リクエストパラメータ変換によるWebアプリケーション脆弱性診断ツールの精度向上に関する研究

Improving Web Application Vulnerability Testing Tool by Request Parameter Conversion

木村正太朗・ネットワーク分科会・情報セキュリティ大学院大学

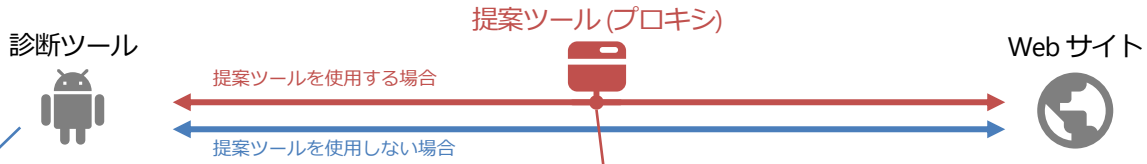
Abstract: Tools are commonly used in web application vulnerability testing for automation, but they sometimes cannot detect vulnerabilities properly due to the occurrence of false negatives. In this research, we investigated using actual assessment data and conducted verification experiments in order to clarify the causes of false negatives generated by such tools. As a result, we found that some tools could not properly recognize request parameters such as HTTP request headers and file names when uploading files. To solve this problem, we propose a method to convert the request parameters between the tool and the web application. This method uses a proxy to add request parameters that the tool can recognize, and to replace the values of those request parameters with the values of ones that the tool cannot recognize. With this method, it is possible to expand the number of request parameters that can be tested and improved the accuracy of detection.

研究背景

WebAP 脆弱性診断ツールで偽陰性が発生

研究目的

偽陰性が発生する原因の特定と解決策の提案



偽陰性発生原因の調査

- 実際のWeb診断のデータを用いた調査を実施
- 診断ツールが認識できないパラメータがあった
  - → HTTPリクエストヘッダ、ファイル名、JSON 等

提案手法 (提案ツール)

- 診断ツールにパラメータを追加で認識させる
- 追加されたパラメータを目的のパラメータに置換
  - → 診断ツールが診断できないパラメータも診断可能に

Referer ヘッダを診断できないツールに対し	EXPRAM_referer パラメータを追加で認識させて	Referer ヘッダの値に置換 (追加パラメータは削除)
POST /test?query=aaa HTTP/1.1 (省略) Content-Type: application/x-www-form-urlencoded Referer: http://www.example.com/ form=bbb	POST /test?query=aaa HTTP/1.1 (省略) Content-Type: application/x-www-form-urlencoded Referer: http://www.example.com/ form=bbb**&EXPRAM_referer=ccc**	POST /test?query=aaa HTTP/1.1 (省略) Content-Type: application/x-www-form-urlencoded Referer: **ccc** form=bbb~~&EXPARAM_referer=ccc~~

実験と評価

- テスト用の WebAP を作成し 5種のツールで診断
  - → 多様なパラメータに対して脆弱性を埋め込んだ既存のテスト用 WebAP がなかったため
- 診断ツールが対応しているリクエスト形式では認識できないパラメータに対して診断可能に
  - → Vega、Arachni では Multipart リクエストに非対応

本来の検知精度を低下させずに
診断可能パラメータを拡張させることが可能

タイプ	Z	V	S	W	A
一般的なパラメータ	✓	✓	✓	✓	✓
HTTPリクエストヘッダ	✓	✓	✓	★	★
ファイル名	✓	–	★	★	–
JSON	★	–	★		

凡例　✓: 提案手法なしで診断可能　★: 提案手法の使用によって診断可能
–: 提案手法を使用しても診断できず　網掛け: 実施せず
ツール名　Z: OWASP ZAP　V: Vega　S: Sqlmap　W: Wapiti　A: Arachni

今後の方針

- 実用化に向け HTTPS 使用時への対応や影響調査
- JSON 形式の XSS を診断可能にする仕組み作り