パストラバーサル

パストラバーサルとは？

パス（ディレクトリ）トラバーサルは、攻撃者がアプリケーションの実行場所以外のファイルやディレクトリにアクセスしたり、保存したりできる脆弱性です。これにより、他のディレクトリからファイルが読み取られ、ファイルアップロードの場合、重要なシステムファイルが上書きされる可能性があります。

パスについて おさらい

絶対パス

ルートディレクトリと呼ばれる階層構造の頂点から目的地までの経路

```
cat /home/webgoat/.webgoat-8.1.0/data/webgoat.log
```

相対パス

現在位置から目的地までの経路

```
cd /home/webgoat/.webgoat-8.1.0/data/
cat webgoat.log
```

遡って指定するとき

```
cd /home/webgoat/.webgoat-8.1.0/data/
cat ../../.webgoat-8.1.0/data/webgoat.log
```

`./` は現在のディレクトリ
`../` は一つ上の階層のディレクトリ

パストラバーサルとは

たとえば、いくつかのファイルをホストするアプリケーションがあり、それらを次の形式でリクエストできると仮定します。

```
http://example.com/file=report.pdf
```

以下のサーバ上にホストされているファイルをダウンロードすることができる

```
/var/www/download_contents/report.pdf
```

ここにパストラバーサルの脆弱性が含まれていると

```
http://example.com/file=../../../../../etc/passwd
```

例えば、このようにディレクトリを遡って本来ダウンロードできてはいけないファイルをダウンロードすることができてしまいます。

`/etc/passwd`

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
...
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
```

アプリケーションの作りによっては、

- ファイルの上書き
- ファイルの削除

などもできてしまいます。

課題

パストラバーサルの2〜4の課題をやっていきましょう

http://localhost:8080/WebGoat/start.mvc#lesson/PathTraversal.lesson/0

正解例

2

- `Full Name:` に `../test` を入力
- ユーザ名と同じディレクトリ階層にファイルが作られてしまうことを確認

3

- `Full Name:` に `...../test` を入力
- ユーザ名と同じディレクトリ階層にファイルが作られてしまうことを確認

正解例

4

- http://localhost:8080/WebGoat/PathTraversal/profile-upload-remove-user-input に送っているmultipartリクエストのボディの `filename` に `../[画像ファイル名]` を入力
- ユーザ名と同じディレクトリ階層にファイルが作られてしまうことを確認

```
------WebKitFormBoundaryPWtaWgA5KtF5eGal
Content-Disposition: form-data; name="uploadedFileRemoveUserInput"; filename="../9.jpg"
Content-Type: image/jpeg
```