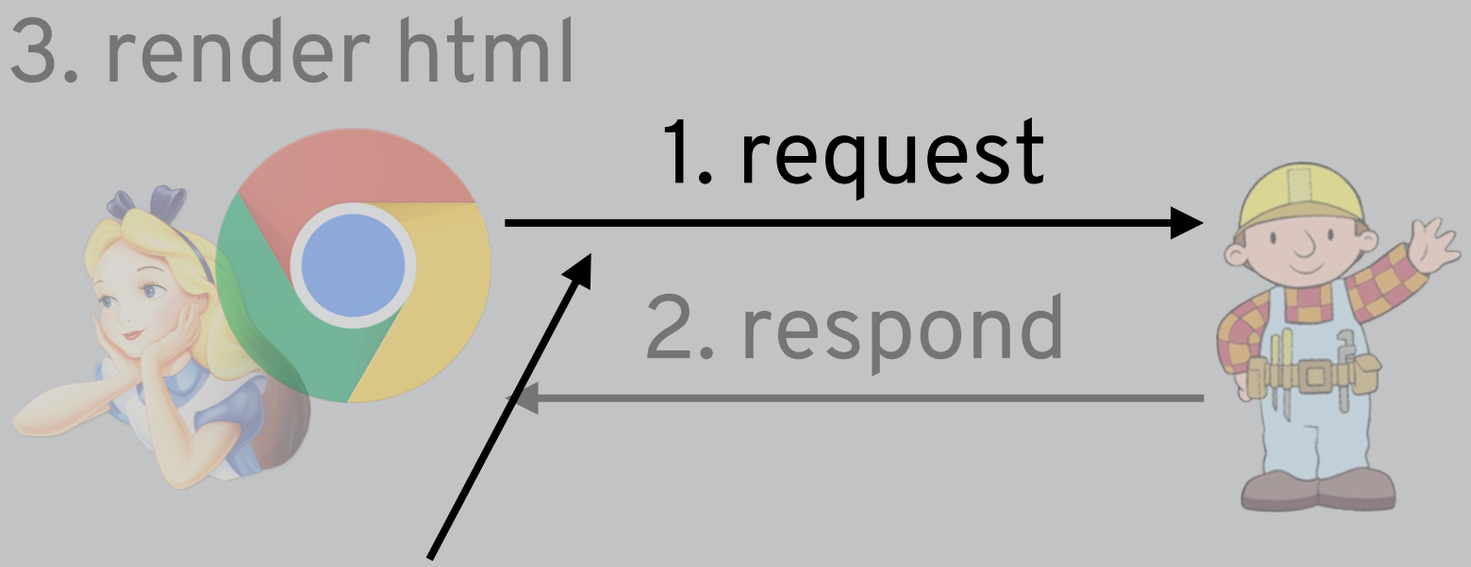
SECURITY (COMP0141):

WEB SECURITY

WEB ARCHITECTURE

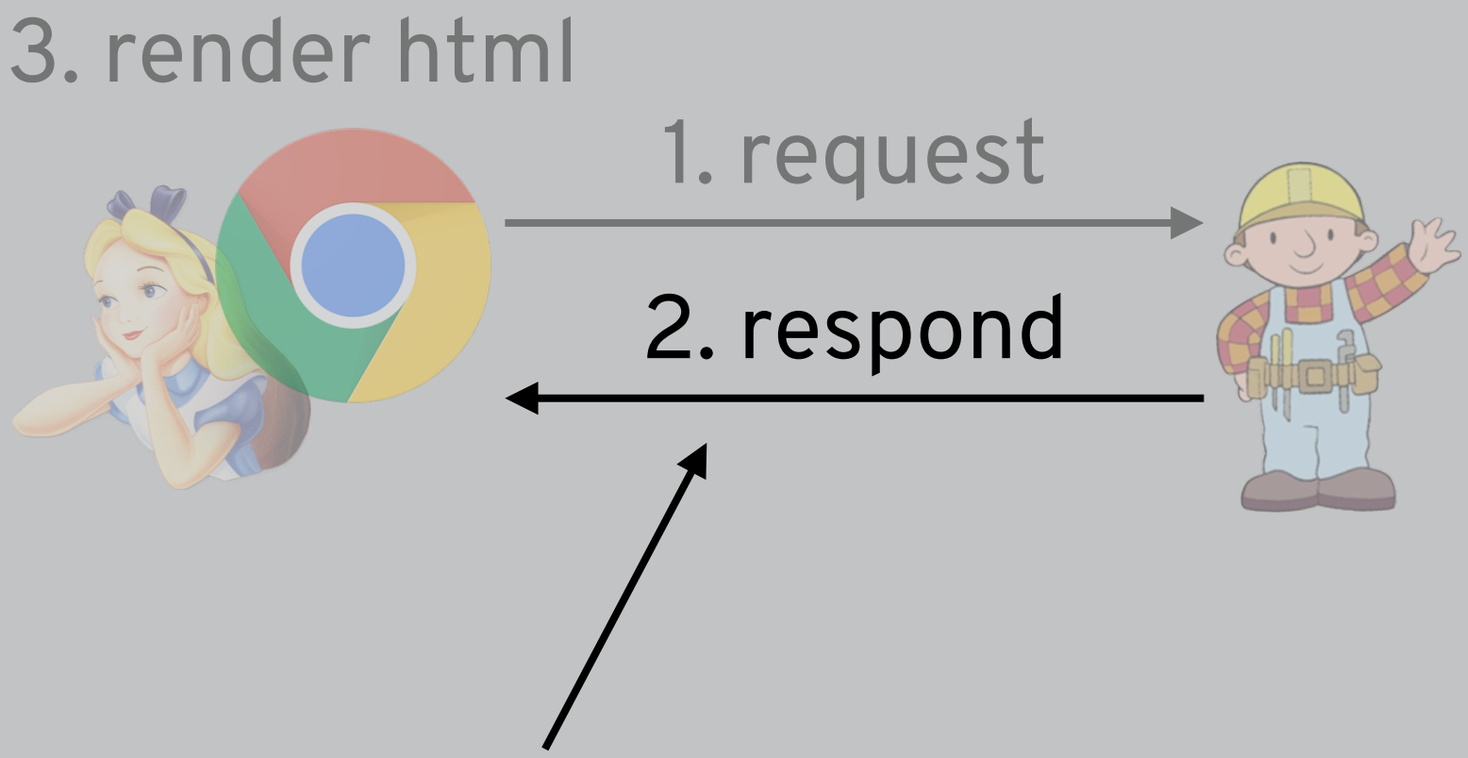
WEB ARCHITECTURE



how? why?

- Alice typed in a URL
- Alice clicked a link
- Alice re-loaded a page
- Web server responded with a redirect
- Web page embedded another page
- Script within web page issued a request

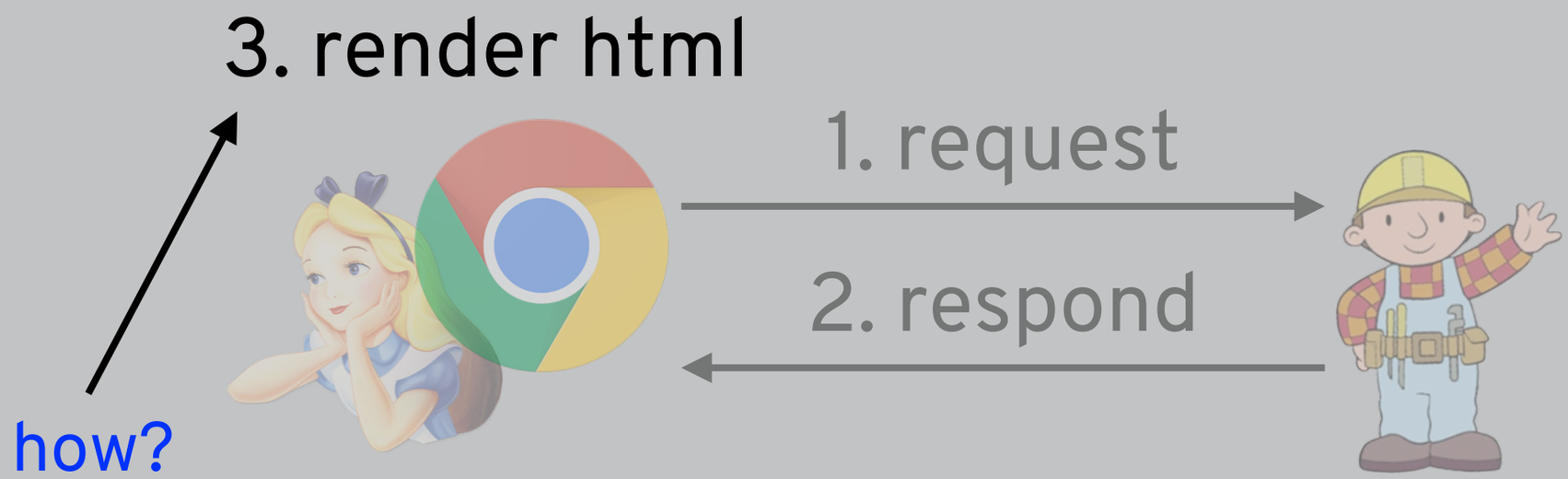
WEB ARCHITECTURE



how?

- returns static file
- invokes a script and returns output
- invokes a plugin

WEB ARCHITECTURE



- renders HTML + CSS
- executes embedded JavaScript
- invokes a plugin

WEB ARCHITECTURE

Websites are programs: HTML + CSS + JavaScript + plugins

HTML: Text with markup and hyperlinks
CSS: Cascading Style Sheets (fonts, colours, etc.)
Javascript: client-side program
Plugins: Java, Flash, etc.

Partially executed by the client (HTML, JavaScript, plugins, etc.)

Partially executed by the server (PHP, Ruby, SQL, etc.)

WEBSITE EXAMPLES

```
    <script type="text/javascript">
      // 27.902kB
      window.viHeadScriptSize = 27.902;
      (function () { var _f=function(e){window.vi=window.vi||{},window.vi.env=Object.freeze(e)};;_f.apply(null,
[{"JKIDD_PATH":"https://a.nytimes.com/svc/nyt/data-
layer","ET2_URL":"https://a.et.nytimes.com","WEDDINGS_PATH":"https://content.api.nytimes.com","GDPR_PATH":"https://us-central1-nyt-wfvi-
prd.cloudfunctions.net/gdpr-email-
form","ABRA_ET_URL":"//et.nytimes.com","NODE_ENV":"production","SENTRY_SAMPLE_RATE":"10","EXPERIMENTAL_ROUTE_PREFIX":"","ENVIRONMENT":"prd",
"RELEASE":"3cc10a2d553a618c5b182ac868d58e1d6106b8f0","AUTH_HOST":"https://myaccount.nytimes.com","SWG_PUBLICATION_ID":"nytimes.com"}]); })
();;
    !function(){if('PerformanceLongTaskTiming' in window){var g=window.__tti={e:[]};
    g.o=new PerformanceObserver(function(l){g.e=g.e.concat(l.getEntries())});
    g.o.observe({entryTypes:['longtask']})}}();
;
    !function(n,e){var t,o,i,c=[],f={passive:!0,capture:!0},r=new Date,a="pointerup",u="pointercancel";function p(n,c){t||(t=c,o=n,i=new
Date,w(e),s())}function s(){o>=0&&o<i-r&&(c.forEach(function(n){n(o,t)}),c=[])}function l(t){if(t.cancelable){var o=(t.timeStamp>1e12?new
Date:performance.now())-t.timeStamp;"pointerdown"==t.type?function(t,o){function i(){p(t,o),r()}function c(){r()}function r()
{e(a,i,f),e(u,c,f)}n(a,i,f),n(u,c,f)}(o,t):p(o,t)}}function w(n)
{["click","mousedown","keydown","touchstart","pointerdown"].forEach(function(e){n(e,l,f)})}w(n),self.perfMetrics=self.perfMetrics||
{},self.perfMetrics.onFirstInputDelay=function(n){c.push(n),s()}}(addEventListener,removeEventListener);
;try {
  var observer = new window.PerformanceObserver(function (list) {
    var entries = list.getEntries();

    for (var i = 0; i < entries.length; i += 1) {
      var entry = entries[i];
      var performance = {};

      performance[entry.name] = Math.round(entry.startTime + entry.duration);
      (window.dataLayer = window.dataLayer || []).push({
        event: "performance",
        pageview: {
          performance: performance
        }
      });
    }
  });
  observer.observe({
    entryTypes: ["paint"]
  });
} catch (e) {};
!function(r,e){var i,a,s,p,c,u=[],
t="object"==typeof r.navigator&&"string"==typeof r.navigator.userAgent&&/iP(ad|hone|od)/.test(
```

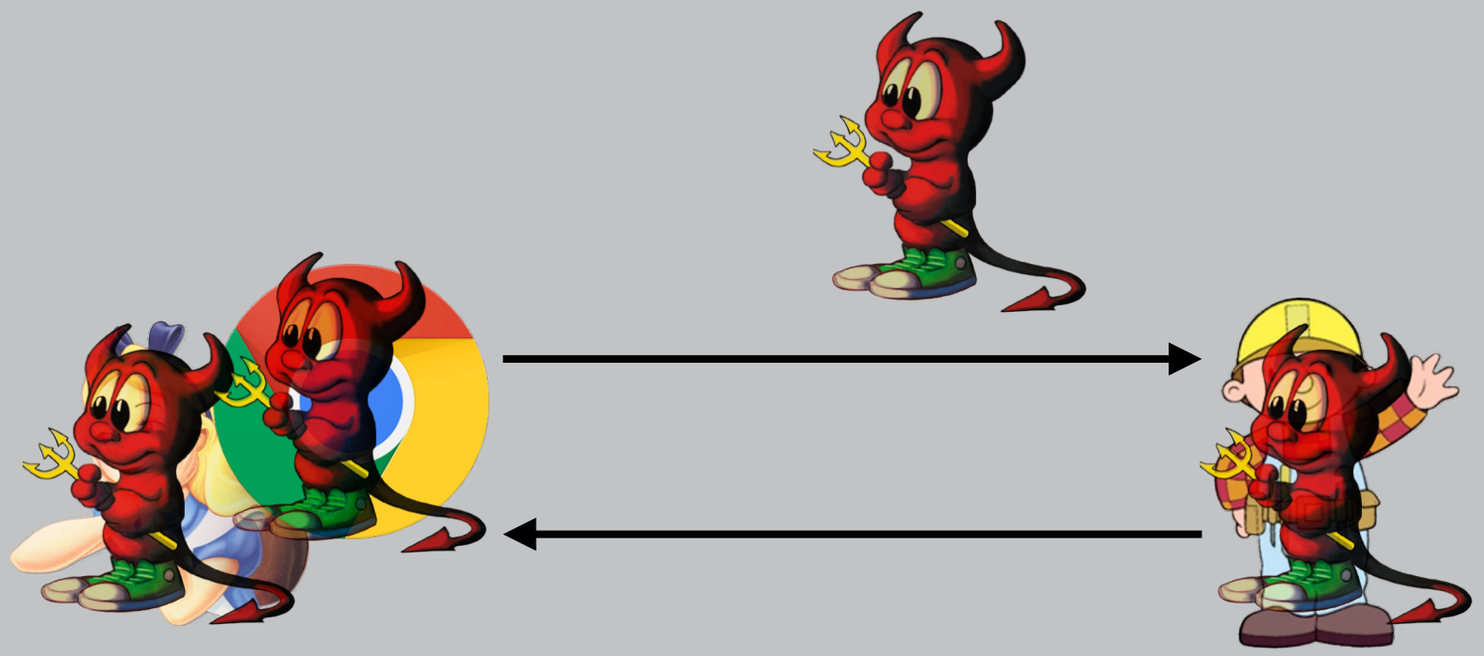
WEB SERVER

Serving static content (HTML + CSS page)

Generating dynamic content

- CGI: PHP, Python, etc.
- Web server modules: Rails, etc.
- Database backend: SQL

THREAT MODEL



Is the server trusted by the browser? or the user?

Is the user trusted by the server? or the browser?

Is the browser trusted by the user? or the server?

Is there an eavesdropper spying on your web traffic?

CIA TRIANGLE