Security Campus e-Learning
エッセンシャルコースご紹介

EGセキュアソリューションズ株式会社
2023/7

Security Campus e-Learningとは

ウェブセキュリティの先駆者かつ現役最前線の徳丸浩が提供/監修する、
EGセキュアソリューションズのサイバーセキュリティe-ラーニングサービスです。

〇3つの特長

**本質的かつセキュリティベンダならでは
の最新トレンドを組み込んだ講習内容。**

**演習環境を利用した実践形式なので
知識だけでなくスキルの習得につながる。**

**短い動画に分割しているため、
すきま時間で繰り返し学習できる。**

第1弾として「エッセンシャルコース」をリリースしております。

エッセンシャルコースご紹介

「ウェブアプリケーションの脆弱性」、「ウェブサイトへの攻撃経路」、といったウェブセキュリティの基礎となる内容をまとめたコースです。すべてのエンジニアと、これからエンジニアを目指す方々へおススメです。

○学習方法	○前提知識	○動画時間/標準学習時間
座学 ※BadTodoを使用したセルフハンズオン有り。	不要ですが、以下の知識を事前に身に着けておくと学習効果が高まることを期待できます。 ・Webサーバとクライアントの概念 ・HTML、JavaScriptの基本	動画時間：2.5時間 標準学習時間：5時間

○カリキュラム

1.導入 総論 基礎 ・はじめに ・導入 ・脆弱性を巡る用語や基準 ・ウェブセキュリティの基礎 ・認証 ・セッション管理 ・HTTPSの利用	2.アプリケーション脆弱性 ・SQLインジェクション ・XSS ・CSRF ・アップロードの問題 ・セキュリティの設定ミス ・コンポーネントやプラットフォームの脆弱性	3.認証・認可 ・認証の強化 ・パスワードの保護 ・認可 ※すきま時間で、繰り返し学習できるよう数分の小単元ごとの動画に分かれております。（総数99の動画） ※各部毎にテキスト、確認テストあり。 ※法人で複数人でのご契約の際は学習状況管理システムもご提供いたします。

エッセンシャルコースで身につくこと

01 **ウェブサイト（アプリ）構築に携わる方として、最低限必要なセキュリティの知識が身につきます**

02 脆弱性診断等で指摘が多く、
旦つ危険な脆弱性についての知識を得られます

03 OWASP Top 10 2021等における
上位項目の基本的な内容を理解できます

04 以下のような事象を避けることができます

- SQLインジェクションXSSなどの基礎的な概念や対策法を知らない
- パスワードを平文で保存してしまう
- id=tanakaをid=yamadaに変えたら山田さんの情報が見えた
- 同時にPDFファイルを生成したらファイル名が衝突した

エッセンシャルコース 講師からのご紹介動画

導入までの流れと価格

○導入までの流れ(法人のお客様)

1. 以下URLよりお申込み
   https://www.security-campus.com/entry-corp
2. ヒアリングシートを送付、記載の上ご返送いただく
3. 御見積ご提示/ご契約
4. ご利用開始

○価格

・エッセンシャルコース　定価30,000円/1ユーザー

※リリース特別価格にて24,000円/1ユーザーにてご提供中

※法人のお客様でまとめてのお申し込み時には人数に応じて別途御見積いたします。

参考：安全なウェブサイトの作り方 第7版 準拠状況

1.1	SQL インジェクション	◎ 準拠
1.2	OS コマンド・インジェクション	× 本脆弱性への攻撃は他と比較し少ないため本コースでは省略
1.3	ディレクトリ・トラバーサル	× 本脆弱性への攻撃は他と比較し少ないため本コースでは省略
1.4	セッション管理の不備	◎ 準拠
1.5	クロスサイト・スクリプティング	◎ 準拠
1.6	CSRF（クロスサイト・リクエスト・フォージェリ）	◎ 準拠
1.7	HTTP ヘッダ・インジェクション	× 本脆弱性への攻撃は他と比較し少ないため本コースでは省略
1.8	メールヘッダ・インジェクション	× 本脆弱性への攻撃は他と比較し少ないため本コースでは省略
1.9	クリックジャッキング	△ X-Frame-Optionsヘッダの説明はあり
1.10	バッファオーバーフロー	△ コンポーネントの脆弱性として
1.11	アクセス制御や認可制御の欠落	◎ 準拠

参考：OWASP Top 10 2021 準拠状況

A01	アクセス制御の不備	認可制御の不備、強制ブラウジング、ディレクトリトラバーサル、CSRF
A02	暗号化の失敗	SSLの利用、SSL (TLS) の設定、HSTS、パスワードの平文保存
A03	インジェクション	SQLi、 XSS、OSコマンドインジェクション、 HTTP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
A04	安全が確認されない不安な設計	アップロードの不備(CWE-434)、エラーメッセージからの情報漏洩(CWE-209)
A05	セキュリティの設定ミス	クッキーへの機密情報の保存(CWE-315)、クッキーのセキュア属性不備(CWE-614)、HttpOnly属性不備(CWE-1004)、セキュリティヘッダの不備
A06	脆弱で古くなったコンポーネント	プラットフォームの問題
A07	識別と認証の失敗	パスワード認証の保護、URL埋め込みのセッションID、セッションIDの固定化、認証回避の脆弱性
A08	ソフトウェアとデータの整合性の不具合	マスアサインメント脆弱性(CWE-915)、安全でないデシリアライゼーション(CWE-502)
A09	セキュリティログとモニタリングの失敗	ログ管理、ログからの情報漏洩(CWE-532)
A10	サーバーサイドリクエストフォージェリ	SSRF(CWE-918)

※赤文字＝準拠