GSLetterNeo Vol.36
2011年7月

Web アプリケーションの脆弱性診断の実際

コンサルタント
比嘉 陽一
Youichi Higa
youichi@sra.co.jp

PC 専用アプリ/Android 端末向けサイトに対し IBM Rational AppScan を使って脆弱性診断を行った事例を紹介します。尚、この事例において、弊社は脆弱性の分析のみを行い、開発等には携わっておりません。

◆AppScan とは

AppScan は Web アプリケーション脆弱性評価ツールです。実際に稼動している Web アプリケーションに対して攻撃を行い、脆弱性診断を行います。AppScan で Web アプリケーションを攻撃する際には、次の二つのパターンがあります。

I. **URL を自動的にたどり、攻撃を行う**
II. **前もってユーザの URL 遷移を記録し、それを元に遷移しながら攻撃を行う**

I. は II.に比べて下準備がいらないため、作業の手間がかからず、比較的容易です。しかし弊社では、これまで手がけてきた脆弱性診断において、II.の方がより多くの脆弱性を検出できるという知見を得ているため、II.を推奨しております。

◆作業内容

今回は下記の手順で作業を行いました。

1. **テストシナリオ作成**
2. **シナリオの手順を記録**
3. **攻撃**
4. **分析**

分析の結果、いくつかの脆弱性を発見し、お客様にご報告しました。

1. テストシナリオ作成

前もってユーザの URL 遷移を記録するために、その操作手順(シナリオ)を作成します。今回は仕様書を元にユーザが行うであろう操作を想定し、それに添った形でシナリオを作成しました。また、全画面が網羅されるようシナリオを作成しますが、長すぎると次作業(2.シナリオの手順を記録)に支障をきたします。その辺りを考慮にいれ、適切な長さに調整しました。このシナリオの出来が診断結果に影響してきます。

2. シナリオの手順記録

AppScan に URL 遷移を記録させます。各種プログラムが対象サイトへアクセスする際の HTTP 通信を傍受することで、AppScan は URL 遷移を記録できます。これは、各種プログラムのプロキシ設定を AppScan に向けることで実現できます。今回は Android エミュレータや PC アプリのプロキシ設定を AppScan へ向け、シナリオに基づく操作を記録させました。

3. 攻撃

2.の手順を元に AppScan が Web アプリケーションを攻撃します。ここでは二つの処理を行います。

・探査

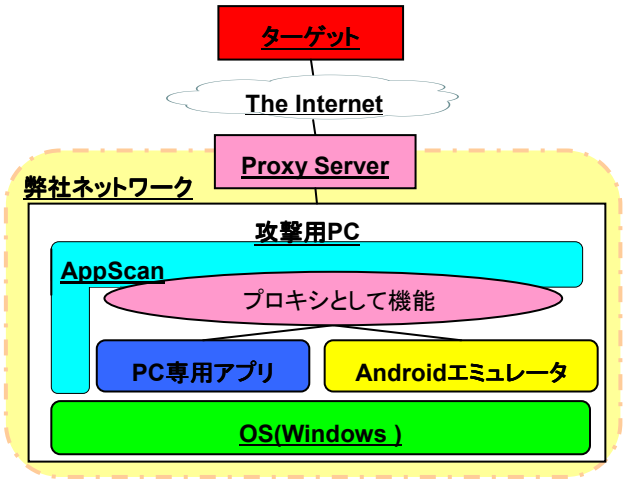
AppScan が記録した URL 遷移を用い、サイトに存在しうる URL を「探査」します。この処理で攻撃対象を洗い出します。サイトにも依りますが、数分程度で完了します。場合によっては探査後環境をリセットする必要があります。これは、探査で行った処理を次の「スキャン」でも繰り返し行うためです。

例) ユーザ登録/削除処理

・スキャン

このフェーズで AppScan は実際に攻撃を行います。ターゲットは必ず「検証環境」またはそれに順ずる環境とします。本番環境の場合、最悪破壊する可能性がある

ので絶対に避けるよう、お願いしております。サイトにも依りますが、この処理には数時間程度（5～6 時間程度）かかり、かつ環境を占有する必要があります。開発期間中は開発チームがテスト等で検証環境を使用することがある為、関係者とスケジュールの調整を行う必要がありました。スケジュール調整の結果、深夜帯にバッチ起動でスキャンを実行するといったこともありました。



攻撃を行った際の構成図

4. 分析

AppScan の出した結果を分析し、以下のように評価しました。

陽性	明らかに疑いようがないもの
要注意	陽性か疑陽性か判断がつかないが、陽性だった場合、影響があまりにも大きいのでお客様に真っ先に確認して頂く
要確認	陽性か疑陽性か判断がつかないので、念のためお客様に確認して頂く 疑陽性の確率が高いが、念のためこのステータスにしておく
疑陽性	明らかに陽性ではないもの、無視しても問題が起こらないもの

それぞれのレベルは、以下のように順位付けしています。

陽性＞要注意＞要確認＞疑陽性

この評価を二名で行い、その結果をさらに検討して最終的な判断を出しました。お客様に分析結果をお伝えした際、今回の疑陽性以外のすべての結果を必ず確認して頂くよう、お願いしました。

◆今回の作業のポイント

シナリオ作成

・実環境での検証

シナリオ作成のために仕様書を読み進めると、矛盾点や足りない情報が明らかになりました。そのため、お客様に質問表を都度出して疑問点の問い合わせを行いました。しかし、このようなやりとりのみではどうしても意識のズレが生じてしまいます。今回の事例では、シナリオ作成を進める一方で、環境を早めに使用させて頂けるよう、依頼しました。そして実環境でシナリオの確認が取れたため、無事分析を行うことが出来ました。

・Android エミュレータ/PC アプリ毎にシナリオ作成

それぞれがアクセスする URL が異なるので、別々の手順が必要となりました。Android の特徴などを考慮して攻撃するのではなく、あくまで対象となるWebアプリに存在しうる URL を正確に網羅したことが、多くの脆弱性の検出につながったのではないかと考察しています。

Android エミュレータ

お客様からエミュレーター一式をお借りして作業を行いましたが、処理が重いためシナリオを記録するのに時間がかかりました。あるシナリオの記録では、長さにして 3～5 分くらいの手順が、エミュレータ上で行った場合 15 分程度かかりました。今回は一式を出来るだけ早く頂くようお願いし、十分に事前検証を行ったことで滞りなく作業を遂行できました。

GSLetterNeo Vol.36
2011 年 7 月 20 日発行
発行者●株式会社 SRA 産業開発第 1 事業部
編集者●土屋正人、柳田雅子、小嶋勉、野島勇

ご感想・お問い合わせはこちらへお願いします●gsneo@sra.co.jp

株式会社SRA
〒171-8513 東京都豊島区南池袋２－３２－８

夢を。Yawaraka Innovation
やわらかいのべーしょん