NISC 内閣参事官

事　務　連　絡
平成２４年１月１９日

各府省庁情報セキュリティ担当課室長あて（注意喚起）
情報ｾｷｭﾘﾃｨ対策推進会議ｵﾌﾞｻﾞｰﾊﾞｰ機関情報セキュリティ担当課室長等あて（情報提供）

内閣官房情報セキュリティセンター
内閣参事官（政府機関総合対策促進担当）

公開ウェブサーバ脆弱性検査において複数の省庁で確認された脆弱性について（注意喚起）

内閣官房情報セキュリティセンターでは、平成 23 年 9 月から 12 月までの間、希望した 11 府省庁の公開ウェブサーバを対象とする脆弱性検査を実施しました。

その結果、危険度高（CVSS（注）基本値 7.0～9.9）に相当する SQL インジェクションやサービス運用妨害（DoS）の脆弱性が複数の省庁で確認されました。特に、SQL インジェクションについては、同手法を用いて政府機関のウェブサイトが改ざんされる事案も発生しています。

脆弱性が確認されたウェブサーバについては各府省庁において既に適切に措置が講じられたところですが、全ての府省庁において、本事務連絡に記載の SQL インジェクション及びサービス運用妨害（DoS）の脆弱性の確認方法等を参考に、管理している公開ウェブサーバについて確認し、脆弱性の存在が疑われる場合には、保守業者又は専門の検査会社に相談することを推奨します。特に、公開ウェブサーバを構築中の場合は、検収時に確認することを強く推奨します。

注　CVSS（共通脆弱性評価システム：Common Vulnerability Scoring System）は、米国家インフラストラクチャ諮問委員会（NIAC）のプロジェクトで 2004 年 10 月に原案が作成。特定のベンダーに依存しない共通の評価方法として、多数の組織で採用（参考 URL：http://www.first.org/cvss/eadopters.html）。

１　SQL インジェクション

(1)　概要

SQLインジェクションの脆弱性が存在すると、攻撃者が用意したSQL文をデータベース上で実行することが可能となるため、データベースに格納されている情報の漏えいや改ざんが発生する可能性があります。ウェブアプリケーションでは、実行される

べきでない悪意のあるSQL文が攻撃者から入力された場合、データベースで実行される前にSQL文として処理されないよう無効化する必要がありますが（図 1①）、無効化されずにデータベースで実行された場合、データベースの操作が可能となります（図 1②）。本脆弱性を悪用するとデータベース接続ユーザの権限の範囲で登録されている情報の取得や改ざん等が可能となります。

この中でも、今回確認されたSQLインジェクションの脆弱性は、

・攻撃を実施するに当たって攻撃が困難（複雑）となる要因が存在しなかった

・認証を必要としない箇所において検出された

ことから、危険度の高いものであるといえます。

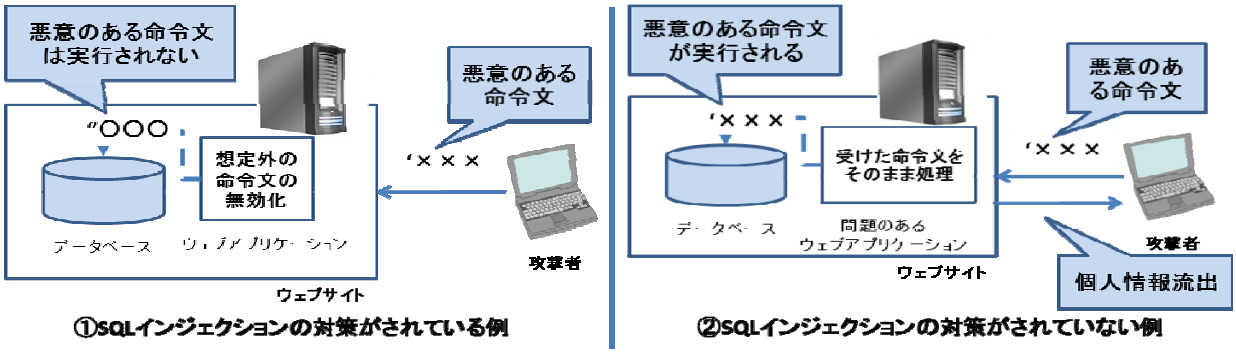

図 1 SQL インジェクションの概要

(2) 確認方法

本確認方法では、ブラウザの入力欄に SQL 文の特殊文字である「’」を含む文字列を入力し、その応答から SQL インジェクションの脆弱性が存在する可能性の有無を判断します。

例えば、ブラウザの入力欄に「テスト’」と入力し、検索ボタンを押下します。

その際、以下のような応答が返された場合には SQL インジェクションの脆弱性が存在する可能性が高いといえます。

・ データベースのソフトウェア名（Oracle, SQL Server, MySQL, DB2, PostgreSQL）を含むエラーメッセージが表示される。

・ SQL 文の一部が表示される。

・ SQL 文の構文エラーに関するメッセージが表示される。

・ 「ORA-01756」などユーザ向けではないメッセージが表示される。

また、SQL インジェクションの脆弱性が存在する可能性が高い場合「テスト’’」（シングルクォート 2 つ）を入力すると上記のような応答は返されません。

なお、上記の確認方法は「SQL インジェクションの脆弱性が存在する可能性」を判別するものであり、実際に SQL インジェクションの脆弱性の有無を保証するものではありません。独立行政法人情報処理推進機構(IPA)の「安全なウェブサイトの作り方 改訂第 5 版」（2011 年 4 月、http://www.ipa.go.jp/security/vuln/websecurity.html）チェックリスト等を参考に確認することを推奨します。

上記確認の結果、SQL インジェクションの脆弱性が存在する可能性が高いと判断した場合は、保守業者や専門の業者に相談するなどの対応を検討願います。

(3) 対策例

- 入力値チェック処理の徹底

  想定外の文字の入力を拒否する必要があります。例えば「値段」を入力するテキストボックスからの入力の場合には、入力値として数字以外の文字を受け付ける必要はないと考えられることから、数字以外の文字が入力された場合には、エラー処理を行うようにアプリケーションを修正します。数字に限らず、入力文字種や文字列の長さが制限できる場合には、指定した制限規則外の文字列を受け付けないようにすることでWebアプリケーションの安全性が高まります。

- エスケープ処理の徹底

  SQL文で使用されている特殊文字をエスケープ処理する必要があります。エスケープが必要な文字種に関しては、データベースサーバの種類やアプリケーション環境に依存します。

【参考情報】

- IPAセキュア・プログラミング講座 第6章 入力対策 SQL注入:#1 実装における対策

http://www.ipa.go.jp/security/awareness/vendor/programmingv2/web06.html

２ サービス運用妨害（DoS）

(1) 概要

Apache 2.0.64以下及び2.2.19以下のバージョンには、Rangeヘッダ及びRequest-Rangeヘッダの処理に問題があり、サービス運用妨害（DoS）の脆弱性が存在します。脆弱性が悪用されると遠隔の第三者によって、サービス運用妨害（DoS）攻撃を受ける可能性があります。また、「Apache Killer」と呼ばれる攻撃ツールが公開されており注意が必要です。

なお、この脆弱性については、Apacheが組み込まれている、又はApacheをベースとして使用するソフトウェア製品においても脆弱性の影響を受ける可能性があります。

また、動作しているApacheのバージョンが1.3系の場合には本脆弱性の影響は受けません。ただし、1.3系は開発が終了しているバージョンであり、今後発見される脆弱性への対応が行われないため、最新の2.2系へのバージョンアップを検討することが望まれます。

(2) 対策例

脆弱性の影響を受けるバージョンを使用している場合には、ベンダーから提供されているセキュリティパッチの適用又は脆弱性の改修された最新バージョンへのバージョンアップを行います。

- Apacheプロジェクト提供の2.2系における最新バージョン（2011年11月時点）

Apache HTTP Server 2.2.21
http://www.apache.org/dist/httpd/

パッチ適用又はバージョンアップができない場合及びApache2.0系を使用している場合には、回避策として以下のいずれかの設定を行います。設定方法の詳細については、参考情報を参照してください。

＜回避策＞

（ｉ）大量のRangeヘッダを含むリクエスト及びRequest-Rangeヘッダの無視又は拒否

使用されているApacheのバージョンに応じて、以下のどちらかを設定してください。

設定１：Apacheの設定ファイルに以下の設定を追加（※Apache 2.2系で有効）

【設定例】

```
SetEnvIf Range (?:,.*?){5,5} bad-range=1
RequestHeader unset Range env=bad-range
RequestHeader unset Request-Range
```

設定２：Apacheの設定ファイルに以下の設定を追加※Apache 2.0系及び2.2系で有効

【設定例】

```
RewriteEngine on
RewriteCond %{HTTP:range} !(^bytes=[^,]+(,[^,]+){0,4}$|^$) [NC]
RewriteRule .* - [F]
```

（ⅱ）Rangeヘッダを完全に無効化

Apacheの設定ファイルに以下の設定を追加

【設定例】

```
RequestHeader unset Range
RequestHeader unset Request-Range
```

（ⅲ）一時的な対策として、Rangeヘッダカウントモジュールを適用

以下のリンクから入手可能。

http://people.apache.org/~fuankg/httpd/mod_rangecnt-improved/

http://people.apache.org/~dirkx/mod_rangecnt.c

【参考情報】

- Apache HTTPD Security ADVISORY（開発元のセキュリティアドバイザリ）
  http://httpd.apache.org/security/CVE-2011-3192.txt
- Apache HTTP Server 2.2.21 Released
  https://www.apache.org/dist/httpd/Announcement2.2.html
- JPCERT/CC Apache HTTP Server のサービス運用妨害の脆弱性に関する注意喚起
  https://www.jpcert.or.jp/at/2011/at110023.html

- 情報処理推進機構（IPA） ウェブサーバ「Apache HTTP Server」の脆弱性（CVE-2011-3192）について
  http://www.ipa.go.jp/security/ciadr/vul/20110831-apache.html
- JVN Apache HTTPDサーバにサービス運用妨害(DoS)の脆弱性
  http://jvn.jp/cert/JVNVU405811/

３ その他

・ 前述の「安全なウェブサイトの作り方 改訂第 5 版」にも各種脆弱性に対する対策が記載されておりますので、これに基づき公開ウェブサイトを構築してください。

・ 内閣官房情報セキュリティセンターでは、平成 24 年度も各府省庁の公開ウェブサーバを対象とする脆弱性検査を実施することを検討しています。なお、検査対象のサーバについては、構築後 1 年程度の比較的新しく導入されたサーバを対象とする予定です。

以 上

本件問い合わせ先
内閣官房情報セキュリティセンター
政府機関総合対策促進担当
木本、戸田、山田、古門
（03-3581-3959）