脆弱性診断情報を用いたWAFのログ精査を支援する手法の提案

Proposal of a Method to Support the Scrutiny of WAF Logs Using Vulnerability Assessment Information

荒木 粛志・システム分科会・情報セキュリティ大学院大学

In recent years, as the number of users of Web applications has increased, the number of attacks targeting the vulnerabilities has also increased. Therefore, the demand for attack detection / prevention technology is increasing, and WAF (Web Application Firewall) is especially important. On the other hand, when operating a WAF, it is necessary to carefully examine the logs output by the WAF, and securing costs and human resources for that purpose is an issue for the operation of the WAF. Therefore, in this paper, we propose a method to support the scrutiny of the log output by the WAF. As an outline of the method, we are considering using the information from the vulnerability diagnosis tool and the WAF log information to judge the effectiveness and threat level of the attack and classify it so that it can be visually grasped.

1.研究背景と目的

・近年、Webアプリケーションを狙った攻撃が増加
攻撃を検知・防御する技術として、
WAF(Web Application Firewall)の需要が高まる
・一方で、WAFの運用には、攻撃検出時にログ精査作業が必要であり、導入・運用上でのコストとなる

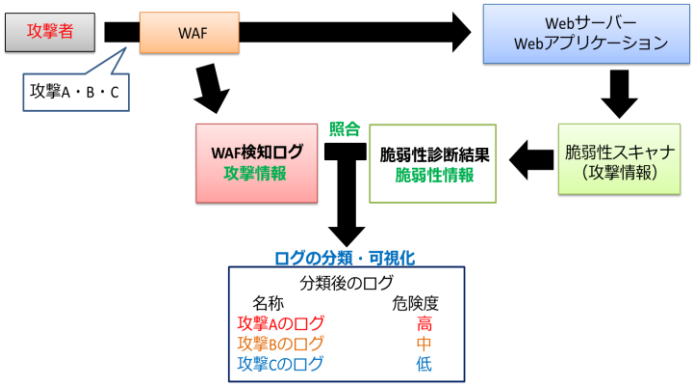
WAFが出力するログの精査を支援する手法を提案

2.提案手法

①Webアプリケーションを対象とする脆弱性診断や脆弱性スキャナを用いて、防御対象の脆弱な箇所を発見

②WAFが出力する攻撃ログ情報と照合することで、攻撃が成功するかどうかや、攻撃の影響度を判定

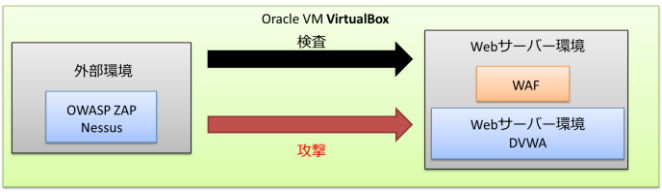
③上記結果をもとに、攻撃検知ログの脅威度を分類し、表の作成や脅威度ごとの色分け等により可視化



3.検証について

①提案した手法による精査・分類・可視化を正しく行うことが可能かどうかを確認
②検証や今後の研究で使用するツール・データについて、検証結果から整理し、選定

※使用するツール・データについては、
基本的には公開されているものを利用
・WAF　Mod Securityを使用
・脆弱性スキャナ
OWASP ZAPとNessusの二種類を用いる
・攻撃対象となる環境
仮想環境においてWebサーバーを構築
そこに脆弱性のあるアプリケーションである
DVWA を用意



4.今後の展望

今後の研究の課題として、
・脆弱性診断情報とWAF出力ログの照合が可能であることの検証を進める
・検知した攻撃の脅威度を評価・分類可能かを確認し、可視化の例を作成　等