18j セキュアなWebアプリケーション開発 ～脆弱性を突いた攻撃方法とその対策～ (NEW)

主催者 （一社）長崎県情報産業協会

1. 研修要領

・募集定員	16名
・研修会場	NISA研修室　（住所：〒850-0032　長崎市興善町4番6号）
・講　　師	富士通九州システムズ（FJQS）：井上龍也
・開催月日	2020年12月02日（水）・03日（木）・04日（金）
・実施時間・日数	9:30 ～ 17:30 （7時間/日）・3日間（21時間）
・受 講 料（税別）	78,800円
・教 材 料（税別）	5,000円

2. 対象者

セキュアなWebアプリケーションを開発したい方。

3. カリキュラムの概要

インターネット時代において**Webアプリケーションのセキュリティは必要不可欠**です。Webアプリケーションに脆弱性があると、攻撃されたり、他社のシステムを攻撃する踏み台にされてしまいます。本コースでは、まず脆弱性を持つ**Webアプリケーションに攻撃する手法を講義・実機演習で学び、それを回避する開発技術や攻撃を受けた場合の痕跡確認方法**（ログファイル）について学んでいただきます。本コースを受講することにより**セキュアなWebアプリケーションを構築するポイントを体得**していただきます。

4. カリキュラムの詳細　　3日間（21時間）

	科目	時間	科目の内容
12月2日	1. 脆弱性を突いた攻撃の分類	1.5hr	・フィッシング ・ファーミング 【個人演習】 これまで作成したWebアプリケーションの脆弱性の棚卸 発表、情報共有
	2. 脆弱性を突いた攻撃の種類	5.5hr	・OSコマンドインジェクション ・ディレクトリトラバーサル ・ファイルインクルード攻撃 ・セッションハイジャック ・HTTPヘッダインジェクション ・クリックジャッキング ・SQLインジェクション ・クロスサイト・スクリプティング（XSS） ・クロスサイト・リクエストフォージェリ 【個人演習1】 各種攻撃の体験 【個人演習2】 各種攻撃の仕組みの解明

	科目	時間	科目の内容
12月3日	3. 各種攻撃の対策法	7.0hr	・OSコマンドインジェクション ・ディレクトリトラバーサル ・ファイルインクルード攻撃 ・セッションハイジャック ・HTTPヘッダインジェクション ・クリックジャッキング ・SQLインジェクション ・クロスサイト・スクリプティング(XSS) ・クロスサイト・リクエストフォージェリ 【個人演習3】 各種攻撃に対する対策の実装 【個人演習4】 各種攻撃が失敗することの確認
12月4日	4. 各種攻撃の追跡法	2.0hr	・Webサーバーのログファイルとその設定法 ・アプリケーションサーバーのログファイルとその設定法 ・DBサーバーのログファイルとその設定法 ・各種攻撃で残る痕跡 【個人演習5】 痕跡を残すログファイルの確認
	5. 総合演習	5.0hr	【総合演習】 先ず脆弱性を突いた攻撃を受けたサーバーのログファイルを調査し、攻撃の特定をする。次に、特定した攻撃が再現できるか確認する。攻撃法が特定出来たら、対策を施し、攻撃を受けないように、Webアプリケーションを修正する。最後に、修正が完了したことを再度攻撃してみて、攻撃を受けないことを確認する。
	計	21.0hr	

5. 使用教材

セキュアなアプリケーション開発～脆弱性を突いた攻撃方法とその対策～(FJQS教材)
FJQS作成総合問題

6. 到達目標

本コース修了後、次の事項ができることを目標としています。
1. 主要なWebアプリケーションの脆弱性を説明できる。
2. Webアプリケーションの脆弱性を突いた攻撃の仕組みを説明できる。
3. 脆弱性を突かれないようにする対策をWebアプリケーションに実装できる。
4. 脆弱性を突いた攻撃があったことを痕跡から確認できる。

7. レベル

ITSS:ITスペシャリスト育成 - [*]テクノロジ【レベル:2-3】
ITSS:アプリケーションスペシャリスト育成 - [*]テクノロジ【レベル:2-3】
ITSS:アプリケーションスペシャリスト育成 - [*]メソトロジ【レベル:2-3】

[*] ITスキル標準研修ロードマップにおけるコース群名