サイバーセキュリティ Assignment 3
Step 4 Analysis

Group 6

2020 年 7 月 15 日

担当者 SubgroupA and SubgroupB

学生番号	氏名	所属研究室
1911403	佐々木 皓大	ユビキタスコンピューティングシステム研究室
2011067	奥村 嶺	情報基盤システム学研究室（Inet-Lab）
2011115	佐伯 雄飛	
2011156	成 泰鏞	ソフトウェア工学研究室
2011231	久田 祥平	ソーシャルコンピューティング研究室
2011271	森本 康太	情報セキュリティ工学研究室

Question

After finishing steps 1 to 3 for each incident, analyse and contrast the two incidents, for instance by highlighting similarities and differences.

Answer

双方のインシデントの類似点と相違点を述べる．以降 SubgroupA が調査した「B.LEAGUE チケットサイトとファンクラブ受付サイトへの不正アクセスによる個人情報流出インシデント」を inciA，SubgroupB が調査した「WordPress を利用する Web サイトが改ざんされたインシデント」を inciB と呼称する．

類似点

双方のインシデントの類似点としては，以下の点が挙げられる．

1. フレームワーク自体が持つ脆弱性によって，攻撃された．
2. 脆弱性をに対する PoC が公開されている．
3. 脆弱性の攻撃条件の複雑さは低い
4. サービス管理者がフレームワークの管理（最新情報の収集や，バージョンアップデート）を怠っていた．

以下にこれらの類似点の概要を述べる．1 点目の類似点は，サービスを展開するための基幹ソフトウェアとして inciA では Apache Struts2 が，inciB では WordPress がそれぞれ使用されており，これらのフレームワークに脆弱性が存在した点である．両インシデントとも，攻撃者はそれぞれのソフトウェアが持つ脆弱性を利用して攻撃を行った．2 点目の類似点は，各フレームワークが持つ脆弱性に対して，PoC が既に公開されている点である．公開されている PoC を利用することで，攻撃者は専門的かつ高度な知識や技術を持たずとも，容易に攻撃を行うことができる．3 点目の類似点は，各フレームワークが持つ脆弱性に対する，攻撃条件の複雑さが低い点である．Apache Struts2 の脆弱性では，攻撃対象サイトや Web サービスに対して細工した Content-Type ヘッダを付与したファイルをアップロードするだけで，攻撃対象サーバにて任意のコードを実行する事が可能となり，攻撃難易度は極めて低いと考えられる．また，WordPress の脆弱性では，POST リクエストを攻撃対象サイトに送信するだけで，攻撃対象サイトを改ざんすることが可能であり，攻撃難易度は極めて低いと考えられる．4 点目の類似点は，両インシデントともにサービス

管理者が使用フレームワークの管理を怠っていた点である．両インシデントとも，実際に攻撃を受けた時点では既に脆弱性の内容と対応策が公開されており，対応を行う時間的余裕は十分にあったと考えられる．しかし，実際には対応が間に合わず攻撃される結果となっている．

相違点

双方のインシデントの相違点としては，以下の点が挙げられる．

1. 各フレームワークの脆弱性が持つ影響範囲
2. アップデートの工数や難易度
3. 脆弱性を修正するアップデートまでの対応
4. 予想される攻撃者の目的として，inciA は個人情報の獲得そのものである直接的な目的であるのに対し，icniB は愉快犯や SEO ポイズニングなどの間接的な目的であること

以下にこれらの相違点の概要を述べる．1 点目の相違点は，各インシデントで使用しているフレームワークが持つ脆弱性の影響範囲の差である．inciA で使用している Apache Struts2 の脆弱性では，Web サービスをホストしているサーバ上で任意のコードが実行できるため，可用性，機密性，完全性すべての範囲に影響を及ぼす．例として，サーバに大量の負荷を与えるコマンドの実行（可用性）や，ls, cat コマンドを用いたサーバ上に保持されている機密情報の閲覧（機密性），データベースの制御コマンドを用いたデータの改ざんや破壊（完全性）が考えられる．対して，inciB で使用している WordPress の脆弱性では，脆弱性によって改ざんが可能であるのは Web ページの表示に関わるフロントエンド部分のみである．つまり，Web ページをホストしている Web サーバ自体を操作することは不可能であり，脆弱性の影響範囲は非常に狭いと考えられる．したがって両インシデントは，使用フレームワークの脆弱性によって可用性，機密性，完全性の影響範囲に大きな差があると言える．2 点目の相違点は各フレームワークのアップデートにおける技術的・心理的難易度である．ここで，Apache Struts2 と WordPress の想定利用者の違いについて示す．WordPress は「ほとんどのユーザがトレーニング無しで使い始める」ことを目標に設計されている[*1]．一方で，Apache Struts2 は，エンタープライズ向けの Java ウェブアプリケーションを構築するためのフレームワーク[*2] と明記されている．したがって，前者は一般のユーザも対象としているのに対し，後者は一般のユーザを対象としてないことが見て取れる．これより，各フレームワークのアップデートの技術的難易度に差が生じると考える．また，文献 [1] によると，Apache Struts2 のようなフレームワークを用いたアプリケーションは，フレームワークのアップデートによって生じる依存関係の変化が，バグの原因になるとされている．それゆえ開発者は，フレームワークのアップグレードを即座に行わない場合も多い．一方で，WordPress のユーザは，依存関係によって生じるバグ等の修正はプラグインの開発者などが対応するため，WordPress ユーザは自身の意志によって，アップデートを即座に適用することが可能である．このように，両インシデントには各フレームワークのアップデートにおける技術的・心理的難易度があると言える．3 点目の相違点は，各フレームワークの脆弱性の修正対応の差である．inciA の Apache Struts2 では，脆弱性の内容と応急処置対応策が Wiki にて同時に公開され，根本的な対策を施したアップデートは 2 日後となっている．一方，inciB の WordPress は脆弱性の報告を受けたのち，対策を施したアップデートは 6 日後，脆弱性の公開は更に 6 日後と，一定期間意図的に脆弱性の内容を公開せずにいた．また，アップデートのリリースから脆弱性の公開までの 6 日間に，WordPress はユーザへ対応を求めていた．以上より，各フレームワークで脆弱性の公開から修正までの一連の流れが異なっていることが分かる．4 点目の相違点は，両インシデントで予想される攻撃者の目的が異なる点である．inciA では攻撃対象 Web サービスが持つ個人情報（例えば，クレジットカード情報）の入手が主な目的であると考えられる．対して inciB では攻撃対象 Web サイトの改ざん自体を目的とする愉快犯が考えられる一方で，攻撃対象 Web サイトから別のサイトへ誘導するフィッシングサイトを表示させたり，SEO ポイズニングに利用することが目的であるとも考えられる．このように，inciA での攻撃者の目的は個人情報の入手という直接的なものであるのに対し，inciB での攻撃者の目的は Web サイトを踏み台にして別の手口に利用する間接的なものであると言える．

[*1] WordPress の機能; WordPress.org 日本語: https://ja.wordpress.org/support/article/wordpress-features/

[*2] Home - Apache Struts 2 Wiki - Apache Software Foundation : https://cwiki.apache.org/confluence/display/WW/Home

参考文献

[1] Gabriele Bavota, Gerardo Canfora, Massimiliano Di Penta, Rocco Oliveto, and Sebastiano Panichella. How the apache community upgrades dependencies: an evolutionary study. *Empirical Software Engineering*, Vol. 20, No. 5, pp. 1275–1317, Oct 2015.