別紙

■学習テーマ一覧

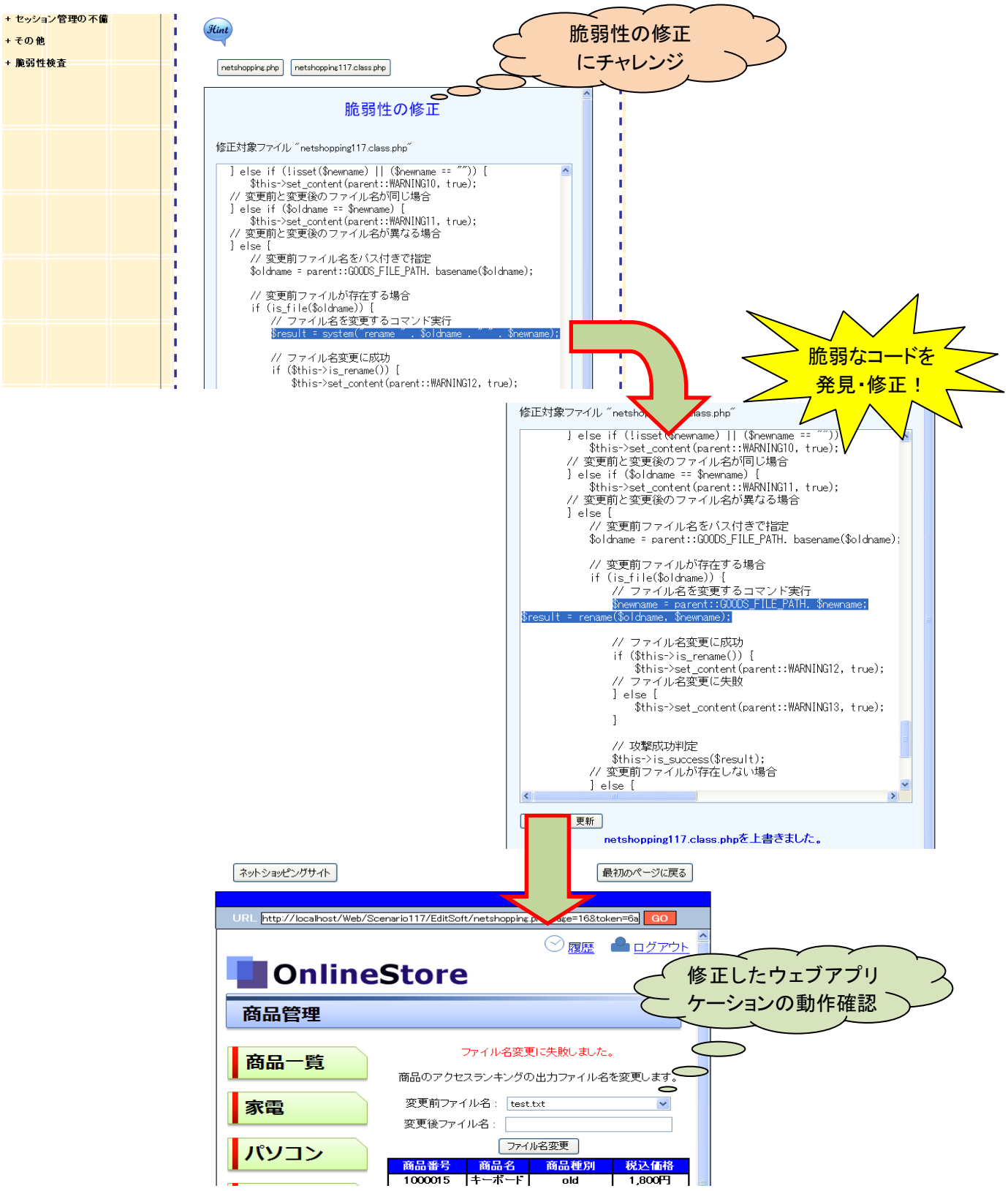
表 1．AppGoat ウェブアプリケーション学習版 学習テーマ一覧

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。



■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。

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。