White Paper

ウェブアプリケーションの機能テストにおける「ウエブテイスター」の活用方法

２０１１年1月２４日

セキュリティフライデー株式会社
中岡　義雄

azbil

1　はじめに

ここ数年、各種アプリケーションにおいては、従来のクライアントサーバ型に対し、Web 型が急増し、更に、クラウドの登場により、今後もこの傾向は続くものと考えられる。ウェブアプリケーションにおいては、新しい技術の開発が優先されてきたように思われるが、今後は、品質面やセキュリティ面の強化がより求められるようになってくると考えられる。

以前に報告の「ウェブアプリケーション統合テストにおける留意点の検討と評価専用ブラウザの開発」にて、Web アプリケーションの特性を検討し、統合（結合）テスト、システムテスト、受入検査での検証（Verification）を目的としたテスト設計において、送信フォーム書換テストの必要性を報告した。

今回は、送信フォームの書換テストを目的に開発された、Web アプリケーションの評価テスト専用ブラウザ「ウエブテイスター」の活用方法に関し、テスト例を挙げて報告する。

2　ウエブテイスターの特長と機能

ウエブテイスターは、弊社のセキュリティ技術を応用し、統合テストの設計から実施、報告までを支援する専用ブラウザとして開発した。特長と主な機能は以下のとおりである

特長

- 完成したアプリケーションに対し、ハッカー視点のブラックボックステストが可能
- 専用の評価環境無しに、インターネットエクスプローラベースの標準ブラウザ環境で評価テストを実現
- 各ページ毎の入力ボックス項目と実際に送信されるデータのリストアップからテストの実施、結果報告までを支援
- ブラウジング中のＳＳＬ暗号化された送信データも簡単に書換テストが可能
- 付属のＳＱＬインジェクション基本テストパターンを利用し、セキュリティテストにも応用可能

機能

- テストケース（評価シート）作成支援
  入力項目を含む送信されるデータ（フォーム）やクッキーの保存機能（CSV 形式）により、実際の完成ページをブラウジングしながらテストケース（評価項目）の元データを生成。
- テスト実施支援
  送信されるデータ（フォーム）やクッキーデータの書換機能
- テストパターンの登録機能
  繰返し利用するテストパターンを登録し効率化、SQL インジェクション
  の基本テストパターンがあらかじめ登録されている。

- 結果報告支援
  実施テストログ機能、レスポンスの HTML、クッキー保存機能

3　オークションシステムの機能テスト

今回、弊社が評価用に提供しているサンプルアプリケーションのオークションシステムを使い、第三者評価を想定した機能テストを例にウエブテイスターの使用方法を説明する。

ウエブテイスターメイン画面

ウエブテイスターを立ち上げると、大きく３つの部分（ブラウザ、簡易ログ、クッキーログ）に分かれたメイン画面が表示される（図１）

(図１) ウエブテイスターメイン画面

3.1　ログインページの機能テスト

ログインページの操作コマンド、ID、パスワードをテスト対象に有効、無効値へのデータ書換テストを実施する。

3.1.1 テストケース（評価シート）の作成

①　ログインページの機能仕様書からテストデータをリストアップすると、「ID」と「パスワード」の入力テストが必要と考えられる。更に外部機

能仕様書から読み取れる送信フォーム以外に Hidden データとして「操作コマンド」の送信等が考えられる。

まずは、ウエブテイスターで実際の送信フォームを確認する。

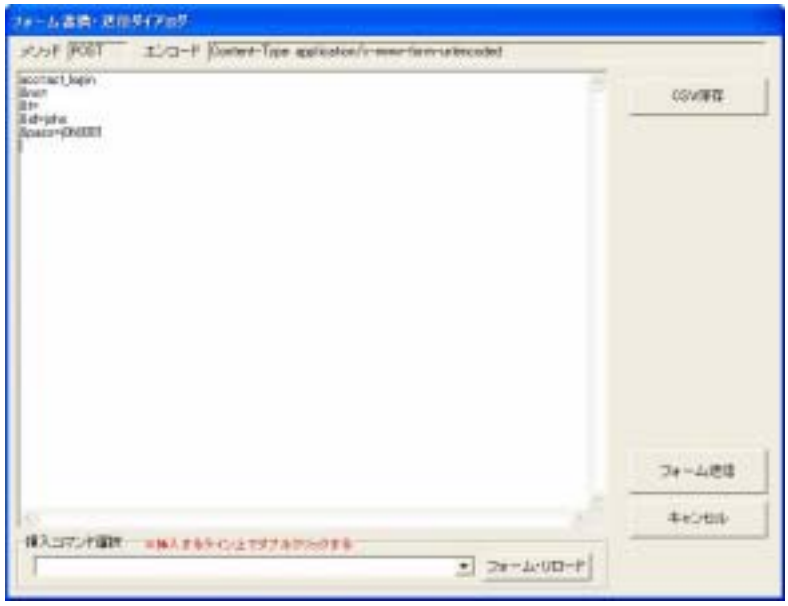
　ウエブテイスターを立ち上げると、評価用サンプルアプリケーションページが表示される。通常のブラウザ（ＩＥ）と同様に操作し、オークションシステムのページから今回のテストターゲットのオークションのログインページへすすむ（図２）

(図２) オークションのログインページ

② ログインページが表示されれば、上部にある「テストモード」と「フォーム書換送信」のチェックボックスにチェックを入れ、実際にログインに必要なデータを投入（ユーザ ID と Password）し、「ログインする」ボタンをクリックする。

③ フォーム書換ダイアログがポップアップされ白枠内に表示された下記データが送信フォームになる（図３）

acc=act_login、&no=、&t=、&id=joho、&pass=j0h0001



(図３) フォーム書換・送信ダイアログ

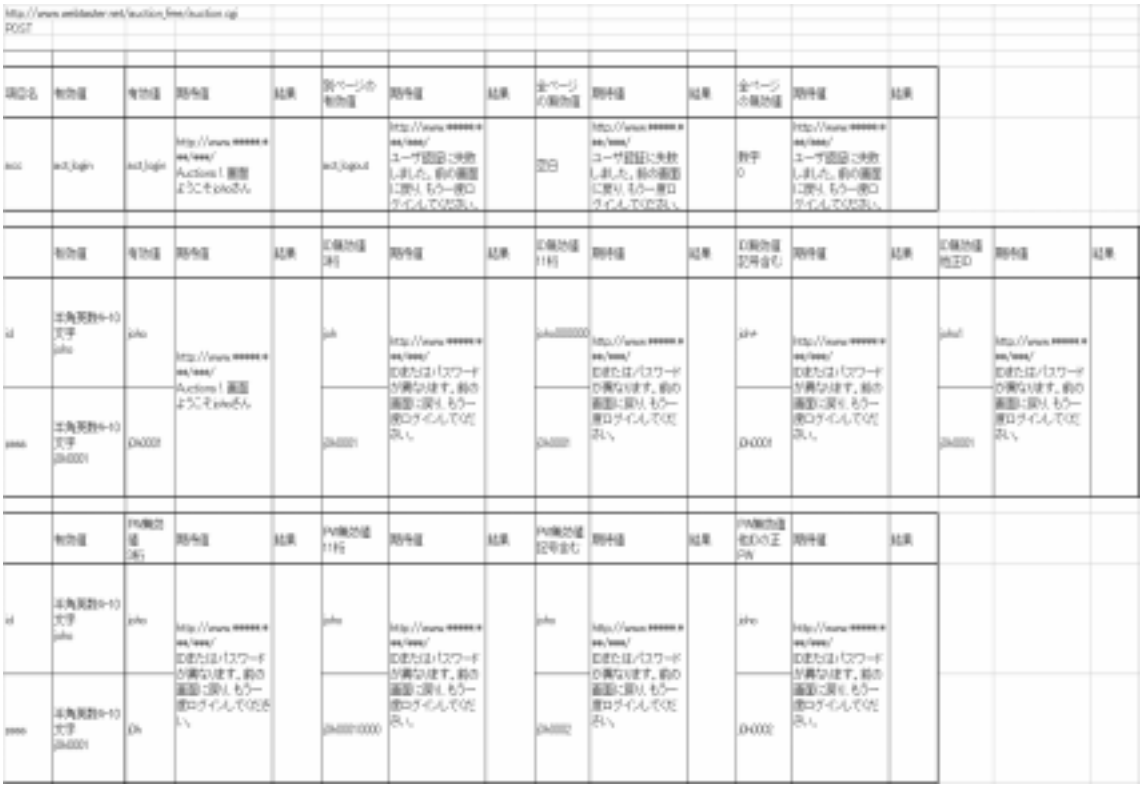
④　右上部のＣＳＶ保存スイッチをクリックし、送信フォームデータを CSV ファイルで保存する(図４)

http://www.webtaster.net/auction_free/auction.cgi				
POST				
項目名	設定値	変更値	予想結果	確認
acc	act_login			
no				
t				
id	joho			
pass	j0h0001			

(図４)送信フォーム CSV 保存データ

⑤　保存した送信フォーム CSV を利用しテストケースを作成する（図５）
　テストケース作成に関しては、外部機能仕様書を参照するとともに、開発者とのコミュニケーションが必要となる。

大項目：ログインページ　中項目：ログイン操作



(図５)送信フォームテストケース

3.1.2 送信フォーム書換テストの実施

ウエブテイスターを使用すると、ブラウザ上からの入力フォームテストではできない、Hidden データ（今回は操作コマンド）の書換テストも簡単に実施できる。

① ウエブテイスターでブラウジングしログイン画面に進む。
② 送信フォームデータの取得と同様に、「テストモード」と「フォーム書換送信」のチェックボックスにチェックを入れ、実際にログインに必要なデータ（ユーザ ID と Password）を入力ボックスに書込み、「ログインする」をクリックする。
③ フォーム書換ダイアログがポップアップされるので、白枠内に表示されたテストターゲットの送信フォームデータにカーソルを持っていき、直接データを書換える。送信フォームボタンをクリックし、ブラウザに表示された画面を確認する。テストケースに沿って順次書換えテストを行う。

例　acc=act_login　→　acc=act_logout

④　結果をテストケースに記入する。

3.2　クッキーの書換テスト

本アプリケーションは、各ユーザのセッション管理にクッキーが使用されており、アプリケーションがクッキー処理を正しく行っているか、オークションホーム画面を例にクッキー書換テストを実施する。

3.2.1 テストケース（評価シート）の作成

①　ウエブテイスターを立ち上げ、ウエブテイスター実験用オークションページのログインページに進む。

②　ユーザ ID：joho とパスワード：j0h0001 を入力ボックスに書込み「ログインする」をクリックする。

（図６）Cookie 書換ダイアログ

③　オークションホームのページが表示されるので、テストモードのチェックボックスにチェックを入れ、Cookie 書換ボタンをクリックする。

④　Cookie 書換ダイアログがポップアップされ、CSV 保存ボタンをクリックしユーザ ID が joho の Cookie を保存（図７）し、一旦ログアウトする。


http://www.webtaster.net/auction_free/search.cgi
COOKIE

項目名	設定値	変更値	予想結果	確認
acf	1292893732:joho:j0h0001			

（図７）クッキーの CSV 出力データ

⑤ 再度ログインページから、ログインユーザ ID：joho1、パスワード：j0h0002 でログインする。

⑥ テストモードのチェックボックスをチェックし、Cookie 書換ボタンをクリック、更に CSV 保存ボタンをクリックしユーザ ID が joho1 の Cookie 情報を保存する。

⑦ 取得したユーザ ID が joho1 のクッキーCSV ファイルを元にテストケースを作成する（図８）

3.2.2 クッキー書換テストの実施

① 送信フォームの書換テストと同様にテストケースに沿ってテストを実施する（図８）

大項目：オークションホーム　中項目：ユーザのセッション管理

http://www.webtaster.net/auction_free/search.cgi
COOKIE

項目名	設定値	変更値	期待値	確認
acf	1293741927:joho1:j0h0002	1292893732:joho:j0h0001	http://www.webtaster.net/****/****/ ユーザID異常が発生しました。ログイン画面に戻り、再度ログインしてください。	×ユーザがjohoに変更された
acf	1293741927:joho1:j0h0002	消去	http://www.webtaster.net/****/****/ ユーザID異常が発生しました。ログイン画面に戻り、再度ログインしてください。	×ユーザがゲストに変更された。

（図８）クッキーの書換テストケースと結果

3.3　テスト実施ログ

3.3.1 ログの確認

① 一連のテスト実施結果がログファイルに保存されており、報告書に添付利用する(図９)

ログ保存場所はデフォルト設定の場合下記となる。

￥Program Files￥SecurityFriday￥WebTaster【評価版】

② ログファイル名には下記のとおり日付時刻が入いる。

web_20101227173932.log

（図９）テスト実施ログの抜粋

③ 上記ログの抜粋最下行に、実際にブラウザが受け取ったレスポンスのHTML、クッキー情報のファイル名が記録されており、テスト実施ログと同じフォルダ内に保存されている(図１０)

web_20101227173932_11.txt

```
http://www.webtaster.net/auction_free/search.cgi
WebTaster実験用オークション・システム

==== COOKIE ====
acf=1292893732:joho:j0h0001

===== HTML =====
<HTML><HEAD><TITLE>WebTaster実験用オーク
ション・システム  </TITLE>
<META content=no-cache http-equiv=Pragma>
<META content="text/html; charset=Shift_JIS" http-
equiv=Content-Type></HEAD>
<BODY background="" link=#0000ff>
<CENTER><!--ここから-->
<TABLE cellSpacing=0 cellPadding=0 width="95%">
<TBODY>
<TR>
<TD>
<HR SIZE=1 noShade>
</TD>
<TD width=15><IMG
src="http://www.webtaster.net/auction_free/img/shim.
gif" width=15></TD>
<TD width=247><A
href="http://www.webtaster.net/auction_free/search.c
gi"><IMG border=0
src="http://www.webtaster.net/auction_free/img/aucti
on_title.gif"></A></TD>
<TD width=15><IMG
src="http://www.webtaster.net/auction_free/img/shim.
gif" width=15></TD>
<TD>
<HR SIZE=1 noShade>
</TD></TR></TBODY></TABLE><BR><!--ここまで--
>
<TABLE cellSpacing=0 width="95%">
<TBODY>
<TR>
<TD><FONT size=2>オークションホーム
</FONT></TD></TR></TBODY></TABLE>
<TABLE cellSpacing=0 cellPadding=5 width="95%">
<TBODY>
<TR>
```

（図１０）HTML レスポンス、クッキーファイルの抜粋

4　おわりに

今回、弊社が提供している実験用オークションサイトを例に機能テストとして、Hidden データを含む送信フォームとセッション管理用クッキーのテスト例を報告した。従来、手間のかかった送信フォームのテストが、ウエブテイスターを使用することで容易に行えることをご理解いただけたのではと考える。ウエブテイスターは、セキュリティテストへの応用が可能で、次の機会では、ウエブテイスターを使ったセキュリティテストについて報告したいと考えている。

2011 年 1 月　発行

セキュリティフライデー株式会社
URL http://www.securityfriday.com/jp/