対象者：セキュリティ初学者
サーバサイド経験者

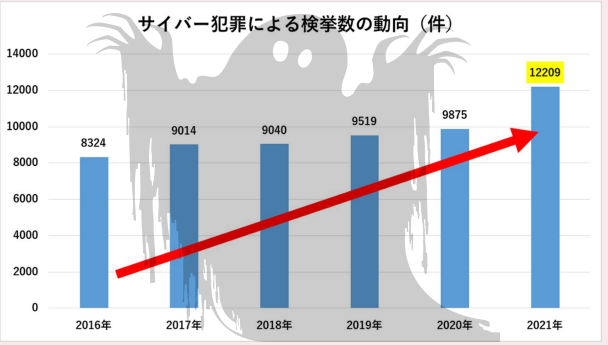
課題部門 登録番号:10020

はじめに

日本がサイバー攻撃の危機に晒されていることを知っていますか？

近年、日本に対する**サイバー攻撃**が急増し、個人情報や企業秘密の漏洩、システムのダウンなど、深刻な被害が報告されています

さらに、サイバー攻撃は**ビジネス化**され、
金銭目的であらゆる機関が狙われるようになったことで**脅威は身近まで迫っています**



サイバー攻撃を防ぐには**セキュリティの知識**を持ったエンジニアが必要です

しかし、既存のセキュリティ学習が持つ**3つの問題**が原因となり、
セキュリティの知識を持ったエンジニアが少ない現状が続いています

- **退屈**：座学ばかりでつまらない、実践的な教材が少ない
- **孤独**：基本的に1人で学習するものが多くモチベが維持できない
- **不安**：攻撃を学ぶ必要があるが、試すと犯罪になりそうで怖い

セキュリティ学習は初学者にとってハードルが高い！

システムの目的

そこで、私たちは新しいセキュリティ学習プラットフォーム

CYBER WARSを提案します！

システムのコンセプト

① セキュリティ分野における最適な学習法に基づいた学習プラットフォーム

最適な学習法：**攻撃して脆弱性について知る** ➡ **脆弱性の防御方法を学ぶ**

② 1vs1の**対戦形式**を取り入れた新しいセキュリティ教材

③ 初学者にも馴染みが深く学習しやすい、**Webサイト**のセキュリティを対象

➡ セキュリティを学び始めた人にとっての大きな**ハードル**を解決！

- **退屈**：座学ばかりでつまらない ➡ 実践形式で楽しく学べる
- **孤独**：1人だとモチベを保てない ➡ 競い合ってモチベを向上
- **不安**：攻撃を試すと犯罪になりそう ➡ 安心して攻撃を試せる

セキュリティ初学者の学びの入り口となるシステムを提供することで
セキュリティの知識を持ったエンジニアを増やします！

システム概要

脆弱性のあるWebサイトを舞台に、プレイヤー同士の攻防を通して
セキュリティ知識を身に付ける学習プラットフォームです

訓練モード >>> 対戦モード

ゲームの進め方・操作方法・
ルールを解説するモードです

簡単な**攻撃方法**と
脆弱性の**修正方法**を学び
対戦に向けて**訓練**できる！

1対1で3つのフェーズを通して対戦し、合計ポイントを競います

アタックフェーズ

プレイヤーはお互いに同じ**課題Webサイト**を**攻撃**し、
取得できた情報の量を**ポイント**として競います

ディフェンスフェーズ

アタックフェーズで攻撃した課題Webサイトの
脆弱性を修正し、次の相手からの**攻撃に備えます**

バトルフェーズ

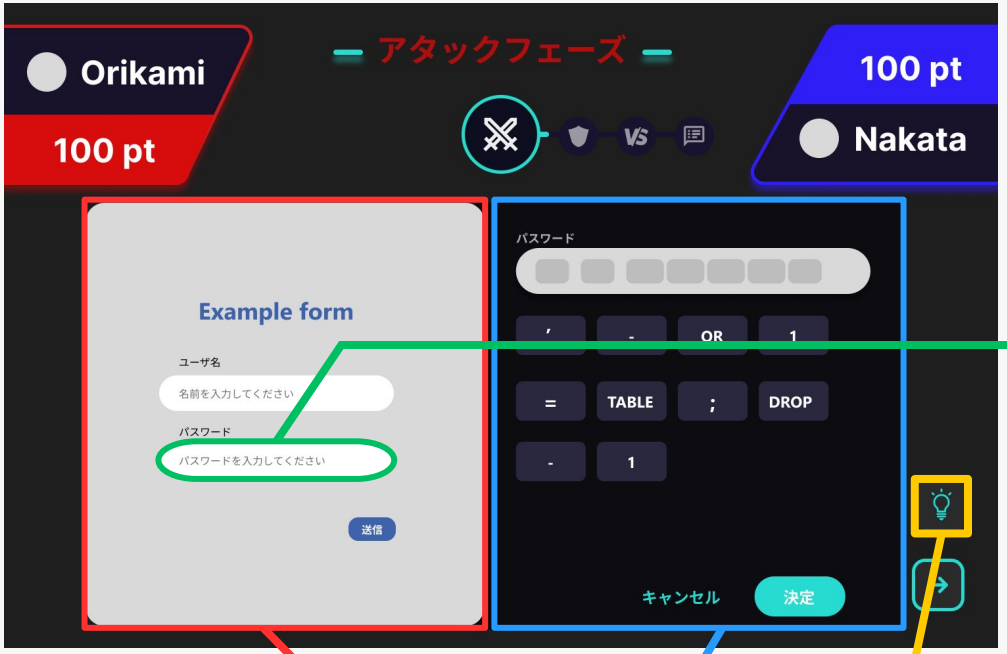
相手が修正した課題Webサイトを**攻撃**します
修正が行き届いてないところを見つけて攻撃しよう！

解説モード

自分では気づけなかった**脆弱性を確認**できます

対戦モード:アタックフェーズ

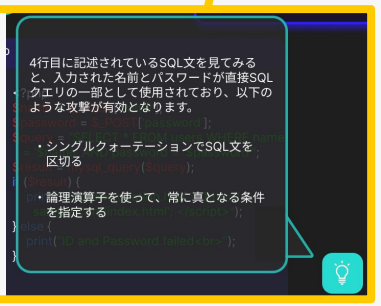
訓練モードで学んだ知識を活かして、**課題Webサイト**を攻撃しよう
選択肢を頼りに**脆弱性**を探してみよう！



課題Webサイトと**攻撃の選択肢**

入力フォームにカーソルを合わせると
攻撃の選択肢が開くので、並べ替えて**攻撃！**

ポイントを使って
ヒントを見ることも可能！



対戦モード:ディフェンスフェーズ

アタックフェーズで気づいた課題Webサイトの**脆弱性**を直接コーディングして**修正**しよう

より多くの脆弱性を修正し
バトルフェーズに備えよう！

脆弱性を含んだソースコード

SQLインジェクション攻撃ができてしまう**脆弱性**がある！

```
3 $password = $_POST['password'];
```

エスケープ処理で脆弱性を修正！

課題Webサイトの元の機能が
壊れていないかどうかは自動でチェック！

```
3 $password = escapeshellcmd($_POST['password']);
```

対戦モード:バトルフェーズ

ディフェンスフェーズで相手が改善した
課題Webサイトに攻撃を仕掛けよう！

相手が改善した**課題Webサイト**の**脆弱性**を
見つけ出せるかが勝敗を左右する！

ディフェンスフェーズで相手が改善したコード

解説モード

課題Webサイトに潜む**脆弱性**、**攻撃例**、
防御例を解説

自身では気づけなかった脆弱性を知る
ことで、**セキュリティの知識**、**対処能力**
を更に養うことができる

実現方法

ChatGPTによる課題Webサイトの自動生成

SQLインジェクションの脆弱性を持った
ログインページを作成してください。

PHP

```php
$username = $_POST["username"];
$password = $_POST["password"];

$sql = "SELECT * FROM users WHERE username = '$username' AND password = '$password'";

$result = mysqli_query($conn, $sql);
```

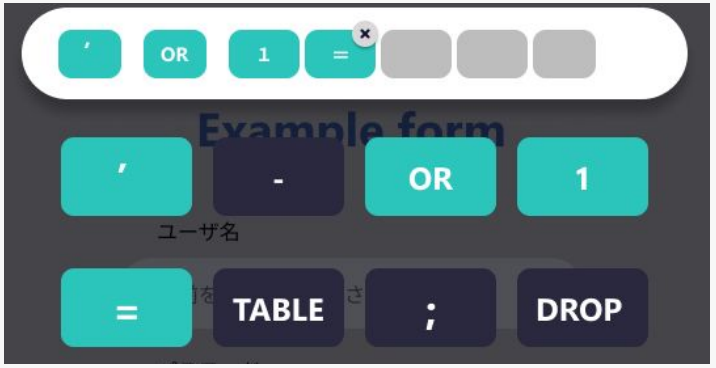
SQLインジェクションの脆弱性を持っている！

脆弱性に対する
攻撃例を生成

攻撃例

command

```
' OR 1 = 1 --
```



実現方法

実際にChatGPTを用いて
課題Webサイトの生成を検証！

ChatGPTに生成させるデータ

- HTML, CSS(フロントエンド)
- PHP(バックエンド)
- データベースのテーブル構成

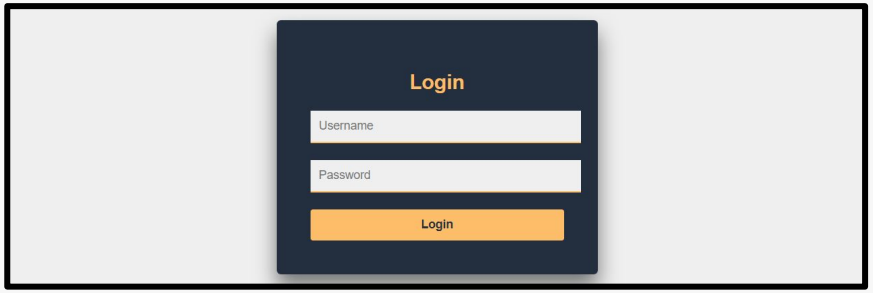
脆弱性の種類、Webサイトの種類、Webサイトのデザインを組み合わせることで
多種多様な課題Webサイトを生成します

```
<h2>Login</h2>
<form action="<?php echo htmlspecialcha
    <div class="textbox">
        <input type="text" name="userna
    </div>
    <div class="textbox">
        <input type="password" name="pa
    </div>
    <p><?php echo $error; ?></p>
    <input type="submit" class="btn" va
</form>
```

```
$sql = "SELECT user_id, username, password FROM users WH
$result = $conn->query($sql);

if ($result->num_rows == 1) {
    $row = $result->fetch_assoc();
    $_SESSION["loggedin"] = true;
    $_SESSION["user_id"] = $row["user_id"];
    $_SESSION["username"] = $row["username"];
} else {
    $error = "Invalid login credentials. Try again.";
}
```

課題Webサイト生成



ログインページ

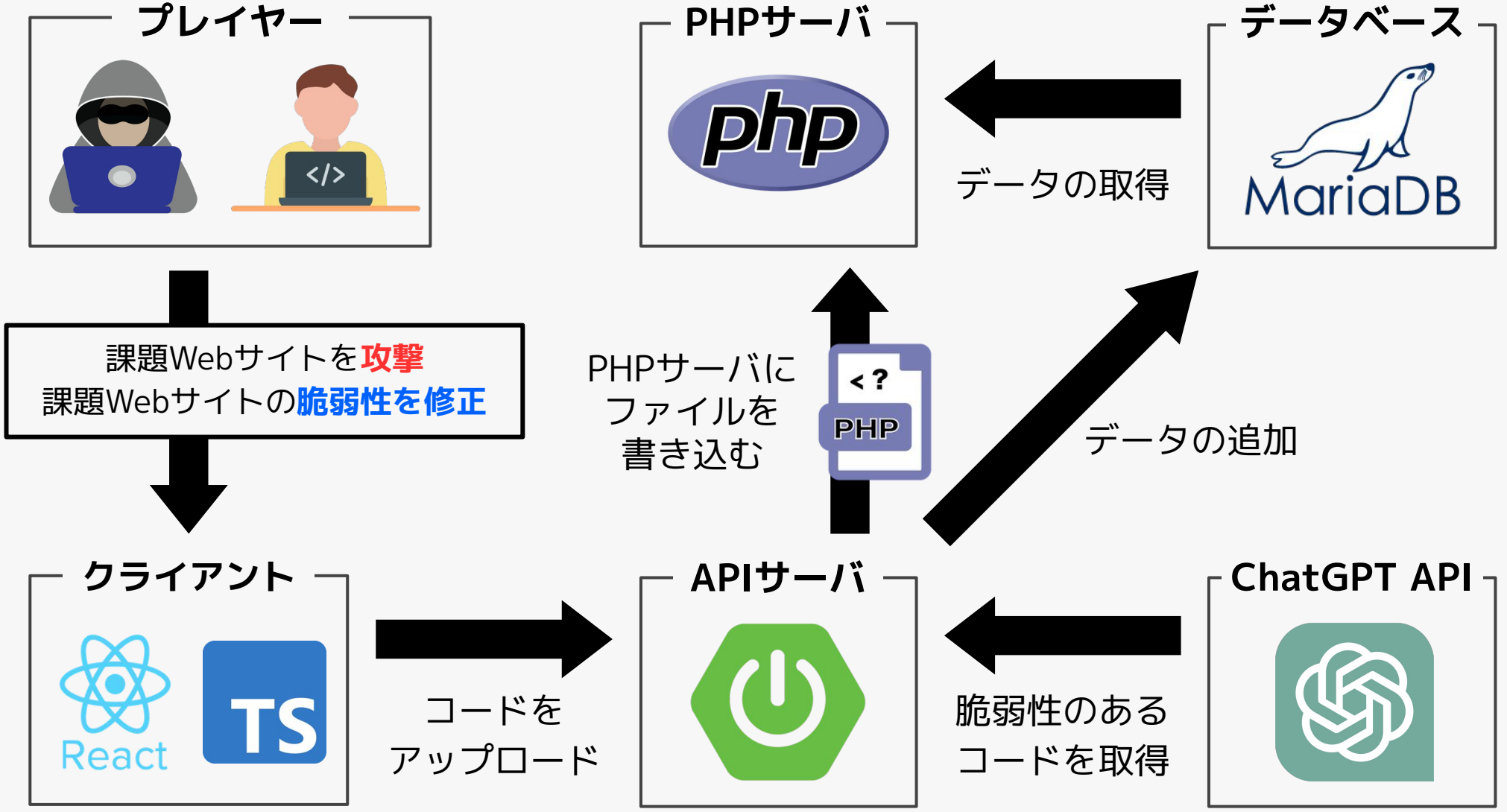
脆弱性の候補

- SQLインジェクション
  - クォート回避
  - コメント化
  - UNION構文による結合
  - オペレーター改変
- OSコマンドインジェクション
  - シェルメタ文字による連結

etc.

⚠ 学んだことを悪用しないように、システム内で十分に注意を促します

システム構成


プレイヤー
PHPサーバ
データベース
データの取得
MariaDB
課題Webサイトを攻撃
課題Webサイトの脆弱性を修正
PHPサーバに
ファイルを
書き込む
データの追加
クライアント
APIサーバ
ChatGPT API
React
TS
コードを
アップロード
脆弱性のある
コードを取得

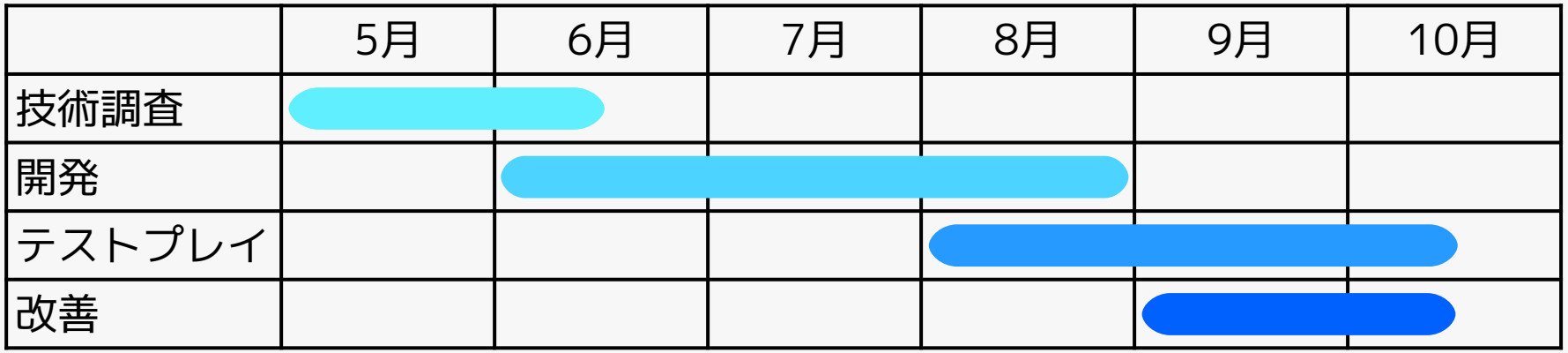
特許調査・開発スケジュール・開発環境

特許調査

・特開2014-021959：情報セキュリティゲームシステム

防御の有無、マルチプレイによる攻防戦の有無、課題となる
Webサイトのコードの生成方法において、本システムとは異なる

開発スケジュール



開発環境

開発OS
Windows 11, Ubuntu

開発言語
TypeScript, Java

使用ユーティリティ・ライブラリ
React, Spring Boot, ChatGPT API

実行環境
Chrome(PC)

類似品・まとめ

類似品

	実践性	ハードルの低さ	対戦要素	問題数の多さ
本システム	○	○	○	○
書籍	×	△	×	△
Paiza	△	○	×	△
(SECCON)	○	×	○	△

※本システムはセキュリティ学習の入門であり、上級者向けのコンテストであるSECCONと競合しているわけではない

まとめ

・訓練モードやヒント機能、選択式の攻撃により**初学者**でも**遊びやすい**
・対戦モードにより友達と**モチベーションを高め合い**ながら**学ぶことができる**
・このシステムで初学者を卒業し、上級者向けの教材やコンテストに挑戦しよう！

セキュリティを学び始めるための**入り口**として最適！
対戦型という要素を取り入れた新しいオンライン学習システムで
セキュリティの楽しさを体感しよう！