科目名	セキュリティ応用							年度	2025
英語科目名	Applied Security							学期	後期
学科・学年	ネットワークセキュリティ科 セキュリティ専攻　2年次	必／選	必	時間数	60	単位数	2	種別※	実習
担当教員	勝島	教員の実務経験		有	実務経験の職種		システムエンジニア		

【科目の目的】

仮想環境下での、XSS、SQLインジェクションなどのWebアプリケーションにおける脆弱性の理解と対策を通じて、安全なWebアプリケーションを構築・検証できる力を身につけることを目指します。

【科目の概要】

脆弱性の種類と影響、攻撃手法の理解から始まり、OWASPトップ10などの主要なセキュリティ脅威に焦点を当てます。実習を通じて脆弱性診断ツールの使用方法や対策技術を仮想環境で実際に体験し、セッション管理、認証、認可、ログ出力、文字コードなどのセキュリティ関連トピックを掘り下げて学びます。

【到達目標】

A. 脆弱性の理由と発生について理解できる。
B. セキュリティバグとその対策について理解できる。
C. ウェブアプリケーションの脆弱性（XSS、SQLインジェクションなど）に関して理解できる。
D. セッション管理と認証・認可の仕組みについて理解できる。
E. Webサイトのセキュリティ対策と脆弱性診断の流れについて理解できる。

【授業の注意点】

ノートパソコンを必ず持参すること。毎回の授業は、前回までの授業の内容が身についていることを前提に行うため、必ず復習をすること。授業時間内に終わらなかった演習問題があった場合には、次の授業までに終わらせておくこと。特別な理由（路線の運休、法定伝染病など）のない遅刻や欠席は認められない。

評価基準＝ルーブリック

ルーブリック 評価	レベル５ 優れている	レベル４ よい	レベル３ ふつう	レベル2 あと少し	レベル１ 要努力
到達目標 A	脆弱性の理由と発生について理解・説明でき、活かすことができる。	脆弱性の理由と発生について理解でき、説明できる。	脆弱性の理由と発生について理解できる。	脆弱性の理由と発生について理解していない。	脆弱性の理由と発生について理解する姿勢がない。
到達目標 B	セキュリティバグとその対策について理解・説明でき、活かすことができる。	セキュリティバグとその対策について理解でき、説明できる。	セキュリティバグとその対策について理解できる。	セキュリティバグとその対策について理解していない。	セキュリティバグとその対策について理解する姿勢がない。
到達目標 C	ウェブアプリケーションの脆弱性（XSS、SQLインジェクションなど）に関して理解・説明でき、活かすことができる。	ウェブアプリケーションの脆弱性（XSS、SQLインジェクションなど）に関して理解でき、説明できる。	ウェブアプリケーションの脆弱性（XSS、SQLインジェクションなど）に関して理解できる。	ウェブアプリケーションの脆弱性（XSS、SQLインジェクションなど）に関して理解していない。	ウェブアプリケーションの脆弱性（XSS、SQLインジェクションなど）に関して理解する姿勢がない。
到達目標 D	セッション管理と認証・認可の仕組みについて理解・説明でき、活かすことができる。	セッション管理と認証・認可の仕組みについて理解でき、説明できる。	セッション管理と認証・認可の仕組みについて理解できる。	セッション管理と認証・認可の仕組みについて理解していない。	セッション管理と認証・認可の仕組みについて理解する姿勢がない。
到達目標 E	Webサイトのセキュリティ対策と脆弱性診断の流れについて理解・説明でき、活かすことができる。	Webサイトのセキュリティ対策と脆弱性診断の流れについて理解でき、説明できる。	Webサイトのセキュリティ対策と脆弱性診断の流れについて理解できる。	Webサイトのセキュリティ対策と脆弱性診断の流れについて理解していない。	Webサイトのセキュリティ対策と脆弱性診断の流れについて理解する姿勢がない。

【教科書】

安全なWebアプリケーションの作り方 第2版　（SBクリエイティブ）

【参考資料】

特になし

【成績の評価方法・評価基準】

積極的な授業態度、学習した知識を活用するパフォーマンス課題、小テスト等で総合的に評価する

※種別は講義、実習、演習のいずれかを記入。

科目名	セキュリティ応用	年度	2025
英語表記	Applied Security	学期	後期

回数	授業テーマ	各授業の目的		授業内容	到達目標＝修得するスキル	評価方法	自己評価
1	Webアプリケーションの脆弱性	Webアプリケーションの脆弱性とは何だろう？	1	脆弱性とは	脆弱性について理解できる	1	
			2	脆弱性が生まれる理由	脆弱性が生まれる理由について理解できる		
			3	セキュリティバグ	セキュリティバグについて理解できる		
2	実習環境のセットアップ	実習環境のセットアップを行おう	1	仮想マシンのインストール	仮想マシンのインストールの流れを理解できる	2	
			2	OWASP ZAPのインストール	OWASP ZAPのインストールの流れを理解できる		
			3	Firefoxの拡張インストール	Firefoxの拡張インストールの流れを理解できる		
3	Webセキュリティの基礎	Webセキュリティの基礎を理解しよう	1	HTTPとセッション管理	HTTPとセッション管理について理解できる	1	
			2	受動的攻撃と同一オリジンポリシー	受動的攻撃と同一オリジンポリシーについて理解できる		
			3	CORS (Cross-Origin Resource Sharing)	CORS (Cross-Origin Resource Sharing) について理解できる		
4	クロスサイト・スクリプティング	クロスサイト・スクリプティングについて理解しよう	1	機能と脆弱性の対応	機能と脆弱性の対応について理解できる	2	
			2	入力処理とセキュリティ	入力処理とセキュリティについて理解できる		
			3	クロスサイト・スクリプティング	クロスサイト・スクリプティングについて理解できる		
5	クロスサイト・リクエストフォージェリ	クロスサイト・リクエストフォージェリについて理解しよう	1	SQLインジェクション	SQLインジェクションについて理解できる	2	
			2	クロスサイト・リクエストフォージェリ	クロスサイト・リクエストフォージェリについて理解できる		
			3	クリックジャッキング	クリックジャッキングについて理解できる		
6	セッションIDの固定化	セッションIDの固定化について理解しよう	1	セッションハイジャックの原因と影響	セッションハイジャックの原因と影響について理解できる	2	
			2	URL埋め込みのセッションID	URL埋め込みのセッションIDについて理解できる		
			3	セッションIDの固定化	セッションIDの固定化について理解できる		
7	HTTPヘッダ・インジェクション	HTTPヘッダ・インジェクションなどについて理解しよう	1	オープンリダイレクト	オープンリダイレクトについて理解できる	2	
			2	HTTPヘッダ・インジェクション	HTTPヘッダ・インジェクションについて理解できる		
			3	リダイレクト処理の脆弱性	リダイレクト処理の脆弱性について理解できる		
8	クッキーのセキュア属性不備	クッキーのセキュア属性不備などについて理解しよう	1	クッキーの不適切な利用	クッキーの不適切な利用について理解できる	2	
			2	クッキーのセキュア属性不備	クッキーのセキュア属性不備について理解できる		
			3	メールヘッダ・インジェクション	メールヘッダ・インジェクションについて理解できる		
9	OSコマンド・インジェクション	OSコマンド・インジェクションなどについて理解しよう	1	ディレクトリ・トラバーサル	ディレクトリ・トラバーサルについて理解できる	2	
			2	OSコマンド・インジェクション	OSコマンド・インジェクションについて理解できる		
			3	ファイルアップロードの問題	ファイルアップロードの問題について理解できる		
10	ファイルインクルード攻撃	ファイルインクルード攻撃などについて理解しよう	1	ファイルインクルード攻撃	ファイルインクルード攻撃について理解できる	2	
			2	evalインジェクション	evalインジェクションについて理解できる		
			3	安全でないデシリアライゼーション	安全でないデシリアライゼーションについて理解できる		
11	JSONとJSONP	JSONとJSONPについて理解しよう	1	キャッシュに関する問題	キャッシュに関する問題について理解できる	2	
			2	JSONとJSONPの概要	JSONとJSONPの概要について理解できる		
			3	JSONエスケープの不備	JSONエスケープの不備について理解できる		
12	Web APIのクロスサイト・リクエストフォージェリ	Web APIのクロスサイト・リクエストフォージェリについて理解しよう	1	JSON直接閲覧によるXSS	JSON直接閲覧によるXSSについて理解できる	2	
			2	JSONPのコールバック関数名によるXSS	JSONPのコールバック関数名によるXSSについて理解できる		
			3	Web APIのクロスサイト・リクエストフォージェリ	Web APIのクロスサイト・リクエストフォージェリについて理解できる		
13	JavaScriptの問題	JavaScriptの問題について理解しよう	1	JavaScriptの問題	JavaScriptの問題について理解できる	2	
			2	認証	認証について理解できる		
			3	アカウント管理	アカウント管理について理解できる		
14	文字コードとセキュリティ	文字コードとセキュリティについて理解しよう	1	認可	認可について理解できる	2	
			2	ログ出力	ログ出力について理解できる		
			3	文字コードとセキュリティ	文字コードとセキュリティについて理解できる		
15	脆弱性診断の概要	脆弱性診断の概要について理解しよう	1	脆弱性診断の概要	脆弱性診断の概要について理解できる	2	
			2	Webサイトの安全性を高める対策	Webサイトの安全性を高める対策について理解できる		
			3	開発マネジメント	開発マネジメントについて理解できる		

評価方法：1.小テスト、2.パフォーマンス評価、3.その他

自己評価：S：とてもよくできた、A：よくできた、B：できた、C：少しできなかった、D：まったくできなかった

備考 等