

# 統合セキュリティ診断ツールに対する Web 診断機能の拡張

河内 清人, 河木 理一, 藤井 誠司†

三菱電機株式会社 ††

## 1. はじめに

インターネットの発展に伴い, インターネットに接続して利用する計算機およびソフトウェアの脆弱性が大きな問題となっている。最近では市販の計算機および有名なソフトウェアの脆弱性だけではなく, クロスサイトスクリプティング等の Web アプリケーションの脆弱性についても問題視されるようになってきている。

過去に我々は, 統合セキュリティ診断ツール[1]を提案, 開発を行ってきたが, 今回, Web アプリケーションの脆弱性診断も可能となるよう, ツールを拡張した。統合セキュリティ診断ツールはスクリプトと呼ばれる検査シナリオに従って攻撃者と同様, 様々な攻撃を組み合わせた侵入テストを行えることが特長であり, 本ツールに Web 脆弱性診断機能を追加することで, より広範な侵入テストを実施することが可能となる。

本稿では今回拡張した Web 診断機能の機能及びその実装方式について述べる。

## 2. Web アプリケーション診断

Web アプリケーションとは Web サーバ上で動作し, ブラウザによって操作可能なアプリケーションを指す。Web アプリケーションは, クライアントが HTTP リクエストを送信することで起動し, リクエスト中の URL や POST データ, Cookie 等に基づいて処理を行い, 結果を HTTP レスポンスとして返す。

本稿で対象としている Web アプリケーション診断は, 上記データや, その他のヘッダ情報に, 脆弱性を発現させる可能性のある様々な検査文字列を入力した HTTP リクエストを送信し, それに対する Web アプリケーションの応答を解析することで行われる。

さらに, Web アプリケーション内に実装された様々な入力データ処理の脆弱性を検査するためには, その処理を呼び出すために必要な条件を整えた上で検査リクエストを送信する必要がある。

今回我々はこの Web アプリケーション診断における条件整備の自動化の必要性に着目し, 以下の機能を持った Web 診断機能を開発した。

- ・ セッション回復

- ・ 重複を避けるパラメータの自動生成
- ・ 等しい入力が必要なパラメータ群への検査文字列の同時投入

次節より, これらの機能を実現した Web 診断機能の動作及び実装方式について述べる。

## 3. Web 診断機能

### 3.1. 基本構成

本 Web 診断機能の基本構成について述べる。本機能はスパイダツール及び Web 診断ツールで構成されている(図 1)。スパイダツールはブラウザを利用して対話的に検査対象サイトのサイト構成情報を収集するツールである。

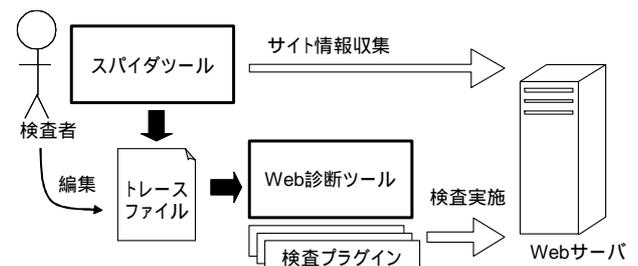


図 1 基本構成

スパイダツールによって収集されたサイト構成情報はトレースファイルとして出力される。ファイルには検査対象サイト内の各ページを表示するために送信した URL 及び POST されたパラメータの情報(以降リンク情報と呼ぶ)のリストがテキストとして記述される(図 2)。

```

1|http://target.com/index.html
1-1|http://target.com/login.asp
1-1-1|http://target.com/login.asp|user=test&password=test
1-1-1-1|http://target.com/shop.asp
1-2|http://target.com/search.asp?q=abcde
  
```

図 2 トレースファイル例

POST パラメータは, 図 2 中の ID1-1-1 のリンク情報のように, パイプ(|)で区切られて記述される。

各リンク情報は, サイトのトップページをルートとして階層的に ID(1-1,1-1-1 等)がふられており, これによりページ間のリンク関係を表現している。

### 3.2. Web 診断ツールの動作

トレースファイルを与えると, Web 診断ツールはその

A Web Vulnerability Assessment Capability for Integrated Security Assessment Tool

†Kiyoto KAWAUCHI, Motokazu KAWAKI, Seiji FUJII

††Mitsubishi Electric Corporation., 2-2-3, Marunouchi, Chiyoda, Tokyo, 100-8310, Japan

中の各リンクに対して検査を開始する。各検査は(1)セッション回復、(2)検査リクエストの送信、という二段階のステップを経て実施される。

### 3.2.1. セッション回復

Web アプリケーションが提供するページの中には、クライアントがある特定の状態にいないとアクセスできないものも存在する。従って検査実行の前に診断ツール自体も、検査可能な状態まで遷移していなければならない。この処理を本稿ではセッション回復と呼ぶ。

セッション回復は、サイトのトップページから検査対象ページの直前まで、トレースファイル内の木構造に従って Web アクセスを行うことで実施される。トレースファイル中のリンク情報には階層的に ID がふられているため、ID を文字列解析するだけで必要なアクセスパスを算出することが可能となっている。

セッション回復は検査対象ページ毎に一度だけ行われ、そのページに対する検査中は再びセッション回復を行わないようにした。ただし、検査者が明に指定することで検査毎にセッション回復を行うことも可能である。

### 3.2.2. 検査リクエスト送信

検査対象のリンク情報と、セッション回復によって取得した Cookie 等の情報をもとに、診断ツールは検査リクエストを生成、送信し、その応答から脆弱性を診断する。

実際には、検査リクエストの生成及び脆弱性の判定は、プラグインと呼ばれる実行時に追加可能なライブラリ内で実施される。現在クロスサイトスクリプティング、SQL インジェクション、バッファオーバーフロー、Format String バグを検査するプラグインが実装されている。

### 3.2.3. 重複を避けるパラメータの自動生成

ユーザ登録のページでは、入力されたユーザ名が既存のものと重複していた場合、エラーとして処理するのが一般的である。

一方、検査は対象となるリンクの個々のパラメータを様々な検査文字列に置換することで行われる。従って検査対象のパラメータ以外は全て同一のパラメータを持ったリクエストを何度も送信することになる。その結果、検査の大部分が重複エラーとして処理されてしまい、正常な遷移の場合を検査できなくなる恐れがある。

そこで、本診断ツールでは、検査毎に特定のパラメータをマクロにより動的に生成することを可能にした。マクロは検査者が Perl コードによってトレースファイル中に記述する(図 3)。図中バックオート( )で囲まれた部分がマクロに相当する。検査リクエストを生成する毎にマクロは Perl によって評価され、その実行結果(図中では rand()の返り値)によってマクロの部分が置換され、それをもとに検査リクエストが生成される。

```
1-1!http://target.com/regist.asp?user=test`rand()`&passwd=test
```

図 3 マクロ記述例

さらに、マクロはセッション回復処理を行う際にも有効である。つまり、セッション回復に必要なリンクのツリー中にマクロを含んだリンクが存在した場合、そのマクロは自動的に評価され、セッション回復のためのリクエストが生成される。この機能により、重複を許さないページから遷移しなければ到達不可能なページに対する検査も実施することが可能となる。

### 3.2.4. 等しい入力が必要なパラメータ群への検査文字列の同時投入

パスワード登録などの処理では、ユーザのタイプミスを防ぐために二度パスワードを入力させ、それらが一致しなかった場合、エラーとして処理される場合が多い。

通常、検査においては個々のパラメータを検査文字列に置き換えたリクエストを送信するため、このようなページに対して検査を行うと、パラメータの不一致が発生し、正常処理が行われた場合の検査が行えない。

そこで、同値の入力を必要とするパラメータ群を明示してやることで、通常の検査に加え、それら全てを同じ検査文字列に置き換えた検査を行ようにした。

例えば、パラメータ a,b に同値の入力が必要であると設定ファイル上に記述することで、(1)a に検査文字列、(2)b に検査文字列という既存の検査パターンに加え、(3)a,b に同じ検査文字列というパターンでも検査が行われる。

## 4. まとめ

統合セキュリティ診断ツールに対する Web 診断機能拡張を行った。本機能はスパイダツールと Web 診断ツールで構成されており、トレースファイルと呼ばれるサイト構成情報を元に診断を実施する。

Web 診断ツールはサイトの構成に従ったセッション回復を行い、その後検査を実施する。検査はプラグインにより実行時に追加可能である。

さらに、パラメータに制約のあるページへの考察を行い、マクロによる動的なパラメータ指定機能及び同値関係にあるパラメータの指定機能を実装した。これらの機能により、より多くの Web アプリケーションに対し効果的に診断を行うことが可能となった。

## 参考文献

[1]河内他, "ハッキング手順模擬機能を有するセキュリティホール診断ツールの実装と評価", 情報処理学会第 62 回全国大会 7F-05