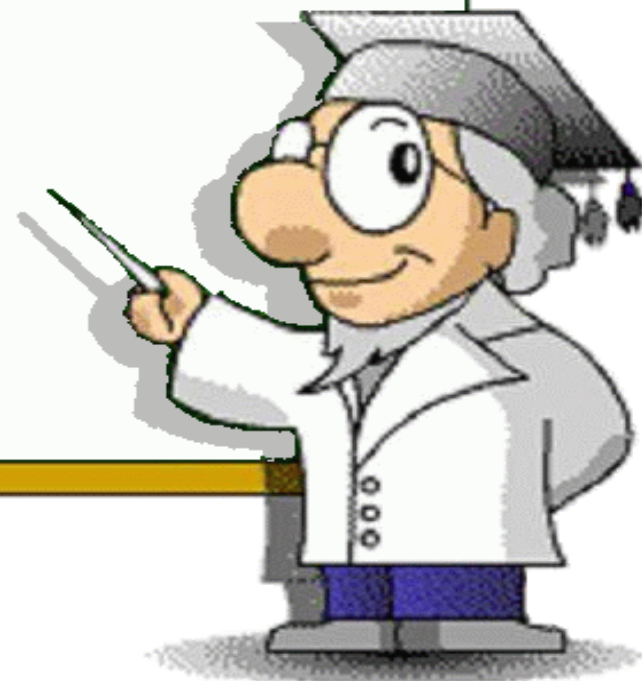


AppGoatを利用した集合教育補助資料 -ディレクトリ・トラバーサル編-

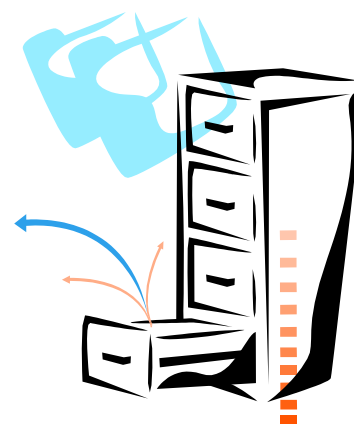
独立行政法人情報処理推進機構 (IPA)
セキュリティセンター

- 脆弱性の原理解説・基礎知識
- 脆弱性の発見方法
- 演習：ファイル情報の漏えい
- 演習解説



ディレクトリ・トラバーサルとは？

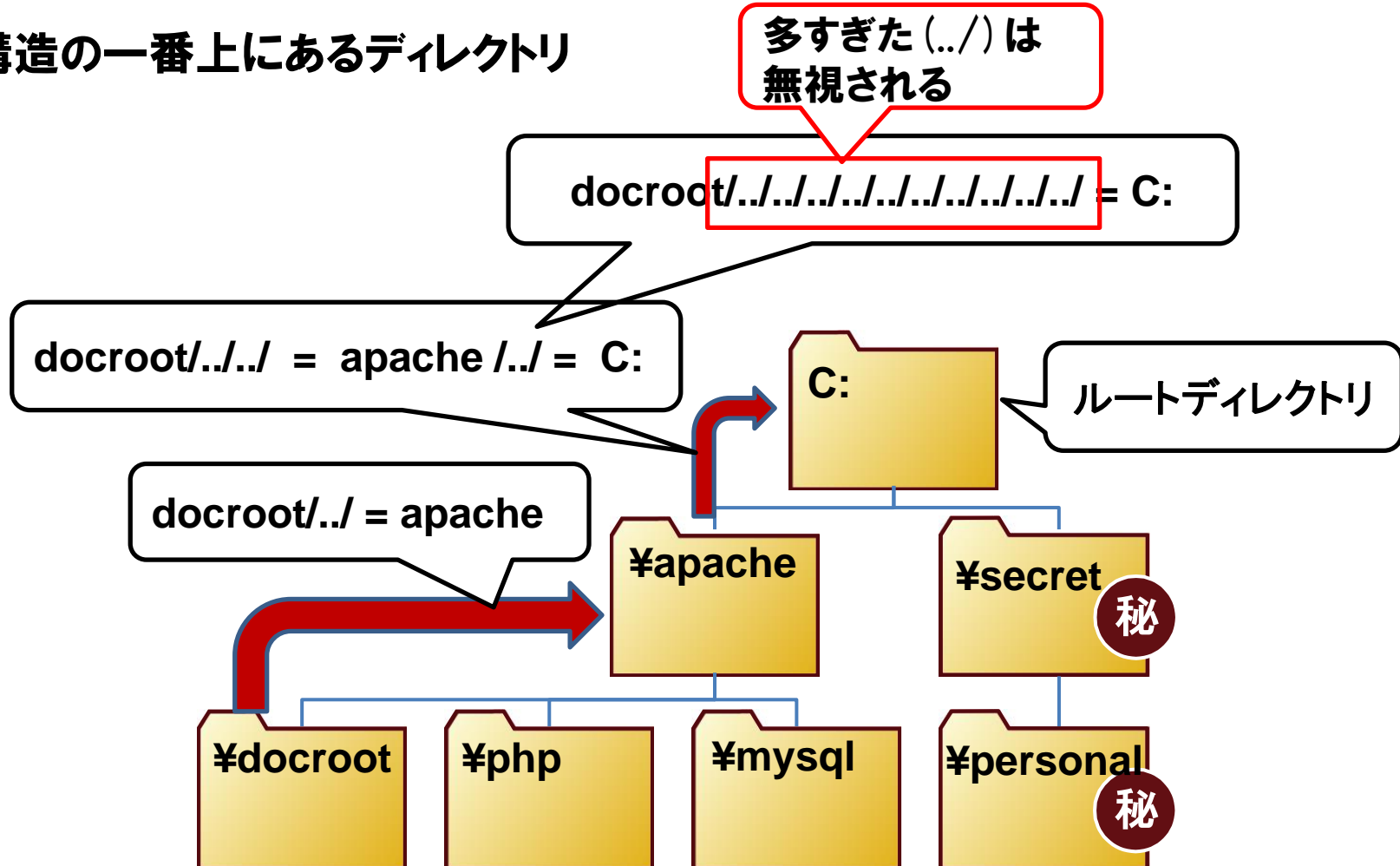
- フォルダ(ディレクトリ)を遡り、任意のファイルにアクセスする脆弱性。
- ウェブアプリケーションは複数のフォルダで構成されており、そのフォルダでパスの解釈に問題があることで生じる。
- (../)【一つ上のフォルダに移動する】
を用いてフォルダを遡る。



ディレクトリの基礎知識

● ルートディレクトリ

ツリー構造の一番上にあるディレクトリ



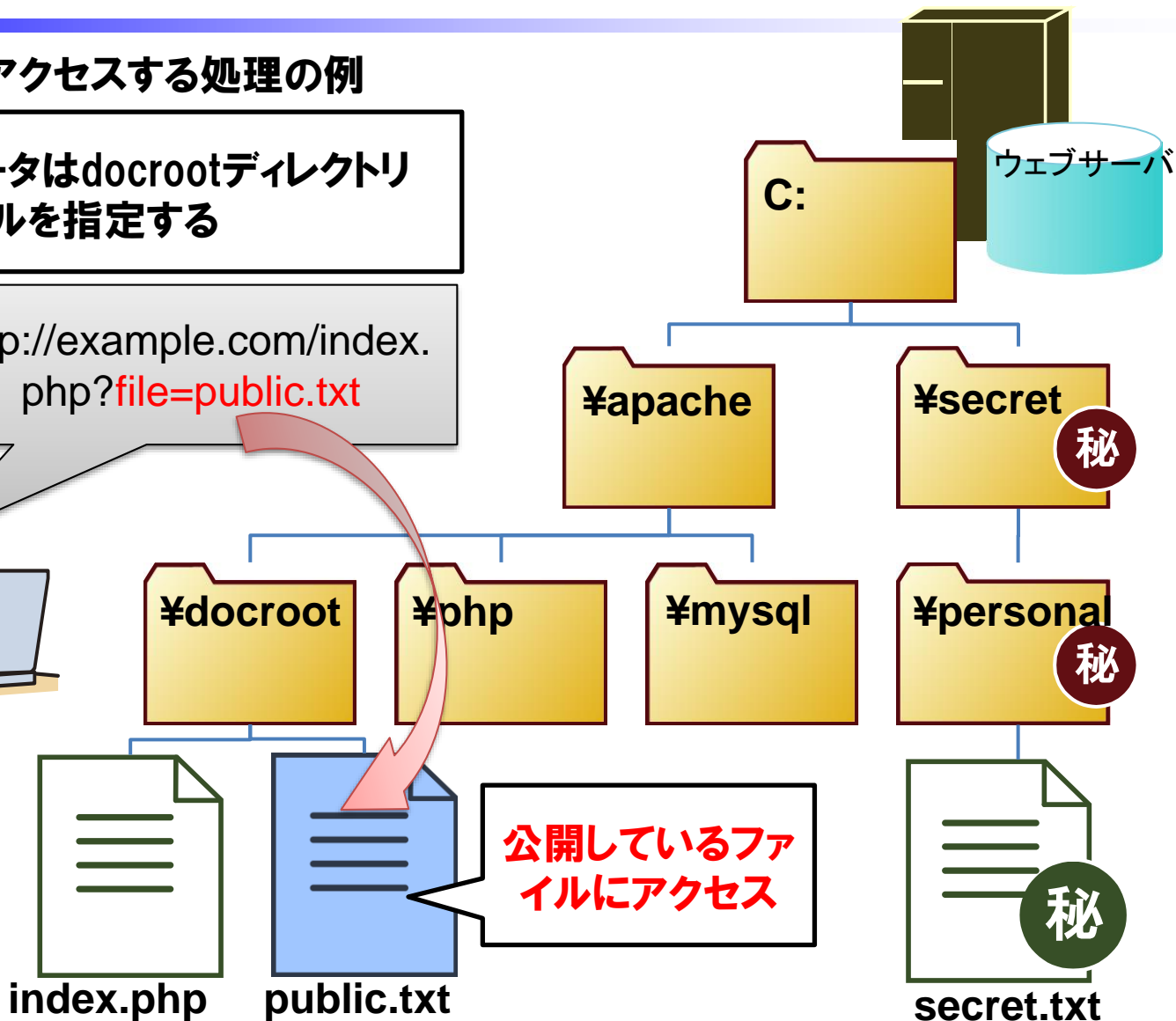
ディレクトリ・トラバーサル攻撃イメージ

～公開されているファイルにアクセスする通常時の動作～

■ファイルにアクセスする処理の例

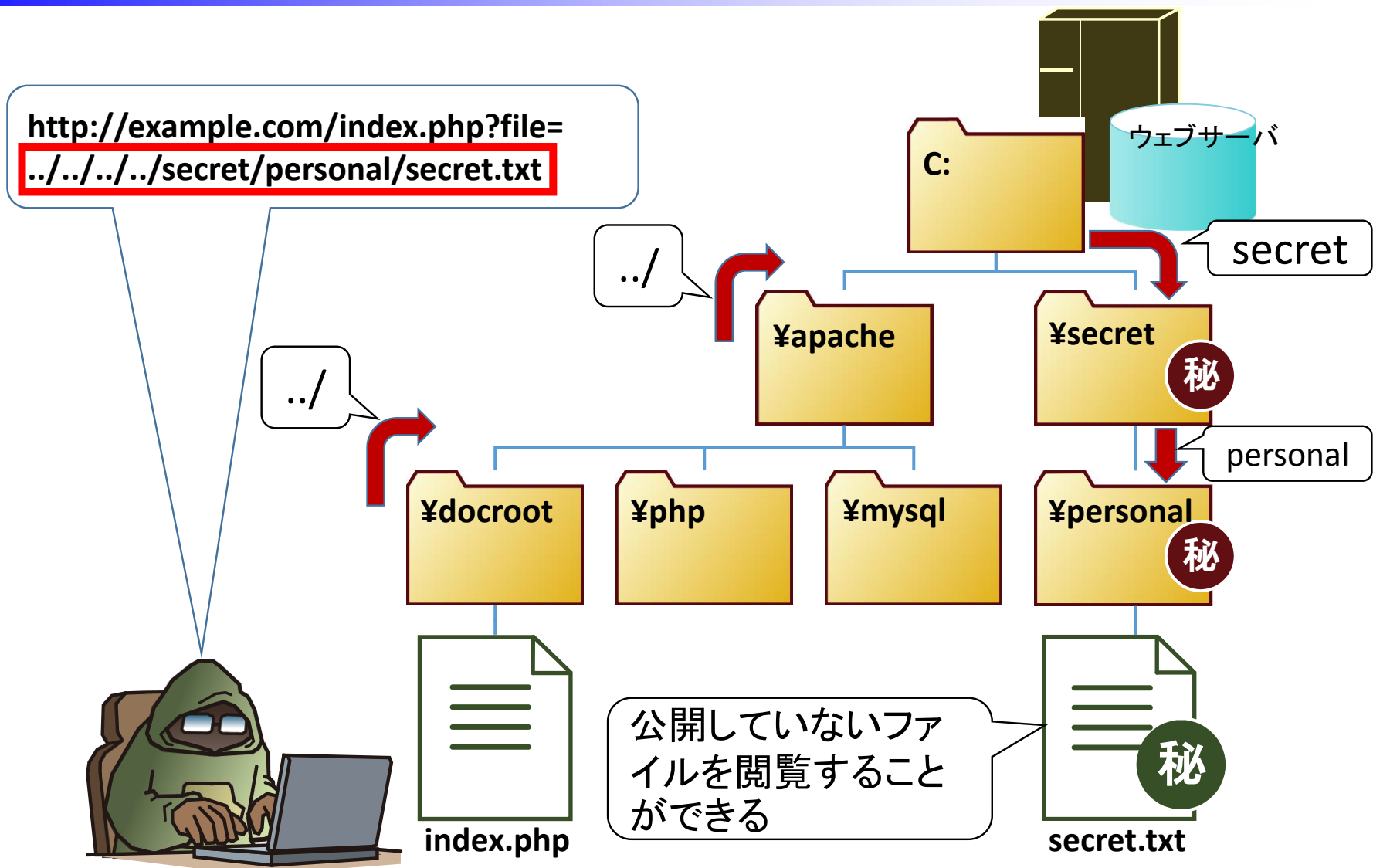
fileパラメータはdocrootディレクトリ内のファイルを指定する

http://example.com/index.php?file=public.txt



ディレクトリ・トラバーサル攻撃イメージ

～公開されていないsecret.txtにアクセス～



ディレクトリトラバーサルを発見するために



●脆弱性が存在する箇所を発見する

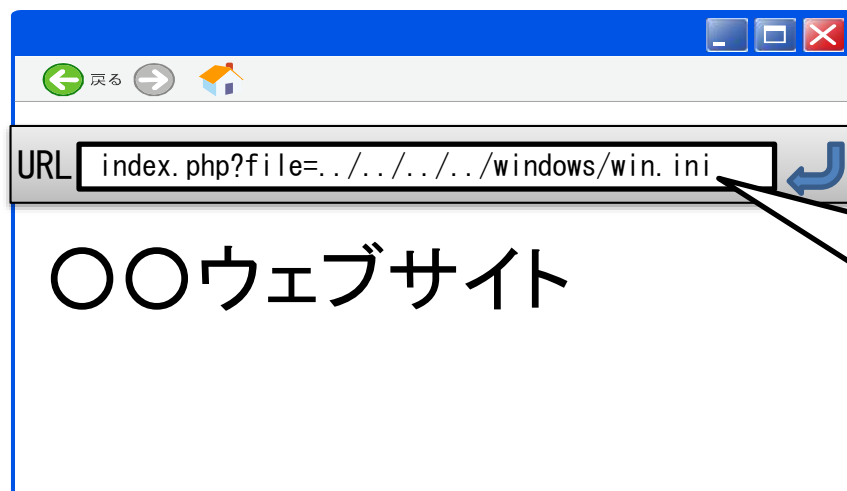
ポイント:ウェブの中でファイルやディレクトリを指定している
箇所を確認する



URLパラメータ

■WebサーバがWindows系OSの場合

「../..../..../..../..../..../..../..../..../..../windows/win.ini」



公開していないファイル

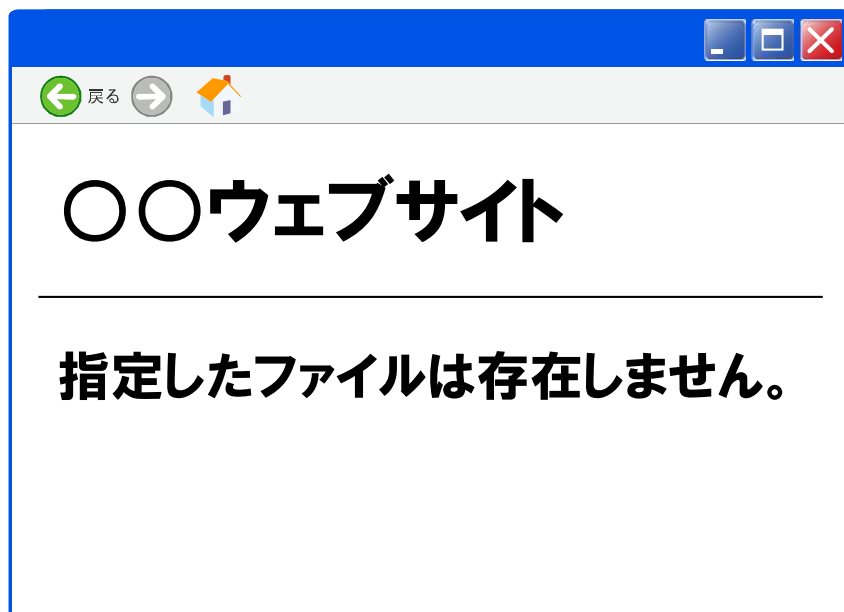
ウェブサイト内のURL
のパラメータに、検出
パターンを入力して送
信する

ディレクトリトラバーサルを発見するために

IPA

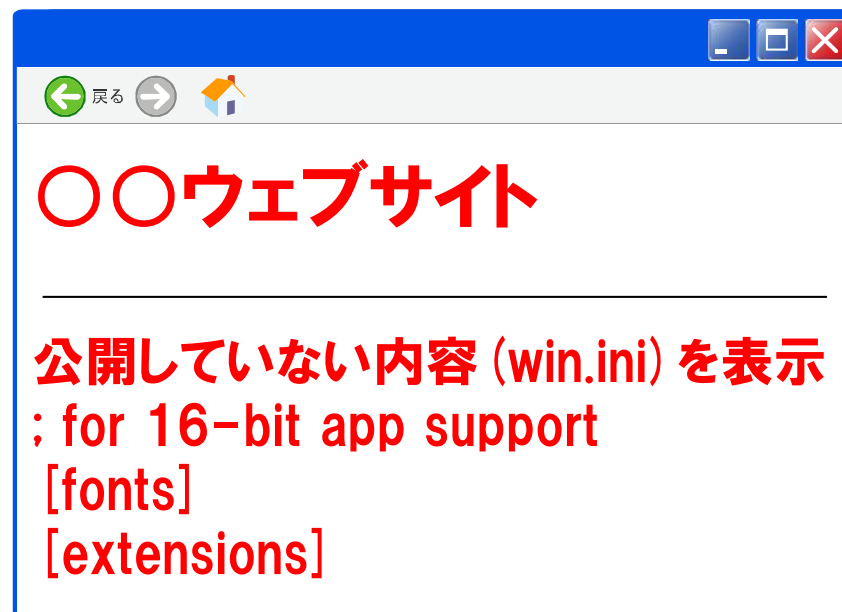


【正常】



機能が正常に稼働して
エラー処理が実行。

【脆弱性あり】



本来見えていけない情報
が表示されたら、脆弱性
ありと判定。

[演習] AppGoatの準備



以下の遷移で演習画面に移動します

-基礎	学習に必要な前提スキル[重要]
+クロスサイト・スクリプティング	AppGoatを使用して学習する上で必要なスキルは以下のとおりです。
+SQLインジェクション	管理者・運用者
+CSRF(クロスサイト・リクエストフォージェリ)	基本情報技術者試験の合格者、または同等のスキル
-ディレクトリトラバーサル	開発者
-イントロダクション ディレクトリトラバーサルとは	・基本情報技術者試験の合格者、または同等のスキル
Level1	・PHPを使ったウェブアプリケーション開発経験が1ヶ月以上
1.「ファイル情報の漏えい」をクリック	・脆弱性の発見および影響確認
Level2	・学習を行う脆弱性によっては以下のスキルがあること
ファイル情報の漏えい	・正規表現を使ったプログラムが作成できる

- 商品一覧
- 家電
- パソコン
- AV機器
- サプライ

3.IDに「admin」、パスワードに「admin123」と入力しログイン

ログインID
admin
パスワード
.....
ログイン クリア

IPA 脆弱性体験学習ツール AppGoat

総合メニュー 学習を進める前に 学習環境へ 学習状況の初期化 学習状況表示 FAQ 利用者マニュアル AppGoatの終了方法

テーマ一覧

- 表示中のページ
- 基礎
- ディレクトリトラバーサル
- Level2
- ファイル情報の漏えい

ファイル情報の漏えい

→ テーマ概要説明 → 原理解説 → 脆弱性の発見手法 → **演習(発見)** → 影響解説

→ 脆弱性コードの発見と修正方法 → 演習(修正) → 動作確認 → 解答例確認

2.「演習」をクリック

チャレンジ
公開されていないはずの、win.iniファイルを表示してみましょう。

- AV機器
- サプライ
- 中古
- セール商品
- カタログ情報
- ユーザ管理
- 商品管理**

商品番号:1000014
マウス
税込価格1,200円
画像ダウンロード

商品番号:1000013【管理用】
ディスプレイ
税込価格6,000円
画像ダウンロード

商品番号:1000012【管理用】
プリンター
税込価格12,000円
画像ダウンロード

商品番号:1000011
カメラ
税込価格1,500円
画像ダウンロード

3.「商品管理」をクリック

[演習] AppGoatを用いた疑似攻撃体験

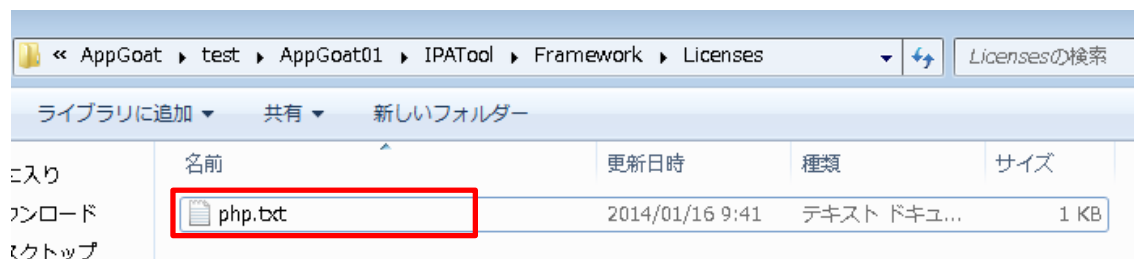
IPA



- 演習テーマ：
「ファイル情報の漏えい」



- ミッション：
公開されていないファイル (php.txt) の表示!



※AppGoatの演習はwin.iniの表示までですが、応用としてIPATool内のフォルダも表示させましょう！

[演習] 演習の進め方

■ Step1:脆弱性がある箇所を特定する

- ・ログイン後の商品管理画面の商品登録ボタンを押して動作を確認する。
- ・win.iniにアクセスできる脆弱性のある箇所を確認する。

■ Step2:脆弱性を突く攻撃を考える

- ・ php.txtファイルにアクセスするURLを考える。

■ Step3:脆弱性を突いてみる

- ・Step2で考えたURLにアクセスする。

実際のphp.txtファイルと表示された情報を比較してみましょう

演習はじめてください。



[Step 1]



脆弱性がある箇所を特定する

演習の手順

URLにファイル名を指定しているようなパラメータがないか探してみましょう

- 商品管理画面の商品登録ボタンを押してみましょう。

ファイル名:

① av.txtファイルを指定して登録

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
1000014	マウス	old	1,200円
1000013	ディスプレイ	old	6,000円

URL



履歴



ログアウト

② 商品登録ボタンを押す

URL末尾のfilenameパラメータに登録ファイルav.txtが指定されている

[Step 1]



脆弱性がある箇所を特定する

IPA



演習の手順

ルートディレクトリに遡り、win.iniファイルにアクセスできることを確認しましょう

win.iniファイルのパスは、C:\Windows\win.ini

- (../) を使ってルートディレクトリに遡りwin.iniにアクセス

http:// (URL省略) &filename=../../../../../../../../Windows/win.ini

多すぎた (../) は
無視される



C:/Windows/win.ini ファイルを呼び出す

[Step 1]



脆弱性がある箇所を特定する

IPA



演習の手順

ルートディレクトリに遡り、win.iniファイルにアクセスできることを確認しましょう

● win.iniにアクセスするURLを作成

ヒント3

- URL欄に次のURLを入力します。
「http://ホスト名ポート番号/Users/アカウント名/Web/Scenario1421/VulSoft/netsh
opping.php?page=15&token=**トークン**&filename=../../../../../../../../windows/win.
ini」
- URLに埋め込むトークンは商品管理ページのソースのhidden属性のtokenに格納されています。すでにURLにトークンが入っている場合もありますが、必ずソースのhidden属性のtokenからコピーします。

トークンは「商品管理」ページのソースを表示し、
<input type="hidden" name="token" value="トークン" />
と書かれている箇所から取得することができます。

[Step 1]



脆弱性がある箇所を特定する

IPA



演習の手順

ルートディレクトリに遡り、win.iniファイルにアクセスできることを確認しましょう

- 作成したURLを、トークンを取得したページのURL欄に入力してアクセスします。

URL

- 画面にwin.iniの情報が表示されることを確認できます。



[Step2]



php.txtにアクセスするURLを考える

IPA

AppGoat

～突いてみますか？脆弱性！～

演習の手順

ルートディレクトリに遡り、php.txtファイルにアクセスしましょう

- (../) を使ってルートディレクトリに遡りphp.txtファイルにアクセス



多すぎた (../) は
無視される

http:// (URL省略) &filename=../..../..../..../..../..../..../ [保存したフォルダ名] /AppGoat_web_v303_XXXX/IPATool/Framework/Licenses/php.txt

php.txtファイルを呼び出す

[Step3]



Step2のURLにアクセスしファイルを確認する

IPA

AppGoat

～突いてみますか？脆弱性！～

演習の手順

Step2で作成したURLにアクセスしてみましょう

- 作成したURLを、トークンを取得したページのURL欄に入力してアクセスします。

URL filename=../../../../../../../../AppGoat/AppGoat_web_v303_0930/IPATool/Frame GO

- 画面にphp.txtの情報が表示されることを確認できます。

この内容で商品登録を行います。よろしいですか？

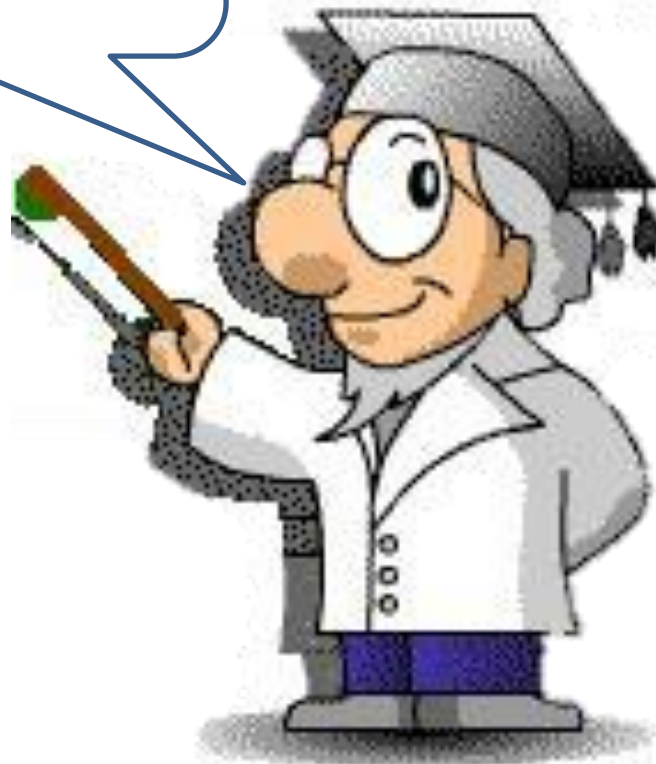
はい

いいえ

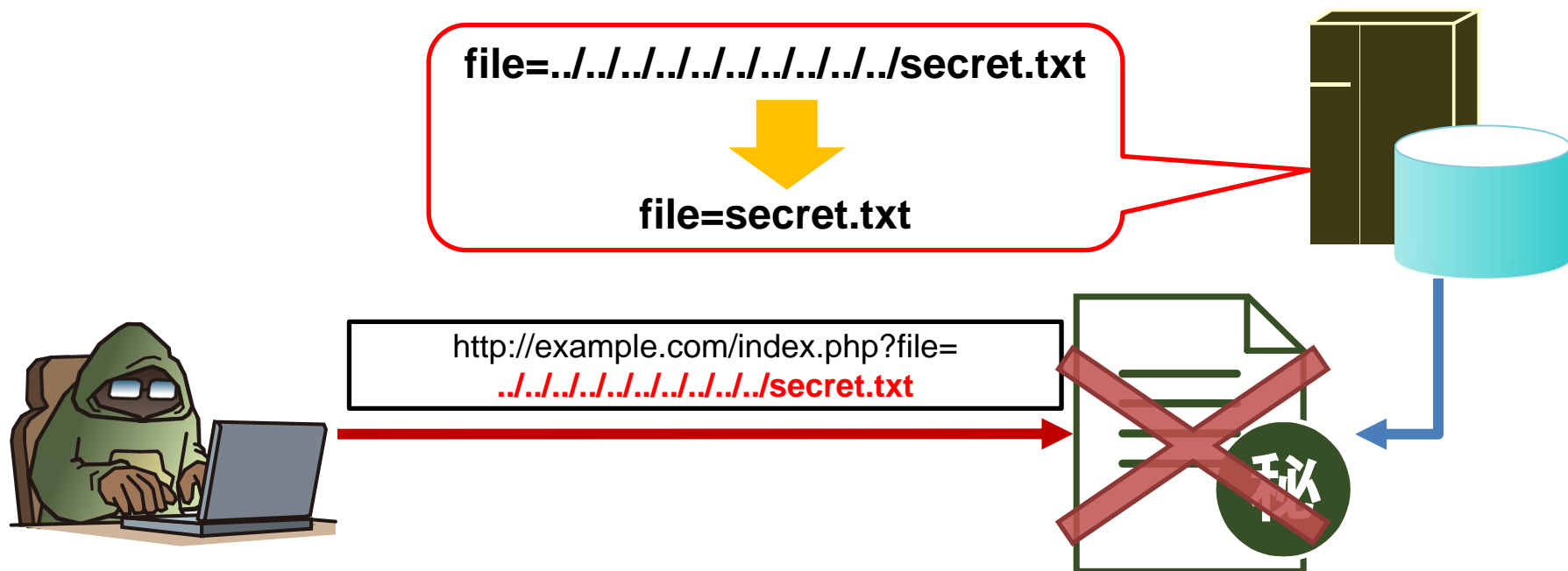
* This is a credit file of IPATool.

This product includes PHP, freely available from
<<http://www.php.net/>>

対策方法



- ファイル名の指定でディレクトリ名が含まれないようにする



● 根本的解決

- ファイル名にディレクトリ名が含まれないようにする

PHPではbasename関数を使用することで、ファイル名のみを取得できる。

- ファイル名を直接指定する実装を避ける

● 保険的対策

- アクセス権限の設定を正しく管理する。

以上で、
ディレクトリ・トラバーサルの解説は
終了です。

