SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

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 * 大久保 隆夫 *
Shotaro Kimura Takao Okubo

キーワード Web アプリケーション，脆弱性診断ツール，偽陰性

あらまし

Web アプリケーション脆弱性診断では，自動化のためにツールを用いることが一般的であるが，偽陰性の発生によって十分に脆弱性を報告できていない場合がある．ツールの偽陰性発生原因を明らかにするため，実際の診断データの調査，及びそれを基に実験を実施した結果，一般的でない入力パラメータに対して診断ができないツールが存在しており，偽陰性発生原因の 1 つとなっていることが明らかとなった．本稿では，こうした一般的でないパラメータに対する診断手法として，プロキシによりリクエストパラメータを変換することで診断を可能にするツールを提案する．

背景

Web アプリケーション脆弱性診断ツール（以下，診断ツール）は定型的な診断の自動化を得意としているが，筆者の経験によれば定型的な診断においても偽陰性が発生し，脆弱性を正しく報告出来ていない場合がある．本稿では診断ツールが偽陰性を発生させる原因を究明し，それに対する解決策を提案することを目的としている．

偽陰性発生原因の調査

実際の Web 診断のデータを用いて，診断ツールが脆弱性を検出できなかった事例を調査した．その結果，一般的でないパラメータに脆弱性が存在していた場合に，脆弱性を正しく検出できない事例が存在していた．

* 情報セキュリティ大学院大学，221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1，Institute of Information Security，2-14-1，Tsuruyacho，Kanagawa-ku，Yokohama，Kanagawa，Japan

既存の研究でこうしたパラメータに対する評価ができているかを調査するため，複数のベンチマーク用 Web アプリケーションの仕様を調査した．その結果，いずれも一般的でないパラメータには脆弱性が存在しておらず，多様な入力パラメータに対して正しく診断できているかを評価できないことが分かった．

診断ツールが多様な入力パラメータに対しても正しく診断できるかを明らかにするため，テスト用の Web アプリケーションを作成し，実験を行った．その結果，そもそも入力パラメータとして認識しておらず，正しく診断できないツールがあることが明らかとなった．

提案手法と結果

診断ツールが診断できないパラメータに対しても診断できるようにするため，診断ツールと診断対象の Web サイトの中間で動作し，診断ツールが発生させたリクエストのパラメータを変換するプロキシを提案する．提案ツールでは，診断ツールが診断できるパラメータを追加させ，実際に診断したいパラメータと置換している．

提案ツールの使用によって，診断ツールが診断できないパラメータに対して診断ができるようになり，脆弱性検出率も向上した．これはプロキシによってリクエストパラメータを改変する方法は，既存の診断ツールを拡張する有効であることが示された．一方で偽陽性の報告の増加や診断時間の増加も確認され，課題も残った．

参考文献

[1] M. Rennhard, et al., “Improving the Effectiveness of Web Application Vulnerability Scanning”, International Journal on Advances in Internet Technology, vol. 12, pp. 12-27, 2019