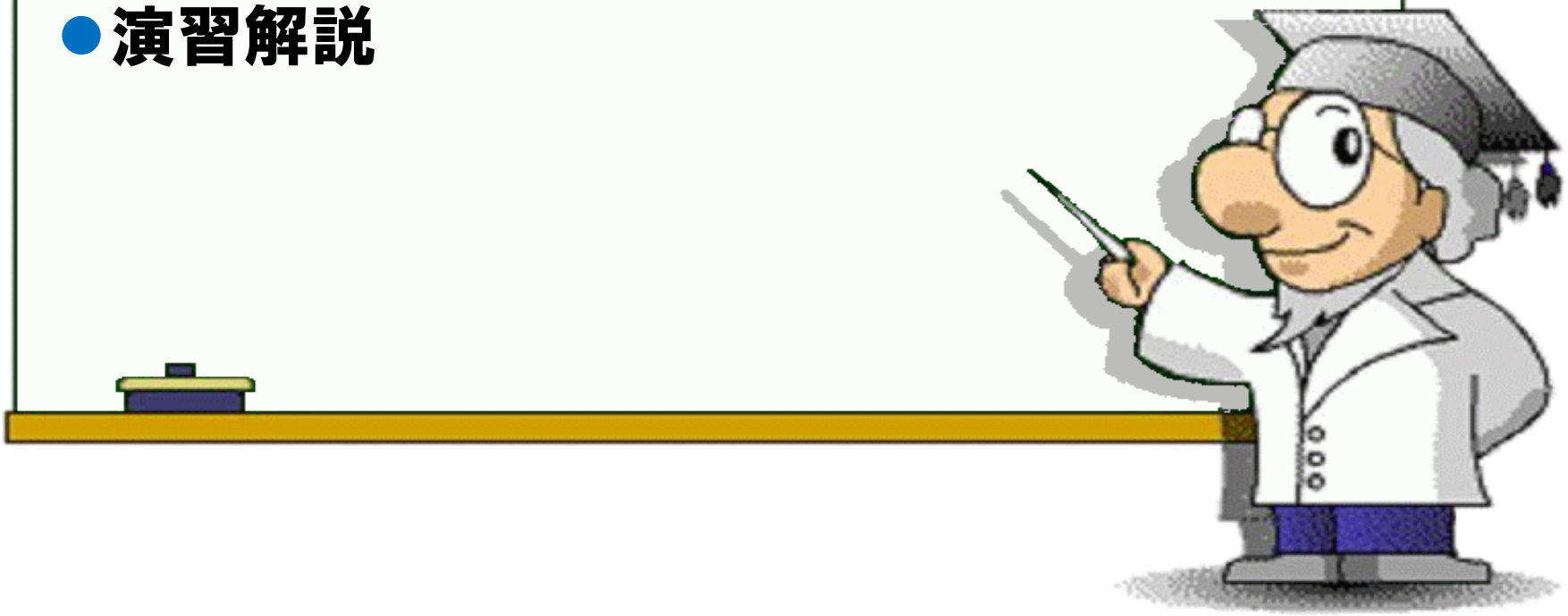
AppGoatを利用した集合教育補助資料
-OSコマンドインジェクション編-

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

内容

- 脆弱性の原理解説・基礎知識
- 脆弱性の発見方法
- 演習：システム情報の漏えい
- 演習解説



OSコマンドインジェクションとは？

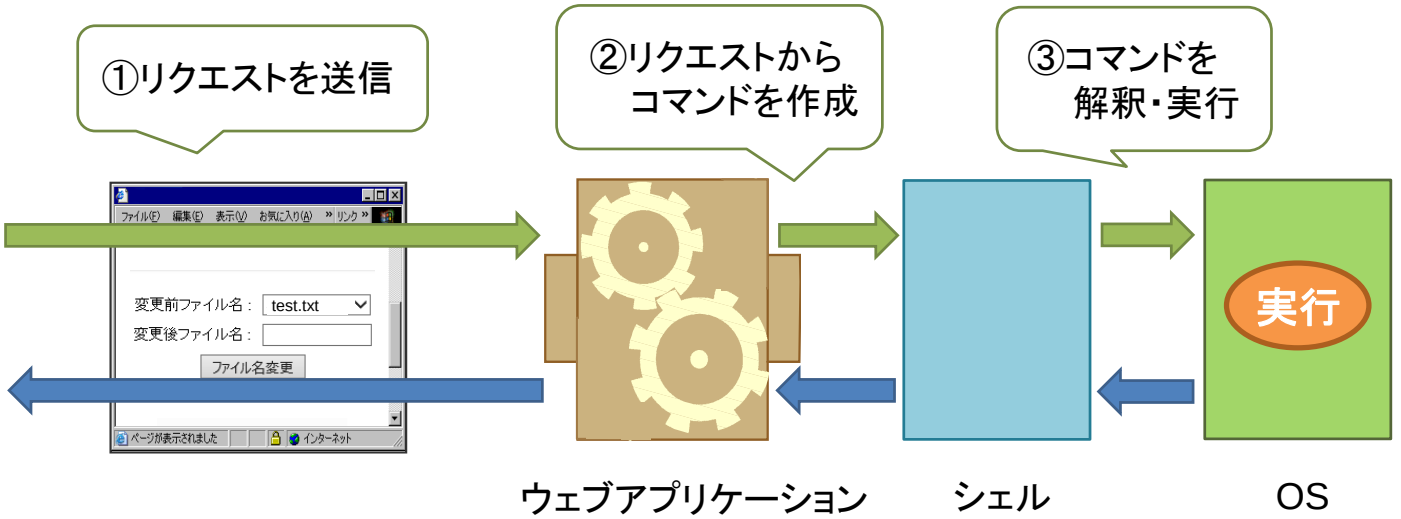
- OSコマンドとは、OS（オペレーティングシステム）を操作するための命令
- OS Command Injection = OSコマンドの注入
- すなわち、OSコマンドインジェクションとは、外部から意図しないOSコマンドを注入し、システムを不正に操作する攻撃
- 外部プログラムを呼び出し可能な関数等を使用しているウェブアプリケーションは注意が必要

OSコマンドの基礎知識

シェル経由によるOSコマンド実行

シェルとは

- OSのユーザーのためにインタフェースを提供するソフトウェア
- シェルを利用することで入力されたコマンドをOSに認識させることが可能



OSコマンドの基礎知識

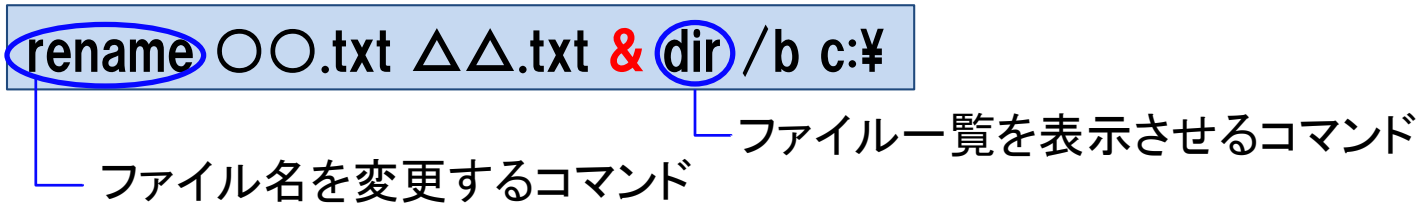
IPA

OSコマンドにおける記号文字

- 「;」「|」「&」等の記号文字には、OSコマンドにおいて特殊な意味がある。
- ウェブアプリケーションが、OSにとって特殊な意味を持つ記号文字を入力値として受け取り、そのままOSに渡してしまうと、意図しないOSコマンドを実行されてしまう可能性がある。

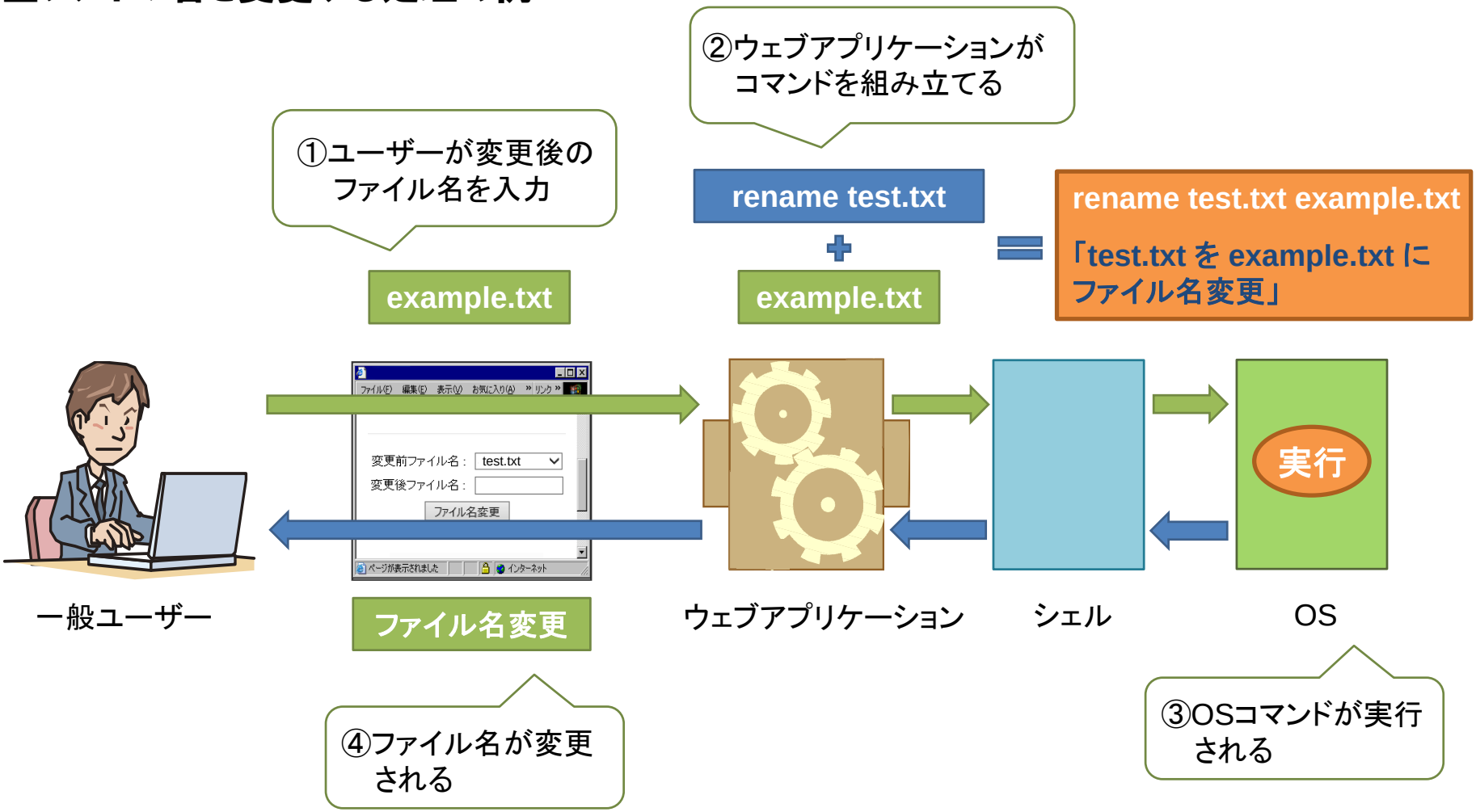
・連結文字「&」

複数のコマンドを繋げることができる。



OSコマンドインジェクションの攻撃イメージ
～通常時の動作～

■ファイル名を変更する処理の例



OSコマンドインジェクションの攻撃イメージ
～攻撃リクエストが送られた時の動作～

IPA

「&」をコマンドを連結させる文字として受け取ってしまっている

②ウェブアプリケーションがコマンドを組み立てる

①攻撃者が攻撃リクエストを送信

rename test.txt

＋

example.txt & dir

＝

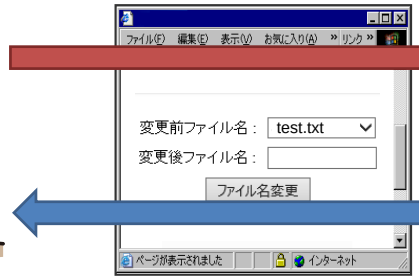
rename test.txt example.txt & dir

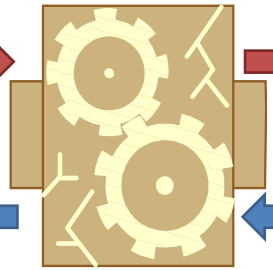
「test.txt を example.txt にファイル名変更」

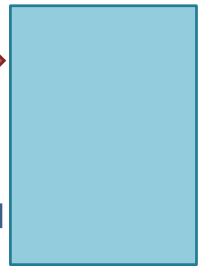
&

「ファイルの一覧を表示」

example.txt & dir







攻撃者

ファイル名変更
&
ファイルの一覧を表示

脆弱性のあるウェブアプリケーション

シェル

OS

③意図しないOSコマンドが実行される

④非公開情報が漏えいする

OSコマンドインジェクションを発見するために

IPA AppGoat ～突いてみますか？脆弱性！～

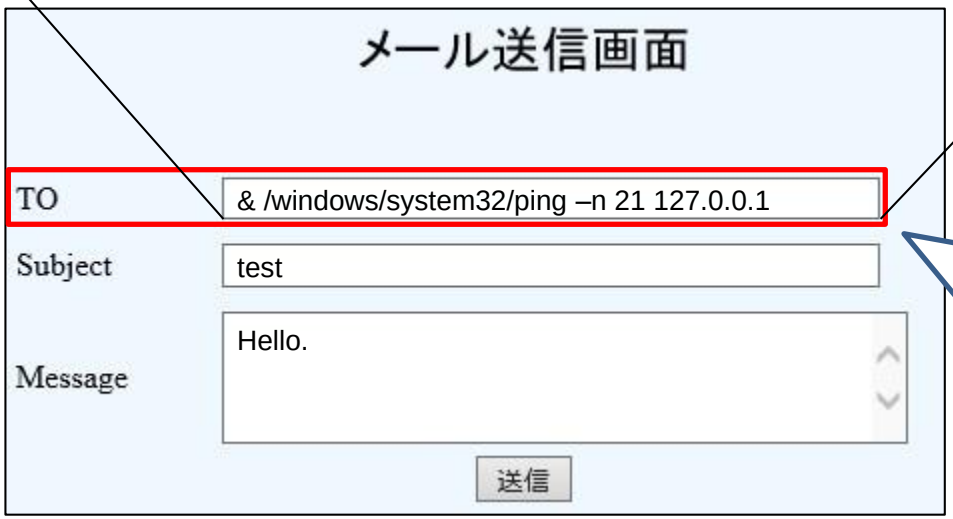
● 脆弱性が存在する箇所を発見する

ポイント：①シェル経由でOSコマンドを実行している箇所を探す。

→OSコマンドで同様の処理（メール送信、ファイル名変更等）を実行できそうな箇所を探す。

②その箇所で別のOSコマンドが実行できるか確認する。

& /windows/system32/ping –n 21 127.0.0.1



メール送信画面の入力項目に、検出パターンを入力して送信する。
（この場合、ネットワーク疎通を21回確認する、という内容のコマンドを送信）

シェル経由のOSコマンド実行処理を行うメール送信画面

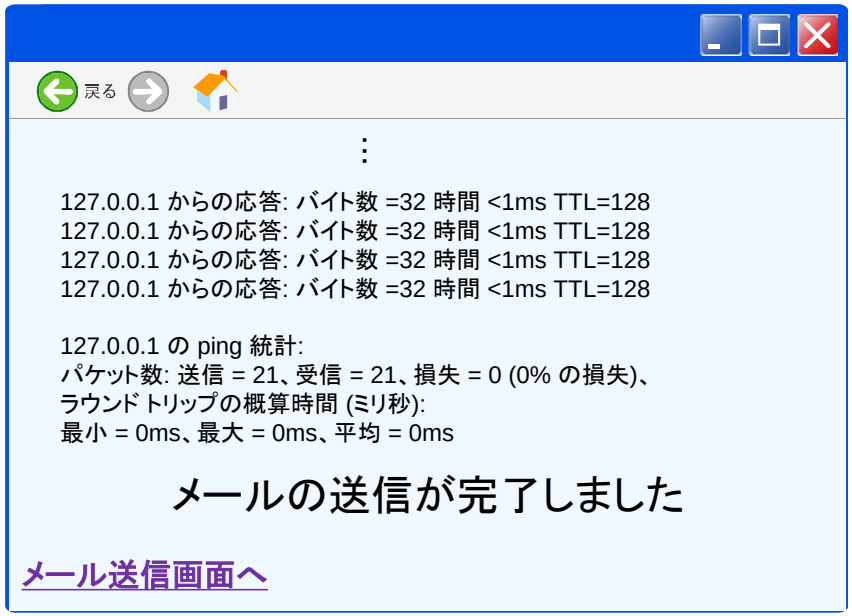
OSコマンドインジェクションを発見するために

IPA AppGoat ～突いてみますか？脆弱性！～

【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】



20秒以上後にレスポンスが返ってきたら、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

[演習] AppGoatを用いた疑似攻撃体験

IPA

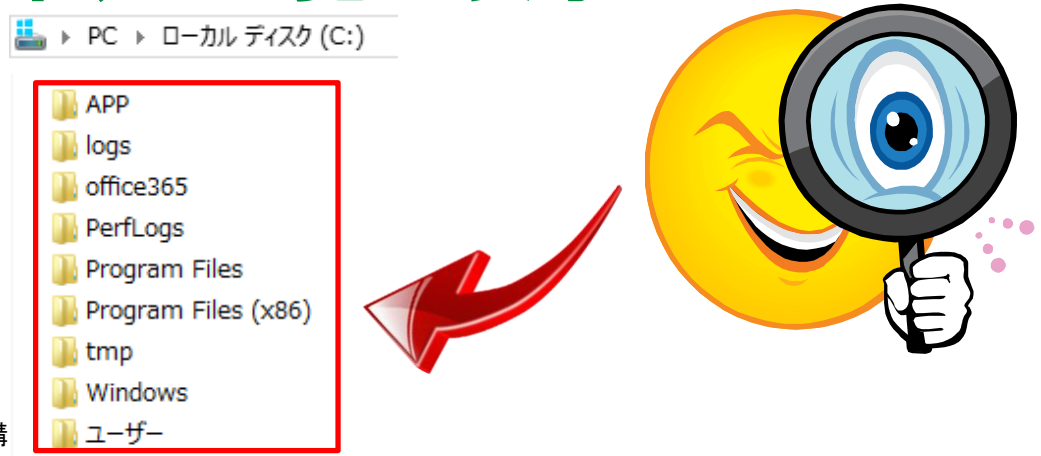
AppGoat ～突いてみますか？脆弱性！～

- **演習テーマ：**

  「システム情報の漏えい」

- **ミッション：**

  公開されていないファイル名とフォルダ名（Cドライブ直下）の一覧の表示!



[演習] 演習の進め方

IPA

AppGoat
～突いてみますか？脆弱性！～

- Step1：脆弱となる箇所を特定する
  - ・ログイン後の商品管理画面のファイル名変更ボタンを押して動作を確認する。
  - ・ping -n 21 127.0.0.1を送り、20秒以上レスポンスが返ってこないことを確認する。
- Step2：脆弱性を突く攻撃を考える
  - ・Cドライブ直下のファイル名とフォルダ名の一覧を表示させる攻撃リクエストを考える。
- Step3:脆弱性を突いてみる
  - ・ログイン後のページでStep2で考えた攻撃リクエストを送信する。

実際のファイル一覧と表示された情報を比較してみよう

演習

IPA

演習はじめてください。

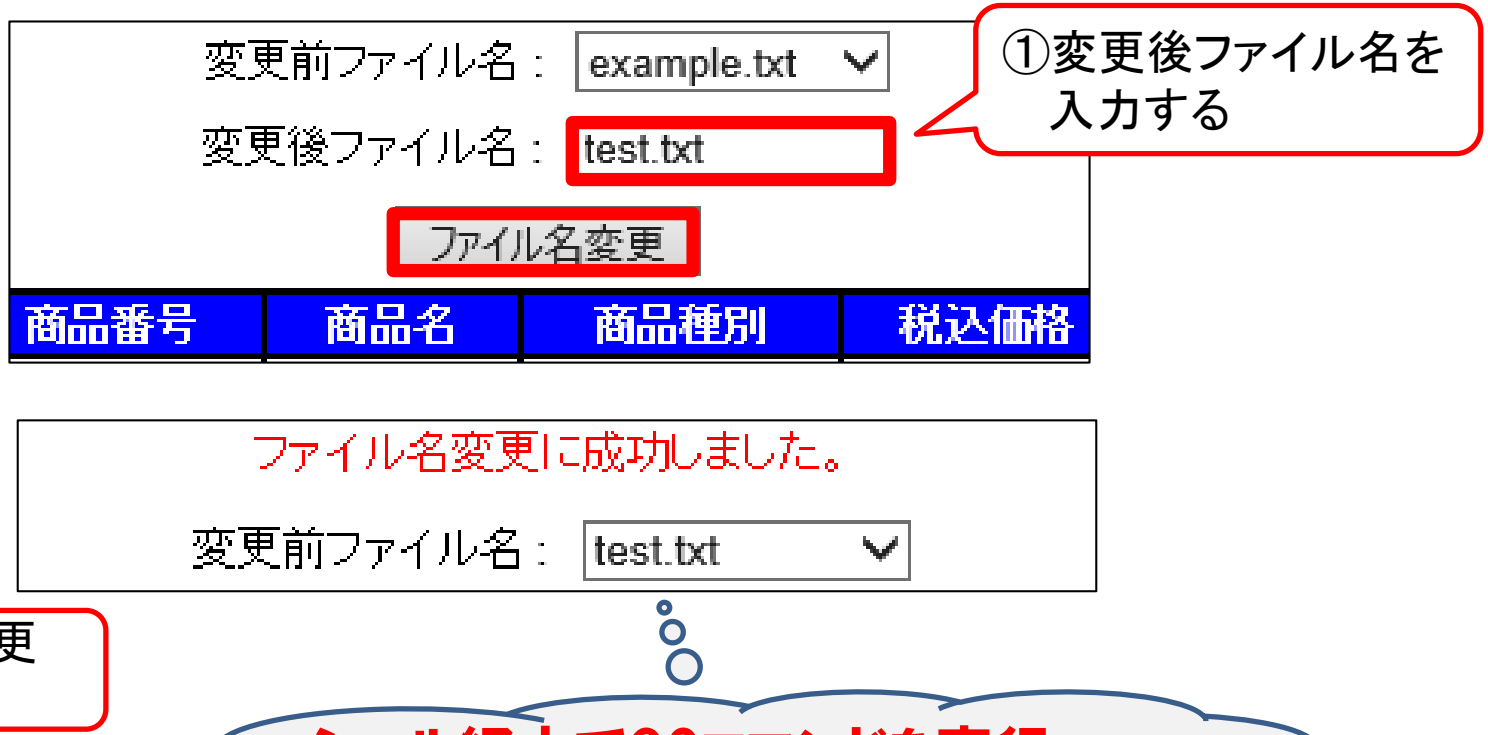
[Step1] 商品管理画面のファイル名変更ボタンを押して動作を確認する

IPA AppGoat ～突いてみますか？脆弱性！～

演習の手順

商品管理ページで実際にファイル名を変更できるか確認しましょう

- **商品管理画面のファイル名変更ボタンを押してみましょう。**



[Step1] pingコマンドを送り、挙動を確認する

IPA AppGoat ～突いてみますか？脆弱性！～

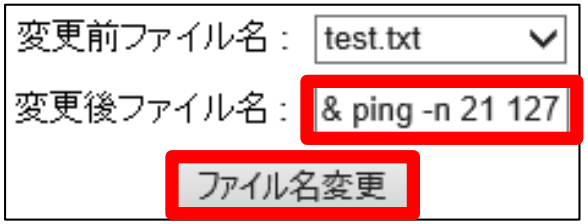
演習の手順

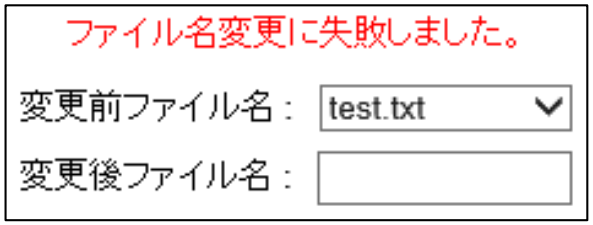
入力画面からpingコマンドを送り、コマンドが実行されるか確認しましょう

※OSコマンドインジェクションが可能な連結文字は「&」、ping送信先に指定できるIPアドレスは「127.0.0.1」のみに制限しています。

- **連結文字（&）を使って 127.0.0.1 にpingを送信**

& ping -n 21 127.0.0.1 ＝ **127.0.0.1 に対してネットワーク疎通を21回確認する**





20秒以上レスポンスが返ってこない

[Step2] ファイル名とフォルダ名の一覧を表示させる攻撃リクエストを考える

IPA

AppGoat ～突いてみますか？脆弱性！～

演習の手順

Cドライブ直下のファイル名とフォルダ名の一覧を取得するリクエストを考えましょう

❸ Cドライブ直下のファイル名とフォルダ名の一覧を取得するOSコマンド「dir /b c:¥」を脆弱性のある箇所で実行しましょう。実行する方法がわからない場合はヒント2を参照しましょう。

- 連結文字（＆）を使って攻撃リクエストを作成

example.txt & dir /b c:¥

||

ファイル名を example.txt に変更する
Cドライブ直下のファイル名とフォルダ名の一覧を取得する

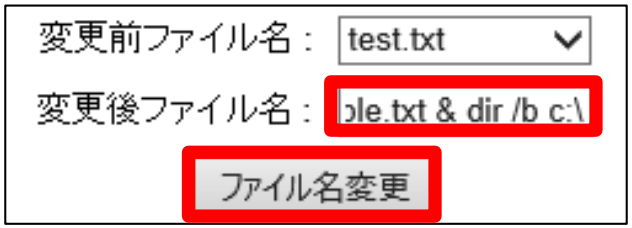
[Step3] 攻撃リクエストを送信し情報を取得する

IPA AppGoat ～突いてみますか？脆弱性！～

演習の手順

手順2で作成した攻撃リクエストを送信してみましょう

1. 変更後ファイル名の欄に攻撃コードを入力し、ファイル変更ボタンを押します。



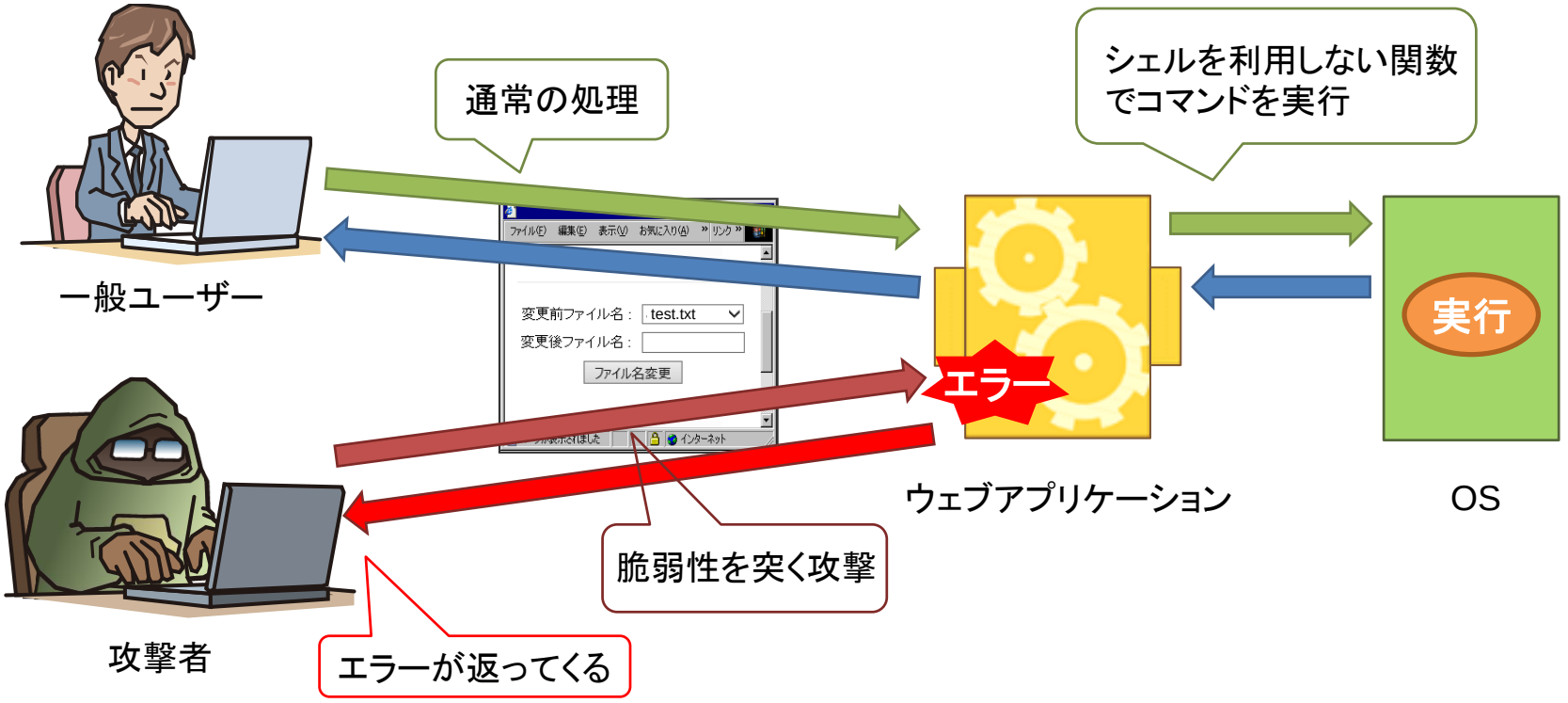
2. 画面にファイル名とフォルダ名の一覧が表示されることを確認できます。

原因の解説

対策方法

対策のポイント

- シェルを起動できる言語機能の利用を避ける



OSコマンドインジェクションの対策

IPA

- **根本的解決**
  - **シェルを起動できる機能の利用は避け、他の関数等で代替するようにする**

    例えば、PHPでは rename () を使用することで、ファイル名の変更を行うことができる。
  - **シェルを起動できる機能を利用する場合は、エスケープ処理を行う（対策の抜け漏れを起こしやすいので注意）**

    OSコマンドにおいて特別な意味を持つ記号文字をそのまま読み込まないようにする。特に以下の文字に注意。

    「;」「|」「&」「`」「(」「)」「$」「<」「>」「*」「?」「{」「}」「[」「]」「!」

以上で、
OSコマンドインジェクションの解説は
終了です。