IPA Technical Watch

2013 年 12 月 12 日
独立行政法人情報処理推進機構

IPA テクニカルウォッチ：「ウェブサイトにおける脆弱性検査手法の紹介」の公開
～ウェブ改ざんに繋がる脆弱性等をコストをかけずに検査する、3 種のツールの使い勝手を比較～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、ウェブサイトの脆弱性を検査するオープンソースのツール 3 種の評価を行い、ツールの特徴と使用における留意点をまとめたレポート「ウェブサイトにおける脆弱性検査の紹介（ウェブアプリケーション編）」を 2013 年 12 月 12 日から IPA のウェブサイトで公開しました。
URL：http://www.ipa.go.jp/about/technicalwatch/20131212.html

2013 年は、ウェブアプリケーションやウェブサイトを構成するミドルウェアの脆弱性が原因で、多数のウェブサイトで改ざんや情報漏洩などが発生しました。例えば、ユーザが改ざんされたウェブサイトを閲覧し、ウイルスに感染した場合、ウェブサイトを運営する組織は、ユーザへの謝罪や風評対策などの対応を迫られることになります。

現在、ウェブサイトを持たない組織はまれである一方で、ウェブサイトの安全性を適切に確認できている組織は、それに必要な技術者やコストの確保の面で決して多くないと IPA ではみています。

そこで IPA では、被害防止を図るため、自組織のウェブサイトが安全かどうかを検査する手法を紹介したレポート「ウェブサイトにおける脆弱性検査の紹介（ウェブアプリケーション編）」を公開しました。

本レポートでは、ウェブサイト管理者がコストをかけずに簡易に利用できるよう、7 つのオープンソースの脆弱性検査ツールからタイプ別に 3 種（「OWASP ZAP(Zed Attack Proxy)(*1)」、「Paros(*2)」、「Ratproxy(*3)」）を選定し、手順に沿った検査によるツールの評価を行い、ツールの特徴や使い勝手をまとめています（表 1）。

表 1：ツールの特徴比較

ツール名	検査者のスキル	操作性	検知精度	効率性	本番環境への影響
OWASP ZAP	初級者向け	使い易い	○	非常に良い	あり
Paros	上級者向け	使い易い	対象外	手間がかかる	あり （検査内容による）
Ratproxy	中級者向け	手間がかかる	△	良い	なし

ウェブサイトの安全性の確認には、オープンソースの利用はコスト面はもちろんのことツールによっては主要な脆弱性にも対応しており、運営者は無償かつ手軽に利用することができます。しかし、これらのツールには、検査方法、その精度、実施者に求められる経験など一長一短があります。そのため、検査実施にあたってはウェブサイトの運用環境や検査実施者のスキルなどを考慮し、適切なツールの選択が必要で、本レポートを参考にツール利用と脆弱性検査の有効性を確認することができます。

IPA では、こうした脆弱性検査が運用開始前だけでなく、運用中のウェブサイトの脆弱性の発見にも取り入れられ、多くのウェブサイトが安全に運営されることを期待しています。

(*1) OWASP で開発された自動検査型のツール。自動的にウェブサイトを巡回し、検査結果をレポートしてくれる。
(*2) クライアントとウェブサーバ間のローカルプロキシとして機能し、ウェブブラウザからの HTTP リクエストを横取りし、パラメータ値を手動で書き換えながら、反応を監視する手動検査型のツール。
(*3) Google が開発したローカルプロキシとして動作する脆弱性検知ツール。検査実施者は、本ツールをプロキシとして設定し、検査対象のウェブサイトを巡回するだけで脆弱性を検出できるのが特徴である。

また、今後もウェブアプリケーションの脆弱性に関する教材[*(4)]の公開や定期的なセミナー[*(5)]開催など、安全なウェブサイト運営に向けた啓発活動に努めていきます。

■ 本件に関するお問い合わせ先
IPA 技術本部 セキュリティセンター 大森／亀山／関口
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／白石
Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: pr-inq@ipa.go.jp

(*4)「安全なウェブサイトの作り方」 http://www.ipa.go.jp/security/vuln/websecurity.html
(*5) 情報セキュリティ対策 脆弱性体験学習コース「AppGoat ハンズオンセミナー」
http://www.ipa.go.jp/security/seminar/isec-semi/standard_course_guide.html#c_appgoat