

ウェブサイト攻撃の検出ツール

iLogScanner V3.0 の開発

株式会社ラック

概要

近年、ウェブサイトを狙った攻撃は、ウェブアプリケーションの脆弱性を突く攻撃に変化してきており、一般のウェブサイト管理者は、脆弱性対策を行う動機付けとして、自社運営のウェブサイトがどれほどの脅威を受けているかを確認する必要がある。

ウェブアプリケーションが受けている攻撃について、ウェブサイト管理者が容易に状況を把握できる手段としてウェブサイト脆弱性検出ツール **iLogScanner** が提供されている。ウェブサイト脆弱性検出ツール **iLogScanner** とは、利用者環境上で Web サイトのアクセスログを解析し、Web アプリケーションへの攻撃有無を利用者へレポートするツールである。今回、前回のバージョンより多くの脆弱性を検出できるようにし、新たなログ形式の解析機能を追加した **iLogScanner V3.0** を開発した。

1. 背景

近年ウェブサイトを狙った攻撃は、OS などの製品ソフトウェアの脆弱性を突く攻撃から、ウェブアプリケーションの脆弱性を突く攻撃に変化してきている。

一般のウェブサイト管理者は、そうした攻撃の対策を行うにあたり、自社運営のウェブサイトがどれほどの脅威を受けているのか、状況を確認する必要がある。また、状況確認の結果として、インターネットに公開しているウェブサイトの危険性を認知してもらうことで、ウェブサイト管理者や経営者が対策を講じるきっかけとなる事も期待される。

2. 目的

ウェブアプリケーションに対してどれほどの攻撃を受けているのか、ウェブサイト

管理者が状況を把握することは通常容易ではないため、容易に把握できる手段を提供していく必要がある。そこで、ウェブサイトのアクセスログおよびエラーログを解析することで、そのサイトへの攻撃痕跡を確認でき、一部の痕跡に関してはその攻撃が成功した可能性を確認できるツールを開発する。

3. 開発報告

(1) システム概要

本プロジェクトでは、ウェブサイト脆弱性検出ツール **iLogScanner V3.0** (以下、「当ツール」という) として、利用者環境上でウェブサイトのアクセスログおよびエラーログを解析し、ウェブアプリケーションへの攻撃の有無を利用者へレポートするツールを開発した。利用者の環境でツール

を実行することで、利用者のウェブサイトのアクセスログを外部に送信せずに解析を行うことが可能である。

システム概念図を図1に示す。

利用者は解析を希望するウェブサイトのアクセスログファイル（および、エラーログファイル）を用意し、ウェブブラウザから検出ツール提供用のウェブページ(HTML)へ接続する（図1-①,②）。検出ツールは独立行政法人 情報処理推進機構（以下 IPA と記す）のウェブサイトに配置し、利用者のウェブブラウザからの要求に従い利用者環境へダウンロードして実行する形態である（図1-③）。検出ツールは利用者が指定したアクセスログファイル（またはエラーログファイル）を解析対象として解析処理を実行し、解析結果を印刷可能な形態で提供する（図1-④,⑤）。

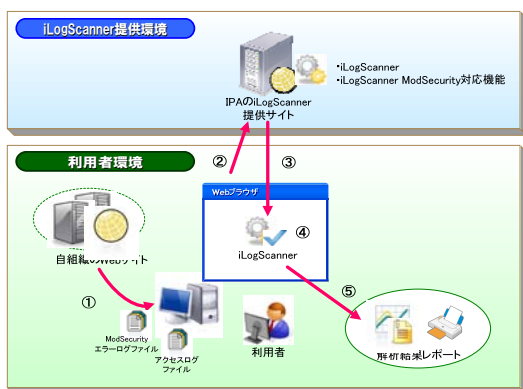


図1. システム概念図

(2) 機能構成

当ツールが実行可能な動作環境を表1に示す。

表1. 実行可能な動作環境

OS :	Microsoft Windows XP Professional SP3
ウェブブラウザ :	Internet Explorer 7.0
JRE :	Sun Java Runtime Environment 6.0 以上 (6.0 系を推奨)

当ツールの機能構成を図2に示す。

HTML コンテンツと当ツールを配置する IPA の検出ツール提供サイトを使用し、アプリケーションは、Java Applet(アプレット)によって実装される。

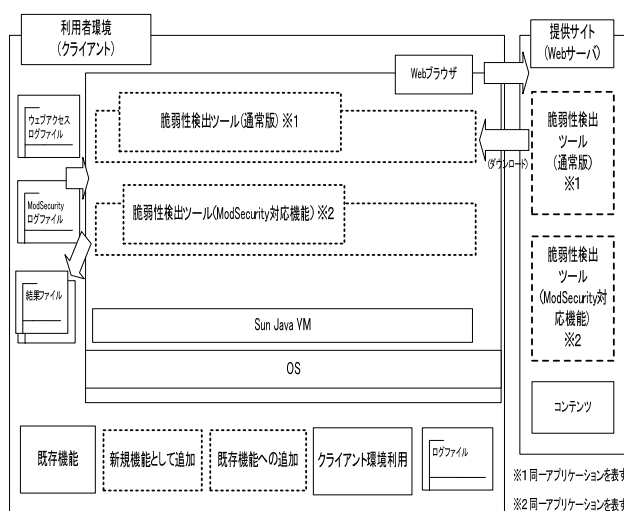


図2. 機能構成

(3) プログラムへの電子署名

Java Applet は、ウェブページの一部として自動的に読み込まれて動作するため、ダウンロード元サーバ以外との通信ができず、実行するクライアントマシンのローカルリソースやデバイスにアクセスできない等のセキュリティ機能による動作制限が課

せられている。この動作制限は、提供する Java Applet に電子署名し、利用者が Java Applet 実行時に許諾することにより、外すことが可能である。

当ツールは、Java Applet によって実装され、実行するクライアントマシンのローカルリソースへアクセスする必要がある。その為、当ツールでは電子署名を行っている。

(4) アクセスログ解析機能

指定されたアクセスログファイルに対し、検出対象カラムにある文字列中から各シグネチャとのマッチングや、設定条件を変更して、脆弱性を突いた攻撃の有無を調査する。また、結果を利用者へレポートする。アクセスログ中に攻撃の痕跡が見つかった場合、攻撃が成功した可能性の高いものについての判定を行う。

当ツールで解析が可能なアクセスログの形式は以下の 3 種類である。

- IIS5.0/5.1//6.0/7.0 の W3C 拡張ログファイルタイプ
- IIS5.0/5.1//6.0/7.0 の IIS ログファイルタイプ
- Apache1.3 系、Apache2.0 系、Apache2.2 系の common タイプまた、検出対象とする脆弱性を表 2 に示す。

表 2. 検出対象脆弱性

No	検出対象脆弱性名	検出
1	SQL インジェクション	◎
2	OS コマンド・インジェクション	○
3	ディレクトリ・トラバーサル	○
4	クロスサイト・スクリプティング	○
5	その他 (IDS 回避を目的とした攻撃)	○

◎ : 攻撃の痕跡と攻撃の成功の可能性を検出

○ : 攻撃の痕跡を検出

解析に使用するシグネチャには、弊社のジャパンセキュリティオペレーションセンター (JSOC) にて検出頻度の高いウェブアプリケーション攻撃文字列を中心にリストアップしたものを、IPA にて精査し使用している。

オプション選択画面で解析レベルの詳細を選択時、以下 3 項目による解析を追加を行っている。これらは、以下の条件を設定し、その条件を満たした場合に攻撃の可能性があると判断している。

- ① 同一 IP アドレスから同一 URL に対する攻撃の可能性

攻撃検出用シグネチャによる解析結果に対して、表 3 に示した基準にて、再解析を行う。表中の全ての条件を満たす場合、攻撃と判断する。

表 3. ①の判定の条件

No	攻撃判定の条件
1	同一 IP アドレスから同一 URL (CGI、ASP、JSP 等を含むウェブアプリケーション全般) に対する攻撃痕跡が一定件数に達している
2	同一 IP アドレスからの攻撃痕跡が一定件数に達している

- ② アクセスログに記録されない SQL インジェクションの兆候

アクセスログに表 4 に示した条件を全て満たすリクエストが記録されている場合、ログに記録されないタイプの

SQL インジェクション攻撃が行われた可能性がある」と判断する。

表 4. ②の判定の条件

No	攻撃判定の条件
1	アクセスログに記録されたリクエストの応答コード（サーバレスポンス）が 5xx 番台であること かつ POST メソッドであること
2	条件 1 に合致するリクエストが ・同一 IP アドレスにより、一定時間以内に規定回数以上行われている

③ ウェブサーバの設定不備を狙った攻撃

アクセスログ内に表 5～表 7 該当するリクエストが検出された場合に、攻撃が行われた可能性がある」と判断する。

表 5. PUT メソッドの設定不備

No	攻撃判定の条件
1	リクエストのメソッドが PUT であること
2	リクエストに対する応答コードが 201 であること

表 6. FrontPage Server Extensions の設定不備

No	攻撃判定の条件
1	FrontPage Server Extensions の設定不備を狙うような、特定ファイル（URL）に対するリクエストが行われていること

表 7. Tomcat の設定不備

No	攻撃判定の条件
1	Tomcat の設定不備を狙うような、特定ファイル（URL）に対するリクエストが行われていること

これらの判断に使用している基準値や条件は、弊社のジャパンセキュリティオペレーションセンター（JSOC）のアナリストが提示したものである。

(5) エラーログ解析機能

ModSecurity 2.5 系（Breach Security 社が提供する WAF の機能を有するソフトウェア）が出力する Apache のエラーログファイルを元に ModSecurity で検出・遮断したデータを解析する。解析したデータの統計情報を出力し、その解析データと Apache のアクセスログから検出された攻撃と思われる痕跡をマッチングして、ウェブアプリケーションへの攻撃の可能性を提示する。

(6) ユーザーインターフェイス（アクセスログ解析機能）

当ツールの実際の画面を図 3～7 に示し、アクセスログ解析処理の流れを説明する。

① 解析対象ログファイルの設定

図 3 にツール実行画面を示す。

【アクセスログファイル入力画面】

※は必須項目です

解析したいアクセスログファイルを指定してください。

アクセスログ形式： ※

解析対象アクセスログファイル名： ※

参照...

解析結果の出力先ディレクトリを指定してください。

出力先ディレクトリ： ※

参照...

下記ファイルの出力先ディレクトリを設定します。
出力するファイルは、実行日をもとにしたファイル名称となります。

- ・ 解析結果レポートファイル(iLogScanner_年月日_時分秒.html)
- ・ 解析結果ログファイル(iLogScanner_年月日_時分秒.log)

【例】 iLogScanner_20071217_121212.html

注意：同じ名称のファイルがある場合は上書きされます。

解析開始...

詳細内容を指定してください。(任意)

* 指定しない場合、解析レベルは「標準」となります。

オプション...

現在の設定内容

- ログフォーマット： -
- 解析対象範囲： -
- 解析レベル：標準

図 3. ツール実行画面

以下の項目を設定し、[解析開始...]ボタンをクリックすると、解析を開始する。

- ・ アクセスログファイルの種類
- ・ 解析対象アクセスログファイル
- ・ 結果ファイル出力先ディレクトリ

② オプション設定

以下の項目が設定できる。[解析開始...]ボタンをクリックすると、解析を開始する。

- ・ Apache アクセスログのフォーマット指定

- ・ 解析対象のログの日付範囲指定解析レベル

【オプション設定画面】

アクセスログファイル入力画面設定内容

現在の設定内容

アクセスログ形式： IIS5.0/5.1/6.0/7.0のIISログファイルタイプ

アクセスログファイル名： iLogScanner_error.log

出力先ディレクトリ： C:\Documents and Settings\togashi\My Documents

※は必須項目です

アクセスログフォーマットを指定してください。

ログフォーマット：

標準で定義されているCommon形式の場合、および先頭からの書式がcombined形式にて記録している場合は、未入力としてください。

【例】 LogFormat "%h %l %u %t" "%r" "%s %b" common

解析対象とするアクセスログ日付の範囲を指定してください。

開始日 (From)：

年 月 日

終了日 (To)：

年 月 日

日付を指定する場合、年月日の全てを指定してください。
解析対象とするアクセスログ日付の範囲を設定します。
アクセスログファイルのすべてのログを解析対象とする場合、未入力としてください。

解析レベルを指定してください。

解析レベル： ※

標準

アクセスログに対する解析の詳細度を設定します。
詳細を選択した場合、標準に比べて解析に時間が掛かる場合がありますので、ご了承ください。

標準に戻す 戻る 解析開始...

図 4. オプション設定画面

③ アクセスログ解析実行

図 5 に解析実行中画面を示す。

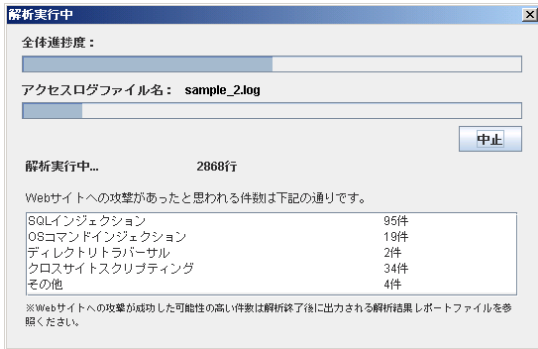


図 5. 解析実行中画面

解析実行中画面には全体解析進捗度と 1 ファイル毎の解析進捗度、検出対象脆弱性毎の攻撃痕跡検出数が表示される。攻撃痕跡の検出数は攻撃を検出する度、更新する。解析中であっても、中止ボタンを押すことによって処理を中断することができる。

解析終了、または解析を中止した場合、指定された出力先に解析結果レポートファイルを保存する。また、攻撃の痕跡が検出された場合は解析結果を詳細ログファイルに出力し保存する。

④ 解析結果

図 6 に、解析結果画面を示す。

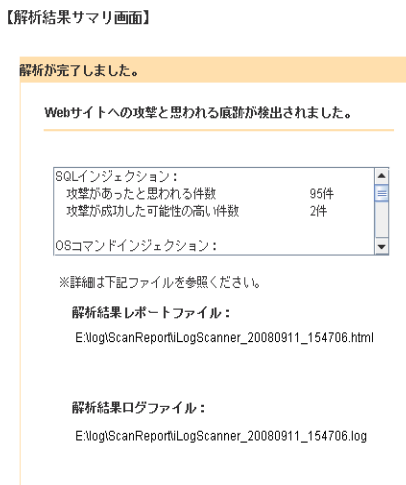


図 6. 解析結果画面

一つの脆弱性項目に対し、攻撃があったと思われる件数、攻撃が成功した可能性の高い件数をそれぞれ表示する。また、解析結果レポートファイル名と解析結果ログファイル名も同様に表示する。

⑤ 出力ファイル

当ツールでは解析終了後、利用者によって指定されたディレクトリに以下のファイルを出力する。

- 解析結果レポートファイル
- 解析結果ログファイル

図 7 に、解析結果レポートファイルを示す。

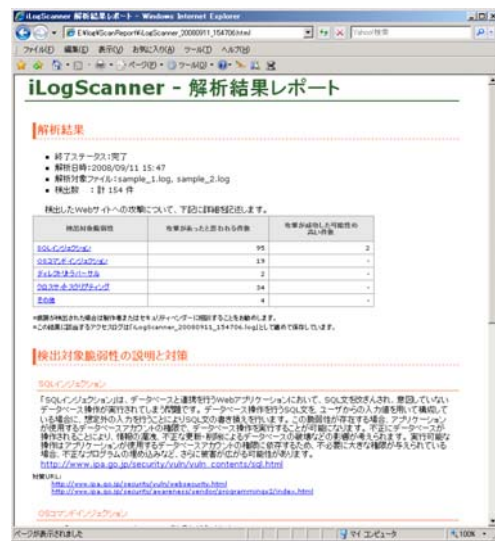


図 7. 解析結果レポート画面

レポートファイルには解析結果サマリ情報が記載される。また、攻撃の痕跡が検出された場合のみ、解析結果の詳細を記載したログファイルが出力される。

4. ツールによる効果

当ツールを用いることで、ウェブサイト管理者はウェブアプリケーションへの攻撃の可能性への有無や、ウェブアプリケーションに潜む脆弱性を比較的簡単に確認することが可能である。

また、当ツールの使用を通じて、インターネットに公開しているウェブサイトの危険性を認知してもらうことは、ウェブサイト管理者や経営者が対策を講じるきっかけとなる等、啓蒙活動としての効果が期待できる。

5. 今後の課題

さまざまな形式のログファイルに対して検出が可能になるように、機能追加や改善が必要である。また、より多くの脆弱性を検出可能にするため、シグネチャの拡充も行っていく必要がある。