おさらい演習

2021. 05. 26

2021. 05. 26 ①

【セキュリティ強化】
以下は「CSRF(クロスサイトリクエストフォージェリ)」対策の簡単な例です。
CSRFとは「サイト横断的に（Cross Site）リクエストを偽装（Request Forgeries）する」攻撃

1. 以前作ったログインの演習プログラムにて
   ログイン直後に「session_regenerate_id()」を追加しなさい。
   https://www.php.net/manual/ja/function.session-regenerate-id.php
2. 以前作ったログアウトを行うユーザー関数「logout」の最後に「session_destroy ()」を追加しなさい。
   https://www.php.net/manual/ja/function.session-destroy.php
3. 参考ページの「CsrfValidator」クラスをfunctions.phpに追加しなさい。
   https://qiita.com/mpyw/items/8f8989f8575159ce95fc
4. マイページのformタグ内に以下を追加しなさい。
   <input type="hidden" name="token" value="<?=CsrfValidator::generate()?>">
5. マイページのsession_start()後に参考ページの検証するとき(返り値チェックタイプ)を追加しなさい。

いろいろなシステム攻撃とセキュリティ対策

【ゼロディ攻撃】

新たな脆弱性（セキュリティホール）が発見されたときに、問題の公表や修正プログラムが提供される前に行われるサイバー攻撃

【インジェクション攻撃】

悪意のある攻撃者は、無効なデータ（バグ）などの脆弱（ぜいじゃく）性の高いプログラムにソースコードを注入して不正な命令を実行し、プログラムを改変する。

【フィッシング】

インターネットのユーザから経済的価値がある情報（例: ユーザ名・パスワード・クレジットカード情報）を奪うために行われる詐欺行為

【スプーフィング】

他のユーザーの情報（IDやパスワード）を盗み出して他のユーザーとして活動し、情報を漏えいさせたり、コミュニティなどに悪意のある書き込み

【二要素認証】

「ID」と「パスワード」の認証に加えて、「指紋」などの生体情報、SMSなど”全く違う要素の認証を複数組み合わせた認証”を行うこと。IDとパスワードの認証を2回行うのでは二要素認証にはならない。

【二段階認証】

違う方法であれ、同じ方法であれ、2回の認証を行うこと。「ID」と「パスワード」という認証を2回行うことも二段階認証となる。

【CAPTCHA】

ログインや登録で次のステップに進むときに確認のため文字入力を要求して、人間の目ではなんとか読み取れてもプログラムでは自動に判読が難しい「歪んだ文字」の画像を表示して認証する仕組み

【reCAPTCHA】

ウェブサービスの画面で表示される「私はロボットではありません」とは、左隣のチェックボックスをオンにすることで悪質なプログラムによるサービスへの侵入や乱用を防ぐ仕組み

2021. 05. 26 ②

【SEO】
以下は「検索エンジン」対策（SEO）の簡単な例です。

6. HTMLファイルを用意しなさい。
7. headタグ内に次ページの内容を追加しなさい。
8. 検索させたい言葉を大項目、中項目、小項目の順に用意しなさい。
9. 上記　3項目を<h1><h2><h3>の順にheaderタグ内に追加しなさい。
10. 本文、フッター内にも3の項目が入るようにしなさい。

headタグ内の追記事項

```
 <meta name="viewport" content="width=device-width">
<meta name="robots" content="index,  follow">
<meta name=“description” content=“概要">
<meta name="keywords" content="キーワード">
<meta name="format-detection" content="telephone=no">
<meta http-equiv="X-UA-Compatible" content="IE=edge"><!--IE対策-->
<!-- ▼OGPの設定 -->
<meta property="og:type" content="article">
<meta property="og:title" content="概要">
<meta property="og:description" content="運営団体">
<meta property="og:locale" content="ja_JP">
<!-- ▼Twitter Cardsの設定-->
<meta name="twitter:card" content="summary"><!--大きい画像があればsummary_large_image-->
<meta name="twitter:site" content="概要">
```