Webアプリケーション原案

残高管理×残高競争アプリケーション

法政大学理工学部応用情報工学科　ネットワーク応用研究室

野尻明理（学籍番号 20X3128 ）

更新日 2022/10/06

システム概要

以下のような銀行口座の残高管理と他者と残高を比較できるサービスを作成する.

アカウント作成時に氏名，生年月日，性別，口座番号，残高，
ID，パスワードを入力

データベースでアカウントごとの残高情報を管理（入出金があると更新される）

WebAPIとして残高が近しい人同士で比較した残高ランキングを取得できる

データベースに追加するデータ

データベースには以下のデータを追加する.

＜ユーザテーブル＞
- 生年月日
- 性別
- パスワード
- 氏名
- ID

＜取引テーブル＞
- 残高
- 入金金額
- 出金金額
- 氏名
- ID

＜残高テーブル＞
- 口座番号
- 残高
- 残高差額
- 氏名
- ID

※「ID」によって3つのテーブルを結び付ける

WebAPIで発信するデータ

WebAPIでは以下のJSON形式のデータを発信する。

```
{
    “username”: “abcde123”,        →アカウント名（半角小文字英数字）
    “sex”: “men”,                  →性別（men/woman）
    ”age“: ”20“,                   →年齢
    "record":[{
        “day”: “yyyy:MM:dd”,       →残高が更新された日
        “balance ”: 123456,        →口座残高
        “difference”: 123          →前回の残高記録との差分
      } ,{・・・} ,{・・・}]          →更新日（降順）ごとに記録を格納する
}
```

対策するべき脆弱性①

本サービスで対策が必要な脆弱性を記す.

SQLインジェクション（SQL injection）

攻撃者がDBと連動したWebアプリケーション等に対して検索ボックスや入力フォームからDBを操作する不正なSQL文を注入し，データの消去・改ざんを行う攻撃手法.

＜被害の代表例＞

- ✓ 不正ログイン
- ✓ 情報漏洩
- ✓ 情報の改ざん

図1　SQLインジェクションの流れ

出典：https://www.nttpc.co.jp/column/security/sql_injection.html

対策するべき脆弱性②

クロスサイトスクリプティング（Cross Site Scripting＝XSS）

利用者が書き込みできる様なWebサイトに存在する欠陥を悪用し，攻撃者が用意した悪意のあるスクリプトを利用者の元に送り込んで実行させる攻撃手法.

＜被害の代表例＞

- ✓ クッキーの漏洩
- ✓ 有害サイトへジャンプ

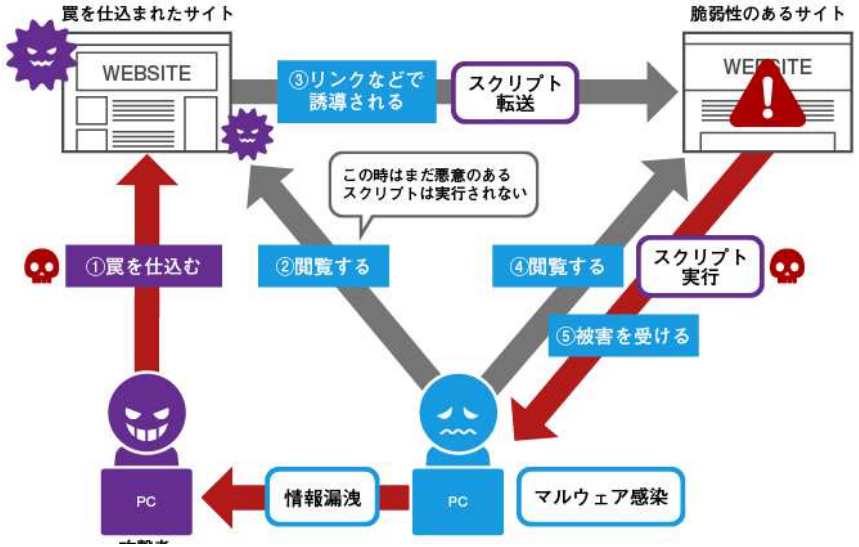

図2　クロスサイトスクリプティングの流れ

出典：https://www.juniper-ne.jp/blog/security/xss.html

対策するべき脆弱性③

クロスサイトリクエストフォージェリ（Cross Site Request Forgeries＝CSRF）

Webブラウザを不正に操作する攻撃手法の一つで，攻撃者は偽装したURLを開かせることで利用者に意図せず特定のサイト上で何らかの操作を行わせる攻撃手法.

＜被害の代表例＞

- ✓ 不正送金
- ✓ 二次的被害

（個人情報流出など）

図3　クロスサイトリクエストフォージェリの流れ

出典：https://activation-service.jp/iso/terms/3006

対策するべき脆弱性④

ディレクトリトラバーサル（Directory Traversal）

ファイル名を扱う様なプログラムに対して特殊な文字列を送信することで，通常はアクセス不可能なファイルの内容を取得するコンピュータシステムへの攻撃手法.

＜被害の代表例＞

- ✓ 情報漏洩
- ✓ データの改ざん・破壊

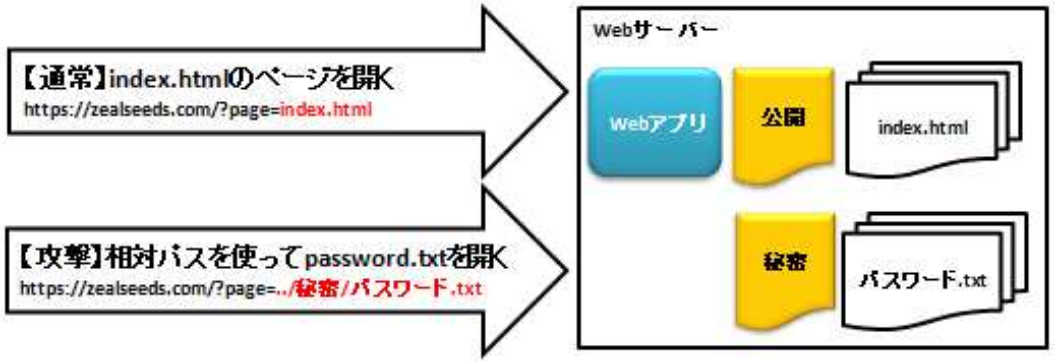

図4　ディレクトリトラバーサルのイメージ

出典：https://learning.zealseeds.com/contents/text/IPA/technology/security/cyber-attack/directory-traversal/index.html

必要な脆弱性対策⑤

クリックジャッキング（Clickjacking）

対象のWebサイトの上に透明に細工した外部サイトを重ねて表示し，利用者に外部サイト上で意図しない操作を行わせる攻撃手法.

＜被害の代表例＞

✓ ログイン後の不正操作

（退会処理など）

✓ フィッシング詐欺

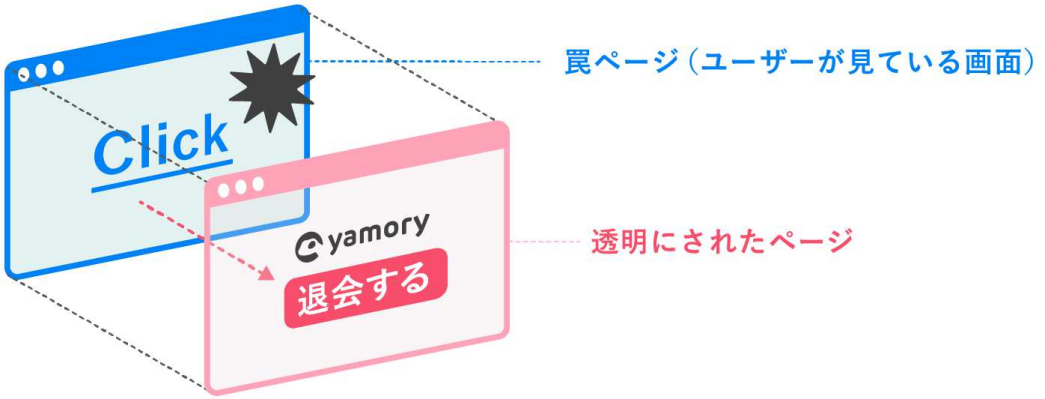

図5　クリックジャッキングのイメージ

出典：https://yamory.io/blog/about-clickjacking/

ファイル遷移

ファイル構成図を以下の図6に示す.

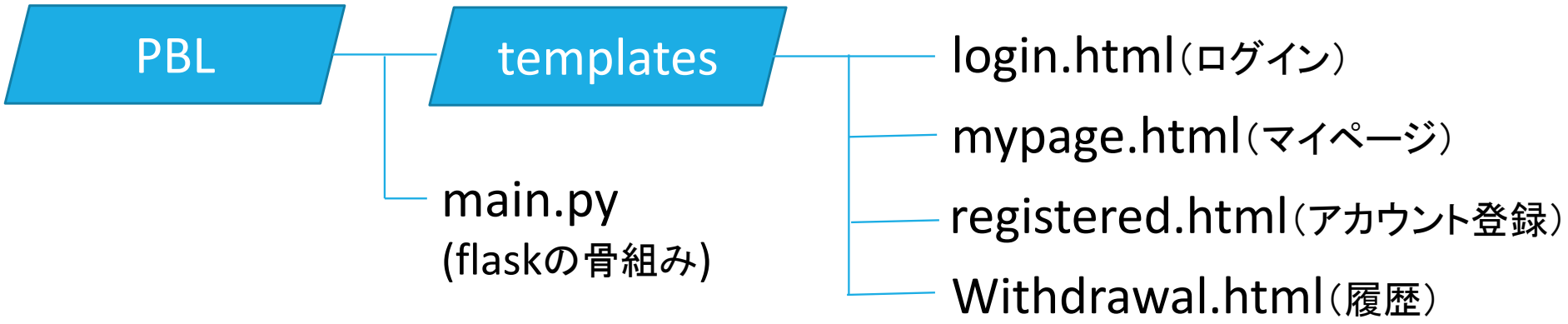

図6　ファイル構成図

参考文献

⑴ 田中直哉，webプログラミング教材，
https://sites.google.com/view/ntanaka1994-web/ホーム，閲覧日 2022/09/30

⑵ Economics Of TEC，WebAPIとは～WebAPIの仕組みと具体例についてご紹介～，
https://it-rpa.hatenablog.com/entry/WebAPI_仕組み，更新日2021/02/03