プレスリリース
2009 年 8 月 17 日
独立行政法人情報処理推進機構

ウェブサイトを狙った攻撃に関する注意喚起

～ウェブサーバのアクセスログ調査およびウェブサイトの脆弱性検査の早急な実施を！～

IPA（独立行政法人情報処理推進機構、理事長：西垣 浩司）は、ウェブサイトを狙った攻撃が継続していることから、ウェブサイト管理者等へ改めて注意を喚起するとともに、ウェブサーバのアクセスログ調査およびウェブサイトの脆弱性検査、脆弱性対策の早急な実施を推奨します。

近年、ウェブサイトを狙った攻撃が継続しています。特に 2008 年 3 月頃から SQL インジェクション攻撃によるウェブサイトの改ざんやウェブサイトへの不正コードの設置が多発したことから、IPA はウェブサイト運営者へ向けて 2008 年 5 月に注意喚起[1]を発行しました。

その後も、ウェブサイトの改ざんやウェブサイトからの機密情報の漏えいなど深刻な被害が頻発していることから、IPA では再度、注意を発することとしました。

攻撃の現状を把握する実例として、IPA が公開している「脆弱性対策情報データベース JVN iPedia[2]」について、2009 年 4 月から 7 月までのアクセスログを、「SQL インジェクション検出ツール iLogScanner[3]」で解析したところ、図 1 のような攻撃と思われる痕跡を検出しました。

昨年激増した SQL インジェクション攻撃が 6 月ごろから再び急増し、2009 年 4 月の 21 件に対して 7 月は 534 件と、約 25 倍の攻撃と思われる痕跡を検出しました。また、ディレクトリ・トラバーサルの脆弱性を狙った攻撃も継続しています。これらの、iLogScanner が検出可能なウェブサイトを狙った攻撃の概要は別紙を参照して下さい。

ウェブサイトを狙った攻撃があったと思われる件数

解析対象のウェブサイト：JVN iPedia（脆弱性対策情報データベース）
解析したウェブサーバのアクセスログの期間：2009年4月～7月
攻撃があったと思われる件数：1,944件、攻撃が成功した可能性の高い件数：0件

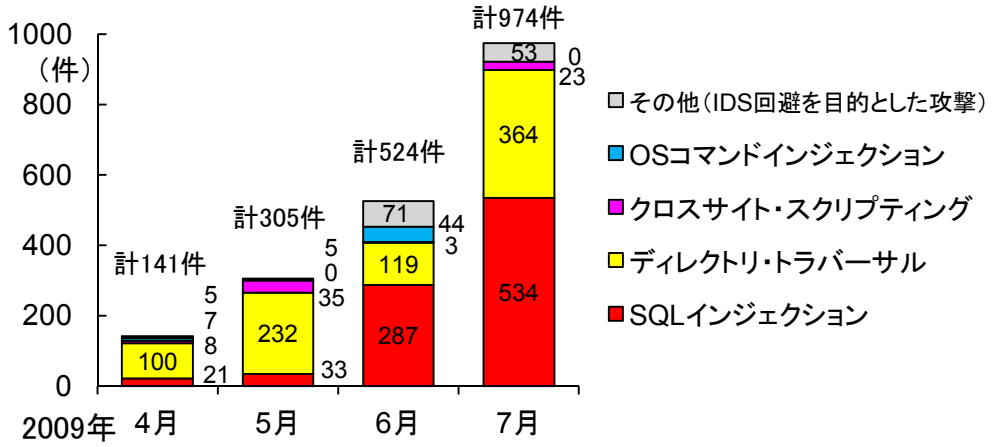

図1．SQLインジェクション検出ツール「iLogScanner」での解析事例

[1] SQL インジェクション攻撃に関する注意喚起。
http://www.ipa.go.jp/security/vuln/documents/2008/200805_SQLinjection.html

[2] 脆弱性対策情報データベース JVN iPedia（ジェイブイエヌ アイ・ペディア）は、国内で利用されているソフトウェアを対象にした脆弱性対策情報を網羅・蓄積し、公開しています。http://jvndb.jvn.jp/

[3] ウェブサイトの脆弱性検出ツール iLogScanner。http://www.ipa.go.jp/security/vuln/iLogScanner/index.html

1. ウェブサーバのアクセスログ調査の推奨

ウェブサイト運営者は、ウェブサイトがどれほどの攻撃を受けているのか、また攻撃によって被害が発生していないか、常に状況を把握し対策を講ずることが必要です。また、ウェブサイトの脆弱性検査を行い、脆弱性がある場合は早急に脆弱性対策を行うことが必要です。

IPA で公開している「SQL インジェクション検出ツール iLogScanner」は、ウェブサーバのアクセスログの中から、ウェブサイトを狙った攻撃によく用いられる文字列を検出し、ウェブサイトが日頃どれだけの攻撃を受けているか、また、攻撃が成功した可能性があるかを解析する簡易ツールです。

iLogScanner（ http://www.ipa.go.jp/security/vuln/iLogScanner/index.html ）は、ブラウザ上で実行する Java アプレット形式のツールで、無償であり、情報を一切外部に送信することが無いので、誰でも簡単に使用することができます。2008 年 4 月の公開[4]以来、ダウンロード数は 2 万件を超えています。

IPA としてはウェブサイト運営者が iLogScanner を利用することにより、自組織のウェブサイトに潜む脆弱性を確認するとともに、ウェブサイト管理者や経営者に対して警告を発し、セキュリティ監査サービスを受けるなど、脆弱性対策を講じるきっかけとなることを期待しています。

また、ウェブサイトの開発者やセキュリティ企業が、本ツールを取引先等に紹介され、それぞれの顧客システムのセキュリティ向上の契機となることを期待します。

なお、iLogScanner は簡易ツールであり、実際の攻撃による脆弱性検査は行っていません。攻撃が検出されない場合でも安心せずに、ウェブサイトの脆弱性検査を行うことを推奨します。

2. 脆弱性対策について

IPA では、届出を受けた脆弱性関連情報を基に、届出件数の多かった脆弱性や攻撃による影響度が大きい脆弱性を取り上げ、ウェブサイト開発者や運営者が適切なセキュリティを考慮した実装ができるようにするための資料、「安全なウェブサイトの作り方[5]」を公開しています。

第 1 章では、「ウェブアプリケーションのセキュリティ実装」として、SQL インジェクション、OS コマンド・インジェクションやクロスサイト・スクリプティングなど 9 つの項目を取り上げ、それぞれの脆弱性で発生しうる脅威や特に注意が必要なウェブサイトなどを解説し、主に開発面から脆弱性の原因そのものをなくす根本的な解決策、攻撃による影響の低減を期待できる保険的な対策を示しています。

第 2 章では、「ウェブサイトの安全性向上のための取り組み」として、ウェブサーバのセキュリティ対策やフィッシング詐欺を助長しないための対策など 5 つの項目を取り上げ、主に運用面からウェブサイト全体の安全性を向上させる対策を示しています。

第 3 章では、「失敗例」として、SQL インジェクションとクロスサイト・スクリプティングの脆弱性を取り上げ、問題のあったウェブアプリケーションの実装、具体的なコード、解説、修正例を示しています。

本資料は、2006 年 1 月の公開以来、ダウンロード数は 130 万件を超えています。ウェブサイトのセキュリティ問題を解決する一助となれば幸いです。

■ 本件に関するお問い合わせ先
IPA セキュリティセンター　山岸／渡辺
Tel: 03-5978-7527　Fax: 03-5978-7518　E-mail: vuln-inq@ipa.go.jp
■ 報道関係からのお問い合わせ先
IPA 戦略企画部広報グループ　横山／大海
Tel: 03-5978-7503　Fax: 03-5978-7510　E-mail: pr-inq@ipa.go.jp

[4] ウェブサイトの SQL インジェクション脆弱性の検出ツール「iLogScanner」を公開。
http://www.ipa.go.jp/security/vuln/200804_iLogScanner.html
SQL インジェクション検出ツール「iLogScanner」を機能強化。http://www.ipa.go.jp/security/vuln/iLogScanner.html

[5] 「安全なウェブサイトの作り方」改訂第 3 版。http://www.ipa.go.jp/security/vuln/websecurity.html

別紙

iLogScanner が検出可能なウェブサイトを狙った攻撃の概要

1.SQL インジェクション

SQL インジェクションは、データベースと連携したウェブアプリケーションに問合せ命令文の組み立て方法に問題があるとき、ウェブアプリケーションへ宛てた要求に悪意を持って細工された SQL 文を埋め込まれて（Injection）しまうと、データベースを不正に操作されてしまう問題です。これにより、データベースが不正に操作され、ウェブサイトは重要情報などが盗まれたり、情報が書き換えられたりといった被害を受けてしまう場合があります。

2.ディレクトリ・トラバーサル

ディレクトリ・トラバーサルは、相対パス記法を利用して、管理者が意図していないウェブサーバ上のファイルやディレクトリにアクセスされたり、アプリケーションを実行される問題です。これらにより、本来公開を意図しないファイルが読み出され、重要情報が盗まれたり、不正にアプリケーションを実行されファイルが破壊されるなどの危険があります。

3.クロスサイト・スクリプティング

クロスサイト・スクリプティングは、ウェブサイトの訪問者の入力をそのまま画面に表示する掲示板などが、悪意あるスクリプト（命令）を訪問者のブラウザに送ってしまう問題です。これにより、アンケート、掲示板、サイト内検索など、ユーザからの入力内容をウェブページに表示するウェブアプリケーションで、適切なセキュリティ対策がされていない場合、悪意を持ったスクリプト（命令）を埋め込まれてしまい、ウェブページを表示した訪問者のブラウザ環境でスクリプトが実行されてしまう可能性があります。その結果として、cookie などの情報の漏洩や意図しないページの参照が行われてしまいます。

4.OS コマンド・インジェクション

OS コマンド・インジェクションは、ウェブサーバ上の任意の OS コマンドが実行されてしまう問題です。これにより、ウェブサーバを不正に操作され、重要情報などが盗まれたり、攻撃の踏み台に悪用される場合があります。

5.その他（IDS 回避を目的とした攻撃）

その他（IDS[6]回避を目的とした攻撃）は、16 進コード、親パス等の特殊文字を使用して偽装した攻撃用文字列で攻撃が行われることによりアプリケーションの妥当性チェック機構を迂回し、SQL インジェクション、クロスサイト・スクリプティング等の攻撃を行うことを狙ったものです。また、ワームなどが悪用するウェブサーバの脆弱性を突いた攻撃でも、このような特殊文字が使われます。

それぞれの脆弱性の内容に関しては「知っていますか？脆弱性(ぜいじゃくせい)[7] 」を参照下さい。

[6] Intrusion Detection System。侵入検知システム。
[7] 知っていますか？脆弱性 (ぜいじゃくせい)。http://www.ipa.go.jp/security/vuln/vuln_contents/index.html