

科目名	Webセキュリティ実習						年度	2025	
英語科目名	Web security practice						学期	後期	
学科・学年	ITスペシャリスト科 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	中西 真也		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】 本科目では、Webアプリケーションのセキュリティ上の脅威を習得することを目的として、Webアプリケーションの構築時に混在するセキュリティ上の脆弱性の知識を習得し、それら脆弱性の検出技術を学ぶ。									
【科目の概要】 使用予定教材の第4章の「機能別に見るセキュリティ」に沿って脆弱性を機能別に説明しつつ、昨今よく混入される脆弱性や実際に検出された非常に危険な脆弱性例などを捕捉しつつ、授業を進める。									
【到達目標】 さまざまな脅威に対抗する手段や事前にやるべきことを知る。普段使用している機器にどのような危険が含まれているのか、セキュリティ対策としてどのようなことをしておくべきなのか、作成したプログラムにどのような問題が起こる可能性があるかを学習する。さまざまな問題に対応できるように、過去に起こった実例を確認しながら、今後同じような問題が起こらないように対策を考え、実習で体験しながら、今後の実務に備えた知識を身に付ける。									
【授業の注意点】 座学でさまざまな脅威について学び、同時にノートパソコンに環境を作り、セキュリティ上の問題を実際に起こしながら、対応策を学習する。インターネット上でのセキュリティ対策不足は、大問題に繋がるのが想定できるため、それが起こらないように対応できる手段を実習を通して身に付ける。									
評価基準＝ルーブリック									
ルーブリック評価	レベル1 優れている	レベル2 ふつう	レベル3 要注意						
到達目標 A	セキュリティを調査できる環境がひとりで構築できる	セキュリティを調査できる環境が周りのサポートがあれば構築できる	セキュリティを調査できる環境が構築できない						
到達目標 B	セキュリティの調査がひとりでできる	セキュリティの調査が周りのサポートがあればできる	セキュリティの調査ができない						
到達目標 C	セキュリティの調査結果を詳細に報告できる	セキュリティの調査結果を報告できる	セキュリティの調査結果を報告できない						
【教科書】 『安全なWebアプリケーションの作り方 第2版』（徳丸 浩、SBクリエイティブ）									
【参考資料】									
【成績の評価方法・評価基準】 課題、レポート、平常点									

※種別は講義、実習、演習のいずれかを記入。

科目名		Webセキュリティ実習			年度	2025
英語表記		Web security practice			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	イントロダクション	本講座の概要を理解する	1	講座の概要	Webセキュリティの脆弱性に関する検出動向と対策を理解している	3
			2			
			3			
2	環境構築	環境を構築する	1	環境構築	基礎となるWeb技術が理解できている 実習環境の構築に関する説明を理解している	2
			2			
			3			
3	基本操作	基本操作を理解する	1	基本操作	実習環境が構築できる 診断用スキャナ（OWASP ZAP）の基本的な操作ができる	2
			2			
			3			
4	入力値検証	入力値検証を理解する	1	入力値検証	入力値検証を理解している	2
			2			
			3			
5	表示処理	表示処理を理解する	1	表示処理	表示処理に伴う問題を理解している	2
			2			
			3			
6	SQL呼び出し	SQL呼び出しを理解する	1	SQL呼び出し	SQL呼び出しに伴う問題を理解している	2
			2			
			3			
7	CSRFとクリックジャッキング	CSRFとクリックジャッキングを理解する	1	CSRFとクリックジャッキング	CSRFとクリックジャッキングを理解している	2
			2			
			3			
8	セッション管理	セッション管理を理解する	1	セッション管理	セッション管理の不備を理解している	2
			2			
			3			
9	リダイレクト処理	リダイレクト処理を理解する	1	リダイレクト処理	リダイレクト処理にまつわる脆弱性を理解している	2
			2			
			3			
10	クッキー出力	クッキー出力を理解する	1	クッキー出力	クッキー出力にまつわる脆弱性を理解している	2
			2			
			3			
11	メール送信	メール送信を理解する	1	メール送信	メール送信の問題を理解している	2
			2			
			3			
12	ファイルアクセス	ファイルアクセスを理解する	1	ファイルアクセス	ファイルアクセスの問題を理解している	2
			2			
			3			
13	OSコマンド・インジェクション	OSコマンド・インジェクションを理解する	1	OSコマンド・インジェクション	OSコマンド・インジェクションを理解している	2
			2			
			3			
14	ファイルアップロード	ファイルアップロードを理解する	1	ファイルアップロード	ファイルアップロードにまつわる問題を理解している	2
			2			
			3			

15	まとめ	知識を定着させる	1	まとめ	これまで学習してきた内容を思い起こすことができる	2
			2			
			3			
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						