

コースコード：GX-SWAD

税込価格：132,000円 (税抜価格：120,000円)

日数：1日間

前提条件

ご受講に際して特に前提条件はございませんが、下記のようなご経験がありますとよりこのコースの理解度が高まります。

- ・開発言語を使ったプログラム経験（例：VB, C++, PHPなど）
- ・OSのインストール経験（例：WindowsやLinux、MacOSなど）
- ・ホームルーターの設定経験

受講対象者

イントラネット / 内部ネットワーク向けのWebシステム / Webアプリケーションに関わる下記の方が主な対象者となります。

- ・Webシステムの発注者
- ・Webアプリケーションの設計者・開発者

PCI DSSなどで要求されるOWASP Top 10などに基づいた安全なコーディング技法に関するトレーニングが要求されている場合などにも最適です。

コース概要

安全なWebアプリケーション開発のために必要な要件と設計の具体例を学ぶ、短期集中の1日トレーニングです。インターネットまたは内部ネットワーク向けに公開するWebアプリケーションをセキュアに構築するための要件や設計を学ぶことを目的としています。

目的

本講座では下記のスキルを習得することができます。

- ・セキュアなWebシステム / Webアプリケーションを構築するために必要な知識
- ・発注者・開発者に必要なWebシステム / Webアプリケーションのセキュリティ要件
- ・上記セキュリティ要件を満たす設計の具体例

アウトライン

セキュリティ要件

- ・セキュリティ要件の原則
- ・Webアプリケーションのセキュリティ要件

セキュアWebアプリケーションの構築

- ・認証の目的
- ・NIST SP800-63B、Authenticatorのタイプ、AAL
- ・Webアプリケーションで使う主な認証の種類
- ・BASIC認証、DIGEST認証
- ・フォームベース認証
- ・認証を行うべき箇所
- ・強いパスワードとは
- ・パスワードのハッシュ化、salt、ストレッチング
- ・パスワードの作成について
- ・ユーザーへのパスワード通知方法



- ・パスワードの変更機能
- ・パスワードリセット機能
- ・秘密の質問について
- ・認証実行時のエラー処理、ログ記録
- ・アカウントロック
- ・パスワードリスト攻撃対策
- ・二要素認証、リスクベース認証

認可

- ・認可の目的
- ・アクセス制御の失敗例
- ・アクセス制御方法
- ・OpenID, OAuth, シングルサインオン
- ・限定公開URL
- ・FIDO認証

セッション管理

- ・セッションIDの役割
- ・Cookie
- ・設定すべきCookieの属性値
- ・セッションIDを利用した攻撃を防ぐ設計
- ・セッションタイムアウトの設計
- ・ログアウト機能
- ・セッションIDの生成
- ・CSRF対策
- ・トークン方式
- ・SameSite属性

入力処理

- ・クライアント側での入力値チェック
- ・Webアプリケーション側でのチェック
- ・パラメーターについて
- ・入力値の文字種や文字長の検証
- ・文字エンコーディングの統一
- ・入力値としてファイルを扱う場合
- ・XMLファイルを扱う場合
- ・デシリアライズについて

出力処理

- ・出力処理で必要なこと
- ・特殊文字のエスケープ処理
- ・HTMLを生成する際の処理
- ・HTMLのエスケープ処理
- ・その他のスクリプト埋め込み原因の排除
- ・クライアント側でHTMLを生成する際の処理
- ・SQL文を組み立てる際の処理
- ・JSONの生成
- ・OSコマンドを呼び出す処理
- ・HTTPレスポンスヘッダーについて
- ・リダイレクタを使う際の注意事項

HTTPS

- ・SSL/TLS
- ・HTTPSの仕組み
- ・証明書に対する攻撃
- ・HTTPSを使う際の注意
- ・証明書の種類、用途による使い分け
- ・安全なプロトコルと暗号アルゴリズム
- ・フィッシングサイトに対抗するには？



その他

- ・エラーメッセージハンドリング
- ・暗号アルゴリズムと乱数について
- ・疑似乱数生成器
- ・言語・フレームワーク・ミドルウェア・ライブラリなどの選定
- ・ログの記録
- ・ユーザーへの通知
- ・Access-Control-Allow-Originヘッダーについて
- ・クリックジャッキング対策
- ・キャッシュ制御について
- ・CAPTCHAについて
- ・言語環境のセキュリティ設定
- ・用意すべきドキュメント