


セキュリティ基礎

セキュアコーディング入門

自己紹介

- 名前: 高橋雄紀 @takapi86
- 所属: GMOペパボ EC事業部 カラーミーショップグループ DXチーム
 - 開発基盤の改善、コンテナ化、セキュリティ改善など

講義の形式

- 基本は座学で進め講義を行い、デモは動画で流します
- わからないこと、質問がある場合は適宜チャット欄にコメントしてもらって大丈夫です

- 思ったこと、感想などもチャット欄にコメントはしてもらってOKです

セキュアコーディングとは

攻撃者やマルウェアなどの攻撃に耐えられる、堅牢なプログラムを書くこと

- 今回は Webのアプリケーション のセキュアコーディングについてお話していきます。

なぜセキュアコーディングを学ぶのか

我々はWebサービスの開発を行っており、日常的にプログラム修正・リリースを行っている

- リリースを行うということは、サービスに変更を加えている
- 変更した内容に脆弱性が含まれた場合、Webサービスが脅威に晒されることになる
- 日々の開発で脆弱性が混入しないよう、セキュアコーディングを覚え事故を未然に防ぐこと大事

今回学ぶ脆弱性とその対策方法

Webアプリケーションの脆弱性は多種多様ありますが、今回は代表的な以下の脆弱性と修正方法を学びます。

- SQLインジェクション
- クロスサイトスクリプティング (XSS)
- クロスサイトリクエストフォージェリ (CSRF)

PHPのコードを用いて説明していきます。

前提

- HTML
- JavaScript
- SQL
- HTTPのリクエスト・レスポンスの仕組み
- Cookie・セッション

この辺りがわかっていること

(今わからなくても、あとで復習してもらえればOKです👉)

用語をおさらい

- エスケープ処理
 - マークアップ言語やプログラミング言語、スクリプト言語等で文字列を扱う際に、その言語にとって特別な意味を持つ文字や記号を、別の文字列に置き換えること
 - sql(mysql) ' => \'
 - html ' => ' (HTMLエンティティ)

SQLインジェクション

SQLインジェクションとは

どんな攻撃か

外部から悪意を持って細工されたSQL文を埋め込まれ、データベースが不正に操作されてしまう脆弱性

どのような影響があるか

- DBに入っている情報が流出する・書き換えられる
- 認証が回避される

など

脆弱性のあるコード例

```
// 外部から入力された値(name)をそのまま入れている。  
$sql = "SELECT * FROM users WHERE name = '" . $_GET["name"] . "'";  
$stmt = $dbh->prepare($sql);  
$stmt->execute();
```

たとえば、このようにSQLに直接値を入れるようなコードは脆弱性が含まれております。

※ `$_GET` は、PHPではクエリパラメータをサーバ側で受け取る際に使います。このケースでは `https://www.example.com/index.php?name=XXXXX` というリクエストが送られたケースを想定しています。

この場合 `$_GET["name"]` に `' OR 1=1; --` という文字列を渡すと . . .

```
SELECT * FROM users WHERE name = '' OR 1=1; -- '
```

条件として、

- nameが空文字であること
か
- 1が1であること

の条件を満たすもの、つまりusersテーブルの内容全件が抽出されてしまう。

脆弱性のあるコード例

他にはどんなことができてしまうか . . .

- `$_GET["name"]` に `' ; DROP databases app --` という文字列を渡すと . . .



appというデータベースすべてのデータを削除できてしまいます。

- `$_GET["name"]` に `' ; UPDATE users SET name = 'cracked!' --` という文字列を渡すと . . .

nameの内容が更新され、レコードの内容を改ざんすることができています。

=> つまり、侵入したWebアプリケーションが使っているDBの権限の範囲であれば何でもできてしまう

対策

- プレースホルダを使うことで暗黙的にエスケープする（後ほど説明します）
- 直接文字列をエスケープする
 - 言語・ライブラリの用意している専用のエスケープ処理を使いましょう。（独自でエスケープの実装はしないのが望ましい）
- SQLインジェクション対策が行われているフレームワークを使う（後ほど説明します）
 - Ruby  . . . Ruby on Rails (Active Record)
 - PHP  . . . Laravel (Eloquent)

デモ

SQLインジェクションの再現からコードの修正まで

<https://www.youtube.com/watch?v=iNFnNO3sb4k>

修正例

プレースホルダを使う修正例

`:name` を置き換えるようにする。

```
$sql = "SELECT * FROM users WHERE name = :name";  
$statement = $dbh->prepare($sql);  
$statement->execute(  
    [':name' => $_GET["name"]]  
);
```

Laravel (Eloquent) を使う修正例

```
// (Usersモデルを作った上で)  
$user = Users::where('name', $_GET["name"])->first();
```


保険的対策

- 入力値のチェックを行う
 - 入力値が正しい形式かどうかをチェックすることで、結果的にSQLインジェクションを防ぐ効果もある。（ただし、根本解決にはならないので、先ほど説明した根本対策を行うようにしましょう。）
- DBの権限設定を適切行う
 - 被害を最小限に抑えるため、Webアプリケーションに必要な最低限の権限のみ与えるようにしましょう。（例えば、読み込み専用のアプリケーションであればSELECTのみ実行できるようにする）


実装時のセルフチェック

まずはコードを確認する

- 入力値のチェックを行う
- SQLに直接値を埋め込んでいる箇所はないか
 - フレームワークを使っている場合、直接SQLを発行するようにしている場合は、エスケープなど対策する必要があるため、注意が必要


実装時のセルフチェック

実際に文字列を入れてみる

- ' や " を含んだ文字列を入れてみる
 - SQLの構文エラーが出たら、SQLインジェクション対策漏れの可能性ありと疑う
- 検査文字列を入れてみる
 - 先程紹介した ' OR 1=1 -- などを入れてみる。
 - 値が画面に出力されないようなものは、sleepを入れて確認してみる。 
 - 例えば、 ' ; select sleep(10); -- を入れて10秒返ってこなかったら、SQLインジェクション対策漏れの可能性ありと疑う

実装時のセルフチェック

ツールを使ってチェック

- `OWASP ZAP` や `sqlmap` のような脆弱性診断ツールを使ってチェックする
 - 外部サイトではやらないように（誤って外部のサイトに攻撃すると悪質な場合逮捕されてしまうケースもあるので注意 )
 - もちろん手動で検証する場合も注意が必要

※ 必ずローカル環境やテスト環境で実行するようにしましょう

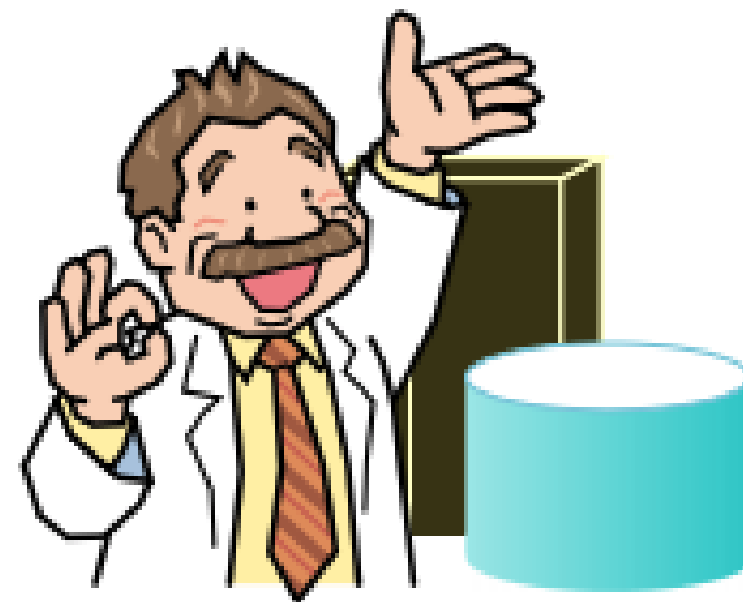
詳しくは

安全なSQLの呼び出し方 をご参照ください

<https://www.ipa.go.jp/files/000017320.pdf>



「安全なウェブサイトの作り方」別冊



クロスサイトスクリプティング (XSS)

クロスサイトスクリプティング (XSS) とは

どんな攻撃か

スクリプトをサイトに送り込み、スクリプトを含むHTMLを出力し、ブラウザ上で実行させる攻撃

どのような影響があるか

- セッションクッキーの値が盗まれ、不正ログインされる
- サイト利用者の権限で、Webアプリケーションの機能を悪用される
- Webサイトの内容が書き換えられ、フィッシングにより個人情報が盗まれる

など

XSSの種類

- 反射型 (Reflected XSS)
 - 外部から入力されたスクリプトが直接実行されてしまうケース
 - 攻撃者が悪意のあるスクリプトを含んだリンクを作成し、ターゲットがリンクを踏んだ時に攻撃が実行される
- 保存型 (Stored XSS)
 - 一度、DBなどに悪意のあるスクリプトを保存し、それが発火してしまうケース
 - 攻撃者が悪意のあるスクリプトを掲示板に保存し、ターゲットが掲示板を開いたときに攻撃が実行される
- DOM型 (DOM Based XSS)
 - サーバ上でのHTMLの生成時には問題はなく、ブラウザ上で動作するJavaScript上のコードに問題があるときに実行されるケース

脆弱性のあるコード例

HTML要素への埋め込み

```
<div><?php echo $_GET["name"] ?></div>
```

属性値の埋め込み

```
<input type="text" name="name" value="<?php echo $_GET["name"] ?>" />
```

リンク (href, src) への埋め込み

```
<a href="<?php echo $_GET["url"] ?>">
```

HTML要素への埋め込み

`</div><script>alert(document.cookie);</script>` を外部から入力

```
<div></div><script>alert(document.cookie);</script></div>
```

属性値の埋め込み

`"><script>alert(document.cookie);</script>` を外部から入力

```
<input type="text" name="name" value=""><script>alert(document.cookie);</script> " />
```

リンク (href, src) への埋め込み

`javascript:alert(document.cookie);` を外部から入力

```
<a href="javascript:alert(document.cookie);">戻る</a>
```

※ `alert(document.cookie);` は、あくまでも一例で、ここに好きなスクリプトを埋め込むことができます。

対策

基本は出力時のエスケープ

- 属性値はダブルクォートで囲う
- メタ文字 `<>"'&` をエスケープ
 - HTML要素・・・`< &` は最低限
 - 属性値・・・`<>"'&` は最低限
 - `src, href`に値を入れるケースの場合は、`javascript`スキームなどが入らないよう、バリデーションを行い、属性値のエスケープをおこないましょう

※ `&` は直接XSSの原因になるわけではありませんが、この文字をエスケープしなければユーザーから入力された `&` を正しく表示できないのでエスケープが必要

デモ

XSSの再現からコードの修正まで

<https://www.youtube.com/watch?v=qUcfaFQyw68>

修正例

PHPには、htmlspecialcharsという関数が用意されているので、それを使います。

HTML要素への埋め込み

```
<div><?php echo htmlspecialchars($_GET["name"], ENT_QUOTES, "UTF-8") ?></div>
```

属性値の埋め込み

```
<input type="text" name="name" value="<?php echo htmlspecialchars($_GET["name"], ENT_QUOTES, "UTF-8") ?>" />
```

修正例

リンク (href, src) への埋め込み

- `http://` `https://` など、意図したURLに限定するようプログラム側でバリデーションをかけましょう

```
// URLのチェック
if (preg_match("/\Ahttps?:/", $url) !== 1) {
    $errorMessage = "不正なURLです";
}
```

- 属性値のエスケープをしましょう

```
<a href="<?php echo htmlspecialchars($_GET["url"], ENT_QUOTES, "UTF-8") ?>">戻る</a>
```

実装時のセルフチェック

実際に文字列を入れてみる

- メタ文字 `<>"&'` を入れてみる
 - エスケープされていなければ、XSS対策漏れの可能性ありと疑う
- 先程紹介した検査文字列を入れてみて、アラートがでないか確認する

ツールを使ってチェック

- OWASP ZAP のような脆弱性診断ツールを使ってチェックする
 - 外部サイトではやらないように注意

保険的対策

入力値のチェックも忘れずに

- 入力チェックを行う（入り口対策）
 - 入力値が正しい形式かどうかをチェックすることで、結果的にXSSを防ぐ効果もある
 - 自由入力欄などは仕様上、チェックするのがむずかしい場合もある
 - 根本解決にはならないので、必ずエスケープして対策を行うようにしましょう
- Session Cookie にhttponly属性をつける
 - スクリプトからクッキーの値を読み込めないようにする

詳しくは

安全なウェブサイトの作り方 をご参照ください

<https://www.ipa.go.jp/files/000017316.pdf>



ウェブアプリケーションのセキュリティ実装と
ウェブサイトの安全性向上のための取り組み



SQLインジェクション、XSSはインジェクション系の脆弱性と呼ばれますが、他にもあります。

- OSコマンドインジェクション
 - メールヘッダインジェクション
 - HTTPヘッダー・インジェクション
 - CSSインジェクション
- ・・・など

基本的に、プログラム側から何かコンテキストの異なるものを組み立てるときには、外部から不正な値が入力されても問題ない作りになっているか疑うようにしましょう。

クロスサイトリクエストフォージェリ (CSRF)

CSRFとは

どんな攻撃か

別のサイトに用意したコンテンツ上の罠のリンクを踏ませること等をきっかけとして、インターネットショッピングの最終決済や退会等Webアプリケーションの「重要な処理」を呼び出すようユーザを誘導する攻撃である。

『IPA セキュア・プログラミング講座』
より引用

<https://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/301.html>



どのような影響があるか

例えば、次のような重要な処理を含む機能に対し、罨のリンクを踏ませることで罨を踏んだ利用者の権限で、意図しない処理を行うことができます。

- 商品の購入
- パスワードやメールアドレスの変更
- 退会処理

など

脆弱性のあるケース

- Webアプリケーションがユーザ・クライアントからのリクエストを十分検証しないで受け取るようになっている
 - どんなリクエストも直接受理されるケース（意図したルート以外からのリクエストが受け付けられてしまうなど）

対策

- 事前にトークンを発行しておき、処理を行う前に検証する
 - 推奨の対策（後ほどご説明します。）
- パスワードを再入力させる
 - 多用しすぎると、煩雑なアプリケーションになってしまう
 - パスワード変更など、限定して使うのが良いでしょう
- Refererでチェックする（非推奨）
 - 多くのブラウザはウェブページ画面遷移時に前のページのURLをリクエストヘッダーに付与します。これを利用し意図したサイトから遷移してきているかチェックすることができます。
 - Refererを送信しないブラウザや設定で無効にしている場合、正常にアプリケーションが動かないため、ユーザを限定するケースにおいては有効

デモ

CSRFの再現からコードの修正まで

<https://www.youtube.com/watch?v=BSeZ-z3Cz4w>

対策例

- Formにトークンを埋め込む

```
<form method=post>
  <input type="hidden" name="token" value="予測不可能なトークン" />
  <input type="text" name="password" value="" />
</form>
```

- サーバ側に送信されてきたトークンを検証

```
if ($_POST["token"] !== $token) {
    $message = "不正リクエストです";
    exit;
}
```

実装時のセルフチェック

- CSRF対策が必要かどうか判断する
 - パスワード変更、退会処理など
- 上記で確認した処理はCSRF対策が行われてるか？
 - curlで対象の画面のリクエストを直接叩いてみる
 - デベロッパーツールなどで、HTMLにレンダリングされているトークンを変えて操作してみる

詳しくは

安全なウェブサイトの作り方 を読みましょう

<https://www.ipa.go.jp/files/000017316.pdf>



開発のサイクルにセキュリティチェックを組み込もう

- 実装時、コードレビュー時のセキュリティチェック（今回はこのお話）
 - チェックリストがあると良い
- 静的スキャン
 - Java・・・JTest
 - Ruby・・・brakeman
- 動的スキャン
 - AppScan, Owasp Zap, Vaddyなど
- ライブラリ脆弱性チェック（GitHubセキュリティアラート、Trivy）
- 定期的な外部の診断
 - 外部セキュリティ診断会社での脆弱性診断

もし、緊急度の高い脆弱性を見つけてしまったら

すぐに上長などに報告しましょう

- （報告する人）報告して怒られないかな？など躊躇するかもしれませんが、強い気持ちを持って報告しましょう💪
 - スルーしないこと
- （報告される人）報告しやすい環境づくりをしていきましょう
 - 報告されたら怒ったりしないこと、見つけてくれたことに感謝しましょう

セキュリティ基礎

セキュアコーディング入門

研修は以上です。

ご清聴、ありがとうございました。