

SQL インジェクション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を推奨～

独立行政法人 情報処理推進機構（略称：IPA、理事長：西垣 浩司）は、近年、SQL インジェクション攻撃が急増していることから、ウェブサイト管理者等への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等の対策実施を推奨します。

近年、ウェブサイトを狙った SQL インジェクション攻撃が急増しています。特に 2008 年 3 月頃より、有限責任中間法人 JPCERT コーディネーションセンター（JPCERT/CC）¹や内外の情報セキュリティ対策企業が、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不正コードを仕掛けられたページ数が数十万に達している旨の注意喚起を相次いで発表しています。また、5 月 6 日には、SQL インジェクション攻撃を行う悪質プログラム（ワーム）が確認された旨の注意喚起を米国 SANS Institute²が実施しています。IPA に届出られたウェブサイト（ウェブアプリケーション）の脆弱性の約 3 割が SQL インジェクションの脆弱性となっています³。

SQL(Structured Query Language)とは、データベースへの問い合わせ(Query)命令文を組立てて(Structured)実行するために、ウェブアプリケーションが使用しているコンピュータの言語(Language)です。ウェブアプリケーションの多くは利用者からの入力情報を基に SQL 文を組立てています。この組み立て方法に問題があると、悪意を持って細工された SQL 文もデータベースへの問い合わせの一部として埋め込んで(Injection)しまう可能性があります。この問題を悪用した攻撃を SQL インジェクション攻撃と呼んでいます。攻撃された場合、データベースに蓄積された情報の漏えい・改ざん、不正操作などの脅威があります⁴。

このため、データベースを利用しているウェブサイトの運営者は、SQL インジェクション攻撃によりウェブサイトに被害が発生していないか、ウェブサーバのアクセスログを常に調査し、攻撃があった場合は、データベースに認知していないリンクが含まれていないかを確認する必要があります。また、ウェブサイトの脆弱性検査を行い、脆弱性対策を講ずることが必要です。

IPA では、SQL インジェクション攻撃への対策を、「安全なウェブサイトの作り方」で公開しています。また、SQL インジェクション脆弱性の検出を行うツール「iLogScanner」を 4 月 18 日に公開しました⁵。このツールは、ウェブサーバのアクセスログの中から、SQL インジェクション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、ウェブサイトの脆弱性により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。

¹ 有限責任中間法人 JPCERT コーディネーションセンター。http://www.jpccert.or.jp/at/2008/at080005.txt

² SANS Internet Storm Center。http://isc.sans.org/diary.html?storyid=4393

³ ソフトウェア等の脆弱性関連情報に関する届出状況[2008 年第 1 四半期（1 月～3 月）]。
http://www.ipa.go.jp/security/vuln/report/vuln2008q1.html

⁴ SQL インジェクションの概要は「知っていますか？脆弱性（ぜいじゃくせい）」を参照。
http://www.ipa.go.jp/security/vuln/vuln_contents/index.html

⁵ 「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」を公開。
http://www.ipa.go.jp/security/vuln/iLogScanner.html

例えば、IPA で公開しているオープンソース情報データベース「OSS iPedia⁶」の2008年1月から4月のアクセスログを「iLogScanner」で解析したところ、合計44件のSQLインジェクション攻撃を検出しました。攻撃に成功した件数は0件でしたが、図1に示すように、4月は29件のSQLインジェクション攻撃があり、1～3月に比べて増加しています。

「iLogScanner」は、ブラウザ上で実行するJavaアプレット形式のツールであり、誰でも簡単に使用することができます。4月18日の公開以来、2千件を超えるダウンロードを記録しています。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。また、ウェブサイトの開発者やセキュリティ企業が、「iLogScanner」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。

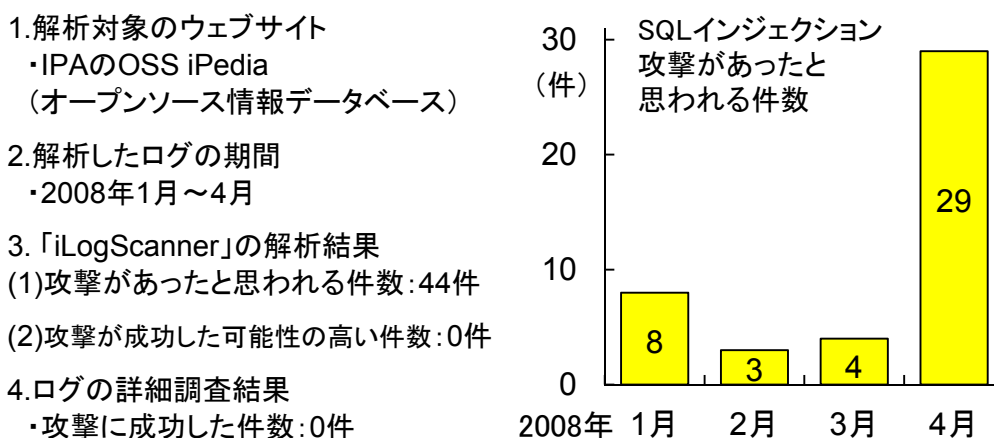


図1. SQLインジェクション脆弱性検出ツール「iLogScanner」の解析事例

(参考)

- 「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>

- ウェブサイトの脆弱性検出ツール「iLogScanner」
～ウェブサーバのアクセスログを解析して脆弱性検出を簡易に行うツール～
<http://www.ipa.go.jp/security/vuln/iLogScanner/index.html>

■ 本件に関するお問い合わせ先
独立行政法人 情報処理推進機構 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
独立行政法人 情報処理推進機構 戦略企画部広報グループ 横山
Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: pr-inq@ipa.go.jp

⁶ OSS iPedia (オーエスエスアイペディア) は、OSS(Open Source Software)の利用促進を進めることを目的とし、OSSの活用事例、技術情報、またオープンソースに関する基本的な知識を整理しています。“OSS”、情報 (information) の“i”、ギリシャ語で教育・知識・学問を意味する“Pedia(Paideia)”からの造語です。 <http://ossipedia.ipa.go.jp/>