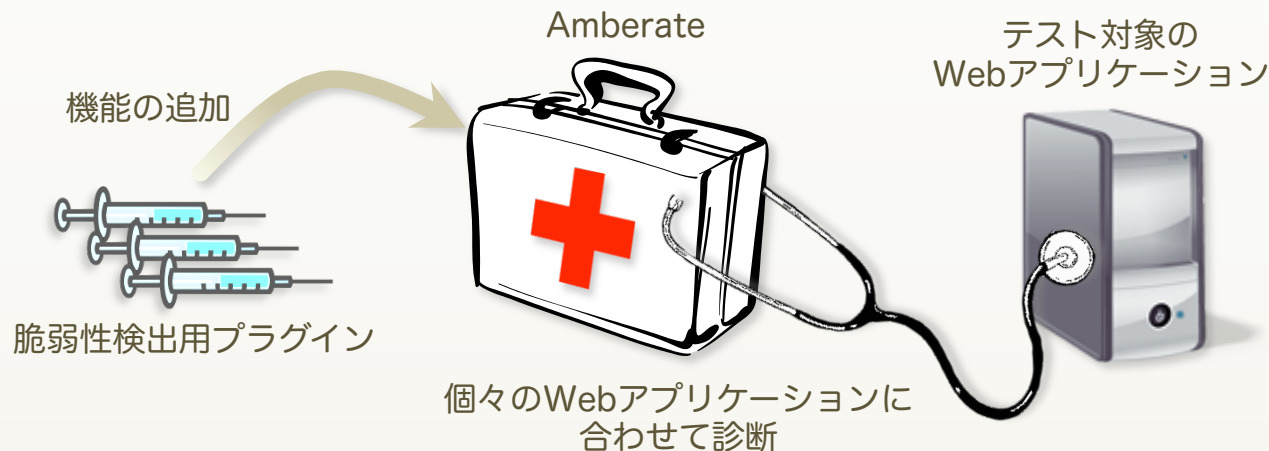


AMBERATE

ハッカーの頭脳を超える
高精度脆弱性検出

Webアプリケーション・セキュリティの自動検証フレームワーク



効率的かつ正確な脆弱性検出を実現

Amberateは、Webアプリケーションの脆弱性を検出するための攻撃テストをサポートします。各Webアプリケーションの仕様に合わせて、以下の3つのステップを実行します。

- ・ 攻撃が可能な箇所を正確に特定
- ・ 強力な攻撃を独自のアルゴリズムで自動生成
- ・ 構文解析や文脈解析を用いた高精度の脆弱性検出

本開発では以下の3つの攻撃に対する脆弱性を検出する手法を実装しました。

- ・ SQLインジェクション攻撃
- ・ クロスサイト・スクリプティング
- ・ JavaScript Hijacking

他の攻撃への対策手法も引き続き開発を行っています。

近年の巧妙な攻撃手法に対応

Web技術の高度化によって、攻撃手法が巧妙化しています。その結果、多種多様な脆弱性が報告されています。例えば、以下の特徴を持つ脆弱性が挙げられます。

- ・ 永続的データの不完全な安全化による存在する脆弱性
- ・ 複数のターゲットの相互作用により顕在化する脆弱性
- ・ ブラウザやWebアプリケーションの環境依存の脆弱性

既存の脆弱性検出ツールでは、これらの脆弱性を検出することができない、あるいは誤検知を引き起こしやすいという特徴があります。一方、Amberateはこれらの脆弱性検出を可能にします。本開発後半で行った既存のツールとの性能比較実験において、Amberateの優位性を具体的に示しました。

yuji@ssllab.ics.keio.ac.jp, <http://www.ssllab.ics.keio.ac.jp/~yuji/>