研究・技術シーズ集
ピックアップ

12

抽象構文木　静的解析，フロー解析

DOM-Based XSS対策

9 産業と技術革新の基盤をつくろう

Web開発者向けXSS対策支援システム

小林孝史
総合情報学部　総合情報学科

Point1　本研究の概要

Webアプリケーションの開発段階において、開発者へDOM-Based XSS脆弱性となりうる箇所を警告するシステムを提案しています。　本システムでは、JavaScriptによるプログラム開発時に、DOM-Based XSSの脆弱性が存在する場合には、SourceとSinkの箇所を開発者へ警告します。フロー解析に静的解析技術を使用しているため、従来の動的解析時に実行されずに発見できなかったSourceとSinkの組み合わせも発見することができます。

Point2　応用可能な分野

・Webデザインシステム
・Webプログラミング　等におけるXSS脆弱性対策

Point3　連携を希望する業種等

上記、応用可能な分野に関連すれば業種は問いません。

詳細な研究・技術シーズは次のページへ

情報通信

Web開発者向けXSS対策支援システム

用途・応用分野

- Webデザインシステム
- Webプログラミング等におけるXSS脆弱性対策

本技術の特徴・従来技術との比較

- 現在のWebアプリケーションには、XSS攻撃が可能なポイントが多数存在する。その対策は開発者（および開発者群）任せになっており、開発者のスキルに依存している
- このシステムにより、自動的に攻撃可能なポイントを検出し、開発段階でその修正が可能になる。検出に要する時間もごく僅かである

技術の概要

【DOM based XSS対策】

Webアプリケーションの開発段階において、開発者へDOM-Based XSS脆弱性となりうる箇所を警告するシステムを提案している。抽象構文木（Abstract Structure Tree）を用いたフロー解析を行うことで、動的解析における特定ブラウザへの依存や網羅性の限界といった課題を改善している。

本システムは、ESLintのカスタムルールとして実装されており、コマンドラインおよび対応したエディタにおいてリアルタイムに動作する。JavaScriptによるプログラム開発時に、JavaScriptが読み込まれると、パーサによって抽象構文木へ変換される。その後、カスタムルールにおいて、抽象構文木からユーザーからの入力等の箇所（location.hash等：Source）を探索し、ノードの種類に基づいて変数を遡りつつその箇所のデータを使用している部分（document.write(), eval()等：Sink）が存在していれば、DOM-Based XSSの脆弱性が存在するとして、SourceとSinkの箇所を開発者へ警告する。既にサニタイズ関数等が使用されていれば、警告はしない。

この技術は、フロー解析に静的解析技術を使用しているため、従来の動的解析時に実行されずに発見できなかったSourceとSinkの組み合わせも発見することができる。XSSサンプル集（Firing Range）の68サンプルで検証した結果、従来型の動的解析では62サンプルの検出であったところが、本システムにおいては68サンプルすべてを検出できている。本システムによる検出時間としては、全68サンプルの検出に約0.4秒しかかかっていない。

特許・論文

＜論文＞

中原・井手・前田・波多・小林、抽象構文木による開発者向けDOM-Based XSS対策支援システムの提案、信学技報, vol. 121, no. 410, ICSS2021-72, pp. 78-86, 2022年3月

研究者

小林　孝史
総合情報学部　総合情報学科
小林研究室

お問合わせ先
関西大学 社会連携部 産学官連携センター
TEL：06-6368-1245
MAIL：sangakukan-mm@ml.kandai.jp