Web Mechanisms & XSS

HTTP

wireshark = packet capture/analysis

Me

\[ \text{GET} \ /\text{index.html} \]

\[ \text{GET} \ /\text{page.cgi} \ ? \ k=\text{val} \ & \ \text{blah} = \text{foo} \ .... \]

Server

\[ 200 \text{ OK} \]
\[ \text{headers} \]
\[ \text{HTML page...} \]

Chrome:
F12 for developer tools
network tab = requests

\[
\text{HTML} = \ \langle \text{a} \ \text{href} = "...." \rangle \\text{tag} \]

Isn't this nice? \[ \text{URL encoding} \]

27 = hex value of '
3F = hex value of '?'
CWE-79:
"the software does not neutralize or incorrectly neutralizes
user-controllable input before it is placed in output
that is used as a web page that is served to other users"

Example:

```
<p>parsed</p>  -->  search results: parsed
  blat
  bleh
```

examples to
insert:
```
<u>
  <li>fake search result ...
  <form action= ...>
```

Javascript: code executed in the browser
(chrome "console")

```
<Ex>  Window.location = "URL";

Include in document via:
```
  <script type="text/javascript">
    ...
  </script>
```
Cookies: small amount of data stored in browser, associated w/ website

Me

Cookie: header

Server

Set-Cookie: header

Steal via javascript: document.cookie