演習6

学号：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

姓名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

(演習6-1)

以下の（）に当てはまる用語を書いてください

- Webアプリケーションにフォームの入力データやパラメータを渡す仕組みとして、（　**GET**　）メソッドと、（　**POST**　）メソッドがある。

- 前者のメソッドは、入力データやパラメータをURLの後ろに付加して送信する方式であり、~~付加されたデータ~~　**処理要求の問合せ**を（　**クエリ**　）文字列と呼び、HTTPアクセスログに記録される

- 後者のメソッドは、入力データやパラメータをメッセージボディにセットし、入力データがHTTPアクセスログに記録されない。そのため、秘匿性は高いが、攻撃が行われたかどうかをHTTPアクセスログから検出することはできない

(演習6-2)

以下の文章の（）に当てはまるのはどれですか？

- 「HTTP は（　**d. ステートレス**　）通信のため，処理単位に通信が切断されるプロトコルである」

a. コラボレーション
b. コネクションフル
c. ステートフル
d. ステートレス

(演習6-3)

- XSS に関する記述として，適切なものはどれですか？

XSS

a. Webサイトの運営者が意図しないスクリプトを含むデータであっても，利用者のブラウザに送ってしまう脆弱性を利用する。

OSコマンドインジェクション

b. Webページの入力項目にOSの操作コマンドを埋め込んでWebサーバに送信し，サーバを不正に操作する。

ソーシャルエンジニアリング 社会工程

c. 複数のWebサイトに対して，ログインIDとパスワードを同じものに設定するという利用者の習性を悪用する。

コンピュータウィルス

d. 利用者に有用なソフトウェアと見せかけて，悪意のあるソフトウェアをインストールさせ，利用者のコンピュータに侵入する。

伪装成对使用者有用的软件，安装恶意的软件，侵入使用者的计算机。

(演習6-4)

- XSSに関する記述として，適切なものはどれですか？

a. **XSS**
Webページに，ユーザの入力データをそのまま表示するフォーム又は処理があるとき，第三者が悪意あるスクリプトを埋め込むことでクッキーなどのデータを盗み出す。

b. **セッションハイジャック**
サーバとクライアント間の正規のセッションに割り込んで，正規のクライアントに成りすますことで，サーバ内のデータを盗み出す。

c. **SQLインジェクション**
データベースに連携しているWebページのユーザ入力領域に悪意あるSQLコマンドを埋め込み，サーバ内のデータを盗み出す。

d. **フィッシング** Fishing
電子メールを介して偽のWebサイトに誘導し，個人情報を盗み出す。

(演習6-5)

- XSS の対策などで用いられ，処理の誤動作を招かないように，利用者がWebサイトに入力した内容に含まれる有害な文字列を無害な文字列に置き換えることを何と呼ぶでしょうか？

a. ストリーミング
b. テザリング
c. サニタイジング
d. リバースエンジニアリング

(演習6-6)

- Webサーバに対するアクセスが，どのPCからのものであるかを識別するために，Webサーバの指示によってブラウザにユーザ情報などを保存する仕組みはどれですか？

a. CGI
b. cookie
c. SSL
d. URL

(演習6-7)

- SQLインジェクションの説明はどれですか？

SQLインジェクション

a. Webアプリケーションに問題があるとき，データベースに悪意のある問合せや操作を行う命令文を入力して，データベースのデータを改ざんしたり不正に取得したりする攻撃

CSRF

b. 悪意のあるスクリプトを埋め込んだWebページを訪問者に閲覧させて，別のWebサイトで，その訪問者が意図しない操作を行わせる攻撃

SQL Slammer （ワーム）

c. 市販されているDBMSの脆弱性を利用することによって，宿主となるデータベーサーバを探して自己伝染を繰り返し，インターネットのトラフイツクを急増させる攻撃

XSS

d. 訪問者の入力データをそのまま画面に表示するWebサイトに対して，悪意のあるスクリプトを埋め込んだ入力データを送ることによって，訪問者のブラウザで実行させる攻撃

(演習6-8)

- SQLインジェクションによる攻撃を防ぐ方法はどれですか？

a. 入力中の文字がデータベースへの問合せや操作において，特別な意味をもつ文字として解釈されないようにする。

b. 入力にHTMLタグが含まれていたら，HTMLタグとして解釈されない他の文字列に置き換える。

c. 入力に，上位ディレクトリを指定する文字(../)を含むときは受け付けない。

d. 入力の全体の長さが制限を超えているときは受け付けない。

(演習6-9)

- 悪意のあるスクリプトを埋め込んだWebページを訪問者に閲覧させて，別のWebサイトで，その訪問者が意図しない操作を行わせる攻撃はどれですか？

a. なりすまし
b. XSS
c. CSRF
d. SQLインジェクション
e. 認証回避

(演習6-10)

- Webアプリケーションのセッションが攻撃者に乗っ取られ，攻撃者が乗っ取ったセッションを利用してアクセスした場合でも，個人情報の漏えいなどの被害が拡大しないようにするために，Webアプリケーションが重要な情報をWebブラウザに送信する直前に行う対策として，最も適切なものはどれか。

a. Webブラウザとの間の通信を暗号化する。
b. 発行済セッションIDをCookieに格納する。
c. 発行済セッションIDをURLに設定する。
d. パスワードによる利用者認証を行う。