108. Webアプリケーション開発のための情報セキュリティ対策

1. 研修要領

・ITSS	3
・研修実施日	2024年02月01日(木)～2024年02月02日(金)
・研修実施時間・日数	9:30 ～ 16:30 （6時間/日）
・研修会場	福岡ソフトウェアセンター　福岡研修室
・研修受講料(税別・テキスト代込）	58,000円

2. 対象者

今後Webアプリケーションを開発される予定の方、または運用を行う方
※「ルータを中心に学ぶネットワーク基礎とセキュリティ」の受講又は同等の知識を有していることが望ましい

3. カリキュラムの概要

Webアプリケーションシステムの脆弱性が原因で発生するWebページの改ざん、情報漏えい、利用者に被害が及ぶ攻撃のしくみを実機を通して体験的に学習します。
グループディスカッションで問題対策技術を話し合うことにより、必要なWeb技術をより深く理解します。

4. カリキュラムの詳細　　2日間（12時間）

科目		時間	科目の内容
1日目	1. Web技術基礎 【講義／演習】	2.0h	(1)HTML、CSS、XHTML、XML、DOM (2)HTTP、Cookie、セッション管理 (3)サーバサイド言語、クライアントサイド言語 (4)Webサービス
	2. Webアプリケーションに関連する攻撃	4.0h	(1)パラメータ改竄 (2)スクリプトインジェクション (3)クロスサイトスクリプティング (4)クロスサイトリクエストフォージェリ (5)SQLインジェクション (6)LDAPインジェクション (7)XQuery、XPathインジェクション、XMLインジェクション (8)HTTPヘッダインジェクション (9)HTTPレスポンススプリッティング (10)強制ブラウズ (11)ディレクトリトラバーサル (12)ヌルバイト攻撃 (13)OSコマンドインジェクション

4. カリキュラムの詳細　　2日間（12時間）

科目		時間	科目の内容
2日目	3. Webサーバのセキュリティ設定	0.5h	(1)一覧表示の抑止 (2)プログラム名／バージョン情報送出の抑止
	4. SSL（Secure Sockets Layer）	1.0h	(1)暗号技術、認証技術 (2)認証局、デジタル証明書 (3)ApacheのSSL設定
	5. Webで利用されるアクセス制限	1.0h	(1)ユーザ認証によるアクセス制限 (2)接続元ホストによるアクセス制限 (3)接続元ホストとユーザ認証を組み合わせたアクセス制限 (4)アプリケーションによる認証機能の実装
	6. DNSサーバのセキュリティ	1.0h	(1)DNSキャッシュ汚染攻撃とは (2)DNSキャッシュ汚染対策
	7. プロキシサーバ	1.0h	(1)フォワードプロキシ、リバースプロキシ (2)プロキシを使う上での問題点
	8. データベース	1.0h	(1)スキーマの管理 (2)アクセス権限の管理 (3)ビュー表の利用 (4)三層構造における完全な監査証跡の保存（SOX法対策）
	9. セキュリティ運用	0.5h	(1)セキュリティ診断 (2)侵入検知（IDS） (3)ログの監視
計		12.0Hr	

※最低開催人数は4名とさせていただきます。中止の場合は、開催日の2週間前までにご連絡させて頂きます。

※改善のためカリキュラムは予告なく変更させていただくことがあります。

5. 使用教材

オリジナルテキスト

6. 到達目標

1. 安全なWebアプリケーションの設計ができる
2. 安全なWebアプリケーションのコーディングができる
3. Webサーバのセキュリティを設定できる
4. Webシステムの安全な運用環境を構築できる