

1 目的

現代ではゲームサーバ・通販サイトなどのサービスを、ネットワーク知識がなくても容易に解説できるまでになっている。しかし、これらのサービスには脆弱性を意図せず含んでしまう場合があり、アカウント情報が盗まれるなどの被害が出る可能性がある。そのため、本実験では実際に脆弱性を体験し、適切な対策を考察することを目的とする。

2 SQL インジェクションによるデータベースの不正ログイン データベース

データベースは決まった条件で整理されたデータの集まりであり、コンピュータ上で大量のデータを効率よく利用するために使用される。図1にデータベースの例を示す。データベースはテーブル(表)を単位として構成され、カラム(列)、レコード(行)、フィールド(セル)の要素を持つ。カラムにはデータの属性を示し、レコードは1件分のデータのまとめである。フィールドには、実際の個々のデータが格納される。

テーブル	データを「行」と「列」で表す	
カラム	テーブル内の列	
レコード	テーブル内の行	
フィールド	レコード内の1つの項目	
商品コード	商品名	数量
001	アイスクリーム	6
002	サンドウィッチ	3

図1 データベースの名称

SQL インジェクション

SQL(StructuredQueryLanguage)とは、データベースに対してデータの検索・追加・更新・削除といった操作を行うための言語である。SQL インジェクションは、図2のようにアプリケーションがデータベースとやり取りを行う際に、悪意のある SQL コードを挿入することで、不正な操作を実行させる攻撃手法である。この攻撃により、攻撃者はデータベース内の情報を不正に取得、改ざん、削除することが可能となる。



図2 SQL インジェクションの例

実験 1：XAMMP を用いた GET・POST の動作確認

本実験では、 XAMMP を用いて仮想的なサーバを立ち上げて実験を行う。 XAMMP はウェブ開発に必要なソフト Apache, MariaDB(MySQL), PHP, Perl を一括でインストールできるパッケージソフトウェアである。ローカル環境で動作するため、既存のシステムに影響を与える検証が可能である。

以下のリンクより、 XAMMP をインストールする。

<https://www.apachefriends.org/index.html>

図 3 のように、 Start ボタンを押して→ Stop に切り替わった後、 Status マークが緑色になると準備が完了となる。

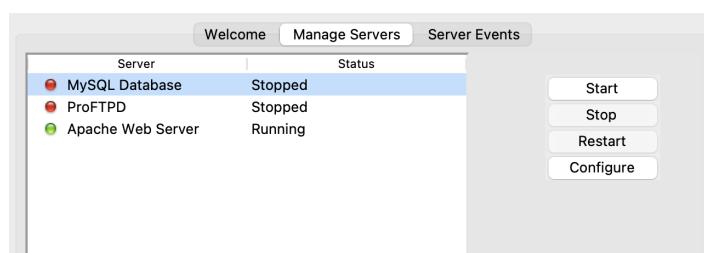


図 3 XAMMP の起動画面

XAMMP インストール後、xampp/htdocs フォルダが生成される。
(デフォルトは C:/xampp/htdocs)
このフォルダに HTML, PHP ファイルなどを置くことで、ブラウザ上からアクセスできるようになる。

(例)

C:/xampp/htdocs/index.html を置く→ブラウザで http://localhost/index.html で動作確認できる。

課題 1

login.html および session.php を作成し、 login.html 上で GET・POST の動作の違いが何か、 URL 欄を見て確認する。また、 GET・POST の使い分けは何か調査し、まとめよ。

login.html をソースコード 1 に示す.

ソースコード 1 login.html

```
1 <html>
2   <head>
3     <title>Login Page</title>
4   </head>
5   <body>
6     <h1>Login</h1>
7     <form action="login.php" method="post">
8       user:<input type="text" name="username" value=""><br />
9       password:<input type="password" name="password" required><br />
10      <input type="submit" name="login" value="Login">
11    </form>
12  </body>
13 </html>
```

session.php をソースコード 2 に示す.

ソースコード 2 session.php

```
1 <?php
2 session_start();
3
4 $_SESSION["loginname"] = $_POST["username"];
5 $_SESSION["pass"] = $_POST["pass"];
6
7 if($_SESSION["loginname"] != "hoge" || $_SESSION["pass"] != "pass"){
8 ?>
9 Login Failed<br />
10
11 <?php
12
13 exit;
14
15 }
16
17 if(isset($_POST["username"])) setcookie("username", $_POST["username"], time
());
18 ?>
19 Login Succeeded<br />
```

2.1 目的

... ...

2.1.1 構成

3 初めに

3.1 背景

... ... SW

3.2 目的

... ...

3.2.1 構成

こんにちは dchweqodejqc フェくいう fdcbwdw

②

平田は自身の LaTeX 講座の集大成として学習ガイドを執筆した [1].

参考文献

- [1] 塚原壮平, 「初めての LaTeX 講座」, 九大新書, 2023.
- [2] 塚原壮平, 「素粒子物理学入門」, きゅうり図書, 2023.