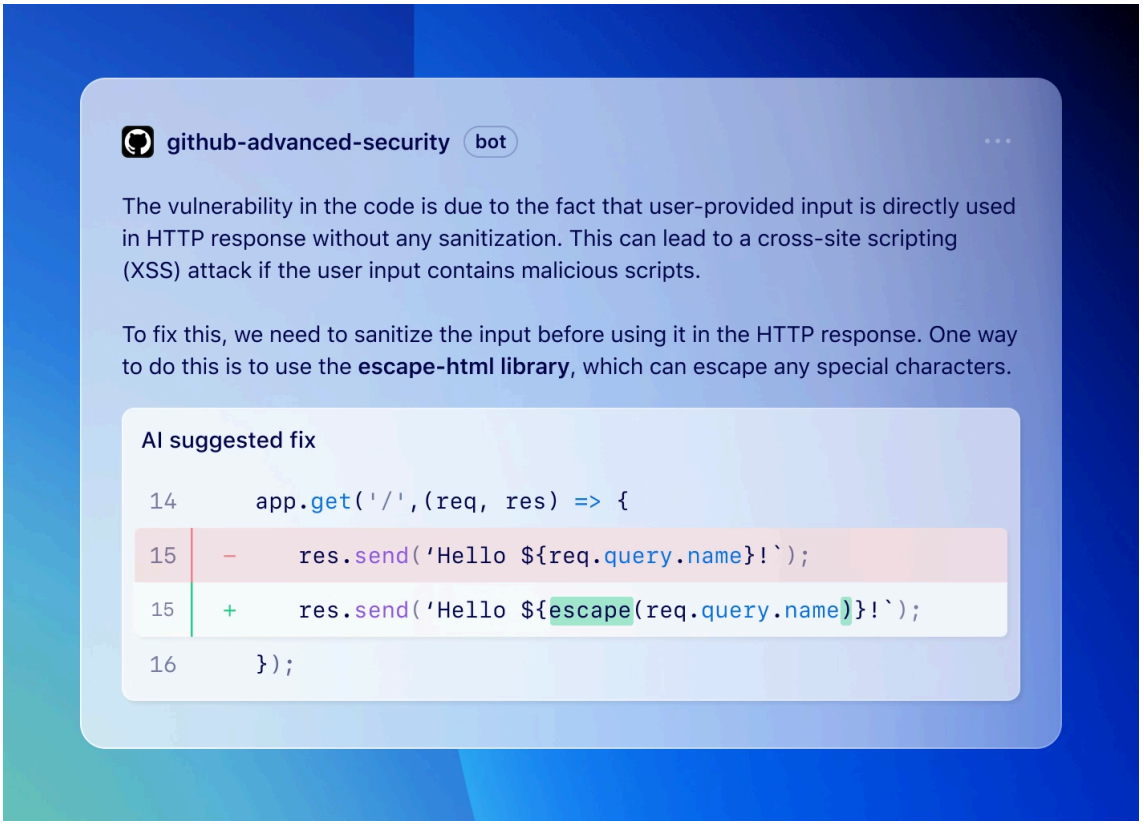
AIを活用したソフトウェア開発者プラットフォームとして世界をリードするGitHub, Inc.（本社：米国サンフランシスコ）は、2024年3月20日(米国時間)、GitHub Advanced Securityのすべての利用者を対象に、GitHub CopilotとCodeQLを利用したCode Scanningの自動修正機能のパブリックデータ版の提供を開始しました。



Code Scanningの自動修正機能は、JavaScript、TypeScript、Java、Pythonのアラートタイプを90%以上カバーし、検出された脆弱性の ⅔ 以上のほとんど、あるいはまったく編集することなく修正できるコードを提案します。

脆弱性の検出から修正提案まで

アプリケーションセキュリティに対するGitHubのビジョンは、「検出」が「修正」を意味する環境を構築することです。GitHubは、GitHub Advanced Securityでの開発者エクスペリエンスを優先事項としており、開発者チームは既に従来のセキュリティツールより7倍も迅速に修正可能になっています。Code Scanningの自動修正機能は、次なる飛躍的な進歩であり、開発者が修正に費やす時間と労力を大幅に削減できるよう支援します。

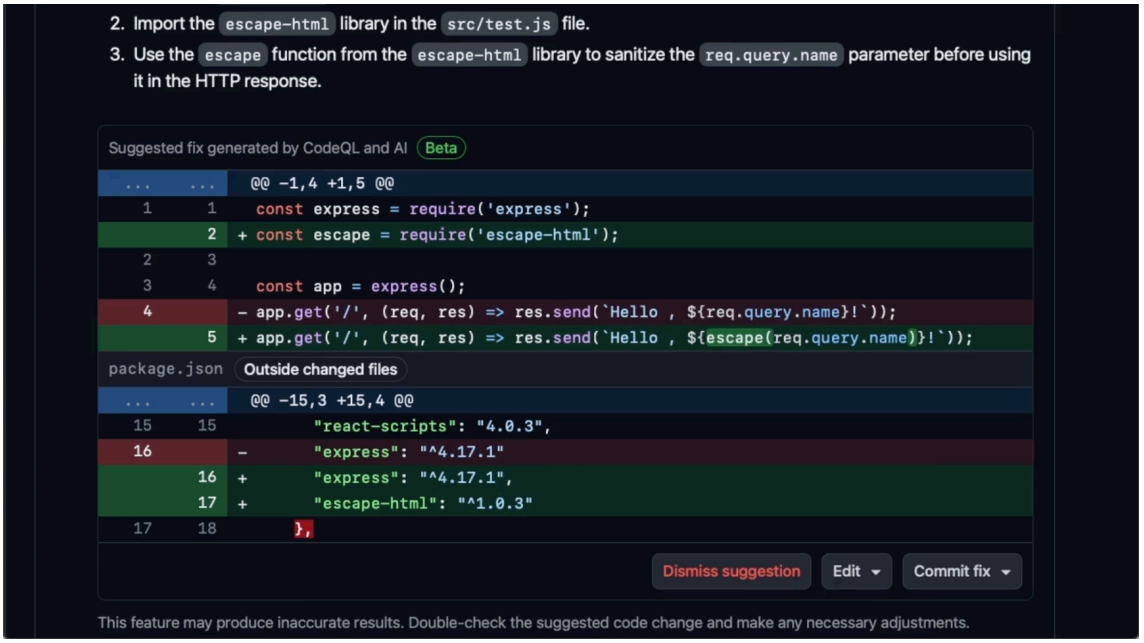


アプリケーションが依然として主要な攻撃ベクトルであるにも関わらず、多くの組織は、本番環境のリポジトリに存在する未修正の脆弱性の数が増え続けていることを認めています。Code　Scanningの自動修正機能を使うことで、開発者がコーディング中に脆弱性を容易に修正できることで、組織は「アプリケーションセキュリティ負債」の増加を抑制できるようになります。

GitHub Copilotが開発者を煩雑な反復作業から解放するように、Code Scanningの自動修正機能によって、開発チームはこれまで修復に費やしていた時間を取り戻すことができます。さらに、セキュリティチームにとっても、日常的な脆弱性の量が減ることで、加速し続けるソフトウェアの開発ペースに対応しながらビジネスを保護するための戦略に集中することが可能になります。

Code Scanningの自動修正機能の仕組み

サポート対象言語で脆弱性が検出された場合、修正提案には提案された修正に関する自然言語での説明とコード提案のプレビューが含まれます。開発者はこのコード提案を受け入れて編集、または却下することができます。これらのコード提案には、現行ファイルへの変更に加えて、必要に応じて複数のファイルへの変更、プロジェクトに追加すべき依存関係も含まれます。



Code Scanningの自動修正機能の仕組みについて詳しく知りたい方は、「セキュリティの脆弱性をAIで修正する」をご確認ください。

Code Scanningの自動修正機能は、裏側でCodeQL エンジン、ヒューリスティックとGitHub Copilot APIを組み合わせることによってコード提案を生成します。自動修正機能とそのデータソース、機能、制限の詳細については、「About autofix for CodeQL code scanning」をご確認ください。

今後の展望

今後も、C#とGoなどさらに多くの言語のサポートを追加を予定してます。

各種リソース

さらに理解を深めていただくために、GitHubはCode Scanningの自動修正機能を管理するシステムアーキテクチャ、データフロー、AIポリシーに関する広範なリソースとドキュメントを公開しています。

- Changelog: Code ScanningがプルリクエストのCodeQLアラートに対してAIを活用した自動修正を提案するように（ベータ版）
- エンジニアリングブログ: AIによるセキュリティ脆弱性の修正
- ドキュメント: CodeQL コード スキャンの自動修正について
- ディスカッション: 自動修正機能のフィードバックとリソース

GitHub Blog
英語:
https://github.blog/2024-03-20-found-means-fixed-introducing-code-scanning-autofix-powered-by-github-copilot-and-codeql/

日本語:
https://github.blog/jp/2024-03-28-found-means-fixed-introducing-code-scanning-autofix-powered-by-github-copilot-and-codeql/

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】
GitHubは、すべての開発者のためのグローバルなホーム(家)として、安全なソフトウェアの開発、拡張、提供を実現に向け世界有数のAI搭載開発者プラットフォームです。『Fortune 100』(グローバル企業の総収入ランキングトップ100)に名を連ねる90社の開発者を含む1億人以上の人々がGitHubを利用し、4億2,000万以上のリポジトリで素晴らしい共同作業を行っています。GitHubが提供するあらゆるコラボレーション機能により、個人やチームはかつてないほど容易に、より速く、より良いコーディングを実現しています。
GitHub.com (日本語サイト https://github.co.jp)

【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