OWASP Top 10 演習教材（初心者向け）

目的：Webアプリケーションの主要な脆弱性を理解し、防御策を学ぶための演習問題集。

構成：10問 ／ 難易度：★＝初級、★★＝中級、★★★＝上級

※本教材は学習・防御目的であり、攻撃手法を助長するものではない。

目次

問題 1：アクセス制御の不備 （難易度：★）

【シナリオ】

一般ユーザーが管理者用ページ「/admin」に直接アクセスできてしまう。

【問題】

なぜ問題なのか。どのような設計ミス・実装ミスが考えられるか。

【ヒント】

・認証と認可の違いを確認する

・アクセス制御をどこで行っているか考える

【解説】

アクセス制御の不備は、サーバ側で権限チェックをしていないことが原因である。表示制御のみでは不十分。対策として、サーバ側で権限検査を行い、最小権限原則を徹底する。

問題 2：暗号化の不備 （難易度：★）

【シナリオ】

パスワードをbase64エンコードで保存している。

【問題】

なぜ安全でないのか。正しい保存方法は何か。

【ヒント】

・可逆なエンコードと非可逆なハッシュの違いを理解する

【解説】

base64は暗号化ではなく単なるエンコードである。安全な保管にはbcryptやArgon2などのハッシュ関数を使用し、ソルトを付与して保存する。

問題 3：インジェクション（難易度：★★）

【シナリオ】

ユーザー入力をSQL文に直接結合して実行している。

【問題】

この実装の危険性と防御策を説明せよ。

【ヒント】

・入力を信頼しない

・SQL発行方法を確認する

【解説】

文字列結合でSQLを生成すると、意図しない命令を実行される危険がある。プリペアドステートメントを使用し、入力値を検証することが必要である。

問題 4：安全でない設計 （難易度：★★）

【シナリオ】

ログイン試行回数に制限がなく、エラーメッセージに内部情報を含んでいる。

【問題】

設計段階で考慮すべきセキュリティ要件は何か。

【ヒント】

・エラーメッセージの扱いを考える

・レート制限を設計段階で入れる

【解説】

設計時に脅威モデリングを行い、ブルートフォース防止のための試行制限や汎用的なエラーメッセージを設計に含める。

問題 5：設定ミス （難易度：★）

【シナリオ】

本番環境でデバッグモードが有効になっている。

【問題】

設定ミスで起こるリスクと対策を挙げよ。

【ヒント】

・環境設定を明確に分ける

・公開ディレクトリを最小限にする

【解説】

デバッグモードでは内部情報が表示される危険がある。本番環境では必ず無効にし、不要な機能を削除する。構成管理を自動化して定期的に点検する。

問題 6：脆弱・古いコンポーネント （難易度：★★）

【シナリオ】

古いライブラリを使用しており、脆弱性の報告がある。

【問題】

どのように対応すべきか。

【ヒント】

・依存関係を可視化する

・脆弱性情報を確認する

【解説】

使用中のライブラリのバージョンを定期的に確認し、脆弱性がある場合は早期にアップデートする。自動スキャンやSBOMの活用も有効である。

問題 7：認証・識別の不備 （難易度：★★）

【シナリオ】

パスワードリセットURLが推測可能な形式で発行されている。

【問題】

安全なリセットフローを説明せよ。

【ヒント】

・トークンをランダムに生成する

・有効期限を短くする

【解説】

パスワードリセットリンクには推測困難な一時トークンを使用し、短時間で失効させる。必要に応じて多要素認証を利用する。

問題 8：ソフトウェア／データ整合性の失敗 （難易度：★★★）

【シナリオ】

外部ライブラリを署名検証なしで取り込んでいる。

【問題】

このリスクと対策を説明せよ。

【ヒント】

・署名やハッシュを利用する

・信頼できる配布元を使用する

【解説】

外部ライブラリの改ざんにより不正コードが混入する危険がある。署名やハッシュ値を検証し、信頼できるソースからのみ取得する。

問題 9：ログ・監視の不備 （難易度：★★）

【シナリオ】

認証失敗や権限エラーの記録が残っていない。

【問題】

なぜ問題なのか。対策を挙げよ。

【ヒント】

・重要な操作はすべて記録する

・ログの保全と監視を考える

【解説】

不正アクセスを検知できず、原因分析も困難になる。重要な操作を記録し、集中管理・監視を行う。改ざん防止の仕組みも必要である。

問題 10：SSRF（サーバーサイドリクエストフォージェリ）（難易度：★★★）

【シナリオ】

ユーザー指定のURLをサーバー側で取得している。

【問題】

どのような攻撃が起こりうるか。対策を挙げよ。

【ヒント】

・内部ネットワークへのリクエストを防ぐ

・入力値を制限する

【解説】

SSRFにより内部ネットワークやメタデータサービスにアクセスされる可能性がある。ホワイトリスト方式のURL検証やアクセス制限を行う。

参考資料

・OWASP Top Ten 公式サイト：https://owasp.org/
・OWASP Cheat Sheet Series：対策の詳細解説集
・IPA 安全なウェブサイトの作り方
・依存関係管理とSBOMの活用