

「安全なウェブサイトの作り方 改訂第4版」を公開

～ウェブアプリケーションに脆弱性を作り込んでしまった「失敗例」を拡充～

IPA(独立行政法人情報処理推進機構、理事長:西垣 浩司)は、ウェブサイト開発者・運営者が適切なセキュリティを考慮したウェブサイトを作成するための資料、「安全なウェブサイトの作り方」を改訂し、改訂第4版を2010年1月20日(水)からIPAのウェブサイトで公開しました。

URL: <http://www.ipa.go.jp/security/vuln/websecurity.html>

「安全なウェブサイトの作り方」は、IPAが届出¹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ウェブサイトを作成するための資料です。

今回の改訂第4版では、実践的な脆弱性対策の更なる普及促進のため、「失敗例」を拡充しました。前版のSQLインジェクション²とクロスサイト・スクリプティング³に関する失敗例に加え、改訂第4版ではOSコマンド・インジェクション⁴、パス名パラメータの未チェック⁵、クロスサイト・リクエスト・フォージェリ⁶、HTTPヘッダ・インジェクション⁷の4種類の脆弱性に関する失敗例を第3章に追記しました。これらは、ウェブアプリケーション⁸開発に携わるベンダにおける脆弱性の事例を参考にしています。

また新たに、WAF(Web Application Firewall)⁹の活用に関して、WAFの動作原理、WAFの使用が有効な状況、導入検討における留意点を第2章に追記しました。

「安全なウェブサイトの作り方 改訂第4版」各章の内容:

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種類の脆弱性を取り上げ、それぞれの脆弱性で発生する脅威や特に注意が必要なウェブサイトの特徴などを解説し、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¹⁰を助長しないための対策など6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ための方策を示しています。

第3章では、「失敗例」として、第1章で取り上げた脆弱性の中から6種類を取り上げ、ウェブアプリケーションに脆弱性を作り込んでしまった際のソースコード、その解説、修正例を示しています。

巻末には、ウェブアプリケーションのセキュリティ実装の実施状況を確認するためのチェックリストも付属しています。

本資料は、2006年1月の第1版の公開以来、130万件を超えるダウンロードを記録しています。今後も、ウェブサイトのセキュリティ問題の解決の一助となることを期待します。

本資料(全92ページ)は、下記URLよりダウンロードの上、ご参照ください。

<http://www.ipa.go.jp/security/vuln/websecurity.html>

■ 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

脚注:

- ¹ IPA セキュリティセンターでは、経済産業省の告示に基づき、脆弱性情報に関する届出を受け付けています。「脆弱性関連情報の届出」を参照下さい。<http://www.ipa.go.jp/security/vuln/report/index.html>
- ² SQL インジェクションとは、データベースと連携したウェブアプリケーションに、データベースへの命令文の組み立て方法に問題があるとき、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、ウェブサイトから重要情報が漏洩したり、ウェブサイトの情報が書き換えられたりといった被害を受ける場合があります。詳細は「知っていますか？脆弱性(ぜいじゃくせい)」を参照下さい。
http://www.ipa.go.jp/security/vuln/vuln_contents/sql.html
- ³ クロスサイト・スクリプティングとは、ウェブサイトの利用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)を利用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、利用者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利用者のブラウザ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、Cookie 情報の漏洩や意図しないページの参照などが行われてしまいます。詳細は「知っていますか？脆弱性(ぜいじゃくせい)」を参照下さい。
http://www.ipa.go.jp/security/vuln/vuln_contents/xss.html
- ⁴ OS コマンド・インジェクションとは、ウェブサーバ上で任意の 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、ウェブサイトから重要情報が漏洩したり、攻撃の踏み台に悪用される場合があります。詳細は「知っていますか？脆弱性(ぜいじゃくせい)」を参照下さい。
http://www.ipa.go.jp/security/vuln/vuln_contents/oscmd.html
- ⁵ ディレクトリ・トラバーサルとは、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、ウェブサイトから重要情報が漏洩したり、ウェブサーバ上のファイルが破壊されるなどの危険があります。詳細は「知っていますか？脆弱性(ぜいじゃくせい)」を参照下さい。
http://www.ipa.go.jp/security/vuln/vuln_contents/dt.html
- ⁶ クロスサイト・リクエスト・フォージェリとは、ログインした利用者からのリクエストについて、その利用者が意図したリクエストであるかどうかを識別する仕組みを持たないウェブサイトが、外部サイトを経由した悪意のあるリクエストを受け入れてしまう問題です。このようなウェブサイトログインした利用者は、悪意のある人が用意した罠により、意図しない処理を実行させられてしまう可能性があります。詳細は「知っていますか？脆弱性(ぜいじゃくせい)」を参照下さい。
http://www.ipa.go.jp/security/vuln/vuln_contents/csrf.html
- ⁷ HTTP ヘッダ・インジェクションとは、ウェブサーバからブラウザに送信する HTTP ヘッダに、意図しない情報を埋め込まれてしまう問題です。ウェブアプリケーションの中には、HTTP ヘッダを、ブラウザから送信される情報を基に作成するものがありますが、ウェブアプリケーションに問題があると、悪意を持って細工された情報を HTTP ヘッダに埋め込まれ(Injection)、埋め込まれた情報を基に偽ページを表示してしまうなどの危険があります。詳細は「知っていますか？脆弱性(ぜいじゃくせい)」を参照下さい。
http://www.ipa.go.jp/security/vuln/vuln_contents/hhi.html
- ⁸ ウェブサイトで稼動するシステムです。一般に、Java, PHP, Perl などの言語を利用して開発され、サイトを訪れた利用者に対して動的なページの提供を実現しています。
- ⁹ ウェブアプリケーションと利用者の間で交わされる通信を検査し、攻撃などの不正な通信を自動的に遮断するソフトウェア、もしくはハードウェアです。
- ¹⁰ 巧妙な文面のメール等を用い、実在する企業(金融機関、信販会社、ネットオークション等)のサイトを装った偽りのサイトにユーザを誘導し、機密情報(クレジットカード番号、ID、パスワード等)を盗み取る不正行為です。