

■学習テーマ一覧

表 1. AppGoat ウェブアプリケーション学習版 学習テーマ一覧

No.	脆弱性タイプ	学習テーマ名
1	クロスサイト・スクリプティング	クロスサイト・スクリプティングとは
2		アンケートページの改ざん（反射型）
3		掲示板に埋め込まれるスクリプト（格納型）
4		入力情報の漏えい（反射型）
5		ウェブページの改ざん（DOM ベース）
6		不完全な対策
7	SQL インジェクション	SQL インジェクションとは
8		不正なログイン（文字列リテラル）
9		情報漏えい（数値リテラル）
10		他テーブル情報の漏えい（数値リテラル）
11		データベースの改ざん（数値リテラル）
12	CSRF （クロスサイト・リクエスト・フォージェリ）	CSRF(クロスサイト・リクエスト・フォージェリ)とは
13		意図しない命令の実行
14		不完全な対策
15	OS コマンド・インジェクション	OS コマンド・インジェクションとは
16		システム情報の漏えい
17	ディレクトリ・トラバーサル	ディレクトリ・トラバーサルとは
18		ファイル情報の漏えい
19	HTTP ヘッダ・インジェクション	HTTP ヘッダ・インジェクションとは
20		Cookie 値の変更
21	認証制御や認可制御の欠落	認証制御や認可制御の欠落とは
22		認証不備によるページの参照
23		認可制御不備によるページの参照
24	セッション管理の不備	セッション管理の不備とは
25		セッション ID の漏えい
26		セッション ID の固定化
27		セッション ID の推測
28	その他	エラーメッセージからの情報漏えい

※網掛け部分：今回追加した学習テーマ

脆弱性修正演習イメージ

利用者は、ソースコードを見て脆弱性の要因となっている問題箇所を発見し、修正します。もし脆弱性の発見や修正方法が分からない場合は、ヒントを参照しながら、演習を進めます。ソースコード修正後、演習環境で動作確認を行い、修正方法が適切だったかどうかをチェックします。

- + セッション管理の不備
- + その他
- + 脆弱性検査

Hint

netshopping.php
netshopping117.class.php

脆弱性の修正

修正対象ファイル "netshopping117.class.php"

```

} else if (!isset($newname) || ($newname == "")) {
    $this->set_content(parent::WARNING10, true);
    // 変更前と変更後のファイル名が同じ場合
} else if ($oldname == $newname) {
    $this->set_content(parent::WARNING11, true);
    // 変更前と変更後のファイル名が異なる場合
} else {
    // 変更前ファイル名をパス付きで指定
    $oldname = parent::GOODS_FILE_PATH. basename($oldname);

    // 変更前ファイルが存在する場合
    if (is_file($oldname)) {
        // ファイル名を変更するコマンド実行
        $result = system("rename . $oldname . $newname");

        // ファイル名変更に成功
        if ($this->is_rename()) {
            $this->set_content(parent::WARNING12, true);
        }
    }
}
                    
```

修正対象ファイル "netshopping117.class.php"

```

} else if (!isset($newname) || ($newname == "")) {
    $this->set_content(parent::WARNING10, true);
    // 変更前と変更後のファイル名が同じ場合
} else if ($oldname == $newname) {
    $this->set_content(parent::WARNING11, true);
    // 変更前と変更後のファイル名が異なる場合
} else {
    // 変更前ファイル名をパス付きで指定
    $oldname = parent::GOODS_FILE_PATH. basename($oldname);

    // 変更前ファイルが存在する場合
    if (is_file($oldname)) {
        // ファイル名を変更するコマンド実行
        $newname = parent::GOODS_FILE_PATH. $newname;
        $result = rename($oldname, $newname);

        // ファイル名変更に成功
        if ($this->is_rename()) {
            $this->set_content(parent::WARNING12, true);
        }
        // ファイル名変更に失敗
        } else {
            $this->set_content(parent::WARNING13, true);
        }
    }

    // 攻撃成功判定
    $this->is_success($result);
    // 変更前ファイルが存在しない場合
} else {
                    
```

ネットショッピングサイト
最初のページに戻る

URL: <http://localhost/Web/Scenario117/EditSoft/netshopping.php?page=16&token=6a> GO

履歴
ログアウト

OnlineStore

商品管理

- 商品一覧
- 家電
- パソコン

ファイル名変更に失敗しました。

商品のアクセスランキングの出力ファイル名を変更します。

変更前ファイル名: test.txt
▼

変更後ファイル名:
ファイル名変更

商品番号	商品名	商品種別	税込価格
1000015	キーボード	old	1,800円

脆弱性の修正
にチャレンジ

脆弱なコードを
発見・修正!

修正したウェブアプリ
ケーションの動作確認

■脆弱性検査演習のイメージ

脆弱性検査演習では、演習環境にランダムに埋め込まれた脆弱性に対して、各入力フィールドに検査用コードを投入しながら、脆弱性の有無を確認します。演習環境に内在している全ての脆弱性が発見できると、演習は終了します。

チャレンジ

【脆弱なネットショッピングサイトアプリケーション】を想定した脆弱性発見の総合演習です。各テーマで学習した脆弱性の発見手法を基に、内在する脆弱性を発見しましょう。脆弱性は全部で以下の6種類あります。

- セッション管理の不備
- ディレクトリトラバーサル
- HTTPヘッダ・インジェクション
- 認証制御や認可制御の欠落
- SQLインジェクション
- 認証制御や認可制御の欠落

内在している脆弱性
一覧

Hint

脆弱ネットショッピング セッション不備の演習問題 最初のページに戻る

URL http://localhost/Web/Scenario130/VulSoft/netshopping.php

OnlineStore

ログイン

商品一覧
家電
パソコン
AV機器
サプライ

ログインIDとパスワードを入力し「ログイン」ボタンを押してください。

ログインID
パスワード

ログイン クリア

複数の脆弱性を発見!

検査演習結果

検査演習の結果を確認してみましょう。

次のページで検査方法の解説を行います。

検査結果を確認

検査演習結果

6件中2件の脆弱性の攻撃に成功しました。
以下の脆弱性を発見しました。

- ディレクトリトラバーサル
- SQLインジェクション

検査演習の初期化を行う場合は初期化ボタンを押してください。

初期化