

# 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

- 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？

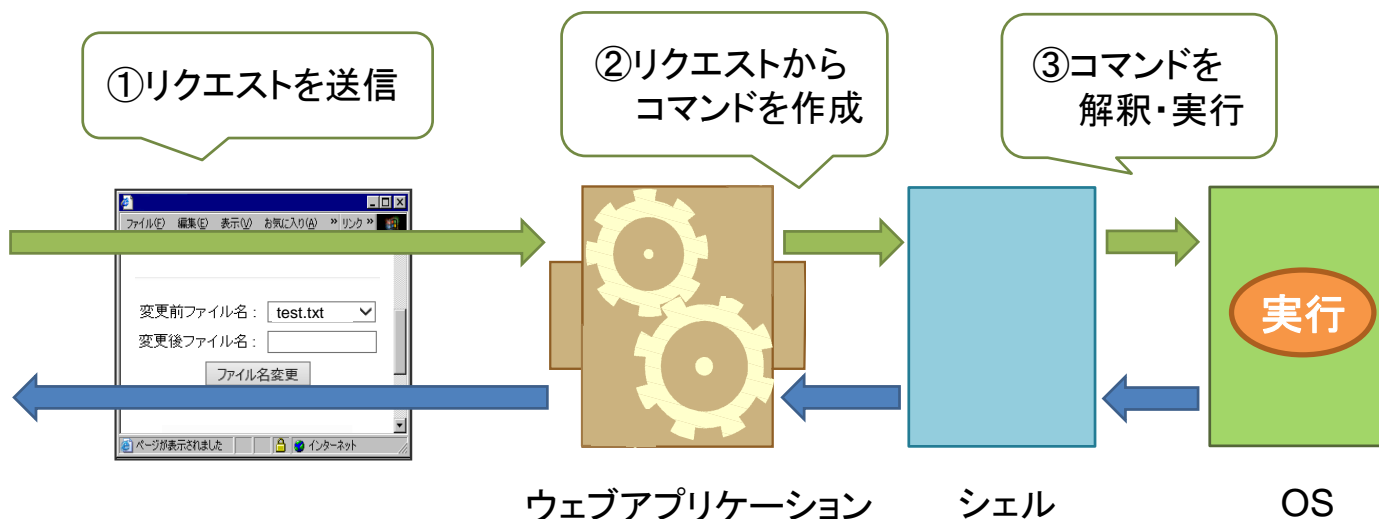
- OSコマンドとは、OS（オペレーティングシステム）を操作するための命令
- OS Command Injection = OSコマンドの注入
- すなわち、OSコマンドインジェクションとは、外部から意図しないOSコマンドを注入し、システムを不正に操作する攻撃
- 外部プログラムを呼び出し可能な関数等を使用しているウェブアプリケーションは注意が必要



## ● 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。

```
rename ○○.txt △△.txt & dir /b c:¥
```

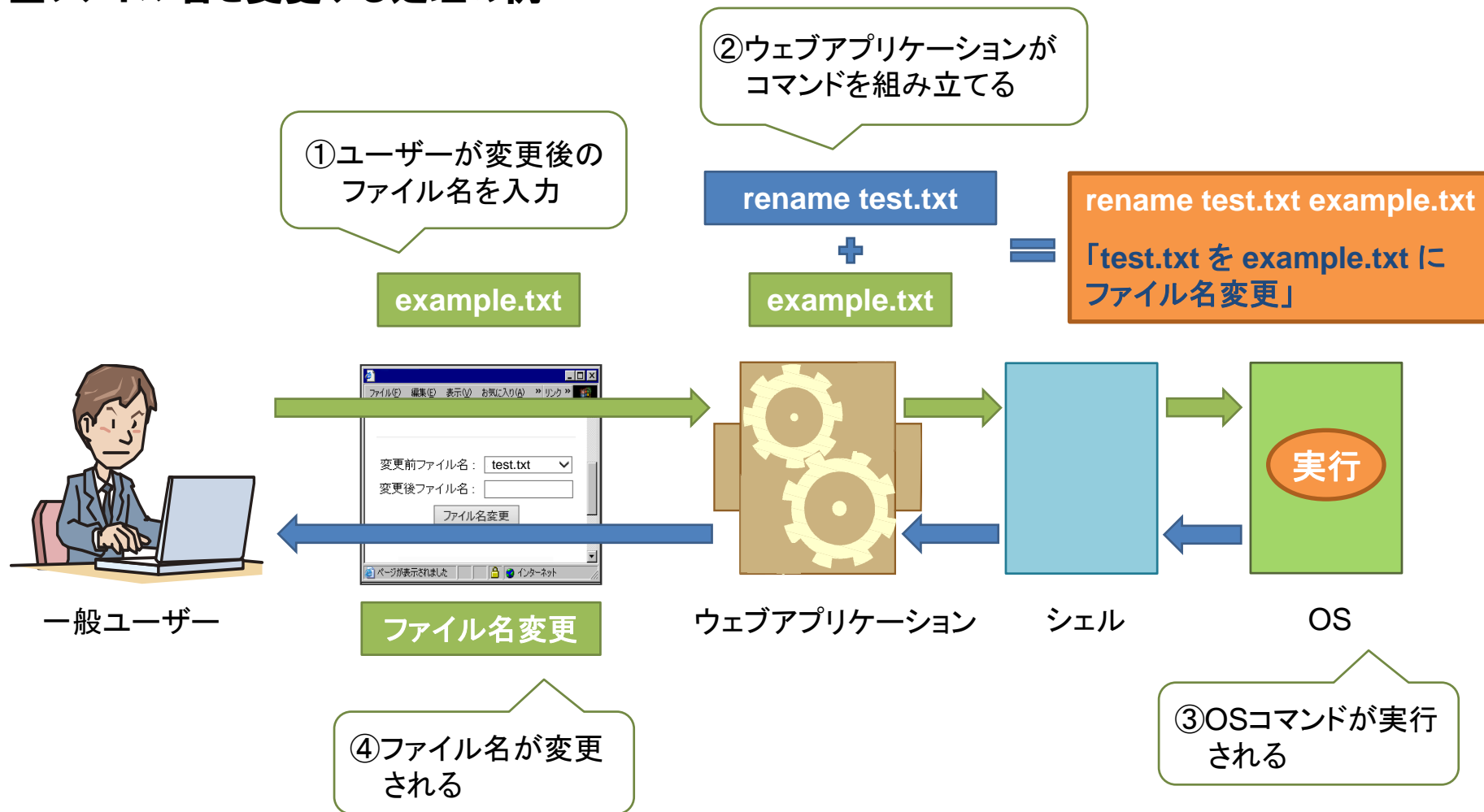
— ファイル名を変更するコマンド

— ファイル一覧を表示させるコマンド

# 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～

① 攻撃者が攻撃リクエストを送信

example.txt & dir

② ウェブアプリケーションが  
コマンドを組み立てる

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」

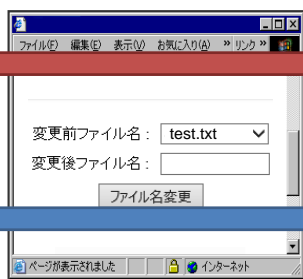
&

「ファイルの一覧を表示」

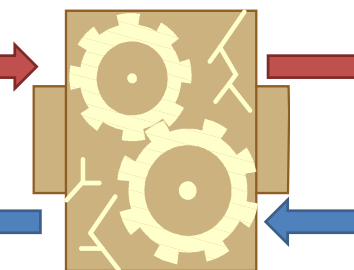
「&」をコマンドを連結  
させる文字として受け  
取ってしまっている



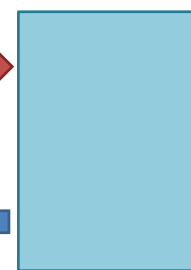
攻撃者



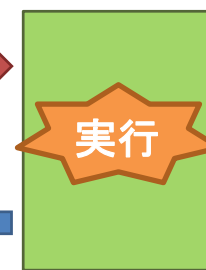
ファイル名変更  
&  
ファイルの一覧を表示



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  
漏れいする

## ●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

TO	<input type="text" value="&amp; /windows/system32/ping -n 21 127.0.0.1"/>
Subject	<input type="text" value="test"/>
Message	<input type="text" value="Hello."/>

送信

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



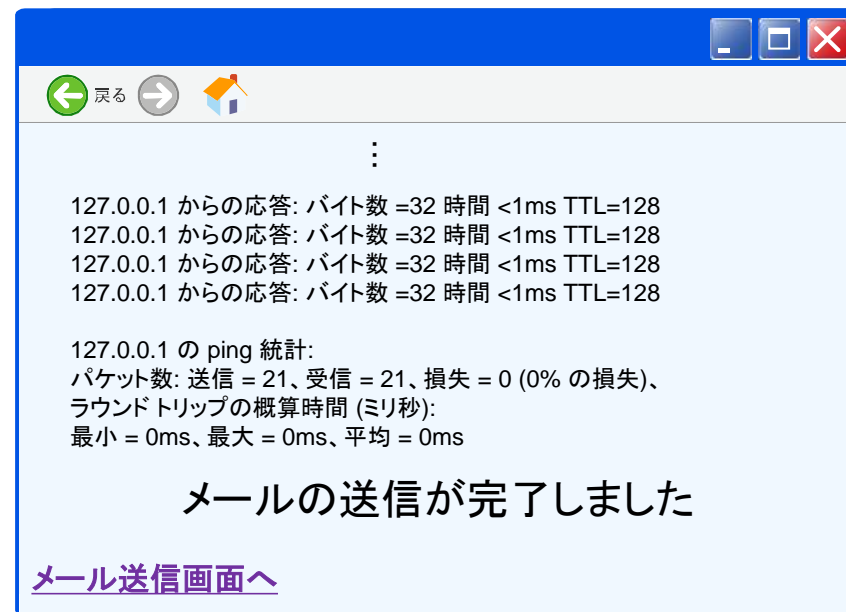
# OSコマンドインジェクションを発見するために IPA



## 【正常】



## 【脆弱性あり】



機能が正常に稼働して  
エラー処理が実行

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

# IPA



## 以下の遷移で演習画面に移動します

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
  - OSコマンド・インジェクション
  - Level2
  - システム情報の漏えい
- 基礎
  - +クロスサイト・スクリプティング
  - +SQLインジェクション
  - +CSRF(クロスサイト・リクエストフォージェリ)
  - +ディレクトリトラバース
  - OSコマンド・インジェクション
  - イントロダクション

システム情報の漏えい

→ テーマ概要説明 → 原理解説 → 脆弱性の発見手法 → 演習(発見)  
→ 脆弱性コードの発見と修正方法 → 演習(修正) → 動作確認 → 解答

テーマ概要説明

このテーマでは、【脆弱Webネットショッピングサイト】な演習を通して、OSコマンド・インジェクションの脆弱性を発見していきましょう。

この脆弱性は、ユーザからの入力値をそのまま利用して、シェル経由によるOSコマンド・インジェクションを実行することで、OSコマンド・インジェクションの脆弱性を引き起こします。

では、この脆弱性の原理を見てみましょう。

1.「システム情報の漏えい」クリック

システム情報の漏えい

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

パスワード

ログイン クリア

システム情報の漏えい

2.「演習」クリック

→ 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

演習(発見)

URL http://localhost/Users/\_personal/Web/Scenario1521/VulSoft/netshopping.php? GO

家電

パソコン

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

キーボード  
税込価格 1,800円  
画像ダウンロード

マウス  
商品番号:1000014  
税込価格 1,200円  
画像ダウンロード

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

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

4.「商品管理」クリック

# [演習] AppGoatを用いた疑似攻撃体験

IPA

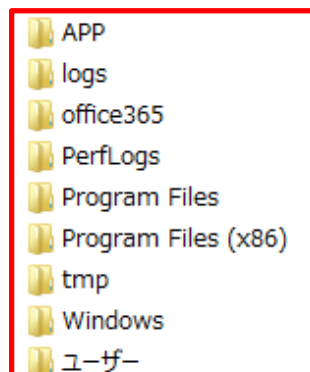


- 演習テーマ:  
「システム情報の漏えい」



- 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!

PC > ローカル ディスク (C:)



# [演習] 演習の進め方

## ■ 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

- ・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

## 演習はじめてください。



# [Step 1]



## 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



### 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。

変更前ファイル名:  ▼

変更後ファイル名:

商品番号	商品名	商品種別	税込価格
------	-----	------	------

① 変更後ファイル名を入力する



ファイル名変更になりました。

変更前ファイル名:  ▼

② ファイル名変更ボタンを押す

シェル経由でOSコマンドを実行している可能性

# [Step 1]



## pingコマンドを送り、挙動を確認する

### 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

変更前ファイル名:

変更後ファイル名:

ファイル名変更に失敗しました。

変更前ファイル名:

変更後ファイル名:



## 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

- ③ 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行いましょう。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。

変更前ファイル名 : test.txt

変更後ファイル名 : `ble.txt & dir /b c:\`

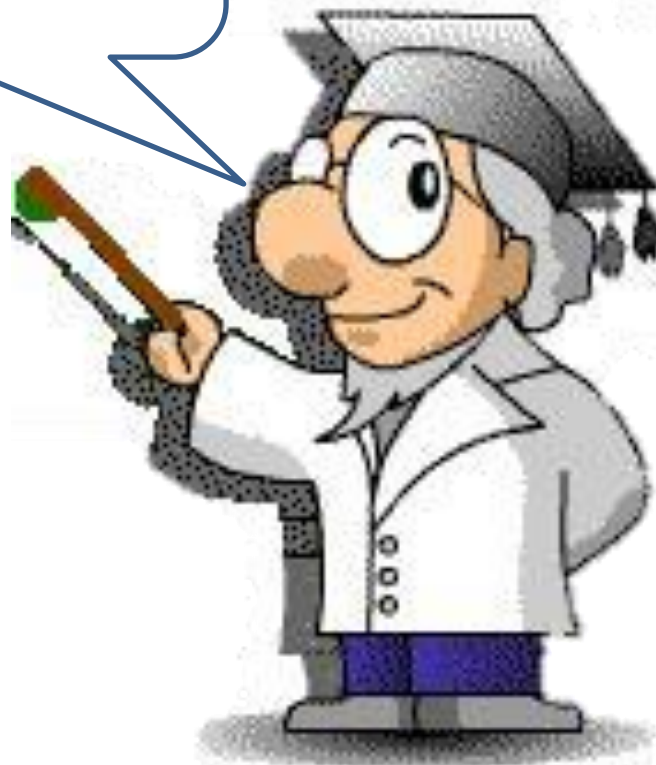
ファイル名変更

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。

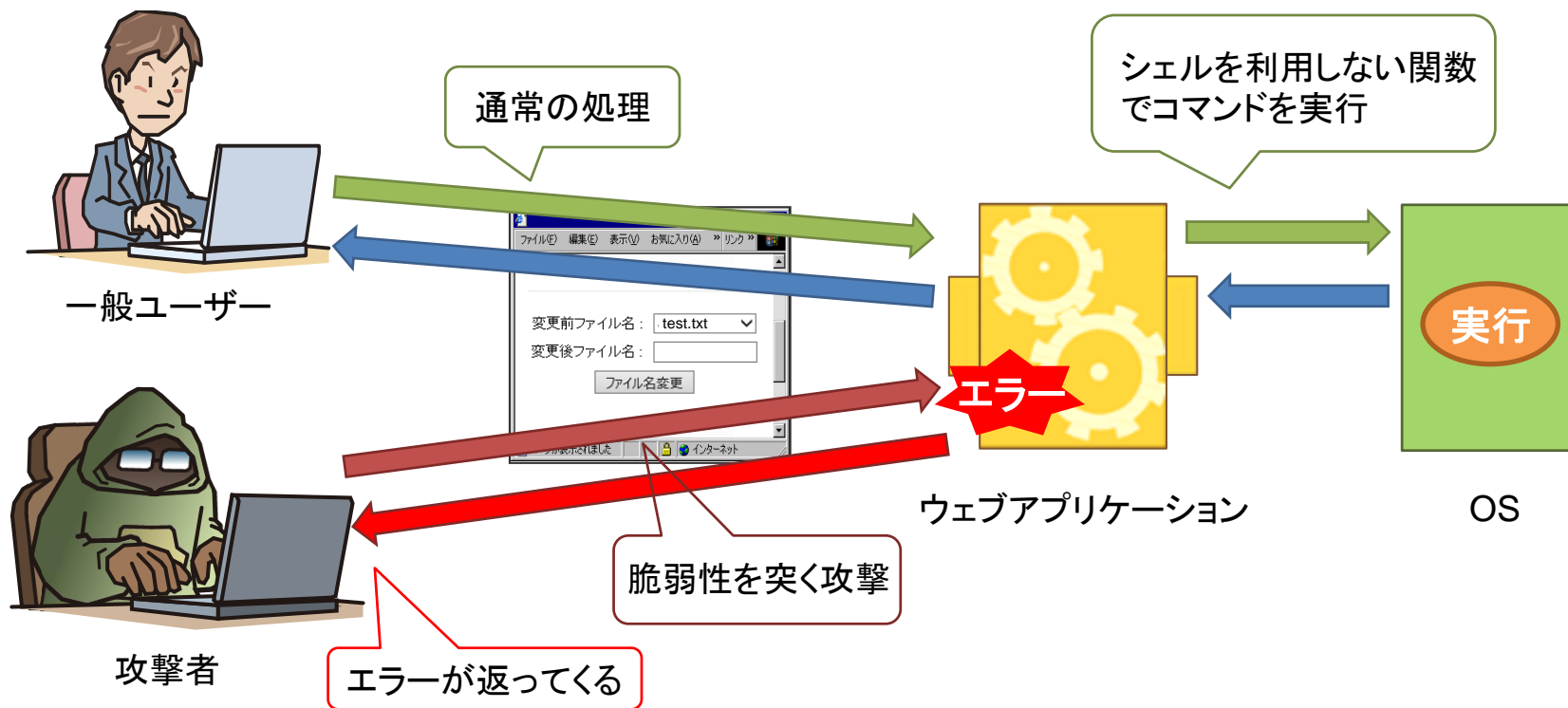
```
logs
Program Files
Program Files (x86)
Users
Windows
APP
office365
PerfLogs
tmp
```

Congratulations!!演習の目標を達成しました。

**対策方法**



## ● シェルを起動できる言語機能の利用を避ける



## ● 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。

