学校法人宮崎総合学院　宮崎情報ビジネス専門学校

授業科目名	セキュリティ実践			科目コード	MJIK 0006
学科・コース名	情報システム科 IT高度専門士コース			履修区分	選択必修
授業形態	演習	開講学年	2年次	学期	後期
担当教員	内山田　隆司	実務経験	有	単位数	1 単位
授業の 目的・目標	セキュリティ技術の授業で学んだセキュリティに関する理論を使用し、演習を通してセキュリティ対策実践を経験する。				
授業の概要	1.用意した脆弱サンプルを使用し、実物の脆弱性に触れてその原理を知り、発生防止策について学ぶ。 2.代表的な脆弱性診断ツール(Nessus)を使用し、脆弱性診断を体験する。 3.実際のセキュリティ事故報告書を精読し、レポートにまとめる				

回	授業計画・内容	授業外学習の内容	授業外学習時間
1	授業目的の確認。チャットアプリによるソケット通信の実際を体験	使用したPythonアプリの内容確認	30分
2	チャットアプリへの攻撃例を体験	実践した攻撃手法以外の方法を考案	60分
3	OWASP ZAP、Chrome拡張Proxy機能の導入と試用	ZAPが登場した背景を調査	30分
4～5	ZAPを使用したwebアプリのセッション管理方式の体験	クッキーとセッション管理の復習	60分
6～7	CORS脆弱性の原理と対策方法	教科書による授業内容再確認	60分
8～9	クロスサイトスクリプティング脆弱性の原理と対策方法(基本)	教科書による授業内容再確認	60分
10～11	クロスサイトスクリプティング脆弱性の原理と対策方法(発展)	教科書による授業内容再確認	60分
12	SQLインジェクション脆弱性の原理と対策方法	データベース入門のSQL確認	60分
13～14	OSコマンドインジェクション脆弱性の原理と対策方法	Linux主要コマンドの再確認	30分
15	クロスサイトリクエストフォージェリ脆弱性の原理と対策方法	教科書による授業内容再確認	60分
16～17	セッションハイジャック型脆弱性の原理と対策方法	教科書による授業内容再確認	60分
18	文字コードによる脆弱性が発生する原因と対策方法	教科書による授業内容再確認	30分
19～20	ポートスキャナ(Nmap)の導入。スキャン体験。原理解説。	家庭内機器へのスキャン体験	60分
21～22	ZAPによる脆弱性診断の体験と診断結果の見方	診断レポートの確認	30分
23～25	脆弱性診断ツール(Nessus)導入。脆弱性サンプルの診断体験	診断レポートの確認	30分
26	脆弱性の管理方式。IPAのセキュリティ啓蒙動画の視聴	IPAの啓蒙動画視聴	60分
27～28	セキュリティ事故研究(利用された脆弱性と防止できなかった原因)	授業以外の事故事例調査	60分
29～30	事故事例の発表。レポート課題の目的及び予備調査実施	レポート課題完成	120分

評価方法	・授業中の演習取組み状況(40%) ・レポート課題の内容評価(60%)
教科書参考書	徳丸浩著「体系的に学ぶ 安全なWebアプリケーションの作り方 第2版 脆弱性が生まれる原理と対策の実践」