EC サイト向け無償脆弱性診断の診断予定項目

1. ネットワーク診断内容

ネットワーク調査(TCP･UDP･サービススキャン、OS 推測、ホスト名調査)、各種サービスの脆弱性スキャン、FTP 調査、SSH 調査、TELNET 調査、SMTP 調査、POP 調査、DNS 調査、HTTP/HTTPS 調査、SNMP 調査、NTP 調査、バックドア調査(ポートスキャン)

2. ウェブアプリケーション診断内容

－ 「OWASPTOP10」に掲載の項目

SQL インジェクション、NoSQL インジェクション、OS コマンドインジェクション、LDAP インジェクション、認証の不備、機微な情報の露出、XML 外部エンティティ参照(XXE)、アクセス制御の不備、不適切なセキュリティ設定、クロスサイトスクリプティング(XSS)、安全でないデシリアライゼーション、既知の脆弱性のあるコンポーネントの使用等

－ 「安全なウェブサイトの作り方」の「セキュリティ実装チェックリスト」掲載項目

SQL インジェクション、OS コマンド・インジェクション、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、セッション管理の不備、クロスサイト・スクリプティング、CSRF(クロスサイト・リクエスト・フォージェリ)、HTTP ヘッダ・インジェクション、メールヘッダ・インジェクション、クリックジャッキング、バッファオーバーフロー、アクセス制御や認可制御の欠落等

－ 「OWASP アプリケーションセキュリティ検証標準 4.0」に掲載の項目

認証の検証要件、セッション管理の検証要件、アクセス制御検証要件、バリデーション、無害化とエンコーディング検証要件、保存時の暗号化の検証要件、データ保護の要件、通信の検証要件、悪性コードの検証要件、ビジネスロジックの検証要件、ファイルとリソースの検証要件、API、Web サービスの検証要件、構成の検証要件等

※上記記載の各要件に含まれている項目で、レベル 1、レベル 2、レベル 3 の全てがチェックされている項目を想定