サイエンティフィック・システム研究会　　2008 年 8 月 26 日
システム技術分科会 2008 年度第 1 回会合資料

大学・研究所における Web アプリケーションのセキュリティ

― 「守るべき情報を持たない」Web サイトにおけるセキュリティの在り方 ―

株式会社ソフテック
セキュリティソリューション事業部
事業部長　芝田 幸彦

[Abstract]
昨今「SQL インジェクション」を悪用した無差別の Web サイト改竄が多発しており、Web アプリケーションを取り巻く状況は悪化の一途を辿っている。
Web アプリケーションに攻撃を受けた際のリスクとして、一般的には Web サイトからの情報漏洩が着目されがちだが、個人情報を持たない多くの学術系サイトにおいても、情報漏洩以外に守るべき Web セキュリティが確固として存在する。
それを実現し、安全に Web サイトを開発・運用していくために必要なポイントについて紹介する。

[Keyword]
Web アプリケーション脆弱性、セキュリティリスク、 安全な Web サイト開発

1. はじめに

2005 年前後から Web アプリケーション脆弱性による個人情報漏洩、不正侵入の事件が急激に増加しており、実際に多大な被害・損失を被るケースも確認されている。また、今年に入ってからが「SQL インジェクション」を悪用した無差別の Web サイト改竄が多発しており、Web アプリケーションを取り巻く状況は悪化の一途を辿っている。

個人情報漏洩や不正侵入により組織が受ける被害・損失は、直接的（サーバ再構築費用、セキュリティ対策費用等）・間接的（組織イメージの悪化等）に多大なものになることが想定されるが、一般的に情報漏洩に関するリスクのみが注目される傾向にあり、個人情報を持たない大学や研究所の Web サイトにおいては、Web アプリケーションのセキュリティリスクについて十分に配慮した開発・運用を行っているとは言えない状況にある。

本稿では、現状を整理した上で、大学・研究所における適切なセキュリティレベルを備えた Web アプリケーションの開発、及びそれを利用した Web サイトの運用を行うために必要なポイントについて紹介する。

2. Web アプリケーションにおける脆弱性の現状

Web アプリケーションに関する脆弱性については様々なものがあるが、その中でも特に「SQL インジェクション」については、2005 年にそれを悪用した大規模な攻撃が発生し、大規模 EC サイトが実際に運用されている EC サイトとして初のサイト閉鎖に追い込まれる事件に発展する等、大量の個人情報漏洩が発生したことから、Web アプリケーションの代表的な脆弱性として知られている。今年に入ってからも「SQL インジェクション」を悪用した大規模な不正アクセスが発生しており、やはり EC サイトのデータベース内に登録された個人情報の漏洩事故が発生している。

また、Web アプリケーションに対する不正アクセスの動機も、以前は Web サイトのコンテンツ改竄など愉快犯や自己顕示欲が中心だったものが、不正に入手した個人情報の売買など具体的な金銭目的に変化している傾向もあり、データベースに不正に侵入することで大量のデータを奪取可能な「SQL インジェクション」の悪用を助長させている。

3. 大学・研究所サイトにおける Web アプリケーションセキュリティの認識

Web アプリケーションの脆弱性を悪用した攻撃は増加の一途を辿っているが、その被害が商用サイトからの個人情報漏洩に関するものが多いためか、大学や研究所のような個人情報を持たない「学術系サイト」におけるセキュリティ対策の認識は、決して高いようには思えない。

この状況は「仮に不正アクセスによる情報漏洩が発生したとしても被害は少ない」という認識から端を発しているとも推測できるが、不正アクセスの対象は、もはや個人情報を持たない Web サイトにも拡がっているのが現状である。

例えば、今年に入ってから多発している「SQL インジェクション」を悪用したワームは、Web サイトに SQL インジェクション攻撃を行い、ウィルスやマルウェアをダウンロードさせるスクリプトを不正に Web サイト内に埋め込むため、その Web サイトにアクセスしたユーザの PC がウィルス等に汚染される被害が発生する。

この例のように、個人情報が存在しない Web サイトでも不正アクセスを間接的に幇助する可能性があり、結果として組織としての信頼性を著しく損なうことへのリスクヘッジからも、Web アプリケーションにおけるセキュリティ対策を適切に実施することは、Web サイトを運用する上で必須といえる。

4. セキュアな Web アプリケーションの開発・運用に必要なポイント

Web アプリケーションにおけるセキュリティ対策を適切に行うためには様々な視点からの方策が必要となるが、その中でも「安全な Web アプリケーションの開発・運用」は極めて重要なアイテムといえる。

大学・研究所においては、Web サイトの規模やメンテナンスの容易さから、最低限の予算で担当者（研究者）自身がサイト構築を行うケースが少なくない。自ら Web サイトを構築すること自体には何ら問題はないが、Web アプリケーションセキュリティに対して適切な知識を持たぬまま Web アプリケーション開発を行うことは、非常に危険な状態であると言わざるを得ない。

適切なセキュリティ知識を持たないということは、外部に Web アプリケーション開発を委託する場面でも適切なセキュリティ要件を仕様書に明記することができないことに繋がり、そ

の結果、構築されたWebアプリケーションのセキュリティレベルも非常に脆弱な内容になってしまうケースも多く見受けられる。

このような問題を解決し、セキュアなWebアプリケーションの開発・運用を実現するために「発注時のセキュリティ要件の明確化」「セキュアプログラミング」「脆弱性検査」の観点から、大学・研究所において求められるセキュリティレベルを備えたWebアプリケーションの開発、及びそれを利用したWebサイトの運用を行っていくことが重要である。

5. まとめ

大学・研究所のような学術系サイトにおいて実現すべきWebアプリケーションセキュリティについて、開発・運用に関して必要と考えられるポイントについて紹介した。Webアプリケーションに関する脆弱性を悪用した攻撃は、今後も新しい技術要素をトリガにして派生していくことが予想されるため、リリース後のメンテナンスまでを含めたWebアプリケーションのセキュリティ管理を継続的に行っていくことが、安全なWebサイト運用の必須条件と考える。