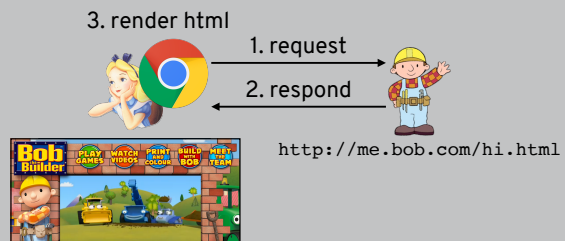


SECURITY (COMP0141): WEB SECURITY



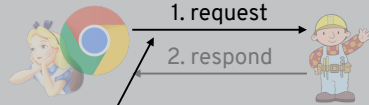
WEB ARCHITECTURE



We've seen that there are three simple steps for getting content in a browser

WEB ARCHITECTURE

3. render html



how? why?

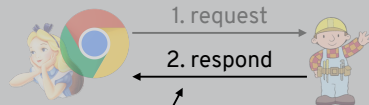
- Alice typed in a URL
- Alice clicked a link
- Alice re-loaded a page
- Web server responded with a redirect
- Web page embedded another page
- Script within web page issued a request

3

Worth digging into each of the steps in a little more detail to understand how and why they happen

WEB ARCHITECTURE

3. render html

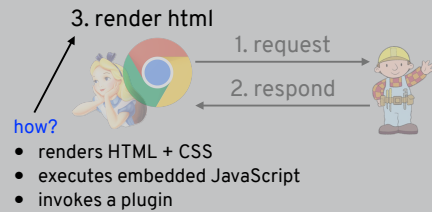


how?

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

4

WEB ARCHITECTURE



5

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.)

6

Just like we saw last time, running programs can be the root of a lot of problems

WEBSITE EXAMPLES

```
<script type="text/javascript">
// 27.902kb
window.onloadScriptSize = 27.902;
(function () { var _f=function(e)(window.vi=window.vi||{}).window.vi.env=Object.freeze(e));_f.apply(null,
["$KID_PATH":"https://a.nytimes.com/web/rpg/data-
layer","RTT_URL":"https://a.nytimes.com","WEDDINGS_PATH":"https://content.api.nytimes.com","GDPR_PATH":"https://us-central1-nyt-vf-w-
prd.cloudfunctions.net/gdpr-email-
form","JABA_ST_URL":"/st.nytimes.com","NODE_ENV":"production","SENTRY_SAMPLE_RATE":"10","EXPERIMENTAL_ROUTE_PREFIX":"","ENVIRONMENT":"prd",
"RELEASE":"3c10a2d55a618c5b182ac68d9e1d6106b8f0","AUTH_HOST":"https://myaccount.nytimes.com","SMG_PUBLICATION_ID":"nytimes.com"]); })
})();
(function(){if('PerformanceLongTaskTiming' in window){var g=window._tti=[{}];
g.o=new PerformanceObserver(function(l){g.o.g.o.concat(l.getEntries());});
g.o.observe({entryTypes:['longtask']});})
}
(function(n,e){var t,o,i,c={},f={passive:10,capture:10},r=new Date,s="pointerup",u="pointercancel";function p(n,e){t|[(t<o,o=n,i=new
Date,w(e,s))]function a(){(o=>{a:1-e(a(c.forEach(function(n){n(o,t)),c=|})function i(t){if(t.cancelable){var on=t.timestamp+127new
Date-performance.now()+t.timestamp;pointerdown"=t.typefunction(t,o){function i(){p(t,o,t)}function z(){
e(a,i,f),e(u,c,f))n(n,i,f),n(u,c,f))o(t),p(o,t))function win
["click","mousedown","keydown","touchstart","pointerdown"],forEach(function(e){n(n,i,f))})n(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,s,s,p,e,u={};
if(typeof r=="string"==typeof s=="string"==typeof t=="string"==typeof u=="string"==typeof v=="string"==typeof w=="string"==typeof x=="string"==typeof y=="string"==typeof z=="string"==typeof aa=="string"==typeof ab=="string"==typeof ac=="string"==typeof ad=="string"==typeof ae=="string"==typeof af=="string"==typeof ag=="string"==typeof ah=="string"==typeof ai=="string"==typeof aj=="string"==typeof ak=="string"==typeof al=="string"==typeof am=="string"==typeof an=="string"==typeof ao=="string"==typeof ap=="string"==typeof aq=="string"==typeof ar=="string"==typeof as=="string"==typeof at=="string"==typeof au=="string"==typeof av=="string"==typeof aw=="string"==typeof ax=="string"==typeof ay=="string"==typeof az=="string"==typeof ba=="string"==typeof bb=="string"==typeof bc=="string"==typeof bd=="string"==typeof be=="string"==typeof bf=="string"==typeof bg=="string"==typeof bh=="string"==typeof bi=="string"==typeof bj=="string"==typeof bk=="string"==typeof bl=="string"==typeof bm=="string"==typeof bn=="string"==typeof bo=="string"==typeof bp=="string"==typeof bq=="string"==typeof br=="string"==typeof bs=="string"==typeof bt=="string"==typeof bu=="string"==typeof bv=="string"==typeof bw=="string"==typeof bx=="string"==typeof by=="string"==typeof bz=="string"==typeof ca=="string"==typeof cb=="string"==typeof cc=="string"==typeof cd=="string"==typeof ce=="string"==typeof cf=="string"==typeof cg=="string"==typeof ch=="string"==typeof ci=="string"==typeof cj=="string"==typeof ck=="string"==typeof cl=="string"==typeof cm=="string"==typeof cn=="string"==typeof co=="string"==typeof cp=="string"==typeof cq=="string"==typeof cr=="string"==typeof cs=="string"==typeof ct=="string"==typeof cu=="string"==typeof cv=="string"==typeof cw=="string"==typeof cx=="string"==typeof cy=="string"==typeof cz=="string"==typeof da=="string"==typeof db=="string"==typeof dc=="string"==typeof dd=="string"==typeof de=="string"==typeof df=="string"==typeof dg=="string"==typeof dh=="string"==typeof di=="string"==typeof dj=="string"==typeof dk=="string"==typeof dl=="string"==typeof dm=="string"==typeof dn=="string"==typeof do=="string"==typeof dp=="string"==typeof dq=="string"==typeof dr=="string"==typeof ds=="string"==typeof dt=="string"==typeof du=="string"==typeof dv=="string"==typeof dw=="string"==typeof dx=="string"==typeof dy=="string"==typeof dz=="string"==typeof ea=="string"==typeof eb=="string"==typeof ec=="string"==typeof ed=="string"==typeof ee=="string"==typeof ef=="string"==typeof eg=="string"==typeof eh=="string"==typeof ei=="string"==typeof ej=="string"==typeof ek=="string"==typeof el=="string"==typeof em=="string"==typeof en=="string"==typeof eo=="string"==typeof ep=="string"==typeof eq=="string"==typeof er=="string"==typeof es=="string"==typeof et=="string"==typeof eu=="string"==typeof ev=="string"==typeof ew=="string"==typeof ex=="string"==typeof ey=="string"==typeof ez=="string"==typeof fa=="string"==typeof fb=="string"==typeof fc=="string"==typeof fd=="string"==typeof fe=="string"==typeof ff=="string"==typeof fg=="string"==typeof fh=="string"==typeof fi=="string"==typeof fj=="string"==typeof fk=="string"==typeof fl=="string"==typeof fm=="string"==typeof fn=="string"==typeof fo=="string"==typeof fp=="string"==typeof fq=="string"==typeof fr=="string"==typeof fs=="string"==typeof ft=="string"==typeof fu=="string"==typeof fv=="string"==typeof fw=="string"==typeof fx=="string"==typeof fy=="string"==typeof fz=="string"==typeof ga=="string"==typeof gb=="string"==typeof gc=="string"==typeof gd=="string"==typeof ge=="string"==typeof gf=="string"==typeof gg=="string"==typeof gh=="string"==typeof gi=="string"==typeof gj=="string"==typeof gk=="string"==typeof gl=="string"==typeof gm=="string"==typeof gn=="string"==typeof go=="string"==typeof gp=="string"==typeof gq=="string"==typeof gr=="string"==typeof gs=="string"==typeof gt=="string"==typeof gu=="string"==typeof gv=="string"==typeof gw=="string"==typeof gx=="string"==typeof gy=="string"==typeof gz=="string"==typeof ha=="string"==typeof hb=="string"==typeof hc=="string"==typeof hd=="string"==typeof he=="string"==typeof hf=="string"==typeof hg=="string"==typeof hh=="string"==typeof hi=="string"==typeof hj=="string"==typeof hk=="string"==typeof hl=="string"==typeof hm=="string"==typeof hn=="string"==typeof ho=="string"==typeof hp=="string"==typeof hq=="string"==typeof hr=="string"==typeof hs=="string"==typeof ht=="string"==typeof hu=="string"==typeof hv=="string"==typeof hw=="string"==typeof hx=="string"==typeof hy=="string"==typeof hz=="string"==typeof ia=="string"==typeof ib=="string"==typeof ic=="string"==typeof id=="string"==typeof ie=="string"==typeof if=="string"==typeof ig=="string"==typeof ih=="string"==typeof ii=="string"==typeof ij=="string"==typeof ik=="string"==typeof il=="string"==typeof im=="string"==typeof in=="string"==typeof io=="string"==typeof ip=="string"==typeof iq=="string"==typeof ir=="string"==typeof is=="string"==typeof it=="string"==typeof iu=="string"==typeof iv=="string"==typeof iw=="string"==typeof ix=="string"==typeof iy=="string"==typeof iz=="string"==typeof ja=="string"==typeof jb=="string"==typeof jc=="string"==typeof jd=="string"==typeof je=="string"==typeof jf=="string"==typeof jg=="string"==typeof jh=="string"==typeof ji=="string"==typeof jj=="string"==typeof jk=="string"==typeof jl=="string"==typeof jm=="string"==typeof jn=="string"==typeof jo=="string"==typeof jp=="string"==typeof jq=="string"==typeof jr=="string"==typeof js=="string"==typeof jt=="string"==typeof ju=="string"==typeof jv=="string"==typeof jw=="string"==typeof jx=="string"==typeof jy=="string"==typeof jz=="string"==typeof ka=="string"==typeof kb=="string"==typeof kc=="string"==typeof kd=="string"==typeof ke=="string"==typeof kf=="string"==typeof kg=="string"==typeof kh=="string"==typeof ki=="string"==typeof kj=="string"==typeof kk=="string"==typeof kl=="string"==typeof km=="string"==typeof kn=="string"==typeof ko=="string"==typeof kp=="string"==typeof kq=="string"==typeof kr=="string"==typeof ks=="string"==typeof kt=="string"==typeof ku=="string"==typeof kv=="string"==typeof kw=="string"==typeof kx=="string"==typeof ky=="string"==typeof kz=="string"==typeof la=="string"==typeof lb=="string"==typeof lc=="string"==typeof ld=="string"==typeof le=="string"==typeof lf=="string"==typeof lg=="string"==typeof lh=="string"==typeof li=="string"==typeof lj=="string"==typeof lk=="string"==typeof ll=="string"==typeof lm=="string"==typeof ln=="string"==typeof lo=="string"==typeof lp=="string"==typeof lq=="string"==typeof lr=="string"==typeof ls=="string"==typeof lt=="string"==typeof lu=="string"==typeof lv=="string"==typeof lw=="string"==typeof lx=="string"==typeof ly=="string"==typeof lz=="string"==typeof ma=="string"==typeof mb=="string"==typeof mc=="string"==typeof md=="string"==typeof me=="string"==typeof mf=="string"==typeof mg=="string"==typeof mh=="string"==typeof mi=="string"==typeof mj=="string"==typeof mk=="string"==typeof ml=="string"==typeof mm=="string"==typeof mn=="string"==typeof mo=="string"==typeof mp=="string"==typeof mq=="string"==typeof mr=="string"==typeof ms=="string"==typeof mt=="string"==typeof mu=="string"==typeof mv=="string"==typeof mw=="string"==typeof mx=="string"==typeof my=="string"==typeof mz=="string"==typeof na=="string"==typeof nb=="string"==typeof nc=="string"==typeof nd=="string"==typeof ne=="string"==typeof nf=="string"==typeof ng=="string"==typeof nh=="string"==typeof ni=="string"==typeof nj=="string"==typeof nk=="string"==typeof nl=="string"==typeof nm=="string"==typeof nn=="string"==typeof no=="string"==typeof np=="string"==typeof nq=="string"==typeof nr=="string"==typeof ns=="string"==typeof nt=="string"==typeof nu=="string"==typeof nv=="string"==typeof nw=="string"==typeof nx=="string"==typeof ny=="string"==typeof nz=="string"==typeof oa=="string"==typeof ob=="string"==typeof oc=="string"==typeof od=="string"==typeof oe=="string"==typeof of=="string"==typeof og=="string"==typeof oh=="string"==typeof oi=="string"==typeof oj=="string"==typeof ok=="string"==typeof ol=="string"==typeof om=="string"==typeof on=="string"==typeof oo=="string"==typeof op=="string"==typeof oq=="string"==typeof or=="string"==typeof os=="string"==typeof ot=="string"==typeof ou=="string"==typeof ov=="string"==typeof ow=="string"==typeof ox=="string"==typeof oy=="string"==typeof oz=="string"==typeof pa=="string"==typeof pb=="string"==typeof pc=="string"==typeof pd=="string"==typeof pe=="string"==typeof pf=="string"==typeof pg=="string"==typeof ph=="string"==typeof pi=="string"==typeof pj=="string"==typeof pk=="string"==typeof pl=="string"==typeof pm=="string"==typeof pn=="string"==typeof po=="string"==typeof pp=="string"==typeof pq=="string"==typeof pr=="string"==typeof ps=="string"==typeof pt=="string"==typeof pu=="string"==typeof pv=="string"==typeof pw=="string"==typeof px=="string"==typeof py=="string"==typeof pz=="string"==typeof qa=="string"==typeof qb=="string"==typeof qc=="string"==typeof qd=="string"==typeof qe=="string"==typeof qf=="string"==typeof qg=="string"==typeof qh=="string"==typeof qi=="string"==typeof qj=="string"==typeof qk=="string"==typeof ql=="string"==typeof qm=="string"==typeof qn=="string"==typeof qo=="string"==typeof qp=="string"==typeof qq=="string"==typeof qr=="string"==typeof qs=="string"==typeof qt=="string"==typeof qu=="string"==typeof qv=="string"==typeof qw=="string"==typeof qx=="string"==typeof qy=="string"==typeof qz=="string"==typeof ra=="string"==typeof rb=="string"==typeof rc=="string"==typeof rd=="string"==typeof re=="string"==typeof rf=="string"==typeof rg=="string"==typeof rh=="string"==typeof ri=="string"==typeof rj=="string"==typeof rk=="string"==typeof rl=="string"==typeof rm=="string"==typeof rn=="string"==typeof ro=="string"==typeof rp=="string"==typeof rq=="string"==typeof rr=="string"==typeof rs=="string"==typeof rt=="string"==typeof ru=="string"==typeof rv=="string"==typeof rw=="string"==typeof rx=="string"==typeof ry=="string"==typeof rz=="string"==typeof sa=="string"==typeof sb=="string"==typeof sc=="string"==typeof sd=="string"==typeof se=="string"==typeof sf=="string"==typeof sg=="string"==typeof sh=="string"==typeof si=="string"==typeof sj=="string"==typeof sk=="string"==typeof sl=="string"==typeof sm=="string"==typeof sn=="string"==typeof so=="string"==typeof sp=="string"==typeof sq=="string"==typeof sr=="string"==typeof ss=="string"==typeof st=="string"==typeof su=="string"==typeof sv=="string"==typeof sw=="string"==typeof sx=="string"==typeof sy=="string"==typeof sz=="string"==typeof ta=="string"==typeof tb=="string"==typeof tc=="string"==typeof td=="string"==typeof te=="string"==typeof tf=="string"==typeof tg=="string"==typeof th=="string"==typeof ti=="string"==typeof tj=="string"==typeof tk=="string"==typeof tl=="string"==typeof tm=="string"==typeof tn=="string"==typeof to=="string"==typeof tp=="string"==typeof tq=="string"==typeof tr=="string"==typeof ts=="string"==typeof tt=="string"==typeof tu=="string"==typeof tv=="string"==typeof tw=="string"==typeof tx=="string"==typeof ty=="string"==typeof tz=="string"==typeof ua=="string"==typeof ub=="string"==typeof uc=="string"==typeof ud=="string"==typeof ue=="string"==typeof uf=="string"==typeof ug=="string"==typeof uh=="string"==typeof ui=="string"==typeof uj=="string"==typeof uk=="string"==typeof ul=="string"==typeof um=="string"==typeof un=="string"==typeof uo=="string"==typeof up=="string"==typeof uq=="string"==typeof ur=="string"==typeof us=="string"==typeof ut=="string"==typeof uu=="string"==typeof uv=="string"==typeof uw=="string"==typeof ux=="string"==typeof uy=="string"==typeof uz=="string"==typeof va=="string"==typeof vb=="string"==typeof vc=="string"==typeof vd=="string"==typeof ve=="string"==typeof vf=="string"==typeof vg=="string"==typeof vh=="string"==typeof vi=="string"==typeof vj=="string"==typeof vk=="string"==typeof vl=="string"==typeof vm=="string"==typeof vn=="string"==typeof vo=="string"==typeof vp=="string"==typeof vq=="string"==typeof vr=="string"==typeof vs=="string"==typeof vt=="string"==typeof vu=="string"==typeof vv=="string"==typeof vw=="string"==typeof vx=="string"==typeof vy=="string"==typeof vz=="string"==typeof wa=="string"==typeof wb=="string"==typeof wc=="string"==typeof wd=="string"==typeof we=="string"==typeof wf=="string"==typeof wg=="string"==typeof wh=="string"==typeof wi=="string"==typeof wj=="string"==typeof wk=="string"==typeof wl=="string"==typeof wm=="string"==typeof wn=="string"==typeof wo=="string"==typeof wp=="string"==typeof wq=="string"==typeof wr=="string"==typeof ws=="string"==typeof wt=="string"==typeof wu=="string"==typeof wv=="string"==typeof ww=="string"==typeof wx=="string"==typeof wy=="string"==typeof wz=="string"==typeof xa=="string"==typeof xb=="string"==typeof xc=="string"==typeof xd=="string"==typeof xe=="string"==typeof xf=="string"==typeof xg=="string"==typeof xh=="string"==typeof xi=="string"==typeof xj=="string"==typeof xk=="string"==typeof xl=="string"==typeof xm=="string"==typeof xn=="string"==typeof xo=="string"==typeof xp=="string"==typeof xq=="string"==typeof xr=="string"==typeof xs=="string"==typeof xt=="string"==typeof xu=="string"==typeof xv=="string"==typeof xw=="string"==typeof xx=="string"==typeof xy=="string"==typeof xz=="string"==typeof ya=="string"==typeof yb=="string"==typeof yc=="string"==typeof yd=="string"==typeof ye=="string"==typeof yf=="string"==typeof yg=="string"==typeof yh=="string"==typeof yi=="string"==typeof yj=="string"==typeof yk=="string"==typeof yl=="string"==typeof ym=="string"==typeof yn=="string"==typeof yo=="string"==typeof yp=="string"==typeof yq=="string"==typeof yr=="string"==typeof ys=="string"==typeof yt=="string"==typeof yu=="string"==typeof yv=="string"==typeof yw=="string"==typeof yx=="string"==typeof yy=="string"==typeof yz=="string"==typeof za=="string"==typeof zb=="string"==typeof zc=="string"==typeof zd=="string"==typeof ze=="string"==typeof zf=="string"==typeof zg=="string"==typeof zh=="string"==typeof zi=="string"==typeof zj=="string"==typeof zk=="string"==typeof zl=="string"==typeof zm=="string"==typeof zn=="string"==typeof zo=="string"==typeof zp=="string"==typeof zq=="string"==typeof zr=="string"==typeof zs=="string"==typeof zt=="string"==typeof zu=="string"==typeof zv=="string"==typeof zw=="string"==typeof zx=="string"==typeof zy=="string"==typeof zz=="string"==typeof }
```

Here's just a little demo to show how complex (and different) websites can be, we've come a long way from simple text and links

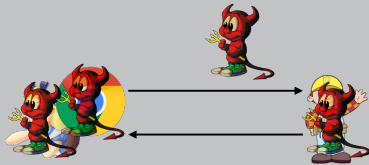
WEB SERVER

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?

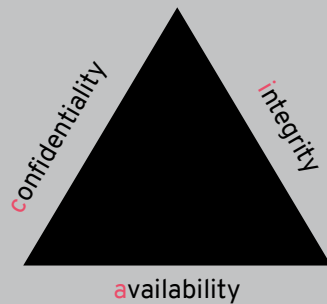
Is the browser trusted by the user? or the server?

Is there an eavesdropper spying on your web traffic?

9

The threat model is very complex here since any component needs to be treated as potentially malicious. We'll explore attacks from all of these different potentially adversaries this week

CIA TRIANGLE



10

Let's go back and revisit these notions of CIA (and in particular confidentiality and integrity) in the context of web security