DOM Based XSS対策におけるTrusted Typesの調査及び検証と構築支援手法の提案

金沢工業大学　工学部　情報工学科
中沢研究室　千村剛芳

研究背景

Webアプリケーションの脆弱性には様々な種類があるが、そのなかでもクロスサイトスクリプティング(XSS)はWebアプリ内に存在しやすく、またIPAなどへの報告件数が多い脆弱性として知られている。

- クロスサイトスクリプティング(XSS)
  Webアプリケーションの入力などに対する出力処理に問題がある場合、スクリプトが埋め込まれてしまう脆弱性。
  この脆弱性を利用することによって、個人情報の搾取や他人へのなりすまし、フィッシング詐欺などが行われてしまう可能性がある。

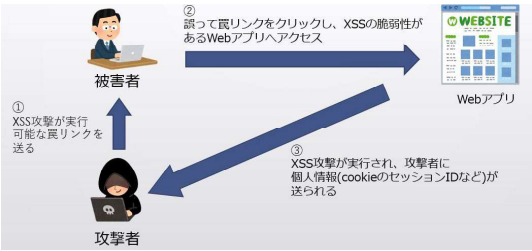

図１：XSSを利用した攻撃の一例

- DOM Based XSS
  Document Object Model(DOM)の操作などによるブラウザ側のJavaScriptの出力処理に不備があることでスクリプトが埋め込まれてしまう脆弱性。
  DOM Based XSSが作りこまれてしまう原因になるメソッドやプロパティをシンクと呼ぶ。

element.innerHTML	HTMLの要素を変更する
location.href	URLを取得する
document.write	文字列を表示する
eval()	スクリプトを評価・実行する

図２：シンクの例

- Trusted Types
  シンクに渡される文字列をDOM Based XSSを防ぐポリシー(ルール)によって検証し、安全な型(Trusted Type)に変更してシンクを実行する、新しいDOM Based XSS対策。
  2019年からChromeなどのブラウザで実験的に導入が進んでいる。
  Trusted Typesがブラウザで有効になっている場合、シンクはTrusted Type型以外受け付けなくなり、Trusted Type型ではない文字列を渡そうとした場合にはエラー処理が行われる。

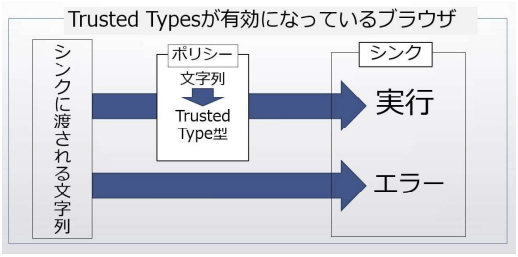

図3：Trusted Types

・シンクによってXSSが実行されなくなる
⇒DOM Based XSSがなくなる

・DOM Based XSSの対策ができているかどうかは、ポリシーを見ることで判断できる
⇒脆弱性診断におけるセキュリティエンジニアの負担軽減

などのメリットを挙げることができる

問題点

・Trusted TypesのポリシーはWebアプリケーション開発者自身の手で作る必要がある
⇒ 開発者にもWebセキュリティ(DOM Based XSS)に関する知識が必要になる

・Trusted Typesは提案されたばかりの対策手法であり、DOM Based XSSを防ぐ「適切なポリシー」が定義されていない
⇒ポリシーに不備があった場合、DOM Based XSSを防止できない可能性がある

・開発時に、Trusted Typesのポリシーの違反が発生しないように意識してコードを書く必要がある
⇒Webアプリケーション開発時の作業コストが増える

・既存のWebアプリケーションでTrusted Typesを構築するには、「ポリシーの追加」と「シンクを見つけ出してポリシーを適用できるように周辺のコードを書き換える」必要がある
⇒Webアプリケーションの規模が大きくなればなるほどTrusted Typesを使えるようにするのに手間がかかる

提案方法

シンクによってDOM Based XSSが発生するWebアプリケーションをいくつか作成し、実際にTrusted Typesを実装して、「適当且つ適切なポリシー」は何か検証する

結果を元に開発者のTrusted Typesの構築を支援する手法の提案・実装を行う

構築支援手法の一例

静的解析などを用いて、全てのシンクに渡される文字列がTrusted Type型に変更されるように、シンク周辺のコードを自動で書き換えるシステム
(ポリシーは検証から得られた「適当且つ適切なポリシー」を使用)

・開発者の作業コストの削減

・既存のWebアプリケーションに対するTrusted Types構築が容易になる

今後の予定

・Trusted Types検証用Webアプリケーションの作成

・構築支援手法の設計・使用技術の検討・実装

・評価方法の検討

参考文献

IPA、IPAテクニカルウォッチ
「「DOM Base XSS」に関するレポート」2013年1月29日発行
URL：https://www.ipa.go.jp/files/000024729.pdf
(2021年9月12日閲覧)