情報ネットワークⅡ（情213）

【第12回】

Webセキュリティ（1）

（教科書：第8章）

担当教員：長田智和

E-Mail: nagayan@ie.u-ryukyu.ac.jp

URL: http://n-lab.info/

（講義日：2018年1月11日）

第8章：Webセキュリティ（1）

8.1 Web技術の復習

- 8.1.1 Webの基本的な構成要素
  - Web（World Wide Web）
    - 文章等の情報を管理するシステム。複数のWebページの集まりがWebサイト。
  - HTML（Hyper Text Markup Language）
    - 文章の構造や単純な見た目を記述。文章中に文字以外のデータやハイパーリンクを埋め込むことが可能。

      2012年にHTML5が登場。
  - HTTP（Hyper Text Transfer Protocol）
    - WebクライアントとWebサーバーとの間で通信を行うための通信プロトコル。

8.1 Web技術の復習

- 8.1.1 Webの基本的な構成要素
  - Webクライアント
    - WebページデータからWebページのレイアウトを解析して、Webページを表示する。一般的にはWebブラウザのこと。
    - 例）Internet Explorer, Firefox, Google Chrome, Safari, etc.
  - Webサーバー
    - Webクライアントからの要求に応じて、Webページデータを応答する。
    - 例）Apache, Nginx, Microsoft IIS, etc.
  - Webアプリケーションサーバー
    - 動的にWebページを作成するシステム（後述）

8.1 Web技術の復習

- 8.1.2 HTTP通信でのデータの受け渡し
  - 静的なWebページ
    - Webサーバー上のHTMLファイルがWebクライアントにダウンロードされ、Webブラウザで表示される。
  - 動的なWebページ
    - Webサーバーを経由してWebアプリケーションサーバーにより動的に生成されるWebページがWebクライアントにダウンロードされ、Webブラウザで表示される。

8.1 Web技術の復習

- 8.1.2 HTTP通信でのデータの受け渡し
  - WebブラウザはWebサーバーにデータを転送可能
    - ２つの方法：「GETメソッド」と「POSTメソッド」
    - GETメソッド
      - ファイル等のリソースや、Formタグ等で取得したパラメータをURI（Uniform Resource Identifier）で渡す場合。
      - 例）http://n-lab.info/search.php?username=taro
    - POSTメソッド
      - パラメータをURIで渡さない場合。（パラメータはHTMLリクエストのbody部に挿入される）
- （教科書p.207の図8.1-8.2を参照）

8.1 Web技術の復習

- 8.1.2 HTTP通信でのデータの受け渡し
  - クエリ文字列に対するセキュリティ上の注意
    - クエリ文字列は平文で送信されるため、盗聴や改竄などの問題を回避するため、HTTP通信をSSL/TLSで保護する。
    - Webサーバーやプロキシサーバーのアクセスログ等にクエリー文字列が記録されている場合がある。

      → GETメソッドではなく、POSTメソッドを用いる。

8.1 Web技術の復習

- 8.1.3 Webアプリケーションサーバー
  - 要素技術と3階層システム
    - Webブラウザにユーザインターフェースや画面デザインを提供するソフトウェア（フロントエンド）
    - DBMSなどのソフトウェア（バックエンド）
    - 上記の中間に配置されてロジックと呼ばれる振る舞いを記述したソフトウェア
  - Webアプリケーションサーバーの実現方式
    - サーバー側で実行：CGI（Common Gateway Interface），PHP, Java Servlet, JSP（Java Server Pages），ASP（Active Server Pages）など
    - クライアント側で実行：Java Script, Java Applet, FLASH, etc.
- （教科書p.211の表8.1を参照）

8.1 Web技術の復習

- 8.1.3 Webアプリケーションサーバー
  - Webアプリケーションサーバーの例1
    - サーバー側で実行する例
    - （教科書で説明）
  - Webアプリケーションサーバーの例2
    - クライアント側で実行する例
    - （教科書で説明）
- （教科書p.212-213の図8.3-8.4を参照）

8.2 Webにおける認証

- 8.2.1 Basic/Digest認証
  - Webサーバーもしくは Webアプリケーションサーバーにあらかじめ登録しておいたユーザー名とパスワードをWebブラウザからのリクエストの際のHTTPヘッダに埋め込む方式（RFC2617）
  - Basic認証:
    - ユーザー名とパスワードはBase64で符号化
  - Digest認証:
    - サーバーからのChallengeとパスワード等をハッシュ化したものをResponseとして返信（3.3.2項を参照）
- （教科書p.216の図8.5を参照）

8.2 Webにおける認証

- 8.2.2 クッキーを用いるセッション管理と認証
  - HTTPクッキー：ユーザー識別やセッション管理等を行うための最大4キロバイト程度の情報。
    - Webアプリケーションサーバーで生成され、Webブラウザに発行される。
    - Webブラウザはクッキーを保存し、Webアプリケーションサーバーにアクセスする際、HTMLヘッダにクッキー情報を含めて送信する。
- （教科書p.217-218の図8.6-8.7を参照）

8.2 Webにおける認証

- 8.2.2 クッキーを用いるセッション管理と認証
  - クッキーの漏洩防止とsecure属性
    - クッキーは発行したWebサーバーにのみ返される。
    - クッキーが漏洩すると第三者の「なりすまし」に利用される。
    - クッキーで認証されたセッションはSSL/TLSで保護する。
    - クッキーの属性
      - secure属性: SSL/TLS通信路でのみクッキーを送信
      - HttpOnlly属性: JavaScriptなどからのクッキー読み出しを禁止。
- （教科書p.218-219の図8.8-8.9を参照）

8.3 XSS攻撃とその対策

- 8.3.1 XSS攻撃とは
  - 動的にWebページを生成するWebアプリケーションサーバーにおいて、必要な入力チェックをおこなわないことで、そのサーバーから悪意のあるスクリプトが送信されてしまう脆弱性。そのスクリプトによる攻撃。
- 8.3.2 XSS攻撃の例
  - （教科書で説明）
- （教科書p.221の図8.10-8.11を参照）

8.3 XSS攻撃とその対策

- 8.3.3 反射型XSS攻撃と格納型XSS攻撃
  - 反射型XSS攻撃
    - Webブラウザからのリクエストに含まれるスクリプトを、Webアプリケーションサーバーが元のWebブラウザに送り返す。
  - 格納型XSS攻撃
    - XSS脆弱性のあるWebサイトに攻撃用スクリプトを埋め込んでおき、利用者をそのサイトに誘導する。
- （教科書p.222-223の図8.12-8.14を参照）

8.3 XSS攻撃とその対策

- 8.3.4 XSS攻撃の対策
  - 入力チェック
    - 入力に対してWebブラウザ上又はWebアプリケーションサーバー上で、目的の処理を行う前にチェックする。

      （Webブラウザ上でのチェックは、意味をなさない場合あり）
  - エスケープ処理
    - Webアプリケーションサーバー上で、メタ文字を単純な文字として扱う（変換する）。
  - その他の対策
    - 扱うURIの限定、スクリプトタグの無効化、など。
- （教科書p.224-225の図8.15-8.16,表8.2を参照）

【次回予告】
第13回
Webセキュリティ（2）
（第8章）

また来週！