News Release

2016 年 11 月 9 日

『VEX』で納品時のセキュリティ要求仕様の対応可視化を実現

～IPA 公開のセキュリティ要件「安全な Web サイトの作り方」に対応～

株式会社ユービーセキュア（本社：東京都港区、代表取締役社長：佐藤　健、以下、ユービーセキュア）は、大手システムインテグレータや IT セキュリティベンダに導入実績がある Web アプリケーション脆弱性検査ツール『VEX』に、検査結果とセキュリティ要件を突き合わして要件を満たしていない項目を確認できる「Web アプリケーション脆弱性検査チェックリスト」を出力する機能を追加いたします。本機能はバージョン 6.2 より標準機能として提供いたします。今回のリリースでは、国内の開発現場でセキュリティ要求仕様等に広く活用されている、独立行政法人情報処理推進機構（IPA）が提供する「安全な Web サイトの作り方」に対応いたします。本対応により、納品前のセキュリティ要求仕様の確認が容易に実施可能、かつ、お客様へ対応状況を可視化し報告可能となります。VEX は、国産ツールとして、国内・海外のセキュリティ要件を順次追加いたします。

■Web アプリケーション脆弱性検査チェックリスト（サンプル）

Webアプリケーション脆弱性検査チェックリスト

【サマリー】
検査条件やセキュリティ要件別の脆弱性の検出数が確認できる。

【詳細】
VEX の検出結果とセキュリティ要件別脆弱性のカテゴリを突き合わせた一覧。要件を満たしていない項目が確認できる。

・検査条件

サイト名	プロジェクト①
検査期間	2016/10/17
ガイドライン	安全なWebサイトの作り方 改定第7版
環境種別	開発環境
対象ホスト	http://x/
対象数	20 リクエスト

・脆弱性の種類別検出数

No	脆弱性の種類	結果
1	SQLインジェクション	23 件
2	OSコマンド・インジェクション	1 件
3	パス名パラメータの未チェック／ディレクトリ・トラバーサル	1 件
4	セッション管理の不備	1 件

No	危険度	VEXカテゴリ	IPAカテゴリ	脆弱性の概要	機能名	URL	パラメータ名	操作内容	対策
1	High	SQL Injection	SQLインジェクション	SQL構文の正誤判定による BlindSQLInjection	ログイン	http://x/shop/	login_id	リンク	SQL特殊文字は適切にエスケープを行ってください。また、可能であれば、バインドメカニズムを利用するようにしてください。
2	Low	HTML5 HTTP Headers To Enhance Security	クリックジャッキング	X-Frame-Optionsヘッダの未出力によるクリックジャッキング	オンラインショップ	http://x/shop/top.cgi	_	リンク	レスポンスにX-Frame-Optionsヘッダを出力してください。 例えば、フレーム内への表示を同じオリジンの Web ページでのみ許可する場合、X-Frame-Options:
3	High	OS Command Injection	OSコマンド・インジェクション	Ruby on Rails における任意の Ruby コード実行による OS Command Injection(CVE-2013-0156)	ログイン	http://x/shop/	-	リンク	ベンダより提供される情報を元に Ruby on Rails のバージョンを最新版にバージョンアップして下さい。

■「安全なウェブサイトの作り方」について

IPA への届け出件数の多かった脆弱性や影響の大きい脆弱性を解説し、セキュアな Web サイト構築のためのポイントがまとめられています。

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

【会社概要】
所　在　地：東京都港区芝 5-29-14　田町日エビル 4 階
設　　立：2007 年 4 月
代　表　者：代表取締役社長　佐藤　健
資　本　金：4,200 万円
事 業 内 容：情報セキュリティに関するコンサルテーション、検査サービス、検査ツール開発等
U　R　L：http://www.ubsecure.jp/

【お問い合わせ先】営業統括部　Mail：vex@ubsecure.jp　TEL：03-5730-3033　FAX：03-5730-3055