SecHack365

セキュリティの学習をもっと簡単に

SEC-CUBE

学習駆動コース 社会実装ゼミ 石田優希

SEC-CUBEとは

SEC-CUBEとは**面倒な環境構築なしで始めることのできるセキュリティ学習アプリケーション**です。
SEC-CUBEでは学習に必要な機能やツールはすべてアプリケーション側からブラウザ経由で提供されます。

セキュリティ学習の問題点とSEC-CUBEで解決する方法

1. 環境構築が大変

バージョンの違いや端末による差異などが関係し、学習に必要な環境構築がスムーズに完了せず挫折してしまう

Webブラウザさえあれば学習を始められるように学習環境を用意

2. 周辺知識の取得が難しい

セキュリティの学習は事前知識などが多く必要となるが、どういった知識が必要なのか明示されていないことが多く、取得が難しい

必要な事前知識もアプリ内で学習できるようにし、必要な内容も明示する

3. 解説が無い、または少ない

既存の学習サイトやCTFなどでは公式による解説が少なかったり、無かったりするため正しい理解などが得られない場合がある

SEC-CUBEではわかりやすい解説を多く設けて、それを見ながら学習する

SEC-CUBEでの学習手順

1. サイトにアクセスし、学習したい項目を選択

2. コースで学ぶ内容などを学ぶ。準備ができたら環境構築ボタンをクリックし、環境を起動する

3. 学習を行うページでは左側の説明を見つつ、右のパネルを用いてマシンやデータベースなどに攻撃を行ったりして学習する

4. 答えとなるキーワードを獲得できたら回答ボックスから入力

特徴

ボタンを押してから学習環境の構築にかかる時間はおよそ**3秒程度**

右側のパネルには**エディタ**や**Webサイトの埋め込み**などがあり、演習によって様々なものが利用できる

```
<!DOCTYPE html>
<html lang="ja">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" c
    <meta name="viewport" content="width
    <link rel="stylesheet" href="style.c
    <title>ログインフォーム</title>
</head>
<body>
<?php

$dsn = 'mysql:dbname=db;host=db';
$user = 'user';
$password = 'password';

//ログイン認証
if (isset($_POST['name']) && isset($_POS
```

SEC-CUBE本体もDockerコンテナで動作するため、Docker環境さえあればセルフホストも可能

セルフホストできます！！

SEC-CUBEの技術構成

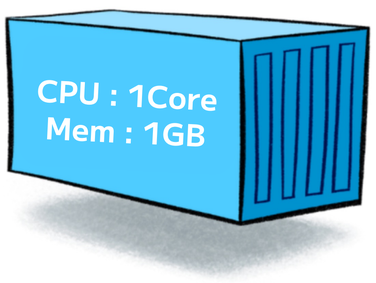
動的ルーティングやSSRなどが必要となるためフロントは**TypeScript**と**Next.js**を採用し、バックエンドはスピードを意識して**Go**を採用している。
バックエンドは学習環境とフロントの通信を中継することを行っている。

基本的に多く機能は永続的な通信を必要としないため、フロント側でAPIを利用する形で実装を行っているが、永続的な通信が必要な場合は**gorilla/websocket**を用いてソケット通信を行うことで対応している。

セキュリティ対策について

環境で利用できるCPUやメモリの量を制限

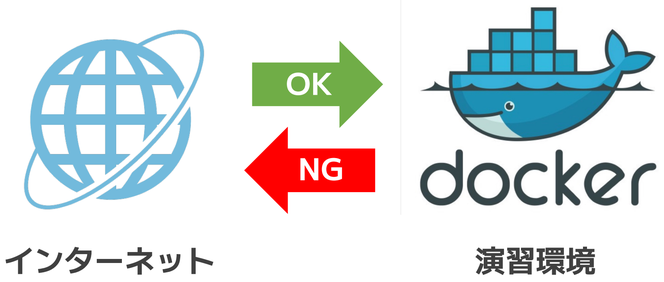
サーバーのリソースを悪用されたり、forkなどでプロセスを増殖されてサービスが停止するのを抑制



また、学習環境を大量に構築されないように、ユーザーごとに構築できる環境の数の制限を設ける予定

外向きの通信を遮断

学習環境を外部サービスへの攻撃やDoS攻撃などの踏み台として悪用されることを抑制



学習環境を一定時間で廃棄

学習環境を悪用して、不正なプログラムを長期に渡り実行されないように、利用された学習環境は一定時間で必ず削除されます

削除されるまでの時間は、コースをクリアするために十分な時間として設定しています
削除されるまでの時間をコースクリアまでの残り時間として表示できるように今後実装していきたい

NICT National Institute of Information and Communications Technology