Free Tools!

Using Developer Tools and Javascript
For Pentesting Webapps

Brian "BB" King - @BBhacKing

Modern Webapp Pentesting

How to Test Webapps In the 2020's

Brian "BB" King - @BBhacKing

"Web 2.0" is *20 Years Old*

The term "Web 2.0" was coined by <u>Darcy DiNucci</u>, an <u>information architecture</u> consultant, **in her January 1999** article "Fragmented Future":[6]

The Web we know now, which loads into a <u>browser window</u> in essentially static screenfuls, is only an embryo of the Web to come. The first glimmerings of Web 2.0 are beginning to appear, and we are just starting to see how that embryo might develop. The Web will be understood not as screenfuls of text and graphics but as a transport mechanism, the ether through which interactivity happens. It will [...] appear on your computer screen, [...] on your TV set [...] your car dashboard [...] your cell phone [...] hand-held game machines [...] maybe even your microwave oven.

https://en.wikipedia.org/wiki/Web_2.0

2011 "50 Websites that Make the Web Great"

Science Daily

Techmeme

Kickstarter

Health Grades

Same Webapps in 2020
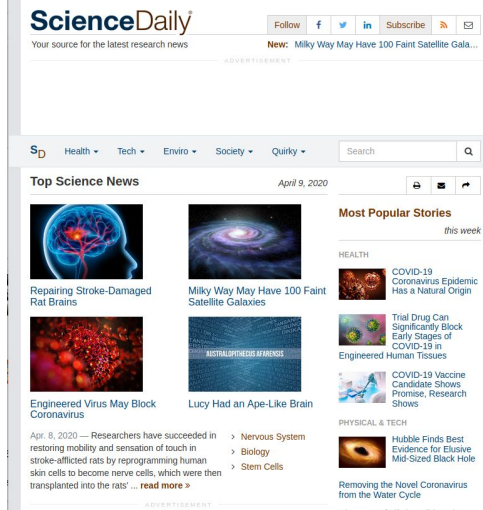
Science Daily
Responsive!
And Pictures!
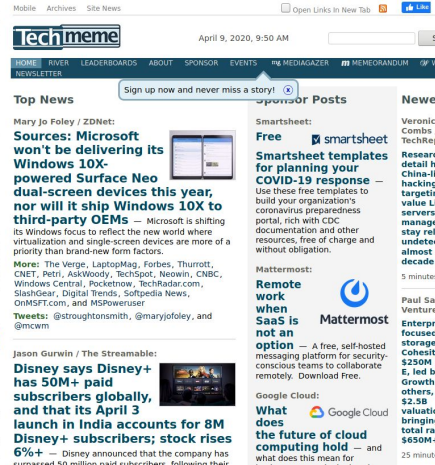
Techmeme
Columns Are Fine!
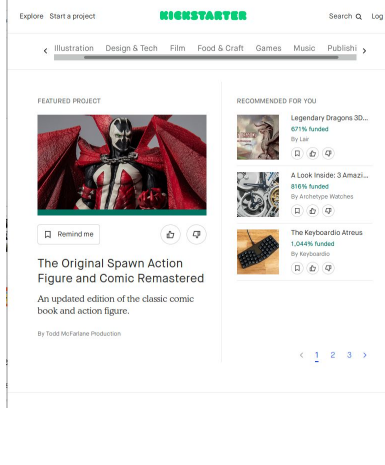
Kickstarter
More Pictures!
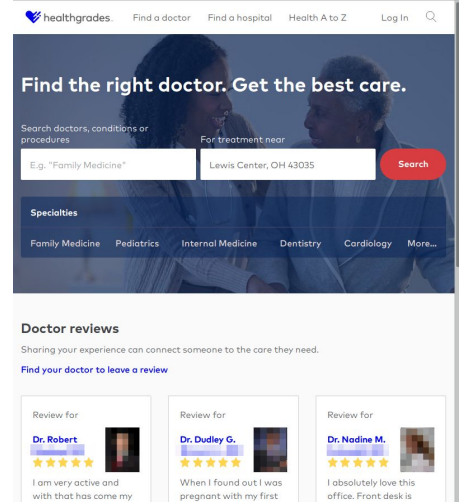
Health Grades
Psychology!

http://content.time.com/time/specials/packages/0,28757,2087815,00.html

Webapps in 2011
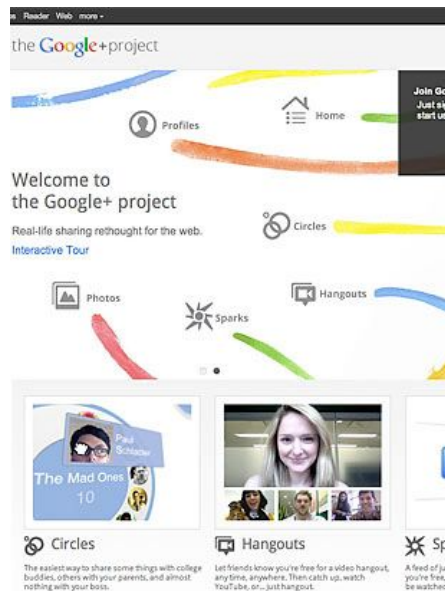
Map My Run

Google+ launches!

Klout
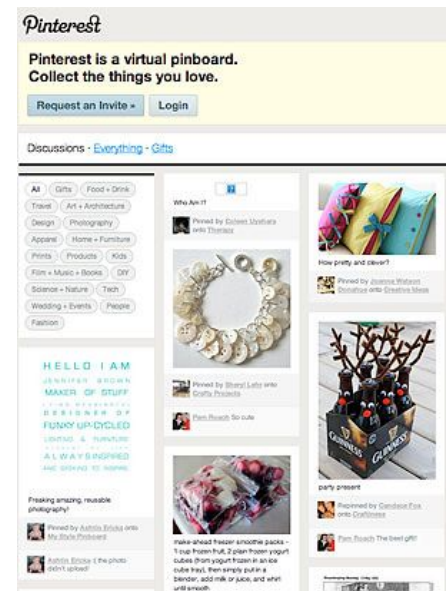
Pinterest

Webapps in 2011
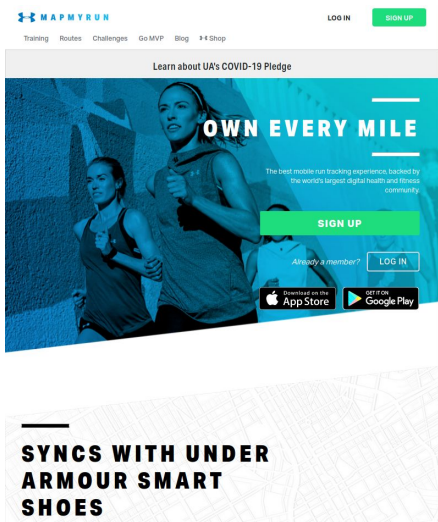
Map My Run
Sync With Yer Shoes!

Google+
sadtrombone.wav
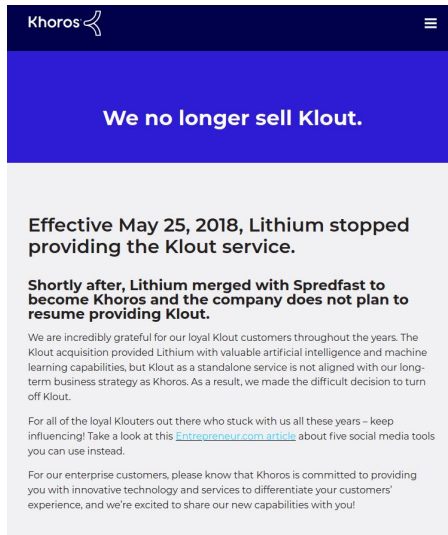
Klout
sadtrombone.wav
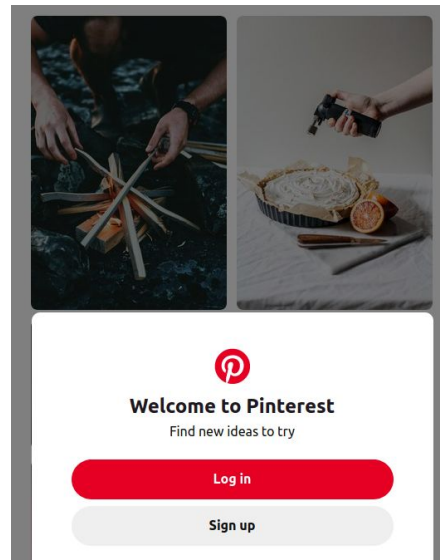
Pinterest
sadtrom... wait.

Black Hills Information Security specializes in security solutions that work and are cost effective. Our team has provided on-point solutions to financial institutions, government agencies, health care providers, and Top Secret/SCI programs. We understand that security is an ongoing process and strive to foster and support those processes in your organization.

Up Coming Events...

SERVICES

-Security Assessments
-Architecture Reviews
-Penetration Tests
-Security Team Training
-Certification and Accreditation Preparation
-Threat Analysis
-Incident Response
-Technical Writing Review

BHIS in 2011, in case you were wondering...

Webapps in 2011

Newspapers   "E-Commerce"   Proto-Social

Largely single-domain.

Analytics? That's ga.js, right?

HTML 5 was a draft, for *three more years*

CORS was a draft, for *three more years*

Java applets, Flash, Silverlight, ActiveX, XHR

https://en.wikipedia.org/wiki/HTML5#Timeline

https://en.wikipedia.org/wiki/Cross-origin_resource_sharing#History

Also 2011...

The Web Application
Hacker's Handbook

Finding and Exploiting
Security Flaws

2 Second Edition

Dafydd Stuttard ■ Marcus Pinto
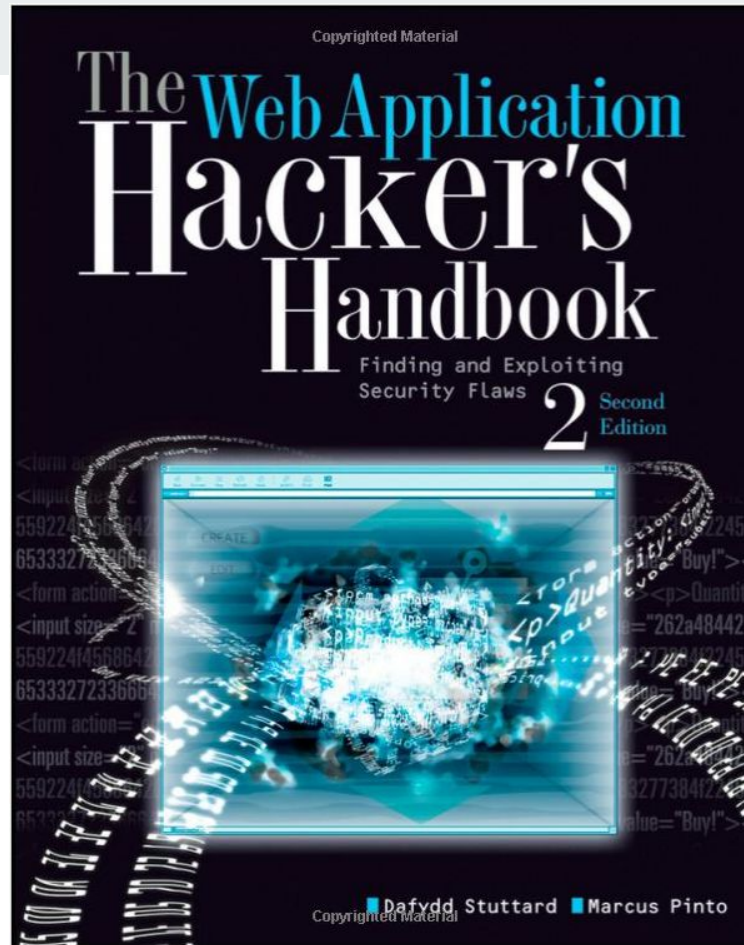
...this is still

the best book

I know of...

Testing Requires Understanding

If you don't know how it works...

You're not gonna break it in interesting ways.

You gotta keep up.

"Changes aren't permanent, but change is."
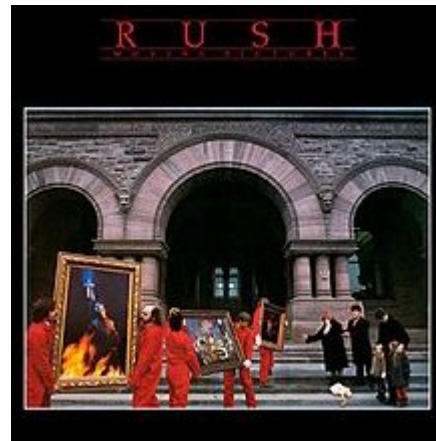
-- Rush, *Tom Sawyer*, 1981

Keeping Up
is just *Learning*

How'd They Do *That?*
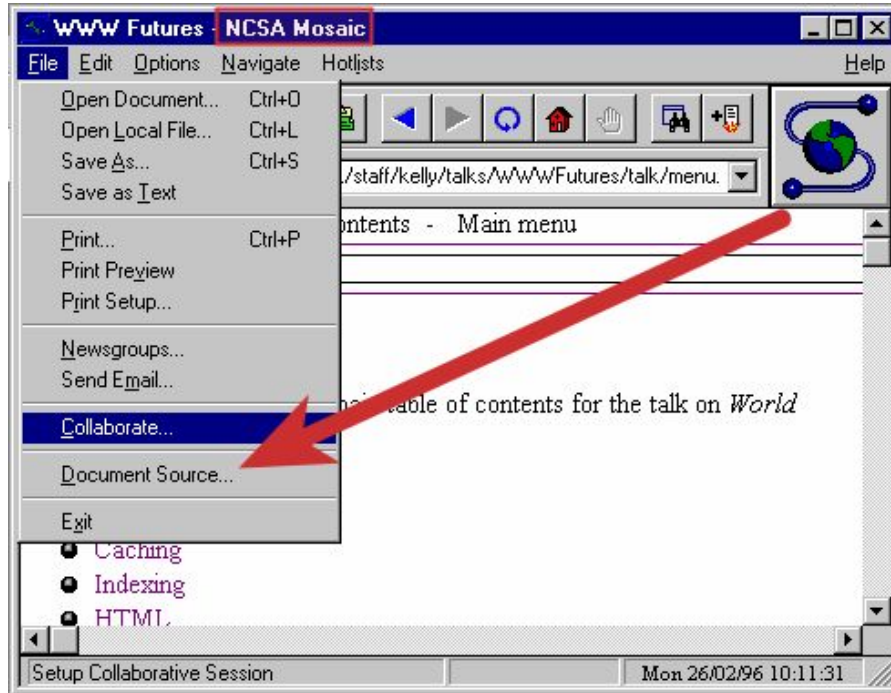
1. View Source (1993 - Mosaic)

   ...still here, but less useful

2. Greasemonkey (2005)

   ...still here...

3. Firebug (2006)

   ...paved the way...

4. Developer Tools

How Does *This Website* Work?

Idea: Share Images.

How complicated can that be?

How do you learn how "they" did it?

Try "View Source" on imgur.com for fun.

What Can You Do With Developer Tools?

- Understand how a page is built.
- See what hosts it's talking to, what content it's bringing in.
- Extract useful information.
- Change the app's behavior.
- Different browsers have similar tools.

- Firefox docs: https://developer.mozilla.org/en-US/docs/Tools
- Chrome docs: https://developers.google.com/web/tools/chrome-devtools/
  - Chrome Dev tools for ... actual developers...
  - https://bit.ly/wickedweapons (Greg Malcolm's "Raiding the Armory" talk and tools)

How Now?

- F12 ... Ctrl-Shift-i ... Cmd-Opt-i

- Console: what's going on.
- Inspector: how it's put together.
- DOM: top-down view.
- Storage: little databases...
- Network: where's it all coming from.
- Debugger: do that again, but slower.

Search HTML

Filter Styles   :hov .cls

Layout   Computed   Changes   Fonts

```
::marker
<a href="/International/">
  Internationalization</a> event
</li>
<li> ⋯ </li>
<li> ⋯ </li>
</ul>
<h3 class="category tMargin"> ⋯
</h3>
<ul class="theme"> ⋯ </ul>
<h3 class="category tMargin"> ⋯
</h3>
<ul class="theme"> ⋯ </ul>
<h3 class="category tMargin"> ⋯
</h3>
<ul class="theme"> ⋯ </ul>
</div>
<div class="w3c_mainCol">
  <div id="w3c_crumbs"> ⋯ </div>
  <div class="line">
    <div class="unit size2on3">
      <div class="main-content">
        <h2 class="offscreen">News
        </h2>
        <div id="w3c_slideshow">
          <div id="w3c_most-
          recently" class="intro
          hierarchy vevent_list">
            <div class="event
            w3c_topstory
            expand_block">
              <div class="headline">
              ⋯ </div>
```

element { } inline

.w3c_mainCol { advanced:71
  overflow: hidden;
  background-color: #fff;
  padding-left: 3%;
  padding-bottom: 3%;
  padding-top: 1.1%;
}

.w3c_mainCol,   minimum:62 @screen
#w3c_footer-inner,
#w3c_crumbs_frame {
  border-left: 0;
}

body, div, dl, dt, dd, ul, ol,   minimum:2
li, h1, h2, h3, h4, h5, h6, pre,
code, form, fieldset, legend, input,
textarea, p, blockquote, th, td, address
{
  margin: 0;
  padding: 0;
  padding-top: 0px;
  padding-bottom: 0px;
  padding-left: 0px;
}

Inherited from div#w3c_container

#w3c_container { advanced:4
  font-size: 108%;
  line-height: 1.41667;
}

Inherited from body#www-w3-org

body { advanced:1

Filter Styles   Browser St...

▶ background-color
  ○ rgb(255, 255, 255)
▶ border-left-color
  ● rgb(51, 51, 51)
▶ border-left-style
  none
▶ border-left-width
  0px
▶ color
  ● rgb(51, 51, 51)
▶ font-family
  "'Helvetica Neue'", Helvetica, Arial,
  Verdana, Geneva, sans-serif
▶ font-size
  14.1667px
▶ line-height
  20.0667px
▶ margin-bottom
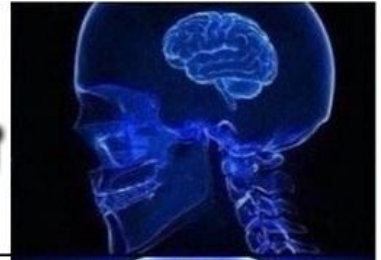 0px
▶ margin-left
  0px
▶ margin-right
  0px
▶ margin-top
  0px
▶ overflow
  hidden
▶ overflow-x
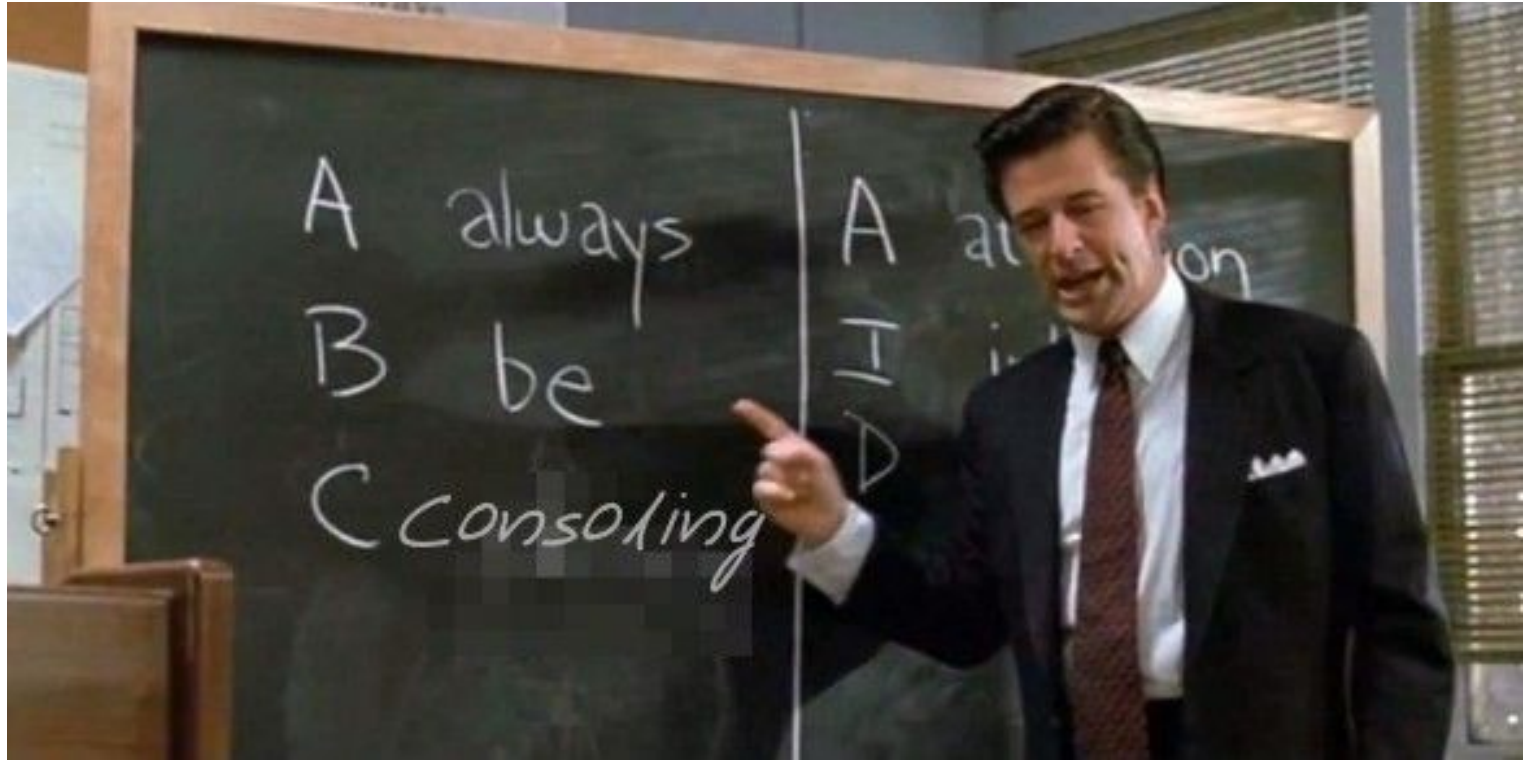 hidden
▶ overflow-y
  hidden

Display area is always limited so...

To the Tools! Console & Separate Window

Keep the Console Visible!

Console

- Its own pane, yes
- But put it everywhere:
  - ...tap Esc on any pane
  - ...except the console pane...

Console

- HTTP Requests (and responses)
  - Summary and detail
  - References for status codes & headers
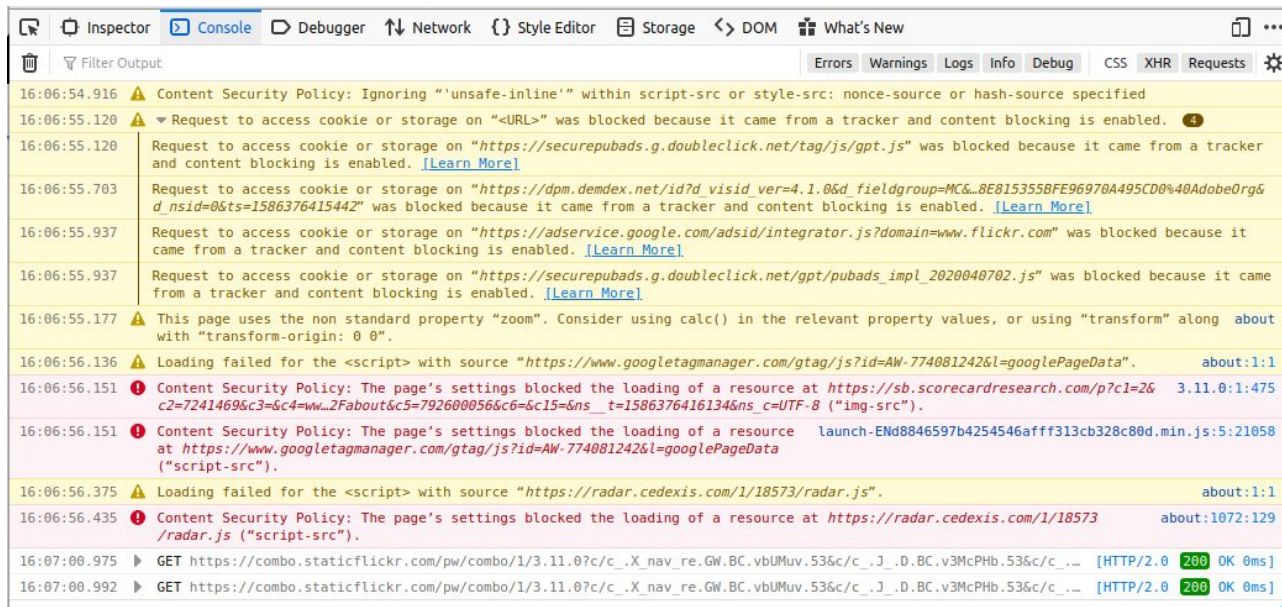 - HTTP version
- Calls to console.log();
- !! \o/   !!
- Browser errors & warnings

What Kinds of Warnings?

- CSP
- Privacy Blocks
- Mixed Content
- TLS Errors
- Deprecation
- "Learn More" !

Network

- Every request & response
  - ...kind of like the console on first look
- Still has links to header documentation
- Adds filters by content-type
- Adds freeform text filter box
- Adds "Edit and Resend" box!

Network Tab: List

Network Tab: Details

To The Tools! Network

Storage
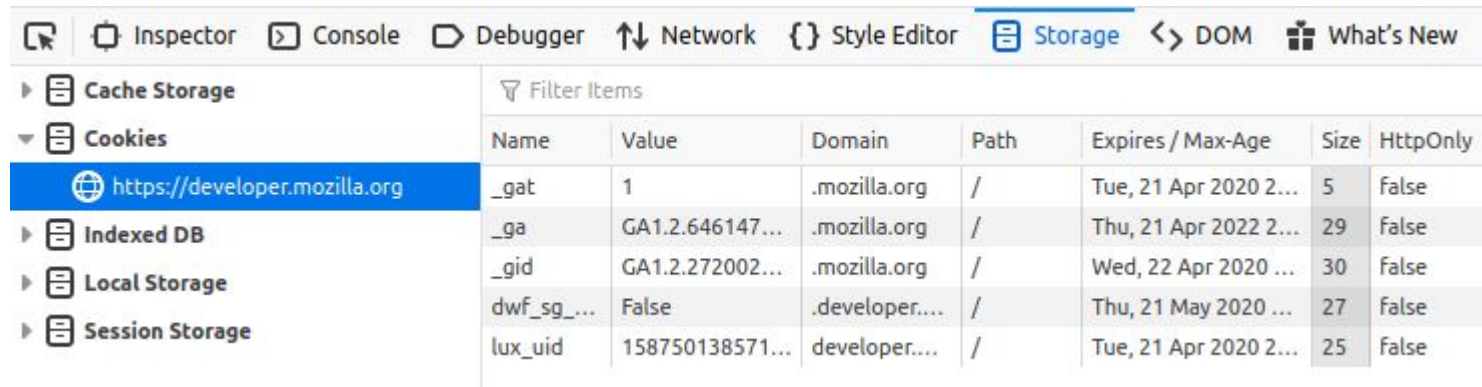
- Cache
  - ...not the disk cache: the Cache *interface* from the Web APIs
  - usually empty
- Cookies (add, view, edit, delete)
  - 4k per cookie, 20 or so per origin
- Indexed DB
  - At least 10MB and no more than 2GB (or 10% of hard disk).
  - Database. Structured data. (also usually empty)
- Local Storage (view and edit)
  - 5MB per origin. Persistent.
- Session Storage
  - 5MB per origin. Purged when browser closes (as with "*session* cookies")
- This stuff won't show up in your proxy!
  - Well, the cookies ~~will~~ *might*.
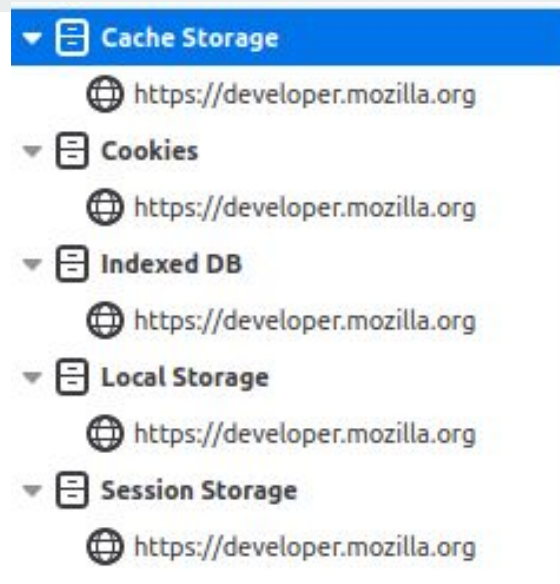
Storage: Cookies

Add, Edit, Delete.

No browser extension needed.

To The Tools! Storage

Inspector (and the Console)

- Like "View Source" (Ctrl-U) but better
- Same as right-click, inspect element
  - shows current state, not just "as-received" from server
  - live view (mouseover to get highlights)
  - live view (can edit: edits show in rendered view)
    - This is a great source for practical jokes, by the way.

Inspector & Console For Useful Things

Reveal text in "password" fields.

Execute functions...

See: **https://cryptojs.gitbook.io/docs/**

AES Encryption

Plain text encryption

```javascript
var CryptoJS = require("crypto-js");

// Encrypt
var ciphertext = CryptoJS.AES.encrypt('my message', 'secret key 123').toSt

// Decrypt
var bytes  = CryptoJS.AES.decrypt(ciphertext, 'secret key 123');
var originalText = bytes.toString(CryptoJS.enc.Utf8);

console.log(originalText); // 'my message'
```

https://www.npmjs.com/package/crypto-js

To The Tools! Inspector

How to Get Fired By Using Inspector

Debugger (and the Console)

- Can set breakpoints in scripts
- Check variable values
- Reveal function arguments
- Find logic in JS-set cookies

Debugger Example

yoyo

Customizing The Tools

- F1 (Settings)
  - Enable/disable panes
  - Dark. mode.
  - Screenshot Button!

Console Tricks - What's Available?

What can I ask the console about?

Ask the console!

console.log(top);

console.log(top === window)

top === document

window === document

Console Tricks

Get every <u>anchor link</u> on a page.

```
var links = document.getElementsByTagName("A");

const links = document.links;

document.links;  // ...actually...
```

Get every <u>image</u> on a page.

```
document.images;
```

Console Tricks - Modify Links

Add an "admin=true" to all the links.

That could work, right?

```
for(link of document.links) {
  link.href  = link.href + "&admin=true";
  link.style = "border: 5px solid blue";
}
```

Console Tricks - Collect Identifiers

Get the URL of Every Image

```
const pic_urls = [];
for(pic of document.images){
  pic_urls.push(pic.src);
}
console.log(pic_urls);
```

```
>> const pic_urls = [];
   for(pic of document.images){
     pic_urls.push(pic.src);
   }
   console.log(pic_urls);
<- undefined
  ▼ (94) [...]
     0: "https://combo.staticflickr.com/pw/images/tour/en-us/create-accou
     1: "https://farm3.staticflickr.com/2853/buddyicons/60065287@N00_r.jp
     2: "https://farm1.staticflickr.com/932/buddyicons/36521981547@N01_r.
     3: "https://farm8.staticflickr.com/7317/buddyicons/15721381@N00_r.jp
     4: "https://farm9.staticflickr.com/8463/buddyicons/20244787@N07_r.jp
     5: "https://farm1.staticflickr.com/892/buddyicons/11797544@N05_r.jpg
     6: "https://farm6.staticflickr.com/5037/buddyicons/78522870@N07_r.jp
     7: "https://farm1.staticflickr.com/873/buddyicons/91720879@N02_r.jpg
     8: "https://farm8.staticflickr.com/7386/buddyicons/63652802@N02_r.jp
     9: "https://farm4.staticflickr.com/3718/buddyicons/26794697@N03_r.jp
     10: "https://farm66.staticflickr.com/65535/buddyicons/66422871@N00_r
```

(or, filter the "Network" tab by "Images")

Free Tools.