

MARKETINVOICE WEBINAR

KEEP CALM AND SECURE YOUR CI/CD PIPELINE

@SONYAMOISSET 🦄🌐

.I WEAR DARK
HOODIES SO I'M
A LEGIT SECURITY
ENGINEER



WHAT IS CYBERSECURITY AND WHY IS IT IMPORTANT?

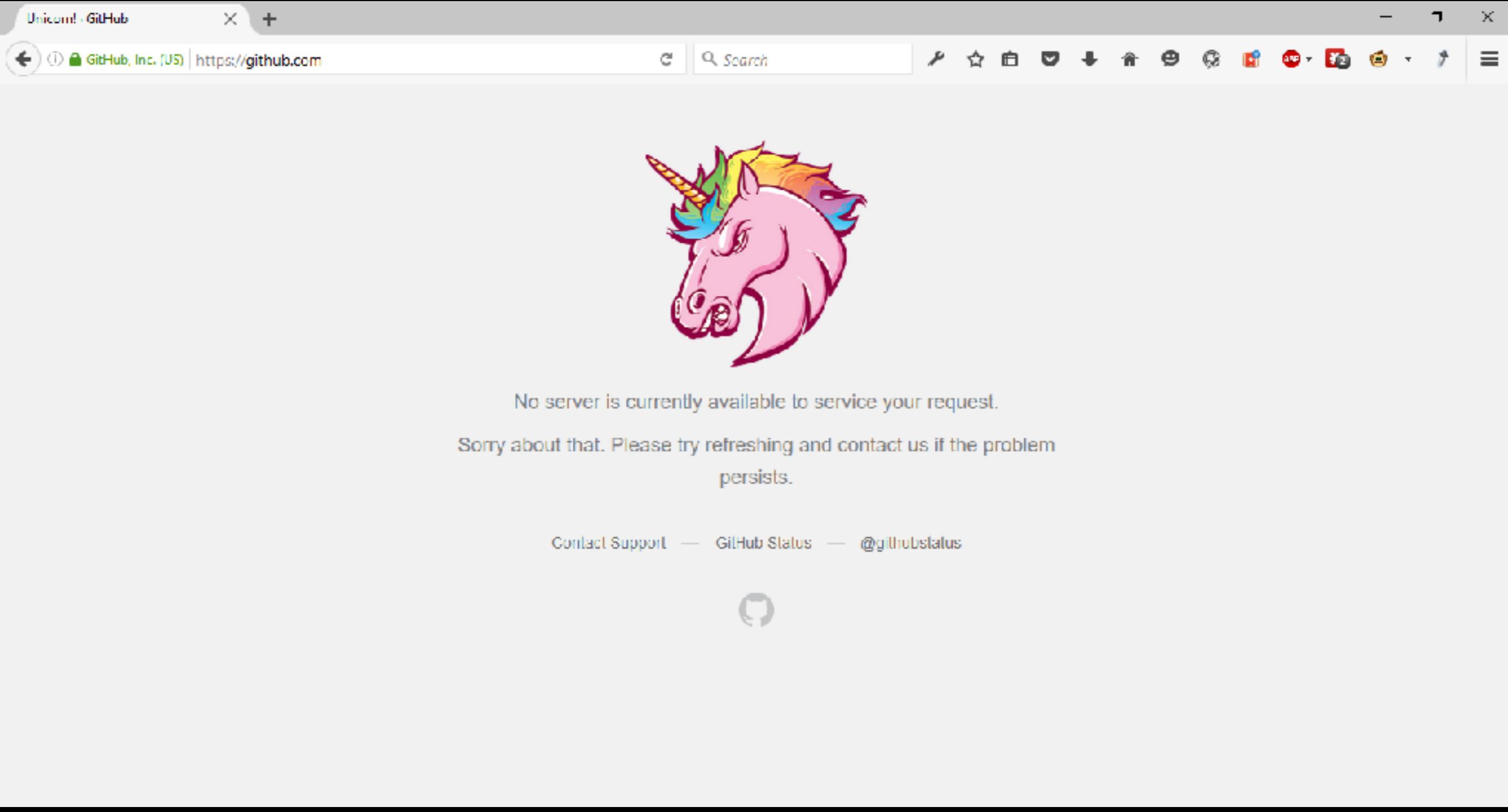
The word cloud is composed of various terms related to cybersecurity, including:

- Computer Design Protection
- Cyber Defects
- Secure Systems Assurance
- Software Engineering
- Hardware Control
- Vulnerabilities
- Common Networks
- Known Critical Cybercrime
- Connected Policy
- Government One
- Information Primary
- Operating System
- Defense Power Level
- International Compromised
- Computers Bill Protect
- House Services
- Well Loss
- Protecting
- Primary Management
- National Internet Order Provide
- Flaws
- Management
- Internet Order Provide
- Network United
- Code High Using Center
- Problem Ensure
- Security

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...)



No server is currently available to service your request.

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

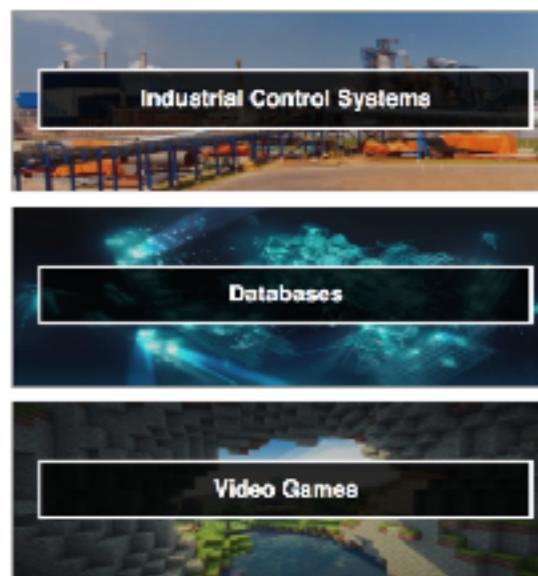
[Contact Support](#) — [GitHub Status](#) — [@githubstatus](#)



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.	2010-03-15
4,089	Cams	admin admin	2012-02-05
2,256	Netcam	Netcam	2012-01-13
1,582	default password	Finds results with "default password" in the ha...	2010-01-14
1,087	dreambox	dreambox	2010-08-13

[More popular searches...](#)

Recently Shared

1	chile	2010-10-08
2	router control panel DD-WRT	2010-10-08
3	1	2010-10-06
1	Logitech Media Server	2010-10-05
3	sushi	2010-10-05

[More recent searches...](#)

Shodan | Developers | Docs | View All... | [Search](#) | [Explore](#) | [Pricing](#) | [Enterprise Access](#)

New to Shodan? | [Login or Register](#)

[Exploits](#) | [Maps](#) | [Images](#)

TOTAL RESULTS
5,402

TOP COUNTRIES

Country	Count
United States	866
Korea, Republic of	698
Germany	405
Poland	331
Italy	297

TOP SERVICES

Service	Count
HTTP (80)	1,803
8081	871
HTTP	232
HTTPS	189
8080	141

TOP ORGANIZATIONS

Organization	Count
Korea Telecom	235
Deutsche Telekom AG	199
RCS & RBS Residential	875
Spectrum	804
Skynet Sp. Z o.o.	82

TOP OPERATING SYSTEMS

OS	Count
Ubuntu	14
QTS	13
Linux 2.6	10
Windows 7 or 8	8
Windows 6.1	4

TOP PRODUCTS

Product	Count
webcam things	376
XnView webcam viewer httpd	365
Apache httpd	218
darwinian web-cam httpd	75
Sendmail	30

RELATED TAGS: [urinet](#)

77.23.232.64 [🔗](#)

ip:77.23.232.64 dynamiclabel-deutschland.de
Vodafone Kabel Deutschland
Added on 2019-04-14 16:11:51 GMT
Germany, Wupper

HTTP/1.1 401 Unauthorized
Content-Length: 8
WWW-Authenticate: Digest realm="IP Webcam", nonce="1555285518", op="auth"

119.196.110.245 [🔗](#)

Korea Telecom
Added on 2019-04-14 17:51:11 GMT
Korea, Republic of, Seoul

self-signed

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

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

HTTP/1.1 401 Unauthorized
Content-Length: 8
WWW-Authenticate: Digest realm="IP Webcam", nonce="1555284267", op="auth"

83.4.254.176 [🔗](#)

ip:83.4.254.176 orangeplus.aditional.pl
Orange Polska
Added on 2019-04-14 16:03:29 GMT
Poland

HTTP/1.1 401 Unauthorized
Content-Length: 8
WWW-Authenticate: Digest realm="IP Webcam", nonce="1555263127", op="auth"

14.49.134.32 [🔗](#)

Korea Telecom
Added on 2019-04-14 17:52:02 GMT
Korea, Republic of, Seoul

HTTP/1.1 401 Unauthorized
Content-Length: 8
WWW-Authenticate: Digest realm="IP Webcam", nonce="1555264546", op="auth"

139.59.28.86 [🔗](#)

Digital Ocean
Added on 2019-04-14 17:53:29 GMT
India, Bangalore

HTTP/1.1 200 OK
X-Powered-By: Express
Accept-Ranges: bytes
Cache-Control: public, max-age=8
Last-Modified: Wed, 04 Apr 2018 07:09:02 GMT
ETag: W/"F59-1020774870"
Content-Type: text/html; charset=UTF-8
Content-Encoding: gzip
Date: Sun, 14 Apr 2019 17:53:23 GMT
Connection: keep-alive

...
...
...



Ooops, your files have been encrypted!

English

▼

not so enough time.

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

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

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

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

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

Payment will be raised on

1/4/1970 00:00:00

Time Left

00:00:00:00

Your files will be lost on

1/8/1970 00:00:00

Time Left

00:00:00:00

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)

How Do I Pay?

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

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

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

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

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

Contact

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

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

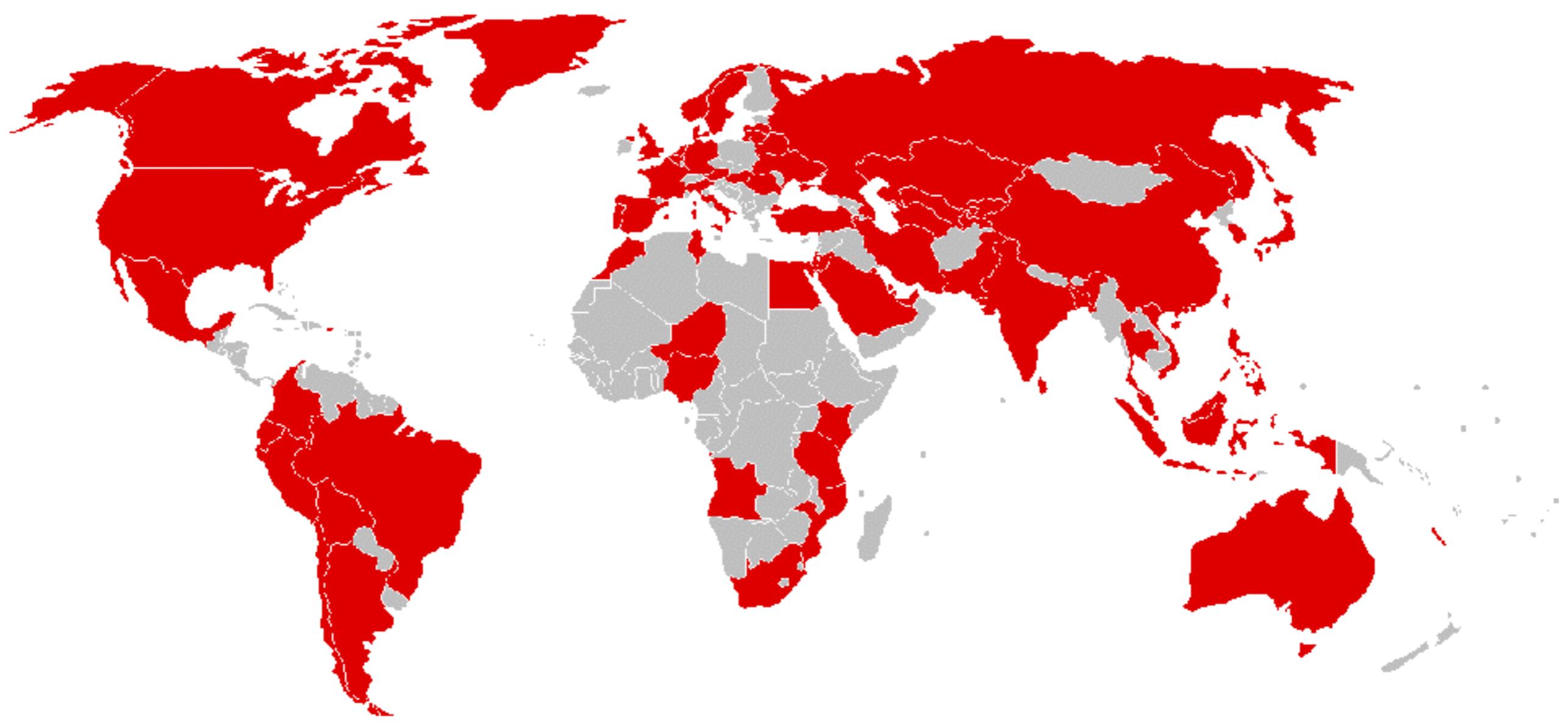


Send \$600 worth of bitcoin to this address:

Copy

[Check Payment](#)

[Decrypt](#)



re: "██████████"

Inbox x



Dirk Saunders <yxpnmjarrettlwq@outlook.com>

12:07 PM (8 minutes ago)



to me ▾

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

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

What exactly did I do?

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

Exactly what should you do?

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

BTC ADDRESS: 1JC99fcQMVR4iHdmf3GbHLGHMkPpyFjBu7

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

Note:

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

**SUMMARY**[USD](#) [BCH](#)

Address

qz7ftpz95v34u0guwn9wqyfkajhkztmxtgj9537f9g

Number of Transactions

0

Final Balance

0.00000000 BCH

Total Sent

0.00000000 BCH

Total Received

0.00000000 BCH

**TRANSACTIONS**[USD](#) [BCH](#)

Date (timestamp)

Hash de transaction

État

Montant



';-have i been pwned?

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

check

Generate secure, unique passwords for every account

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

359
owned websites

7,840,611,051
owned accounts

93,384
pastes

114,064,052
paste accounts

Largest breaches



772,904,991 [Collection #1 accounts](#)



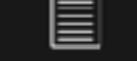
763,117,241 [Verifications.io accounts](#)



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](#)

250,400,608 [MySpace accounts](#)

Recently added breaches



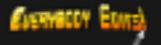
760,561 [DataCamp accounts](#)



808,330 [Knuddels accounts](#)



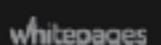
52,623 [Demon Forums accounts](#)



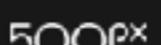
871,190 [Everybody Edits accounts](#)



3,073,409 [Intelimost accounts](#)



11,657,763 [Whitepages accounts](#)



14,867,999 [500px accounts](#)



3,830,916 [Bookmate accounts](#)

[Overview](#)

Repositories 873

Projects 0

Stars 358

Followers 2.9k

Following 28

Pinned

[ssbc/ssb-server](#)

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

JavaScript ★ 1.1k ⚡ 134

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

minimal streams

JavaScript ★ 633 ⚡ 58

[auditdrivencrypto/secret-handshake](#)

JavaScript ★ 155 ⚡ 22

[map-filter-reduce](#)

JavaScript ★ 44 ⚡ 6

[ssbc/patchbay](#)

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

JavaScript ★ 223 ⚡ 56

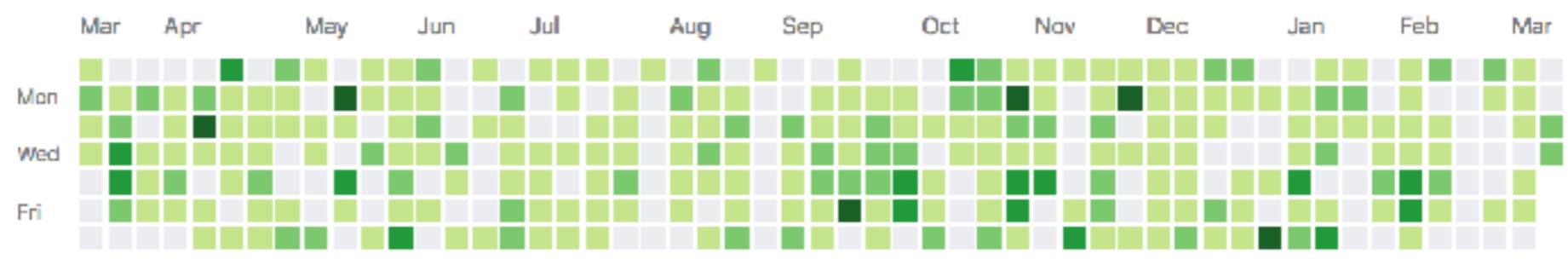
Dominic Tarr

[dominictarr](#)[Follow](#)[Block or report user](#)[antipodean wandering albatross](#) [Protozoa](#) [New Zealand](#) [http://protozoa.nz](#)

Organizations



2,485 contributions in the last year

[Learn how we count contributions.](#)

Less More

Ready to take your JavaScript development to the next level? Meet npm Enterprise - the ultimate in enterprise JavaScript. [Learn more »](#)

event-stream

4.0.1 • [Public](#) • Published 7 months ago

[Readme](#)[7 Dependencies](#)[1,638 Dependents](#)[84 Versions](#)

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](#).

NOTE: I shall use the term "*through stream*" to refer to a stream that is writable *and* readable.

NOTE for Gulp users: Merge will not work for gulp 4. [merge-stream](#) should be used.

simple example:

```
//pretty.js

if(!module.parent) {
  var es = require('event-stream')
```

[install](#)

```
> npm i event-stream
```

[weekly downloads](#)

1,372,033

[version](#)

4.0.1

[license](#)

MIT

[open issues](#)

7

[pull requests](#)

0

[homepage](#)[github.com](#)[repository](#)[github](#)[last publish](#)

7 months ago

[collaborators](#)[Test with RunKit](#)

EVENT STREAM POST MORTEM

- December 2018
 - flatmap-stream was published to npm and added as a dependency to the event-stream package by user right9ctrl
- 8 million downloads
- Applications all over the web were running malicious code in production



[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](#)



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.

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](#) 

 dbj11	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	initial, 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

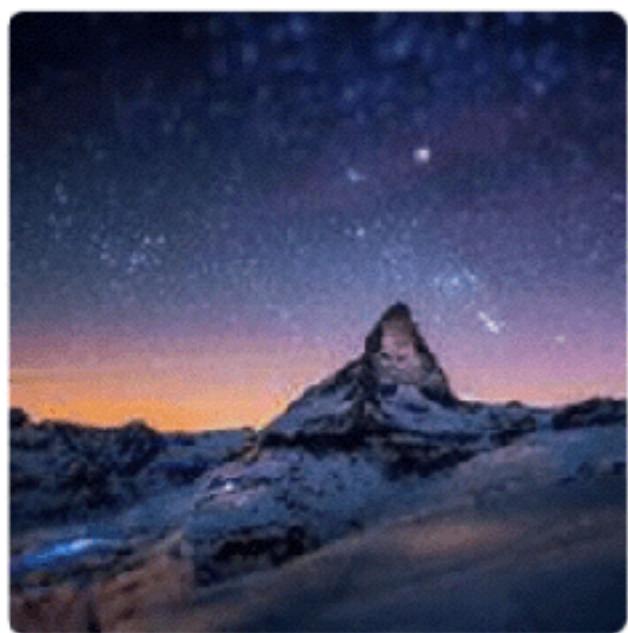
[Streams](#) are node's best and most misunderstood idea, and EventStream is a toolkit to make creating and working with streams easy.

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`.



Overview

Repositories 3

Stars 0

Followers 0

Following 0

Popular repositories

[node-script](#)

● C

[react](#)

Forked from [facebook/react](#)

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

● JavaScript

[event-stream](#)

● JavaScript

北川

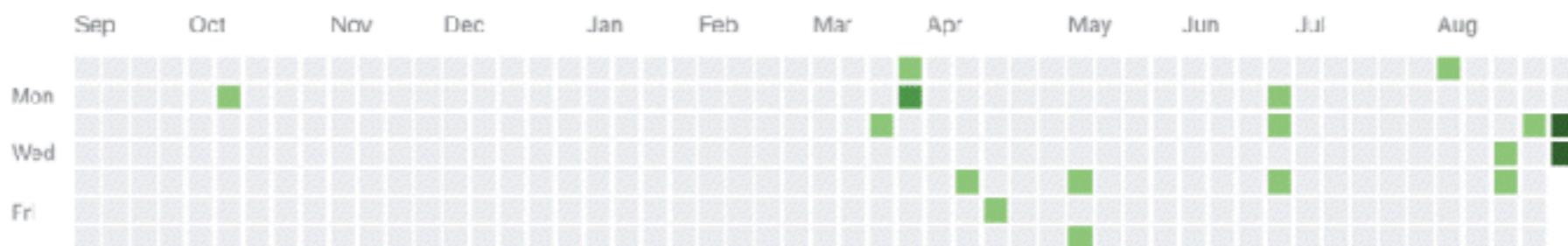
right9ctrl

[Block or report user](#)

👤 株式会社LIG

📍 東京都

22 contributions in the last year



fuck Right9ctrl

[Browse files](#)

master (#1)

 geektheripper committed on Dec 23, 2018

1 parent 706ed02

commit cb0f66a328134bc4f0959a99caf347a6670eadb7

 Showing 2 changed files with 19 additions and 70 deletions.

Unified Split

2  package.json

[View file](#)

86	86	@@ -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

SECURE SOFTWARE DEVELOPMENT LIFE CYCLE



Software Development Life Cycle (SDLC) is a framework that defines the process used by the organisations to build an application from its inception to its decommission

1 PLANNING

Planning focuses on the scope of the project. The outputs of the planning phase include: project plans, schedules, cost estimations, and procurement requirements.

2 REQUIREMENTS

The IT team gathers requirements from business stakeholders and Subject Matter Experts (SMEs.) The output of this phase in a Waterfall project is usually a document that lists these requirements. Agile methods, by contrast, may produce a backlog of tasks to be performed.

4 SOFTWARE DEVELOPMENT

This phase produces the software under development. This could be in "sprints" (Agile), or a single block effort (Waterfall). The output of this phase is testable, functional software.

6 DEPLOYMENT

The deployment phase is, ideally, a highly automated phase. In high-maturity enterprises, this phase is almost invisible; software is deployed the instant it is ready. Enterprises with lower maturity, or in some highly regulated industries, the process involves some manual approvals. The output of this phase is the release to Production of working software.

3 DESIGN AND PROTOTYPING

Once requirements are understood, the design process takes place. It makes use of established patterns for application architecture and software development. Architecture frameworks like TOGAF may be used here. Outputs include: design documents that list the patterns and components selected for the project; code produced by spikes, used as a starting point for development.

5 TESTING

The testing phase of the SDLC is arguably one of the most important. It is impossible to deliver quality software without testing. Methods for testing can include: code quality, unit testing (functional tests), Integration testing, Performance testing, Security testing. The output of the testing phase is functional software, ready for deployment to a production environment.

7 OPERATIONS AND MAINTENANCE

The operations and maintenance phase is the "end of the beginning". Though the SDLC doesn't end here, Software must be monitored constantly to ensure proper operation. Bugs and defects discovered in Production must be reported and responded to, which often feeds work back into the process. Bug fixes may not flow through the entire cycle, however; at least an abbreviated process is necessary to ensure that the fix does not introduce other problems.

A SECURE SDLC PROCESS ENSURES THAT SECURITY ASSURANCE ACTIVITIES SUCH AS PENETRATION TESTING, CODE REVIEW, AND ARCHITECTURE ANALYSIS ARE AN INTEGRAL PART OF THE DEVELOPMENT EFFORT

- .MORE SECURE SOFTWARE AS SECURITY IS A CONTINUOUS CONCERN
- .AWARENESS OF SECURITY CONSIDERATIONS BY STAKEHOLDERS
- .EARLY DETECTION OF FLAWS & COST REDUCTION AS A RESULT OF EARLY DETECTION AND RESOLUTION OF ISSUES

HOW DO I GET STARTED?



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





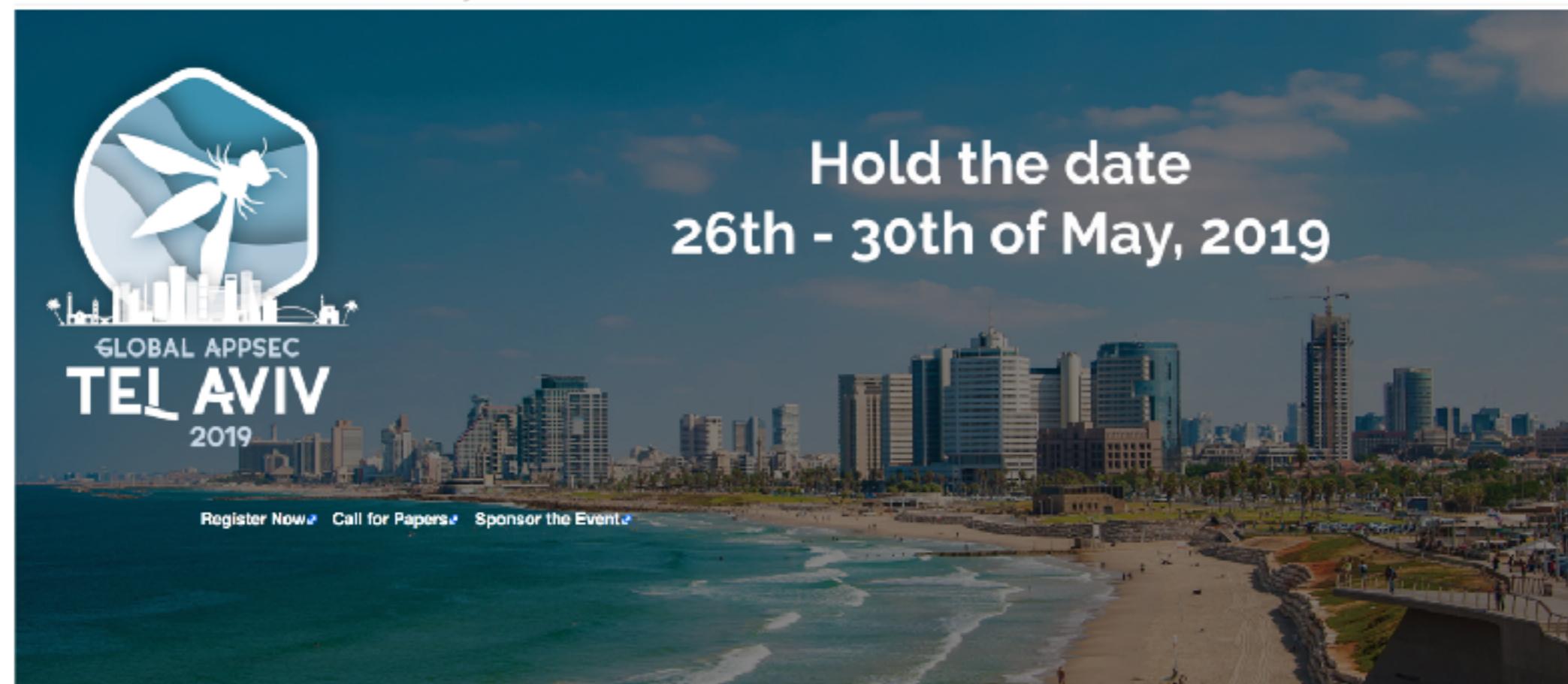
The OWASP™ Foundation

the free and open software security community

[Member Portal](#) • [About](#) • [Browsing](#) • [Editing](#) • [New Article](#) • [OWASP Categories](#) • [Contact Us](#)

[Statistics](#) • [Recent Changes](#)

ANNOUNCING GLOBAL APPSEC TEL AVIV 2019!

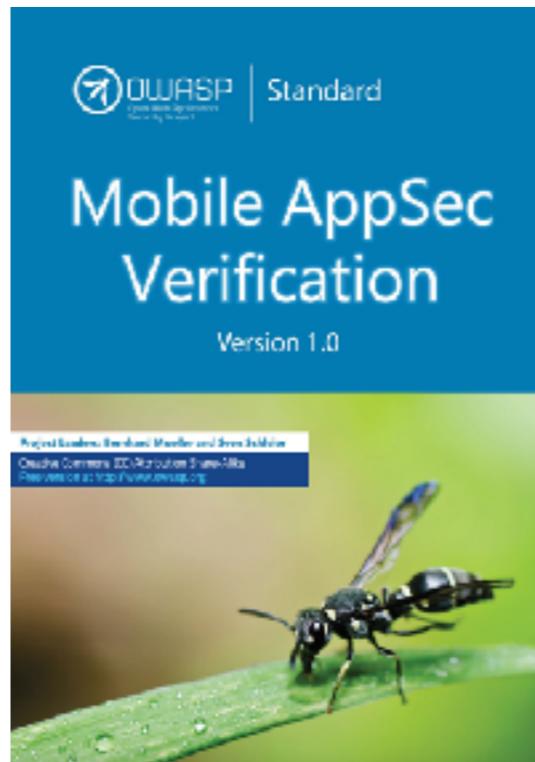
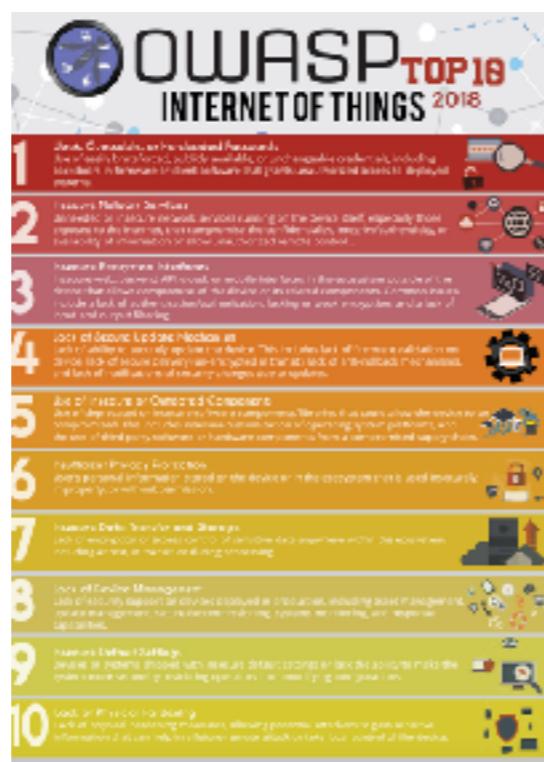
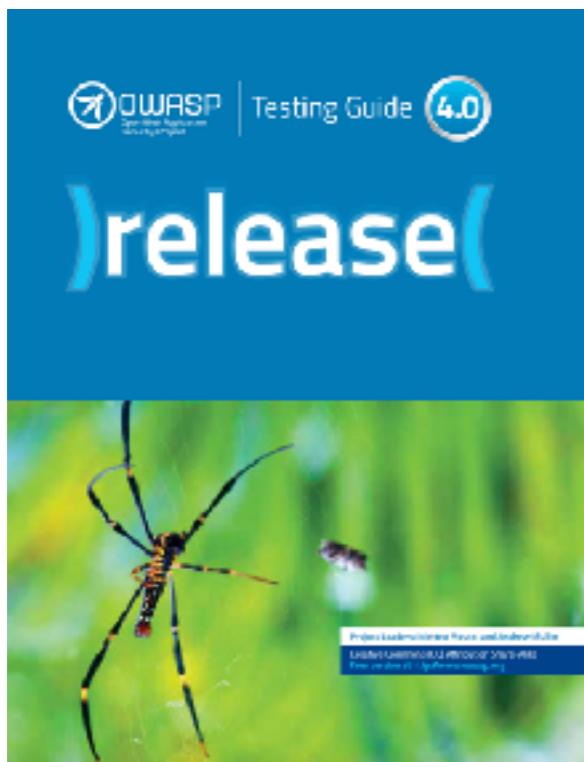


[Home](#)
[About OWASP](#)
[Acknowledgements](#)
[Advertising](#)
[AppSec Events](#)
[Supporting Partners](#)
[Books](#)
[Brand Resources](#)
[Chapters](#)
[Donate to OWASP](#)
[Downloads](#)
[Funding](#)
[Governance](#)
[Initiatives](#)
[Mailing Lists](#)
[Membership](#)
[Merchandise](#)
[Presentations](#)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

[Reference](#)
[Activities](#)
[Attackers](#)
[Code Snippets](#)
[Controls](#)
[Glossary](#)
[How To's](#)
[Java Project](#)
[.NET Project](#)
[Principles](#)
[Technologies](#)
[Threat Agents](#)
[Vulnerabilities](#)

[Tools](#)
[What links here](#)
[Recent changes](#)
[Special pages](#)
[Printable version](#)
[Permanent link](#)
[Page information](#)

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

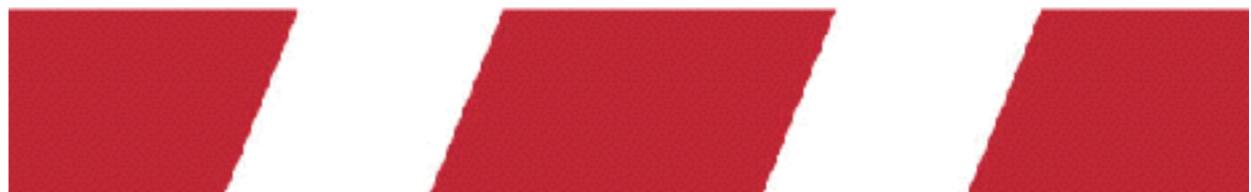




OWASP

OWASP Top 10 - 2017

The Ten Most Critical Web Application Security Risks



OWASP

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



10 Critical Security Areas That Software Developers Must Be Aware Of

PROJECT LEADERS

KATY ANTON
JIM MANICO
JIM BIRD



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

C1. DEFINE SECURITY REQUIREMENTS

- Security requirements define new features or additions to existing features to solve a specific security problem or eliminate a potential vulnerability
- Instead of creating a custom approach to security for every application, standard security requirements allow developers to reuse the definition of security controls and best practices
- OWASP ASVS
- User Stories and Abuse Cases

A2:2017-Broken Authentication

Epic:

Attackers have access to hundreds of millions of valid username and password combinations for credential stuffing, default administrative account lists, automated brute force, and dictionary attack tools. Session management attacks are well understood, particularly in relation to unexpired session tokens.

Abuse Case:

As an attacker, I have access to hundreds of millions of valid username and password combinations for credential stuffing.

Abuse Case:

As an attacker, I have default administrative account lists, automated brute force, and dictionary attack tools I use against login areas of the application and support systems.

Abuse Case:

As an attacker, I manipulate session tokens using expired and fake tokens to gain access.

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

 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

16.8.4

license

MIT

open issues

429

pull requests

159

homepage

reactjs.org

repository



last publish

8 days ago

collaborators



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 and components
- Proactively keep libraries and components up to date

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



OWASP Top 10 - 2017

The Ten Most Critical Web Application Security Risks



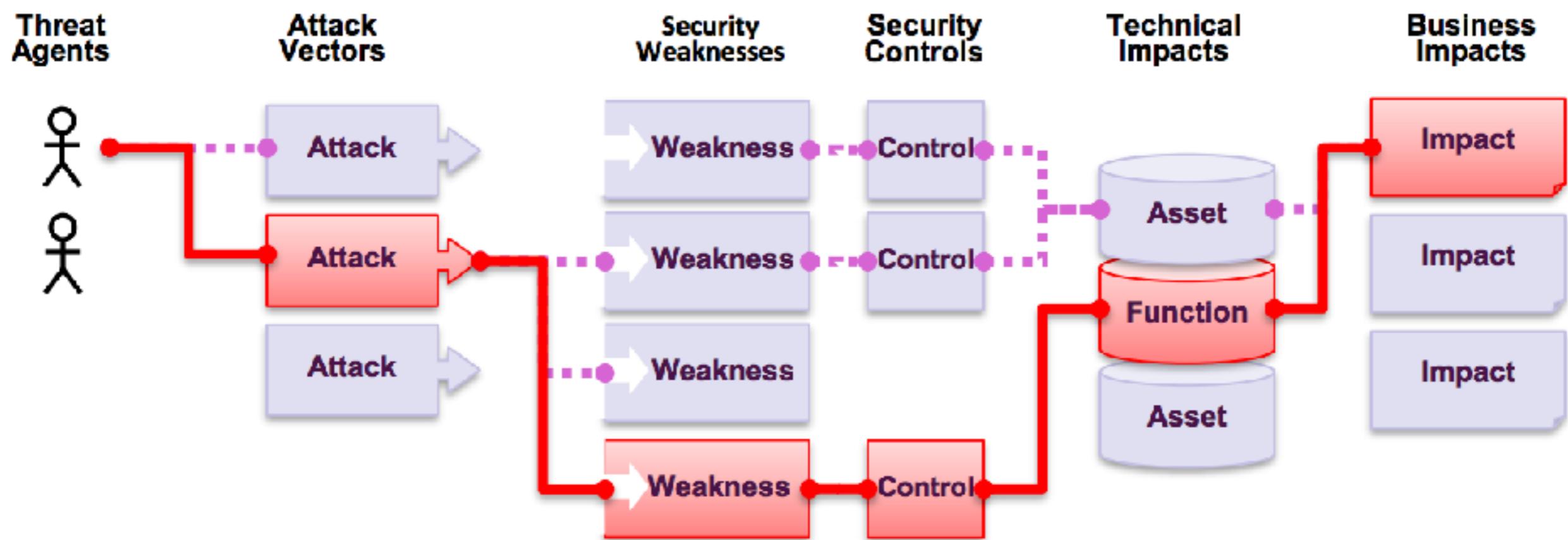
WHAT CHANGED FROM 2013 TO 2017?

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]	↑	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]	↑	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.]

WHAT ARE APPLICATION SECURITY RISKS?

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



ASVS



OWASP

Application Security Verification Standard 4.0

Final

March 2019

- 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

PRIDE IN LONDON

HOW TO SECURE YOUR OPEN SOURCE PROJECT



Open Source Friday

Open source is made by people just like you. This Friday, invest a few hours contributing to the software you use and love.

[Sign up with GitHub](#)



↔ with ❤ by **GitHub**

Hacktoberfest

Support open source and earn a limited edition T-shirt.

En octobre prochain !!

Hacktoberfest '18 was presented by: **DigitalOcean** · **GitHub** · **twilio**



Pride in London

[Repositories 3](#)[People 6](#)[Teams 1](#)[Settings](#)[Type: All ▾](#)[Language: All ▾](#)[Customize pins](#)[New](#)

pride-london-web

Pride In London's New Website

JavaScript MIT Updated 2 days ago



Top languages

JavaScript

pride-london-web-old

Forked from MarcelCutts/pride-london-web-gatsby

Pride in London's front end web platform

JavaScript 2 MIT Updated 19 days ago



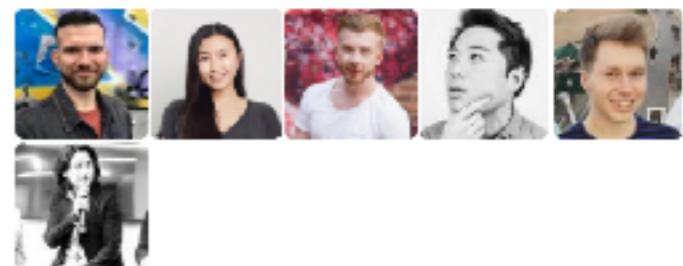
pride-web-webhook

webhook service to help trigger travis builds from contentful

JavaScript MIT Updated on Jun 19, 2018



People

[Invite someone](#)

Saturday 6 July

Pride in London

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

[This years event](#)

Featured events

View events from across the LGBT+ community.

[View all events](#)

From £19

15 – 22 Jun 2018 • 8am – 5.30pm

Headline of event
card lemon drops pie
jujubes macaroon



From £19

15 – 22 Jun 2018 • 8am – 5.30pm

Headline of event
card lemon drops pie
jujubes macaroon



From £19

15 – 22 Jun 2018 • 8am – 5.30pm

Headline of event
card lemon drops pie
jujubes macaroon



GitHub Marketplace

Tools to build on and improve your workflow



Categories

- Chat
- Code quality
- Code review
- Continuous integration
- Dependency management
- Deployment
- Learning
- Localization
- Mobile
- Monitoring
- Project management
- Publishing
- Recently added
- Security
- Support
- Testing
- Utilities

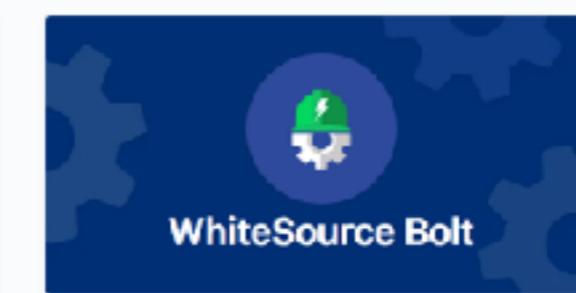
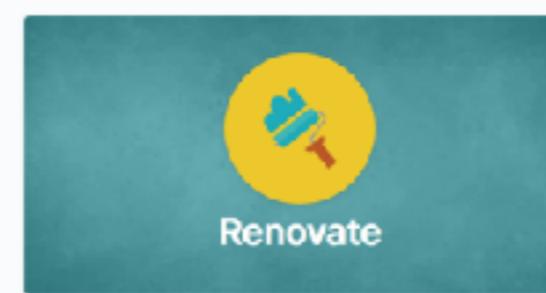
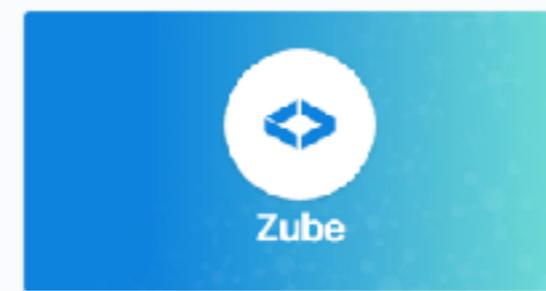
Filters ▾

Your items ▾

- Pending orders
- Purchases

Search for apps

Featured apps



Recently added

The latest tools that help you and your team build software better, together.



CodeScene

The analysis tool to identify and prioritize technical debt and evaluate your organizational efficiency



ImgBot

A GitHub app that optimizes your images



Pull Reminders

Slack reminders and metrics for pull requests



Depfu

Automated dependency updates keep your app secure and maintainable



Instabug

Instabug is a reliable bug reporting and user feedback SDK that enables testers and users to report issues from within the app



Slack + GitHub

Connect your code without leaving Slack



GitKraken Glo Boards

Free issue/task tracking boards that sync



CodeFactor

Automated code review for GitHub

WHAT IS GITHUB MARKETPLACE

- Contains tools that add functionality and improve your workflow
- Almost 2 years
- 50+ tools



Categories

API management

Chat

Code quality X

Code review

Continous integration

Dependency management

Deployment

IDEs

Learning

Localization

Mobile

Monitoring

Project management

Publishing

Recently added

Security

Support

Testing

Utilities

Filters ▼

Verification

Verified

Unverified

Your items ^

Pending orders

Purchases

Search for apps

Code quality

Automate your code review with style, quality, security, and test-coverage checks when you need them.

22 results filtered by Code quality X



codelingo ✔

Your Code, Your Rules - Automate code reviews with your own best practices



TestQuality ✔

Modern, powerful, test plan management



Restyled.io ✔

Restyle Pull Requests as they're opened



PEP 8 Speaks ✔

A GitHub app to automatically review Python code style over Pull Requests



LGTM ✔

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



GuardRails ✔

GuardRails provides continuous security feedback for modern development teams



Datree ✔

Policy enforcement solution for confident and compliant code



Commit Lint ✔

Enforce the conventions of commits



CodeScene ✔

The analysis tool to identify and prioritize technical debt and evaluate your organizational efficiency



Code Climate ✔

Automated code review for technical debt and test coverage



codebeat ✔

Code review expert on demand. Automated for mobile and web



Sider ✔

Automatically analyze pull request against custom per-project rulesets and best practices



Pull Request Size ✔

Apply size labels to Pull Requests based on the total lines of code changed



Lucidchart Connector ✔

Insert a public link to a Lucidchart diagram so team members can quickly understand an issue or pull request



ImgBot ✔

A GitHub app that optimizes your images



GraphQL Inspector ✔

Compare schemas, validate documents, find breaking changes, find similar types, get schema coverage



Coveralls ✔

Ensure that new code is fully covered, and see coverage trends emerge. Works with any CI service



Codecov ✔

Group, merge, archive and compare coverage reports



CodeFactor ✔

Automated code review for GitHub



Codacy ✔

Automated code reviews to help developers ship better software, faster

Organization settings

[Profile](#)[Member privileges](#)[Billing](#)[Security](#)[Verified domains](#)[Audit log](#)[Webhooks](#)

Third-party access

[Installed GitHub Apps](#)[Repository topics](#)[Projects](#)[Teams](#)

Developer settings

[OAuth Apps](#)[GitHub Apps](#)

Moderation settings

[Blocked users](#)[Interaction limits](#)

Third-party application access policy

Policy: Access restricted ✓

Only approved applications can access data in this organization. Applications owned by PrideInLondon always have access.

[Remove restrictions](#)

 CircleCI	...	✓ Approved — 
 Codacy	...	✓ Approved — 
 codebeat	...	✓ Approved — 
 Codecov	...	✓ Approved — 
 codefactor.io	...	✓ Approved — 
 GuardRails		✓ Approved — 
 LGTM		✓ Approved — 
 Snyk	...	✓ Approved — 
 Travis CI for Open Source		✓ Approved — 
 codefactor.io	...	✗ Denied — 
 Coveralls Pro		✗ Denied — 
 Greenkeeper	...	✗ Denied — 

② When authorized, applications can act on behalf of organization members. Your access policy determines which applications can access data in your organization. [Read more about third-party access and organizations](#).

Organization settings

[Profile](#)[Member privileges](#)[Billing](#)[Security](#)[Verified domains](#)[Audit log](#)[Webhooks](#)[Third-party access](#)

Installed GitHub Apps

[Repository topics](#)[Projects](#)[Teams](#)

Developer settings

[OAuth Apps](#)[GitHub Apps](#)

Moderation settings

[Blocked users](#)[Interaction limits](#)

Installed GitHub Apps

GitHub Apps augment and extend your workflows on GitHub with commercial, open source, and homegrown tools.



AccessLint

[Configure](#)

Codecov

[Configure](#)

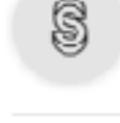
Dependabot

[Configure](#)

GuardRails

[Configure](#)

Netlify

[Configure](#)

Pull Request Size

[Configure](#)

Rollbar

[Configure](#)

Slack

[Configure](#)

Sonatype DepShield

[Configure](#)

Organization settings

[Profile](#)[Member privileges](#)[Billing](#)[Security](#)[Verified domains](#)[Audit log](#)[Webhooks](#)[Third-party access](#)

Installed GitHub Apps

[Repository topics](#)[Projects](#)[Teams](#)

Developer settings

[OAuth Apps](#)[GitHub Apps](#)

Moderation settings

[Blocked users](#)[Interaction limits](#)

Netlify



Installed 3 months ago

Developed by [netlify](#)<https://www.netlify.com>

Permissions

- [Read access to code](#)
- [Read access to metadata](#)
- [Read and write access to checks, commit statuses, and pull requests](#)

Repository access

 All repositories

This applies to all current and future repositories.

 Only select repositories[Select repositories](#) ▾

Selected 1 repository

[PrideInLondon/pride-london-web](#)[Save](#)[Cancel](#)

Uninstall Netlify

When you uninstall Netlify, it will be removed from this account and will lose access to all of its resources.

[Uninstall](#)



circleci



PridelnLondon



Updates

Support



Jobs > PridelnLondon

By project ▾ My branches All branches

Branch	Status	Last Run
pride-london-web	success	PridelnLondon / pride-london-web / master #499
dependabot/npm_and_yarn/gatsby-2.3.13	success	Update README.md file
dependabot/npm_and_yarn/jest-24.7.1	success	Merge branch 'master' into feature/home-page-announcements
dependabot/npm_and_yarn/react-accessible-accordion-3.0.0	failed	PridelnLondon / pride-london-web / feature/blog-details #497
dependabot/npm_and_yarn/react-dates-18.0.0	failed	N/A
feature/blog-details	failed	PridelnLondon / pride-london-web / feature/blog-details #496
feature/home-page-announcements	failed	Exemplary RichText content unpacking
master	success	PridelnLondon / pride-london-web / feature/blog-details #495
refactoring/imagesbanner-styles	success	Merge branch 'master' into feature/blog-details
spike/production-release	success	PridelnLondon / pride-london-web / feature/blog-details #494

Job	Type	Time Ago	ID	Logs
Workflow	build	14 min ago	01:01	#186726t
Workflow	build	2 days ago	01:01	#2284
Workflow	build	2 days ago	00:58	#ba8c768
Workflow	build	2 days ago	00:59	#4ec6f48
Workflow	build	2 days ago	01:52	#15e0816
Workflow	build	2 days ago	01:48	#32628a6
Workflow	build	2 days ago	01:01	#aa8c032
Workflow	build	2 days ago	00:46	#2285
Workflow	build	2 days ago	00:52	#a28c031
Workflow	build	2 days ago	01:00	#2286
Workflow	build	2 days ago	01:01	#1cefa84
Workflow	build	2 days ago	01:01	#2284
Workflow	build	2 days ago	01:08	#1ba8c7



circleci

Jobs » PrideInLondon » pride-london-web » master » 620 (build)

Rebuild

success Finished: 2 days ago (00:51) Previous: 609 Parallelism: 1x out of 4x Queued: 00:00 waiting + 00:01 in queue Resources: 2CPU/4096MB Workflow: workflow Context: N/A

Triggered by:
Sonya Molosse (pushed 0d9acba)

COMMIT (1)

rgryb Sonya Molosse 0d9acba Feature/blog/pagination (#255)

Test Summary

Queue (00:02)

Artifacts

Configuration

Timing

Parameters

Set Up Test Summary

Show containers: All (1) Successful (1) Failed (0)

0
(0:00:00)

0

+

TEST

Spin up Environment

00:02

Checkout code

00:01

Restore Yarn Package Cache

00:06

Install Dependencies

00:10

Save Yarn Package Cache

00:00

yarn lint

00:07

yarn test

00:23



circleci

Jobs > PridelnLondon > pride-london-web > master > 620 (build)

[C Rebuild](#)[SUCCESS](#)

Finished:

2 days ago (00:51)

Previous:

609 Tx out of 4x

Parallelism:

Queued:

00:00 waiting + 00:01 in queue

Resources:

2CPU/6096MB

Workflow:

Workflow

Context:

N/A

Triggered by:

Sonya Moisset (pushed OdBaach6)

COMMENTS (0)

igryb Sonya Moisset → OdBaach6 Feature/blog/pagination (#255)

Test Summary

Queue (00:02)

Artifacts

Configuration

Timing

Parameters

```
1 # Orb 'codecov/codecov@1.0.3' resolved to 'codecov/codecov@1.0.3'
2 version: 2
3 jobs:
4   build:
5     docker:
6       - image: circleci/node:8
7     working_directory: ~/repo
8     steps:
9       - checkout
10      - restore_cache:
11        name: Restore Yarn Package Cache
12        key:
13          - yarn-packages-{{ checksum "yarn.lock" }}
14      - run:
15        name: Install Dependencies
16        command: yarn install --frozen-lockfile
17      - save_cache:
18        name: Save Yarn Package Cache
19        key: yarn-packages-{{ checksum "yarn.lock" }}
20        paths:
21          - ~/cache/yarn
22      - run:
23        command: yarn lint
24      - run:
25        command: yarn test
26 workflows:
27   version: 2
28   workflow:
29     jobs:
30       - build
```



Environment Variables

Environment Variables for PrideInLondon/pride-london-web		
Name	Value	Remove
CODECOV_TOKEN		X
CONTENTFUL_ID		X
CONTENTFUL_TOKEN		X



Application

AccessLint

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

[Continuous integration](#)[Code review](#)[Free Trials](#)[Free](#)[Paid](#)

Supported languages

Handlebars, HTML, HTML+Django and
[3 other languages supported](#)

Customers



Developer

[AccessLint](#)

Developer links

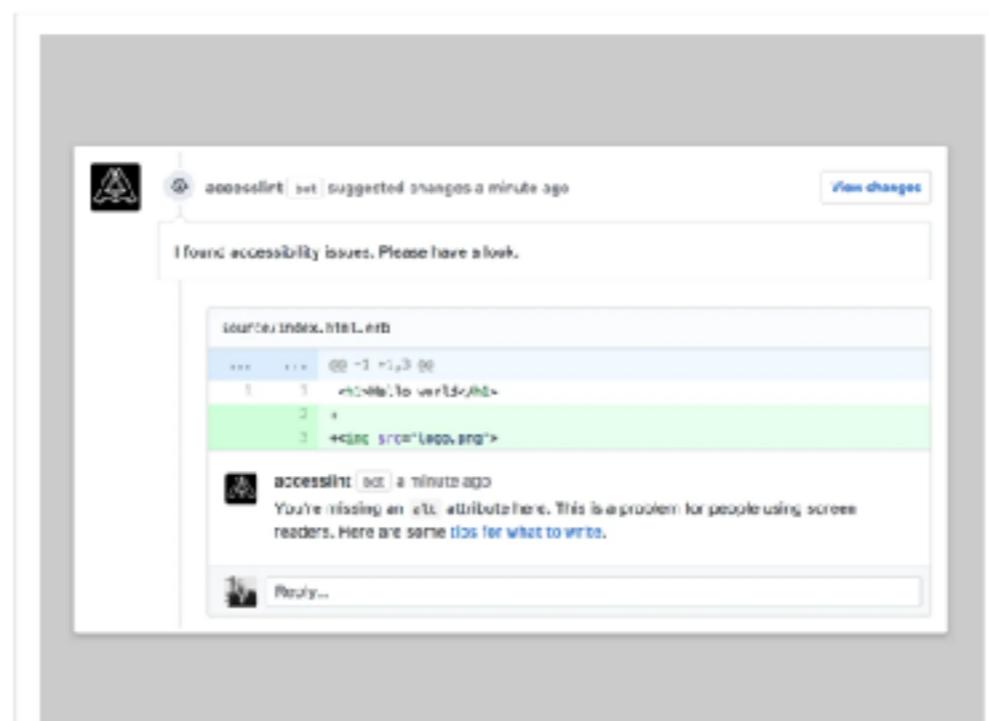
[Support](#)[Documentation](#)[Privacy Policy](#)[Report abuse](#)

AccessLint brings automated web accessibility testing into your development workflow. When a pull request is opened, AccessLint reviews the changes and comments with any new accessibility issues, giving you quick, timely, and targeted feedback, before code goes live.

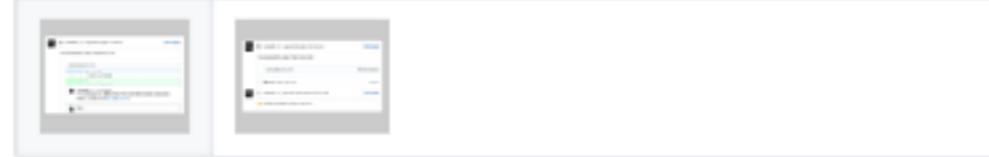
AccessLint helps you keep on target with digital accessibility by giving specific, ongoing accessibility feedback to your team. It can catch simple errors that might break your website for your customers with disabilities.

Accessibility guidelines defined in WCAG 2.0 help us build applications that work better for more people. They also give us a rough measure of compliance with legal requirements outlined in the ADA and Section 508. AccessLint runs a growing list of WCAG 2.0 tests, e.g. missing alt attributes that make pages more opaque for screenreader users, positive tabindex values that can create confusion for keyboard users, invalid ARIA, and unlabelled fields.

Use AccessLint to hold on to the hard-earned progress you've made with accessibility, or to inspire your team to start chipping away at issues. That frees you from costly bug-fixes and remediation, and socializes accessibility to your team. That way you'll have fewer bugs and can focus on delivering features.



When you open a Pull Request, AccessLint works quickly to find accessibility issues in your code, and comments with specific, line-by-line feedback.





accesslint bot suggested changes 23 days ago

[View changes](#)

accesslint bot left a comment

+ ...

There are accessibility issues in these changes.

src/components/imageBanner/_spec.js Outdated

Hide resolved

```
21  20      const wrapper = shallow(<ImageBanner />)
22  21      expect(wrapper.find(BannerSubtitle)).toHaveLength(1)
23  22    })
24  23
25 -   it('should render an <img> if passed an imageSrc prop', () => {
24 +   it('renders an <img> if passed an imageSrc prop', () => {
```



accesslint bot 23 days ago

This image is missing a text alternative (`alt` attribute). This is a problem for people using screen readers.



Reply...

[Unresolve conversation](#)

SonyaMoisset marked this conversation as resolved.



Application

Codecov

① 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

[Code quality](#)

[Code review](#)

[GitHub Enterprise](#)

[Free Trials](#)

[Free](#)

[Paid](#)

Supported languages

C, C#, Go

and [7 other languages supported](#)

Developer



Developer links

[Support](#)

[Status](#)

[Documentation](#)

[Privacy Policy](#)

[Terms of Service](#)

[Report abuse](#)

Codecov provides highly integrated tools to group, merge, archive and compare coverage reports.

1. Upload coverage reports from your CI builds.
2. Codecov merges all builds and languages into one beautiful coherent report.
3. Get commit statuses, pull request comments and coverage overlay via our browser extension via Sourcegraph.

Are you an enterprise user / desiring an on-premises install? Please out instead to enterprise@codecov.io

[Read more...](#)

Code coverage done right.[®]

Upload reports with one line. *Simply*.

Review reports. *Seamlessly*.

Reports merged. *Flawlessly*.



Proudly serving industry leaders and open source





COVERAGE CHART



COVERAGE SUNBURST



ALL RECENT COMMITS

- [Update README.md file](#) [Browse Report](#)
SonyaMoisset 18 minutes ago → master → 13b72a8 ✓ CI Passed
- [Merge branch 'master' into feature/home-page-announcements](#) [Browse Report](#)
SonyaMoisset 2 days ago #204 → 516e3a0 ✓ CI Passed
- [Footer \(#205\)](#) [Browse Report](#)
IajB4 2 days ago → feature/home-page-announcements → d4c3d32 ✓ CI Passed
- [update snapshots, update netlify robots config, remove pledge redirect](#) [Browse Report](#)
IajB4 2 days ago → master → f480139 ✓ CI Passed
- [merge in latest master and fix conflicts](#) [Browse Report](#)
IajB4 2 days ago → master → c1cf484 ✓ CI Passed
- [Merge branch 'master' into feature/home-page-announcements](#) [Browse Report](#)
SonyaMoisset 2 days ago #204 → d831d7b ✓ CI Passed

[View all recent commits](#)

File	LOC	Covered	Partially Covered	Uncovered	Total	Coverage
src	633	440	43	150	633	69.51%
empty-module.js	1	1	0	0	1	100.00%
Project Totals (75 files)	634	441	43	150	634	69.55%



Overview

Commits

Branches

Pulls

Compare

Settings

Viewing commits on all branches and pulls. Choose a single branch or pull request to review more details.

Commits

Update README.md file	SonyaMoisset	19 minutes ago	→ master	→ 10b726f	✓ CI Passed	69.55%		
Merge branch 'master' into feature/home-page-announcements	SonyaMoisset	2 days ago	→ #204	→ 519e3af	✓ CI Passed	70.17%		
Footer (#206)	laij84	2 days ago	→ feature/home-page-announcements	→ dae1d32	✓ CI Passed	69.55%		
update snapshots, update netlify robots config, remove pledge redirect	laij84	2 days ago	→ master	→ 5a6be139	✓ CI Passed	69.55%		
merge in latest master and fix conflicts	laij84	2 days ago	→ master	→ e1ef484	✓ CI Passed	69.55%	-62.50% >	
Merge branch 'master' into feature/home-page-announcements	SonyaMoisset	2 days ago	→ #205	→ d7721de	✓ CI Passed	70.17%		+0.61%
Feature/redirects (#205)	laij84	2 days ago	→ feature/blog-details	→ 10ca3cf7	✓ CI Passed	69.55%		
update invalid redirect	laij84	2 days ago	→ master	→ ee8a261	✓ CI Passed	69.55%		
remove conflicts	laij84	2 days ago	→ master	→ ad807ea	✓ CI Passed	69.55%		
merge in latest from master and resolve conflicts	laij84	2 days ago	→ master	→ 5632508	✓ CI Passed	69.55%	-40.00% >	
update redirects	laij84	2 days ago	→ feature/redirects	→ Bobb27E	✓ CI Passed	69.43%		
fix test	Unknown	2 days ago	→ #204	→ 1ed9a9d	✓ CI Passed	70.17%		+0.61%
Bump gatsby from 2.3.12 to 2.3.13	dependabot-bot	2 days ago	→ #203	→ 50534ef	✓ CI Passed	69.55%		
Bump react-dates from 16.7.0 to 18.0.0	dependabot-bot	3 days ago	→ #118	→ b0b21ef	✓ CI Passed	69.55%		
Bump jest from 23.6.0 to 24.7.1	dependabot-bot	3 days ago	→ #194	→ c910ace	✓ CI Passed	69.37%		(-0.19%)
Bump react-accessible-accordion from 2.4.5 to 3.0.0	dependabot-bot	3 days ago	→ #164	→ a1bdc29	✓ CI Passed	69.55%		
Feature/stop crawlers (#202)	laij84	3 days ago	→ feature/blog-details	→ 5ce3f51	✓ CI Passed	69.55%		
Regenerate lock files	SonyaMoisset	3 days ago	→ master	→ 9a72415	✓ CI Passed	69.55%		

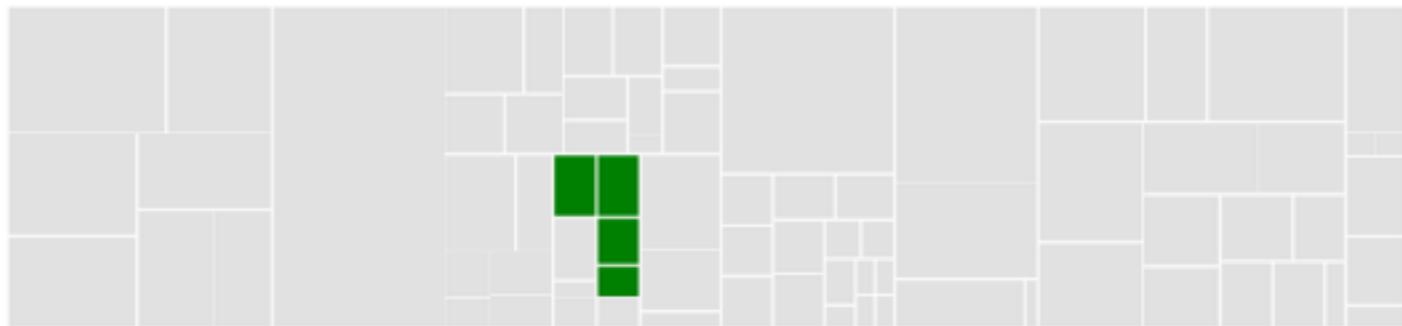


codecov bot commented 2 days ago • edited

+ 😊 ...

Codecov Report

Merging #204 into master will increase coverage by 0.61%.
The diff coverage is 100%.



@@	Coverage	Diff	@@
#	master	#204	+/-
<hr/>			
+ Coverage	69.55%	70.17%	+0.61%
<hr/>			
Files	75	79	+4
Lines	634	647	+13
Branches	87	88	+1
<hr/>			
+ Hits	441	454	+13
Misses	150	150	
Partials	43	43	

Impacted Files	Coverage Δ
...s/homepage/ccmponents/announcementHeader/styles.js	100% <100%> (ø)
...res/homepage/components/announcementCard/styles.js	100% <100%> (ø)
...ures/homepage/ccmponents/announcementCard/index.js	100% <100%> (ø)
...ses/homepage/components/announcementHeader/index.js	100% <100%> (ø)

Continue to review full report at [Codecov](#).

Legend - [Click here to learn more](#)

Δ = absolute <relative> (impact), ø = not affected, ? = missing data

Powered by [Codecov](#). Last update [dae3d32...918e3a0](#). Read the [comment docs](#).



Application

Codacy

ⓘ You have already purchased this app on GitHub Marketplace.

[Set up a new plan](#)

[Edit your plan](#)

[Configure access](#)

Verified by GitHub

CiHub confirms that this app meets the [requirements for verification](#).

Categories

[Code quality](#)

[Code review](#)

[GitHub Enterprise](#)

[Free](#)

[Paid](#)

Supported languages

Go, Java, JavaScript
and [7 other languages supported](#)

Developer



Developer links

[Support](#)

[Status](#)

[Documentation](#)

[Privacy Policy](#)

[Terms of Service](#)

[Report abuse](#)

Codacy is an automated code analysis/quality tool that helps developers ship better software, faster. With Codacy, you get static analysis, cyclomatic complexity, duplication and code unit test coverage changes in every commit and pull request.

You can use Codacy to enforce your code quality standard, save time in code reviews, enforce security best practices and onboard developers faster. Integrate with your GitHub repositories to get quality analysis of every pull request inside GitHub.

[Read more...](#)

Track your project quality evolution

Get a code quality glance at your project and track its quality evolution over time.

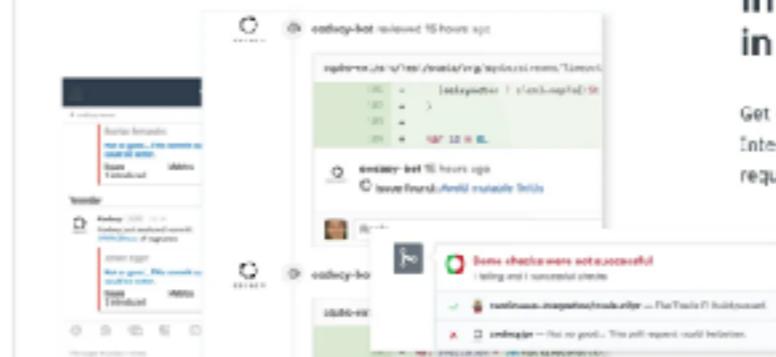
Our dashboard answers three main questions:

What is the state of your projects code quality?
How is it evolving throughout time?
What are the hotspots in my code?



Integrated in your workflow

Get only the updates you need.
Integrate comments and status on your pull requests and know exactly what's wrong and where.





C O D A C Y

pride-london-web master

[Badge](#)

B Project certification

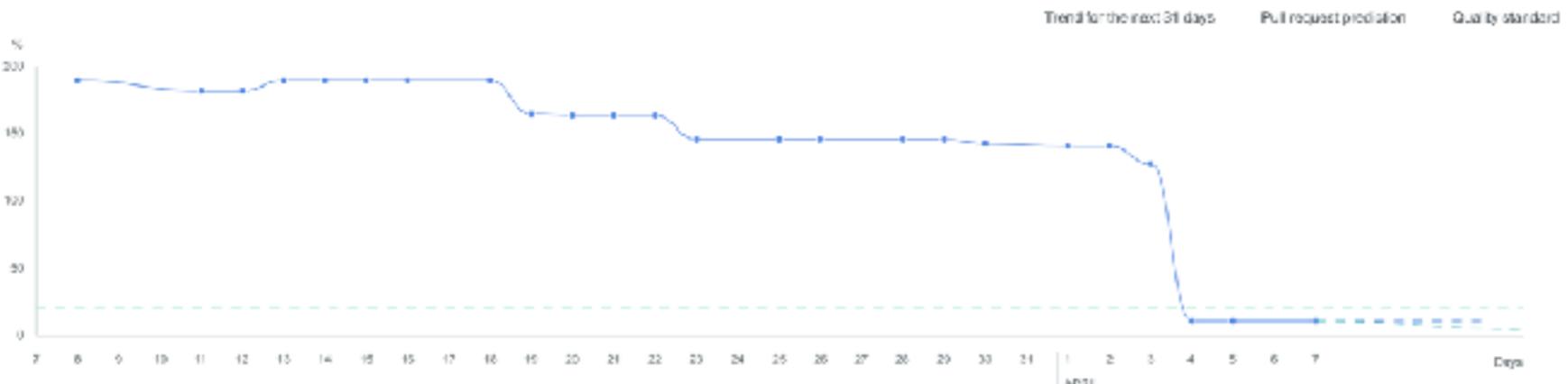
Quality evolution

Issues 11% 178%

Complex files 0%

Duplicated code 5% -2%

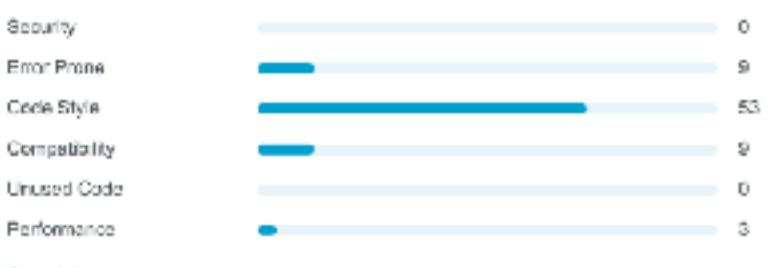
Coverage -

[Last 7 days](#)[Last 31 days](#)

Issues breakdown

74 total issues

Category

[See all issues](#)

Coverage



Make sure your code is all tested. [Set up your coverage here.](#)

Hotspots

⚠ Security pattern Prohibit instances of var[var] reported 9 times in pride-london-web

⚠ pride-london-web has 1 open pull request breaking the standards.

Logs

- Sonya Molisset ignored pattern "ESLint_react_jsx-indent-preps". 6 days ago
- Sonya Molisset ignored pattern "ESLint_react_jsx-indent". 6 days ago
- Sonya Molisset ignored pattern "Require parentheses in arrow function arguments". 18 days ago
- Sonya Molisset ignored pattern "LocalStorage". 24 days ago
- Sonya Molisset ignored pattern "A 'return', 'break', 'continue', or 'throw' statement should be the last in a block.". 25 days ago
- Sonya Molisset ignored pattern "Avoid adjoining classes". 28 days ago
- Sonya Molisset ignored pattern "Enforce coherent multiline dot". 29 days ago
- Sonya Molisset ignored pattern "Enforce Dangling Commas". 29 days ago
- Sonya Molisset disabled JSHint. about a month ago

Pull requests status



- Not up to standards 0
- Up to standards 6



C O D A C Y

Code patterns

CSSLint	<input checked="" type="checkbox"/>
ESLint 5.8.0	<input checked="" type="checkbox"/>
JSHint	<input type="checkbox"/>
JacksonLinter	<input checked="" type="checkbox"/>
Node Security	<input checked="" type="checkbox"/>
PMD 8.4.0	<input type="checkbox"/>
PMD (Legacy) 5.8.1	<input checked="" type="checkbox"/>
RemarkLint 6.0.2	<input checked="" type="checkbox"/>
Stylelint 9.4.0	<input checked="" type="checkbox"/>

Not supported

💡 ESLint is a tool for identifying and reporting on patterns found in ECMAScript/JavaScript code. In many ways, it is similar to JSLint and JSHint with a few exceptions. [Learn more](#)

Your rules configuration

Tool pattern list OR Configuration file

Select your rules for analysis from the ESLint default pattern list We will scan for a ESLint configuration file in your project root

ESLint pattern list

		Languages	Category
<input type="checkbox"/>	ESLint-angular_element ESLint-angular_element <small>JavaScript JSON Code Style</small>	JSON JavaScript	Unused Code
<input type="checkbox"/>	ESLint-angular_component-limit ESLint-angular-component-limit <small>JavaScript JSON Code Style</small>	JSON JavaScript	Error Prone
<input type="checkbox"/>	ESLint-angular_component-name ESLint-angular-component-name <small>JavaScript JSON Code Style</small>	JSON JavaScript	Compatibility
<input type="checkbox"/>	ESLint-angular_controller-as ESLint-angular-controller-as <small>JavaScript JSON Code Style</small>	JSON JavaScript	Security
<input type="checkbox"/>	ESLint-angular_controller-as-route ESLint-angular-controller-as-route <small>JavaScript JSON Code Style</small>	JSON JavaScript	Code Style
		Enabled	10
		Disabled	141
		Active	4
		Enabled	15
		Disabled	287





C O D A C Y



glancarlo88 wants to merge task/blog-page-layout into feature/blog-page · March 16

Task/blog page layout

Current Status: Analyzed View logs
View on GitHub

Not up to standards. This pull request quality could be better.

+83

Issues



Duplication

Complexity (0)

Coverage

New Issues Fixed Issues Hotspots New Duplication Fixed Duplication Files Diff Commits

Showing 16 files with new issues

src/components/horizontalRule/index.js

Rule 'no-empty-class' was removed and replaced by: no-empty-character-class (no-empty-class)

```
1 import styled from 'styled-components'
```

Rule 'no-empty-label' was removed and replaced by: no-labels (no-empty-label)

```
1 import styled from 'styled-components'
```

src/features/blog/components/newsCard/index.js

Rule 'no-empty-label' was removed and replaced by: no-labels (no-empty-label)

```
1 import React from 'react'
```

Rule 'no-empty-class' was removed and replaced by: no-empty-character-class (no-empty-class)

```
1 import React from 'react'
```

JSX not allowed in files with extension '.js' (react/jsx-filename-extension)

```
0 const CenterDot = () => <span></span>
```

Missing JSX expression container around literal string (react/jsx-no-literals)

```
0 const CenterDot = () => <span></span>
```



codebeat

PridelnLondon has already purchased the Public plan for 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

[Code quality](#)
[Code review](#)
[Free](#)
[Paid](#)

Supported languages

Elixir, Go, Java

and [7 other languages supported](#)

Developer



Developer links

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

Tired of manually scraping your code looking for the smallest issues? Take codebeat for a spin!



codebeat is an automated static code analysis tool supporting multiple languages used by both web and mobile developers worldwide. Now also providing style analysis for projects written in Swift! 🎉

We've integrated SwiftLint, the best linter for Swift in our code review app and fixed you with a [help page](#) about the feature. Enjoy!

[Read more...](#)

Check your full stack

codebeat offers unified reporting system across all supported languages. It means that all project stakeholders can easily understand what is happening inside a project.

Code Quality

- Code Review
- Code Coverage
- Code Metrics
- Code Health
- Code Style
- Code Security
- Code Duplication
- Code Complexity
- Code Maintainability

Dependency Management

- Dependency Graph
- Dependency Status
- Dependency License
- Dependency Updates
- Dependency Issues
- Dependency Score
- Dependency Health
- Dependency Risk
- Dependency Coverage

Performance

- Performance Metrics
- Performance Profiling
- Performance Analysis
- Performance Optimization
- Performance Testing
- Performance Monitoring
- Performance Health
- Performance Score
- Performance Risk

Security

- Security Metrics
- Security Profiling
- Security Analysis
- Security Optimization
- Security Testing
- Security Monitoring
- Security Health
- Security Score
- Security Risk

3.68
GPA[github.com/PrideInLondon/pride-london-...](https://github.com/PrideInLondon/pride-london-web)

10b726fb@master

Last updated: Today, 1:51 pm

60 11 3371 -

complexity issues

duplications

lines of code

-

code coverage

[Complexity](#) [Styles](#) [Duplications](#) [Security](#)[Quick Wins](#) [Namespaces](#) [Timeline](#) [Settings](#) [Pull Requests](#)

Don't wait to improve your code. Do it now!

After analysing **pride-london-web** we've found issues with the biggest overall impact on your project's health.

Try to refactor these hot spots first and see how your GPA improves.

> **Function too long** <src/features/events/components/eventsFilters.js.EventsFilters.<anonymous>
critical 92 lines of code

[Mute](#) [Report](#) [Help](#)

> **Function too long** src/components/nav/index.js.Nav
critical 163 lines of code

[Mute](#) [Report](#) [Help](#)

> **Function too long** src/components/icons/genderIcon.js.GenderIcon
critical 84 lines of code

[Mute](#) [Report](#) [Help](#)

> **Function too long** src/pages/support-us/sponsors.js.Sponsors
critical 102 lines of code

[Mute](#) [Report](#) [Help](#)

> **Function too long** src/features/events/components/eventsFilters.js.EventsFilters.render
critical 98 lines of code

[Mute](#) [Report](#) [Help](#)



CodeFactor

PridelnLondon has already purchased the Free plan for this app on GitHub Marketplace.
To complete this installation, you must [grant this app access to PridelnLondon](#).

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

Verified by GitHub

Github confirms that this app meets the [requirements for verification](#).

Categories

[Code quality](#)
[Recently added](#)
[Free Trials](#)
[Free](#)
[Paid](#)

Supported languages

C#, C++, CSS

and [7 other languages supported](#)

Developer



Developer links

[Support](#)

[Documentation](#)

[Privacy Policy](#)

[Terms of Service](#)

[Report abuse](#)

Ensure that your code meets quality standards.

CodeFactor.io seamlessly integrates with GitHub, instantly performs Code Review with every GitHub Commit or PR. Zero setup time. Get actionable feedback within seconds for any branch. Customize rules and ignore irrelevant issues. Get refactoring tips on every issue.

Multilanguage support.

C, C#, C++, CoffeeScript, CSS, GO, Groovy, Java, JavaScript, Less, PHP, Python, Ruby, Scala, SCSS, TypeScript.

[Read more...](#)

Review required At least one approved review is required by reviewers with write access. [Learn more...](#) [Add your review](#)

Some checks were not successful 2 failing and 4 successful checks [Hide all checks](#)

- X** **CodeFactor — 1 issue fixed. 2 issues found.** [Details](#)
- X** **c/bitrise/b811e91a28b1ea80/pr — Failed - Ubuntu Cake** [Required](#) [Details](#)
- ✓** **Cake Develop (Cake) — TeamCity build finished** [Details](#)
- ✓** **c/bitrise/7a9d707b000881436/pr — Passed - OSX Cake** [Required](#) [Details](#)
- ✓** **continuous-integration/appveyor/pr — AppVeyor build succeeded** [Required](#) [Details](#)

Merging is blocked Merging can be performed automatically with one approved review.

Simple statuses within your workflow.





pride-london-web A master

9.84 grade score 20 issues 149 files 5 pull requests 2 active branches

Commit [10b726f](#) by [smaisset](#) about an hour ago No issues
Update README.md file

Commit [dae3d32](#) by [laijB4](#) 2 days ago No issues
Footer (#206)

Commit [10a00c7](#) by [laijB4](#) 2 days ago No issues
Feature/redirects (#205)

Commit [5cc8f54](#) by [laijB4](#) 3 days ago No issues
Feature/stop crawlers (#202)

Commit [02244a9](#) by [smaisset](#) 3 days ago No issues
Rollback codecov update dependency

Hotspots

- D [src\components\NavItem_\spec.js](#)
- C [src\layouts\index.css](#)
- F [.circleci\config.yml](#)

Libraries 58

- [moment/moment](#) 2.24.0
- [@babel\core](#) 7.4.3
- [@babel\plugin-syntax-dynamic-import...](#)
- [@babel\preset-env](#) 7.4.3
- [@babel\preset-react](#) 7.0.0

[Show 53 more libraries...](#)



Application

LGTM

① You have already purchased this app on GitHub Marketplace.

[Set up a new plan](#)

[Edit your plan](#) -

[Configure access](#)

✓ Verified by GitHub

GithHub confirms that this app meets the requirements for verification.

Categories

[Code quality](#)

[Security](#)

[Free](#)

Supported languages

C, C++, Java
and 3 other languages supported

Developer

[lgtmhq](#)

Developer links

[Support](#)

[Documentation](#)

[Privacy Policy](#)

[Report abuse](#)

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

LGTM's extensive security analysis is constantly enhanced by findings from our dedicated team of security researchers, and by contributions from security teams at a number of top tech companies who use our technology, including Google, Microsoft and Mozilla.

Integration is easy, at the click of a button you can set up Pull Request analysis, and catch problems before they get merged.

[Read more...](#)

Pull Request Integration

Enable automatic code review to catch problems before they get merged.

asaphitzi-lgtm-bot commented on 26 Jan Member · 1g

This pull request introduces 1 alert - view on [lgtm.com](#)

new alerts:

- 1 for Regular expression injection

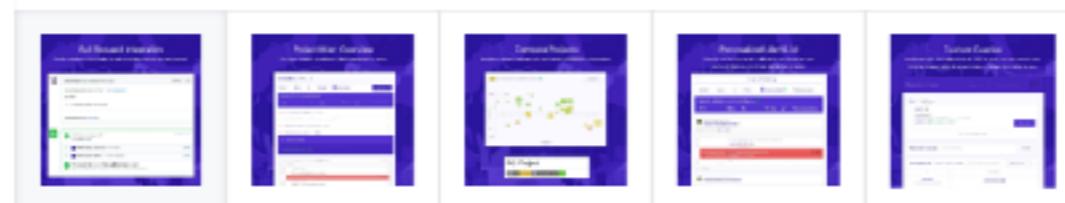
Comment posted by [lgtm.com](#)

All checks have passed 6 successful checks

- LGTM analysis: JavaScript — 1 new alert Details
- LGTM analysis: Python — No alert changes Details

This branch has no conflicts with the base branch Only those with write access to this repository can merge pull requests.

Pull Request Integration: Enable automatic code review to catch problems before they get merged.



[Overview](#)[Alerts 5](#)[Files](#)[Contributors 6](#)[Compare](#)[Dependencies](#)[Integrations](#)

Alert filters

No filter selected

[Export alerts](#)

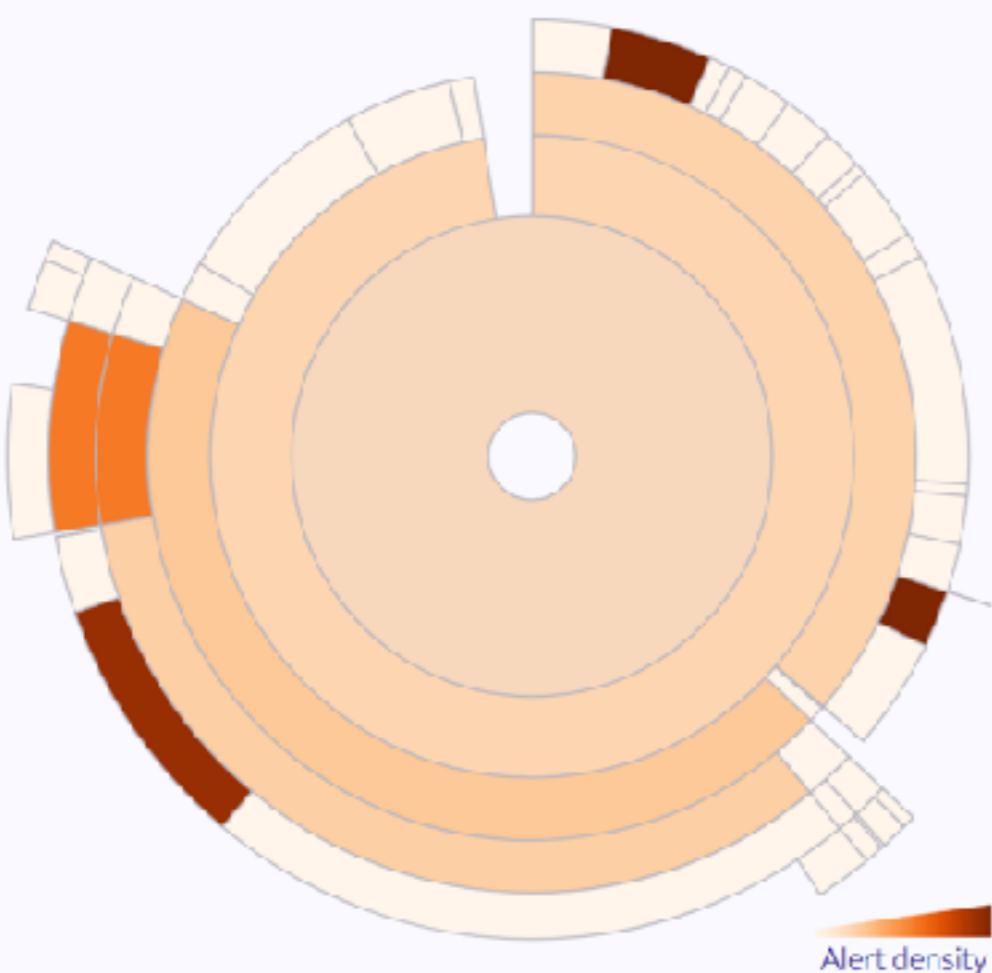
Severity

Query

Tag

 Show excluded files Show heatmap

Source root /



Name	Alerts	Lines of code
src	5	5.2k
.eslintrc	0	0
gatsby-browser.js	0	0
gatsby-config.js	0	30
gatsby-node.js	0	95
gatsby-ssr.js	0	0
package.json	0	0

← Potentially inconsistent state update

reliability

frameworks/react

Updating the state of a component based on the current value of 'this.state' or 'this.props' may lead to inconsistent component state.

[Read more](#)

[Open in query console](#)

Source root/src/.../filters/**eventDropdownFilter.js**

1 alert

```
↑ 1-117  
118  
119   toggleMenu = () => {  
120     this.setState({ isOpen: !this.state.isOpen }, () =>  
121       this.props.closeSiblingFilters(this.props.filterName, this.state.isOpen)  
122     )  
123   }  
124  
↓ 125-172
```

Component state update uses potentially inconsistent value.



Source root/src/.../appContext/index.js

1 alert

```
↑ 1-136  
137  
138   clearFilters = () => {  
139     this.setState({  
140       ...this.state,  
141       filterOpen: null,  
142       filters: getInitialFilterState(),  
143     })  
144   }  
145  
↓ 146-230
```

Component state update uses potentially inconsistent value.



Updating the state of a component based on the current value of 'this.state' or 'this.props' may lead to inconsistent component state.

Query pack: com.igtm/javascript-queries

Query ID: js/react/inconsistent-state-update

Language: JavaScript

Severity: warning

Tags: reliability, frameworks/react

Displayed by default? Yes. Alerts for this query are visible by default, but can be hidden on a per-project basis. [Learn how.](#)

React component state updates using `setState` may asynchronously update `this.props` and `this.state`, thus it is not safe to use either of the two when calculating the new state passed to `setState`.

Recommendation

Use the callback-based variant of `setState`: instead of calculating the new state directly and passing it to `setState`, pass a callback function that calculates the new state when the update is about to be performed.

Example

The following example uses `setState` to update the `counter` property of `this.state`, relying on the current (potentially stale) value of that property:

```
1  this.setState({  
2      counter: this.state.counter + 1  
3  });
```

Instead, the callback form of `setState` should be used:

```
1  this.setState(prevState => ({  
2      counter: prevState.counter + 1  
3  }));
```

References

- React Quick Start: [State and Lifecycle](#).

State and Lifecycle

This page introduces the concept of state and lifecycle in a React component.
You can find a [detailed component API reference here](#).

Consider the ticking clock example from [one of the previous sections](#). In [Rendering Elements](#), we have only learned one way to update the UI. We call `ReactDOM.render()` to change the rendered output:

```
function tick() {
  const element = (
    <div>
      <h1>Hello, world!</h1>
      <h2>It is {new Date().toLocaleTimeString()}.</h2>
    </div>
  );
  ReactDOM.render(
    element,
    document.getElementById('root')
  );
}

setInterval(tick, 1000);
```

[Try it on CodePen](#)

In this section, we will learn how to make the `Clock` component truly reusable and encapsulated. It will set up its own timer and update itself every second.

PrideInLondon/pride-london-web

JavaScript A+

Unfollow

Query this project

Overview

Alerts 3

Files

Contributors 8

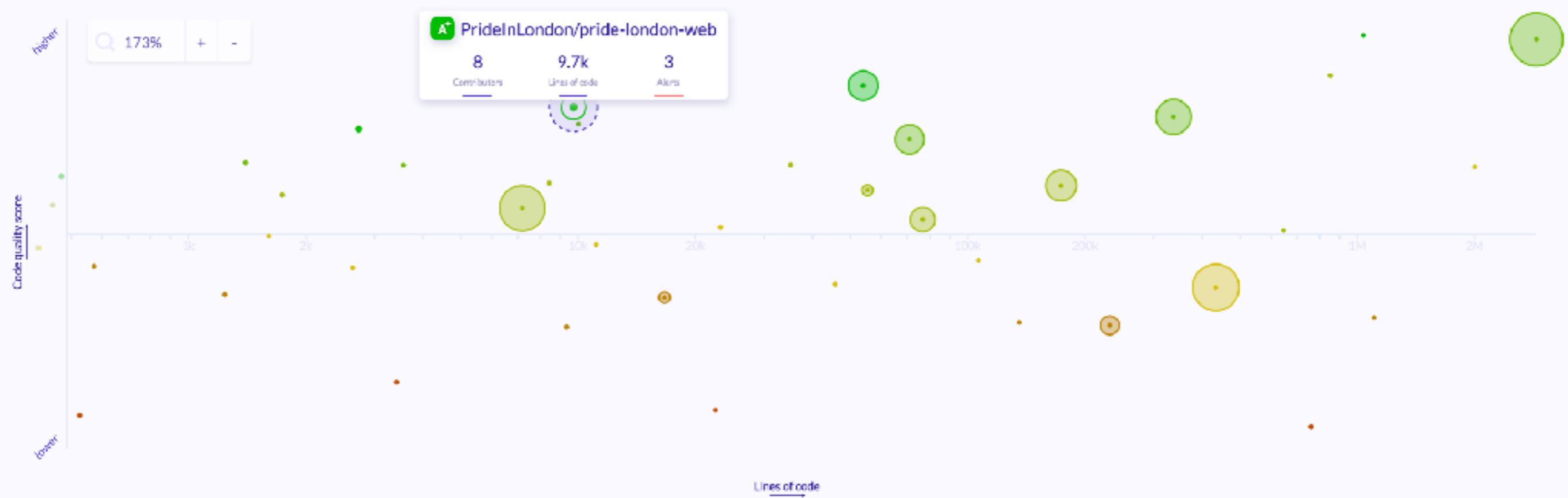
Compare

Dependencies

Integrations

A+ when compared to other JavaScript projects

Language: JavaScript Add a language





Application

GuardRails

i PrideInLondon has already purchased the Open Source plan for this app on GitHub Marketplace.

[Set up a new plan](#)

[Edit your plan ▾](#)

[Configure access](#)

Not verified by GitHub

Categories

[Code quality](#)

[Security](#)

[Free](#)

Supported languages

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

Developer

[guardrailsio](#)

Developer links

[Support](#)

[Status](#)

[Documentation](#)

[Privacy Policy](#)

[Terms of Service](#)

[Report abuse](#)

[Read more...](#)

GuardRails scans new code changes as they occur in your repositories. For pull requests, we will post comments whenever security issues are detected. For branches, you will be able to see reports in [your dashboard](#).

[Read more...](#)

The screenshot shows a GitHub pull request titled "Add users management feature #77" merged by "kytwb". A comment from "guardrails/scan" indicates "All checks have failed" due to "3 new security issues": Hard-Coded Secrets (1), Insecure Use of SQL Queries (1), and Vulnerable Libraries (1). The comment also links to "guardrails.txt" and provides a link to "Details". Below the comment, a message says "Happy with the results? Give your [feedback](#)." On the right side of the pull request interface, there are sections for "Labels", "Projects", "Milestone", "Notifications", and "Unsubscribe". At the bottom, it shows "4 other comments" and "2 participants".

GUARDRAILS

Add users management feature #77
kytwb merged 1 commit into master from Feat/add_users_management on Jan 11

All checks have failed
1 failing check

guardrails/scan — detected 3 new security issues

We detected security issues in this pull request:

- Hard-Coded Secrets (1)
- Insecure Use of SQL Queries (1)
- Vulnerable Libraries (1)

Happy with the results? Give your [feedback](#).

kytwb approved these changes on Jan 11

View changes

4 other comments

2 participants

Labels: None yet

Projects: None yet

Milestone: No milestone

Notifications: Unsubscribe

GuardRails in effect in a pull requests on GitHub.

The bottom section of the screenshot displays three smaller windows illustrating GuardRails integration: a main dashboard view, a detailed report for a specific branch, and a Slack integration interface showing real-time security findings.



fr My Account



SonyaMoisset

fr Organizations



fr Missing an organization?

fr Review your [\[authorized organizations\]](#),
fr then fr synchronize.

PrideInLondon / pride-london-web



Branches 1

Pull Requests

	PR #256	replace background image volunteer	fr No fr Issues	⌚ 00:46.808
	codedev-exp		git 27d1e02	📅 2 days ago
	PR #255	Feature/blog/pagination	fr No fr Issues	⌚ 00:48.687
	rgryb		git 208f1e9	📅 3 days ago
	PR #255	Feature/blog/pagination	fr No fr Issues	⌚ 00:52.741
	rgryb		git 09a530c	📅 3 days ago
	PR #255	Feature/blog/pagination	fr No fr Issues	⌚ 00:48.720
	rgryb		git 306b050	📅 3 days ago
	PR #255	Feature/blog/pagination	fr No fr Issues	⌚ 00:53.181
	rgryb		git 67d1026	📅 3 days ago
	PR #255	Feature/blog/pagination	fr No fr Issues	⌚ 00:49.681
	rgryb		git 2695e45	📅 3 days ago
	PR #254	Bump gatsby-source-contentful from 2.0.47 to 2.0.48	fr No fr Issues	⌚ 00:55.852
	dependabot[bot]		git 6e25d06	📅 3 days ago
	PR #253	Bump gatsby from 2.3.17 to 2.3.21	fr No fr Issues	⌚ 00:48.914
	dependabot[bot]		git 1144d36	📅 3 days ago
	PR #250	[QA #240] Partners Section - Banner H2	fr No fr Issues	⌚ 00:47.448
	SonyaMoisset		git d450f12	📅 3 days ago
	PR #252	Improvement/navigation	fr No fr Issues	⌚ 00:08.234
	leedoughty		git 3916ca7	📅 3 days ago



Application

Sonatype DepShield

ⓘ 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](#).

Sonatype DepShield is a GitHub App used by developers to identify and remediate vulnerabilities in their open source dependencies.

[Read more...](#)

Categories

[Dependency management](#)

[Security](#)

[Free](#)

Supported languages

Java and JavaScript

Developer



Developer links

[Support](#)

[Documentation](#)

[Privacy Policy](#)

[Terms of Service](#)

[Report abuse](#)

The screenshot shows a GitHub issue page for the repository `whyjustin / WebGoat`. The issue is titled `[DepShield] Vulnerability due to usage of commons-fileupload:commons-fileupload:1.2.2 #105`. It was opened by `sonatype-depshield bot` 6 days ago. The issue body contains a message from DepShield reporting a vulnerability due to the usage of `commons-fileupload:commons-fileupload:1.2.2`. The message lists three CVSS 3.0 vulnerabilities:

- (CVSS 9.8) [CVE-2016-100031] Improper Access Control
- (CVSS 7.5) [CVE-2014-0050] Permissions, Privileges, and Access Controls
- (CVSS 7.5) [CVE-2016-3092] Improper Input: Validation

On the right side of the issue page, there are sections for Assignees (No one assigned), Labels (None yet), Projects (None yet), and Milestones (No milestones).

DepShield Generates GitHub Issues for Known Security Vulnerabilities



[DepShield] (CVSS 7.4) Vulnerability due to usage of lodash.get:4.4.2 #88

 Open

sonatype-depshield bot opened this issue a day ago · 0 comments



sonatype-deps... bot commented a day ago

+ ...

Vulnerabilities

DepShield reports that this application's usage of [lodash.get:4.4.2](#) results in the following vulnerability(s):

- (CVSS 7.4) [CWE-471: Modification of Assumed-Immutable Data \(MAID\)](#)
- (CVSS 6.5) [\[CVE-2018-3721\] lodash node module before 4.17.5 suffers from a Modification of Assumed-Immutabl...](#)

Occurrences

lodash.get:4.4.2 is a transitive dependency introduced by the following direct dependency(s):

- [husky:1.3.1](#)
 - └ [cosmiconfig:5.1.0](#)
 - └ [lodash.get:4.4.2](#)

This is an automated GitHub Issue created by Sonatype DepShield. Details on managing GitHub Apps, including DepShield, are available for personal and organization accounts. Please submit questions or feedback about DepShield to the [Sonatype DepShield Community](#).

Vulnerability

CWE-471: Modification of Assumed-Immutable Data (MAID)

The software does not properly protect an assumed-immutable element from being modified by an attacker.

CVSS Score

7.4: Critical

CVSS Vector

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H

CWE

CWE-471

CVE

not recorded

Components

 [Sign In](#) to see affected components and versions.

References

URL

<https://www.npmjs.com/advisories/577>

<https://ossindex.sonatype.org/vuln/0f23ff35-235f-404f-8118-bc1580673fd0>

2 references

severity low

Prototype Pollution

`lodash`

[Advisory](#)

[Versions](#)

Overview

Versions of `lodash` before 4.17.5 are vulnerable to prototype pollution.

The vulnerable functions are '`defaultsDeep`', '`merge`', and '`mergeWith`' which allow a malicious user to modify the prototype of `Object` via `__proto__` causing the addition or modification of an existing property that will exist on all objects.

Remediation

Update to version 4.17.5 or later.

Resources

- [HackerOne Report](#)

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) High (AC:H)

Privileges Required (PR)*

None (PR:N) Low (PR:L) High (PR:H)

User Interaction (UI)*

None (UI:N) Required (UI:R)

Scope (S)*

Unchanged (S:U) Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) Low (C:L) High (C:H)

Integrity Impact (I)*

None (I:N) Low (I:L) High (I:H)

Availability Impact (A)*

None (A:N) Low (A:L) High (A:H)

* - All base metrics are required to generate a base score.

Temporal Score Metrics

Exploitability (E)

Not Defined (E:X) Unproven that exploit exists (E:U) Proof of concept code (E:P) Functional exploit exists (E:F) High (E:H)

Remediation Level (RL)

Not Defined (RL:X) Official fix (RL:O) Temporary fix (RL:T) Workaround (RL:W) Unavailable (RL:U)

Report Confidence (RC)

Not Defined (RC:X) Unknown (RC:U) Reasonable (RC:R) Confirmed (RC:C)

Environmental Score Metrics

Base Modifiers

Attack Vector (AV)

Not Defined (MAV:X) Network (MAV:N) Adjacent Network (MAV:A)

Local (MAV:L) Physical (MAV:P)

Attack Complexity (AC)

Not Defined (MAC:X) Low (MAC:L) High (MAC:H)

Privileges Required (PR)

Impact Metrics

Confidentiality Impact (C)

Not Defined (MC:X) None (MC:N) Low (MC:L)

High (MC:H)

Integrity Impact (I)

Not Defined (MI:X) None (MI:N) Low (MI:L)

High (MI:H)

Impact Subscore Modifiers

Confidentiality Requirement (CR)

Not Defined (CR:X) Low (CR:L)

Medium (CR:M) High (CR:H)

Integrity Requirement (IR)

Not Defined (IR:X) Low (IR:L) Medium (IR:M)

High (IR:H)



Dependabot

ⓘ 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](#)

[Free Trials](#)

[Free](#)

[Paid](#)

Supported languages

C#, Elm, F#,
and [7 other languages supported](#)

Customers



Developer



Developer links

[Support](#)

[Status](#)

[Privacy Policy](#)

[Terms of Service](#)

[Report abuse](#)

Dependabot helps you keep your dependencies up to date. It works with most popular languages – you can see full details of the languages we support [here](#).

Every day, Dependabot checks your dependency files for outdated or insecure 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.

[Read more...](#)

[Security] Bump bower from 1.8.2 to 1.8.8 #80

Merged dependabot merged 1 commit into master from dependabot:use_yourbower-1.x.x 7 days ago

[Conversation](#) 0 [Commits](#) 0 [By Checks](#) 0 [Files changed](#) 0

+2 -2



dependabot bot commented 7 days ago

Contributor [+1](#) ...

Bumps [bower](#) from 1.8.2 to 1.8.8. This update includes security fixes.

▪ Vulnerabilities fixed
Sourced from [The Node Security Working Group](#).

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

Affected versions: <1.8.7
▪ Release notes
▪ Commits
▪ Maintainer changes

compatibility 83%

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

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

[Dependabot commands and options](#)

↳ [!Security Bump bower from 1.8.2 to 1.8.8](#)

verified ✓ merged

↳ [dependabot bot added dependencies security labels](#) 7 days ago

Reviewers

No reviews

Assignees

No one assigned

Lables

dependencies security

Projects

None yet

Milestones

No milestone

Notifications

Subscribed

You're not receiving notifications from this thread.

1 participant:



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



[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

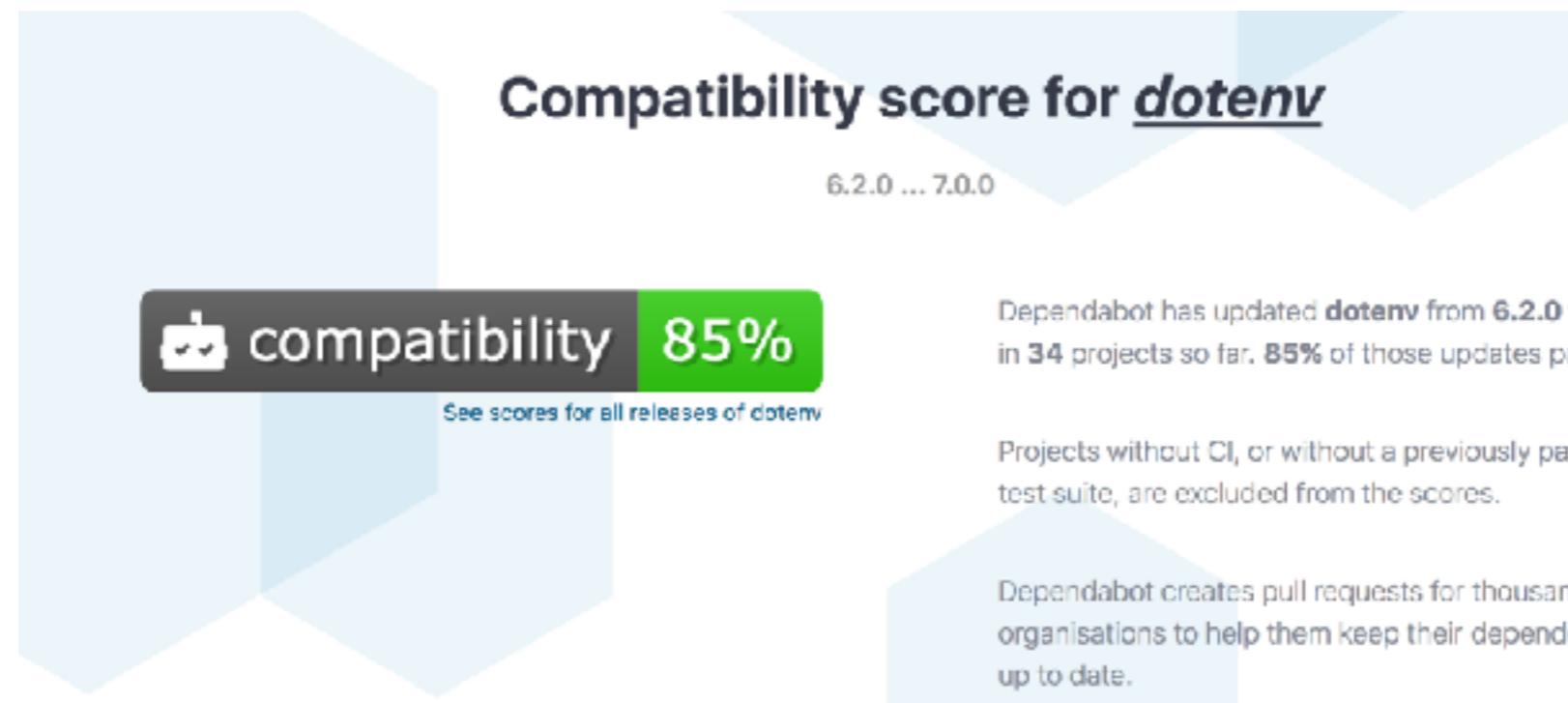
dependencies

Comments 1

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

 All checks have passed

7/7 successful checks





Application

Snyk

① You have already purchased this app on GitHub Marketplace.

[Set up a new plan](#)

[Edit your plan](#) ▾

[Configure access](#)

Verified by GitHub

Github confirms that this app meets the [requirements for verification](#).

Categories

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

Supported languages

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

Developer



Developer links

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

[Report abuse](#)

Snyk is on a mission to help developers use open source and stay secure.

Snyk helps find, fix (and prevent!) known vulnerabilities in your Node.js, Java, Ruby, Python and Scala apps. Snyk is free for open source.

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

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

[Read more...](#)

The screenshot shows the Snyk web interface. At the top, there's a navigation bar with the Snyk logo, company name, and links for 'Vulnerability DB', 'Docs', and 'My account'. Below the navigation is a search bar and project filtering options (GitHub, npm, Maven, etc.). The main area displays a list of projects under the 'Dashboard' tab:

- canidae/pug**: package.json (5 H, 2 M, 14 L), GEMfile.lock (4 H, 1 M, 1 L)
- flat-coated-retriever**: package.json (0 L, 0 M, 0 L)
- canidae/pyrenean-shepherd**: pom.xml (1 H, 0 M, 1 L)
- canidae/anatolian-shepherd**: GEMfile.lock (2 H, 1 M, 7 L)
- canidae/saint-bernard**: (empty)

Each project entry includes a 'View report and fix' button, a 'Test weekly' dropdown, and a timestamp indicating when it was last tested. Below the projects, there's a search bar with placeholder text 'Find: Quickly scan all your repos and get a high level overview on the amount of known vulnerabilities'. At the bottom, there are five small screenshots showing different parts of the Snyk interface.

**snyk**

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
Taken by	Web
Branch	master

Dependencies	1555
Tested with	package-lock.json, package.json
Manifest	package.json

Source	GitHub
Repository	pride-london-web

NEW Prioritise vulnerabilities by those introduced at runtime. [Learn more](#)



snyk

MEDIUM SEVERITY

🛡 Denial of Service (DoS)

Vulnerable module: [mem](#)

Introduced through: [gatsby@2.1.31](#)

Detailed paths and remediation

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

Remediation: No remediation path available.

Vulnerable functions

`index.module.exports.memoized()`

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

Overview

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

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

[More about this issue](#)

Create a Jira issue [UPGRADE](#)

Ignore



snyk-bot APP 10:33 AM

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

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



snyk-bot APP 3:37 PM

Prototype Pollution

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

Severity

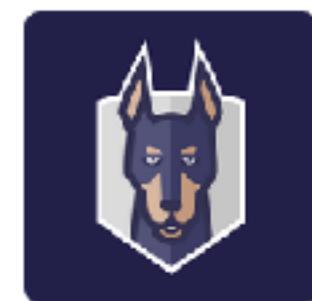
Low

Package

lodash.merge

Issue ID

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



Affected projects:

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

Package version: 4.6.1

[Fix with the CLI wizard](#)

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.

[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

Say 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

[Contact us to enable](#)



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](#)



Application Rollbar

PrideInLondon has already purchased the Free plan for this app on GitHub Marketplace.

[Set up a new plan](#)

[Edit your plan ▾](#)

[Configure access](#)



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

Categories

[Monitoring](#)

[Free](#)

[Paid](#)

Supported languages

C#, Go, Haskell and [7 other languages supported](#)

Developer



Developer links

[Support](#)

[Status](#)

[Documentation](#)

[Privacy Policy](#)

[Terms of Service](#)

[Report abuse](#)

Rollbar provides real-time, full-stack exception reporting and debugging tools for developers. Rollbar integrates in moments with apps built in **JavaScript, Ruby, Python, PHP, Node.js, Android, iOS, Go, Java, .NET** and [more](#).

Rollbar integrates with GitHub to link stack traces to the underlying source code, correlate exceptions to code changes, and create GitHub Issues so teams can manage errors in their existing workflow.

[Read more...](#)

Learn more about advanced search [Search](#)

SOURCE	ENVIRONMENT	OWNER	STATUS
Show All	production	Show All	Active

Environment Level Owner

24hr Trend	Total	IPs	Last 1	Item	Environment	Level	Owner
	42,861	4	41 secs	#167016 IndexError: list index out of range	production	Error	
	113,349	130	1 min	#187810 ApiNotFoundError: java - Resource not found in the JIRA API.	production	Error	
	304,998	-	1 min	#12197 Raw item with crash report doesn't have trace	production	Error	
	4	1	3 mins	#303721 ReferenceError: Can't find variable: auto	production	Error	
	96,875	-	3 mins	#47056 Illegal mix of colatypes for SELECT FROM person by person_id	production	Error	
	141	-	3 mins	#8817 Lost connection to MySQL server from los worker	production	Error	
	234	-	5 mins	#45010 OperationalError: OperationalError(2015, "Lost connection to MySQL server ...")	production	Error	
	37	-	5 mins	#147197 OperationalError: OperationalError(2013, "Lost connection to MySQL server ...")	production	Error	
	14,461	-	5 mins	#269482 KeyError: names'	production	Error	
	7,864	-	6 mins	#1813749 Trying to send email without recipients	production	Error	
	5,906	-	6 mins	#183812 Diving up unhandled max retries ("maxItemIndex" queued)	production	Error	
	27,398	47	7 mins	#377152 ↳ OperationalError - Deadlock	production	Error	
	7,764	293	8 mins	#303082 ↳ ReferenceError: Boomerang is not defined	production	Error	
	81	-	9 mins	#194783 Incorrect number of args for react error	production	Error	

Real-time error stream



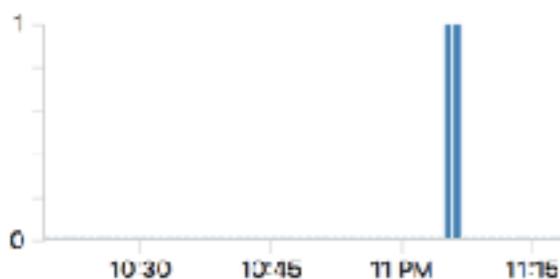
js Browser JS development

#1 TestError: Hello world

Level: Error Status: Active [Resolve](#) [Mute](#) [Report overgrouping](#) [Create GitHub Issue](#) Unassigned Not watching 0

First seen: 12 minutes ago Last seen: 11 minutes ago Occurrences: 2 IPs affected: 1

Last 60 Minutes



Last 60 Hours



Last 60 Days



Traceback [Occurrences](#) People Browser/OS IP Addresses Suspect Deploy Similar Items Co-Occurring Items Community Solutions

Timestamp (PDT)	browser	os	context	request.url	trace.exception.description	trace.exception.message	client.r...
2019-03-15 04:06 pm	Chrome	Mac OS X	node:6.14.3	https://fervent-albattani-72bcb1.netlify.com/	TestError: Hello world	Hello world	11172
2019-03-15 04:06 pm	Chrome	Mac OS X	node:6.14.3	https://5c8c2f281514740008340117--fervent-albattani-72bcb1.netlify.com/	TestError: Hello world	Hello world	31061



Feature/redirects #205

[Edit](#)[Merged](#)SonyaMoisset merged 8 commits into [master](#) from [feature/redirects](#) 2 days ago[Conversation 1](#)[Commits 8](#)[Checks 4](#)[Files changed 1](#)[+54 -20](#)

lalj84 commented 2 days ago

Member + 10 ...

No description provided.

lalj84 added some commits 3 days ago

 fix generic page layout, add default link style to index.css, fix bar... [bcb126f](#) add underline to local links [bcce408](#) add redirects, move sponsors page to new url structure [91b729c](#) Merge branch "master" into feature/redirects [9d2b8bb](#) update redirects [8ebb27f](#) merge in latest from master and resolve conflicts [5432588](#)

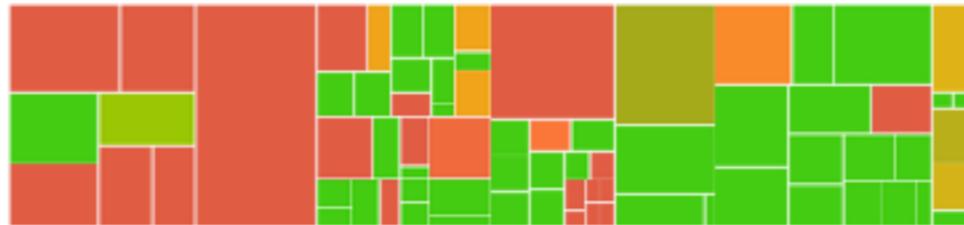
lalj84 requested a review from SonyaMoisset 2 days ago

 pull-request-size bot added the [size/M](#) label 2 days ago

codecov bot commented 2 days ago • edited

+ 10 ...

Codecov Report

Merging [#205](#) into [master](#) will not change coverage.The diff coverage is [n/a](#).

88	Coverage Diff	88
44	master	4285 +/- 44
<hr/>		
Coverage	89.55%	89.52%
Files	75	75
Lines	634	634
Branches	87	87
Hits	441	441
Misses	158	158
Partials	43	43

[Continue to review full report at Codcov.](#)[Legend - Click here to learn more](#)

E = absolute <relative> impact, N = net affected, ? = missing data

Powered by [Codecov](#). Last update [5cc8f54..ce8a261](#). Read the [comment docs](#).

Reviewers

SonyaMoisset ✓

Assignees

lalj84

Labels

 Navigation
 New Component
 New Feature
 size/M

Projects

Done in Pride in London

Milestones

Navigation

Notifications

[Unsubscribe](#)

You're receiving notifications because you modified the open/closed state.

2 participants

[Lock conversation](#)



Application

Pull Request Size

PrideInLondon has already purchased the Free plan for this app on GitHub Marketplace.

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

Not verified by GitHub

Categories

Code quality

Recently added

Free

Customers



Developer



noqks

Developer links

Support

Documentation

Privacy Policy

[Report abuse](#)

Ensure that Pull Request sizes in your organization are trending smaller with the Pull Request Size app. Each Pull Request created will be marked with a label in GitHub based on the lines of code changed.

Size Determination

The Pull Request labels are applied depending on the total lines of code changed (additions + deletions).

Label	Description
size/XS	Denotes a Pull Request that changes 0-9 lines.
size/S	Denotes a Pull Request that changes 10-29 lines.
size/M	Denotes a Pull Request that changes 30-99 lines.
size/L	Denotes a Pull Request that changes 100-499 lines.
size/XL	Denotes a Pull Request that changes 500-999 lines.
size/XXL	Denotes a Pull Request that changes 1000+ lines.

Testing Pull Request Size App #5

[Open](#) noqks wants to merge 1 commit into master from test-pull-request-size[Conversation](#)[Commits](#)[Checks](#)[Files changed](#)[Edit](#)

noqks commented 16 minutes ago

Owner [+20](#) ...

Reviewers 0

Assignees 0

Labels 0

Projects 0

Milestones 0

Notifications 0

A build service has not been set up

We have detected a top-level `build.sbt`. Pick from apps that can perform automatic builds.

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.

Pull Request Size usage



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](#).



Add more commits by pushing to the **task/blog-page-layout** branch on **PrideInLondon/pride-london-web**.



Review requested

[Show all reviewers](#)

Review has been requested on this pull request. It is not required to merge. [Learn more](#).



Some checks were not successful

[Hide all checks](#)

1 errored, 1 failing, and 5 successful checks



LGTM analysis: JavaScript — This pull request can't be analyzed because it ...

[Details](#)



Codacy/PR Quality Review — Not up to standards. This pull request quality ...

[Details](#)



AccessLint — Review complete



ci/circleci: build — Your tests passed on CircleCI!

[Details](#)



codecov/patch — 82.92% of diff hit (target 51.46%)

[Details](#)



codecov/project — 52.4% (+0.94%) compared to ecce520

[Details](#)



This branch has conflicts that must be resolved

Use the [web editor](#) or the [command line](#) to resolve conflicts.

[Resolve conflicts](#)



Add more commits by pushing to the [dependabot/npm_and_yarn/dotenv-7.0.0](#) branch on [PrideInLondon/pride-london-web](#).



Review required

[Show all reviewers](#)

At least 1 approving review is required by reviewers with write access. [Learn more](#).



All checks have passed

[Hide all checks](#)

3 neutral and 9 successful checks



AccessLint — Review complete

Required



Codacy/PR Quality Review — Up to standards. A positive pull request.

Required [Details](#)



LGTM analysis: JavaScript — No new or fixed alerts

Required [Details](#)



Mixed content - fervent-albattani-72bcb1 Successful in 1m — No mixed c...

[Details](#)



ci/circleci: build — Your tests passed on CircleCI!

Required [Details](#)



codecov/patch — Coverage not affected when comparing e805b5d...faeef84

Required [Details](#)



Merging is blocked

Merging can be performed automatically with 1 approving review.

[Update branch](#)



SonyaMoisset approved these changes 2 days ago

[View changes](#)



Pride in London [automation](#) moved this from In progress to Reviewer approved 2 days ago



SonyaMoisset merged commit `dae3d32` into `master` 2 days ago

[Hide details](#)

[Revert](#)

10 checks passed

- AccessLint** Review complete [Details](#)
- Codacy/PR Quality Review** Up to standards. A positive pull request. [Details](#)
- CodeFactor** No issues found. [Details](#)
- LGTM analysis: JavaScript** No new or fixed alerts [Details](#)
- ci/circleci: build** Your tests passed on CircleCI! [Details](#)
- codebeat** no reportable quality changes [Details](#)
- codecov/patch** Coverage not affected when comparing `10a80c7...fa8e139` [Details](#)
- codecov/project** 69.55% remains the same compared to `10a80c7` [Details](#)
- netlify/fervent-albattani-72bcb1/deploy-preview** Deploy preview ready! [Details](#)



Pride in London [automation](#) moved this from Reviewer approved to Done 2 days ago



SonyaMoisset deleted the `feature/footer` branch 2 days ago

[Restore branch](#)



GitHub APP 12:53 PM

Pull request opened by SonyaMoisset

SonyaMoisset

#65 Adding a CONTRIBUTING.md file

Adding a CONTRIBUTING.md file for new starters and updating the README file
removing the old link to Marcel repo

Assignees

SonyaMoisset

Labels

enhancement

PrideInLondon/pride-london-web | Mar 6th

Codacy/PR Quality Review: Hang in there, Codacy is reviewing your Pull request.

✓ 6 other checks have passed

6/7 successful checks



GitHub APP 12:36 PM

Pull request opened by giancarlo88

giancarlo88

#69 Task/blog page layout

Preliminary responsive grid layout (similar to Events page) and filtering.

Comments

2

Reviewers

codacy-bot

PrideInLondon/pride-london-web | Mar 9th

Codacy/PR Quality Review: Not up to standards. This pull request quality could be better.

✓ 6 other checks have passed

6/7 successful checks



Deploys for fervent-albattani-72bcb1

- <https://fervent-albattani-72bcb1.netlify.com>

Deploys from github.com/PrideInLondon/pride-london-web, published master@e805b5d.

Auto publishing is on. Deploys from master are published automatically.

[Deploy settings](#)[Notifications](#)[Stop auto publishing](#) Search deploys[Trigger deploy ▾](#)

Deploy Preview #18: dependabot/npm_and_yarn/react-... @989d9b2

Bump react-dates from 16.7.0 to 18.0.0

Today at 8:49 AM

Deployed in 1 minute



Deploy Preview #79: dependabot/npm_and_yarn/dotenv...@faceef84

Bump dotenv from 6.2.0 to 7.0.0

Today at 8:49 AM

Deployed in 1 minute



Production: master@e805b5d PUBLISHED

Update dependencies

Today at 8:46 AM

Deployed in 1 minute



Deploy Preview #90: dependabot/npm_and_yarn/gatsby...@a7f0804

Bump gatsby-plugin-react-helmet from 3.0.9 to 3.0.10

Today at 5:30 AM

Deployed in 1 minute





Netlify APP 12:13 PM

Successful deploy of **fervent-albattani-72bcb1**

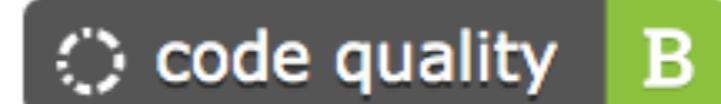
Add Netlify badge on README file (#87)

- * Add Netlify badge on README file
- * Update naming convention
- * Move dotenv package to dependency
- * Add gatsby-source-filesystem
- * Regenerate lock file
- * Fix uppercase to lowercase on gatsby-node.js
- * Remove deploy:ci script
- * Implement Rollbar agent

Or check out the build log

Using git branch master, commit e5d59759d2f | Yesterday at 12:13 PM

Pride London Web



26 labels			
Blog Details	Epic	3 open issues and pull requests	Edit Delete
Blog	Epic	3 open issues and pull requests	Edit Delete
Bug	Helper		Edit Delete
Dependencies	Helper	7 open issues and pull requests	Edit Delete
Documentation	Epic	8 open issues and pull requests	Edit Delete
Event Details	Epic	1 open issue or pull request	Edit Delete
Event	Epic	1 open issue or pull request	Edit Delete
Generic Content	Epic		Edit Delete
Homepage	Epic	7 open issues and pull requests	Edit Delete
Hotfix	Helper		Edit Delete
Idea	Helper		Edit Delete
Improvement	Helper	10 open issues and pull requests	Edit Delete
Mobile	Epic	9 open issues and pull requests	Edit Delete
Navigation	Epic	3 open issues and pull requests	Edit Delete
New Component	Helper	3 open issues and pull requests	Edit Delete
New Feature	Helper	10 open issues and pull requests	Edit Delete
QA	Epic	14 open issues and pull requests	Edit Delete
Refactoring	Helper	8 open issues and pull requests	Edit Delete
Security	Epic	3 open issues and pull requests	Edit Delete
SEO	Epic	3 open issues and pull requests	Edit Delete
size/L		2 open issues and pull requests	Edit Delete
size/M		2 open issues and pull requests	Edit Delete
size/S		1 open issue or pull request	Edit Delete
size/XS			Edit Delete
size/XXL			Edit Delete
Sponsors	Epic	3 open issues and pull requests	Edit Delete

↑ 14 Open ✓ 0 Closed			
Homepage	No due date	Last updated 2 days ago	Edit Close Delete
QA	No due date	Last updated 2 days ago	Edit Close Delete
Sponsors	No due date	Last updated 2 days ago	Edit Close Delete
Navigation	No due date	Last updated 2 days ago	Edit Close Delete
Documentation	No due date	Last updated 2 days ago	Edit Close Delete
Security	No due date	Last updated 2 days ago	Edit Close Delete
Refactoring	No due date	Last updated 3 days ago	Edit Close Delete
Generic Content	No due date	Last updated 3 days ago	Edit Close Delete
Blog	No due date	Last updated 4 days ago	Edit Close Delete
Event	No due date	Last updated 14 days ago	Edit Close Delete
Blog Details	No due date	Last updated 16 days ago	Edit Close Delete
Event Details	No due date	Last updated 16 days ago	Edit Close Delete

Homepage

No due date 61% complete

Homepage Epic

5 Open	✓ 8 Closed
<hr/>	
QA	[QA] Volunteer Section - Replace pixelated Images Homepage Improvement QA
#222	opened 2 days ago by SonyaMolisset
QA	[QA] Volunteer Section - Show more volunteers Homepage Improvement QA
#220	opened 2 days ago by SonyaMolisset
Announcements	X Homepage New Component New Feature size/L
#204	opened 2 days ago by codedev-exp + Review required
Donate	Homepage New Feature
#108	opened 17 days ago by SonyaMolisset
Announcements	Homepage New Feature
#107	opened 17 days ago by SonyaMolisset

PrideInLondon/pride-london-web > Projects > Pride in London

+ Add cards ⌂ Last refresh ⌂ Menu

Filter cards

Backlog

- [GitHub] Add an open source licence #208 opened by SonyaMoloset Documentation Improvement
- [Netlify] Move back to policy: [userAgent: ""] when live #207 opened by SonyaMoloset Navigation Refactoring
- Donate #108 opened by SonyaMoloset Homepage New Feature
- Form #109 opened by SonyaMoloset New Component Sponsors
- Configure Blog landing page to query for Views content type #160 opened by giancarlo88 Blog Improvement
- Configure Blog landing page article categories to use list of categories predefined from Contentful instead of their own content type #165 opened by giancarlo88 Blog Improvement
- Configure Blog landing page articles to use 'Article' content type #187 opened by giancarlo88 Blog Improvement
- Configure Blog landing page featured article to use Featured Article content type #190 opened by giancarlo88 Blog Improvement
- Pagination #171 opened by SonyaMoloset Blog New Component
- OG Tags & Twitter cards #197 opened by SonyaMoloset

In progress

- [QA] Volunteer Section - Replace pixelated images #222 opened by SonyaMoloset Homepage Improvement QA
- [QA] Volunteer Section - Refactor button to match design #221 opened by SonyaMoloset Homepage Improvement QA
- [QA] Volunteer Section - Show more volunteers #220 opened by SonyaMoloset Homepage Improvement QA
- [QA] Volunteer Section - Shapes should be 2x images #218 opened by SonyaMoloset Improvement Navigation QA
- [QA] Header - Add duotone image #218 opened by SonyaMoloset Improvement Navigation QA
- [QA] Footer - Company number link #217 opened by SonyaMoloset Improvement Navigation QA
- [QA] Footer - Add newsletter sign up on events footer #216 opened by SonyaMoloset Improvement Navigation QA
- [QA] Footer - Remove third hashtag #215 opened by SonyaMoloset Improvement Navigation QA
- [QA] Footer - Add hover state to links #214 opened by SonyaMoloset Improvement Navigation QA
- [QA] Partners Section - Responsive logos (RedBadger style) #213 opened by SonyaMoloset Improvement QA Sponsors
- Bump gatsby from 2.3.12 to 2.3.13 #223 opened by dependabot Dependencies Security size/M
- Announcements #204 opened by codedev-exp Homepage New Component New Feature size/M
- Render static content #193 opened by SonyaMoloset Blog Details New Feature
- Blog page content logic #127 opened by SonyaMoloset Blog Details New Feature
- Blog page layout and styling #128 opened by SonyaMoloset Blog Details New Feature
- Announcements #107 opened by SonyaMoloset Homepage New Feature
- Extract ImageBanner styles #173 opened by SonyaMoloset Improvement Refactoring size/M
- Bump react-accessible-accordion from 2.4.5 to 3.0.0 #164 opened by dependabot Dependencies Security size/M
- Bump react-dates from 18.7.0 to 18.8.0 #10 opened by dependabot Dependencies Security size/M

Review in progress

Reviewer approved

Done

- Redirects & rewrite rules #177 opened by SonyaMoloset Improvement Navigation
- Footer #206 opened by laj84 Navigation Refactoring size/M
- Changes approved #205 opened by laj84 Navigation New Component New Feature size/M
- Feature/redirects #203 opened by laj84 Navigation New Component New Feature size/M
- Changes approved #202 opened by laj84 Improvement New Feature size/M
- Feature/stop crawlers #200 opened by laj84 Improvement New Feature size/M
- Changes approved #200 opened by laj84 Navigation New Component New Feature size/M
- Redirects #199 opened by laj84 Navigation New Component New Feature size/M
- Changes approved #199 opened by laj84 Refactoring size/L
- (Hotfix) Props name and delete duplicate Home folder #198 opened by codedev-exp Hotfix Refactoring size/L
- Changes approved #198 opened by codedev-exp
- Add a Digital section #118 opened by SonyaMoloset New Feature Sponsors
- Generic Content page styles #123 opened by SonyaMoloset Generic Content Improvement
- Generic pages layout



GitLab

	Manage	Plan	Create	Verify	Package	Secure	Release	Configure	Monitor	Defend
GitLab is a single application for the entire DevOps lifecycle.	Since 2016 GitLab added:	Since 2011 GitLab added:	Since 2011 GitLab added:	Since 2012 GitLab added:	Since 2016 GitLab added:	Since 2017 GitLab added:	Since 2016 GitLab added:	Since 2018 GitLab added:	Since 2016 GitLab added:	Coming in 2019:
	Cycle Analytics	Project Management	Source Code Management	Continuous Integration (CI)	Container Registry	SAST	Continuous Delivery (CD)	Auto DevOps	Metrics	Runtime Application Self Protection
	DevOps Score	Kanban Boards	Code Review	Code Quality	Maven Repository	DAST	Release Orchestration	Kubernetes Configuration	Logging	Web Application Firewall
	Audit Management	Time Tracking	Wiki	Performance Testing	NPM Registry	Dependency Scanning	Pages	ChatOps	Cluster Monitoring	Threat Detection
	Authentication and Authorization	Agile Portfolio Management	Snippets		Container	Container Scanning	Review apps	Runbook Configuration	Tracing	Error Tracking
		Service Desk	Web IDE		Scanning	License Management	Incremental Rollout	Serverless		Behavior Analytics
				Coming in 2019:	Rubygem Registry	Coming in 2019:	Feature Flags	Coming in 2019:	Coming in 2019:	Vulnerability Management
				System Testing	Linux Package Registry	Secret Detection		PaaS	Synthetic Monitoring	Data Loss Prevention
	Coming in 2019:	Value Stream Management	Coming in 2019:	Usability Testing	Helm Chart Registry	Coming in 2019:	Coming in 2019:	Chaos Engineering	Incident Management	Container Network Security
	Code Analytics	Requirements Management	Design Management	Accessibility Testing	Dependency Proxy	IAST	Release Governance	Cluster Cost Optimization	Status Page	
	Workflow Policies	Quality Management	Live Coding	Compatibility Testing	Fuzzing					
GitLab could replace										

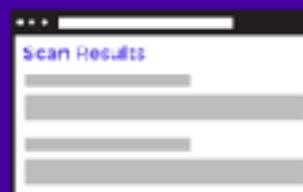
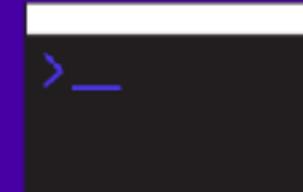
MORE TOOLS

ONLINE SCAN



Use webhint to improve your website

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

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

Why use webhint?



FULLY CUSTOMIZABLE

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



CREATE YOUR OWN HINTS

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



COMMUNITY DRIVEN

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

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

SCANNING 100%

SCAN TIME: 03:00

HINTS

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

DATE: 2019-03-13 13:03

76

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

 ACCESSIBILITY
HINTS
1PASSED
0/1

Compatibility

 expand all

 content-type: 17 hints

 COMPATIBILITY
HINTS
3PASSED
4/7
 highest-available-document-mode: 1 hints

 PWA
HINTS
1PASSED
3/4
 meta charset utf-8: 1 hints

 PERFORMANCE
HINTS
4PASSED
3/7

PWA

 expand all

 apple-touch-icons: 1 hints

 PITFALLS
HINTS
0PASSED
0/0
 SECURITY
HINTS
5PASSED
5/10

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

Lighthouse

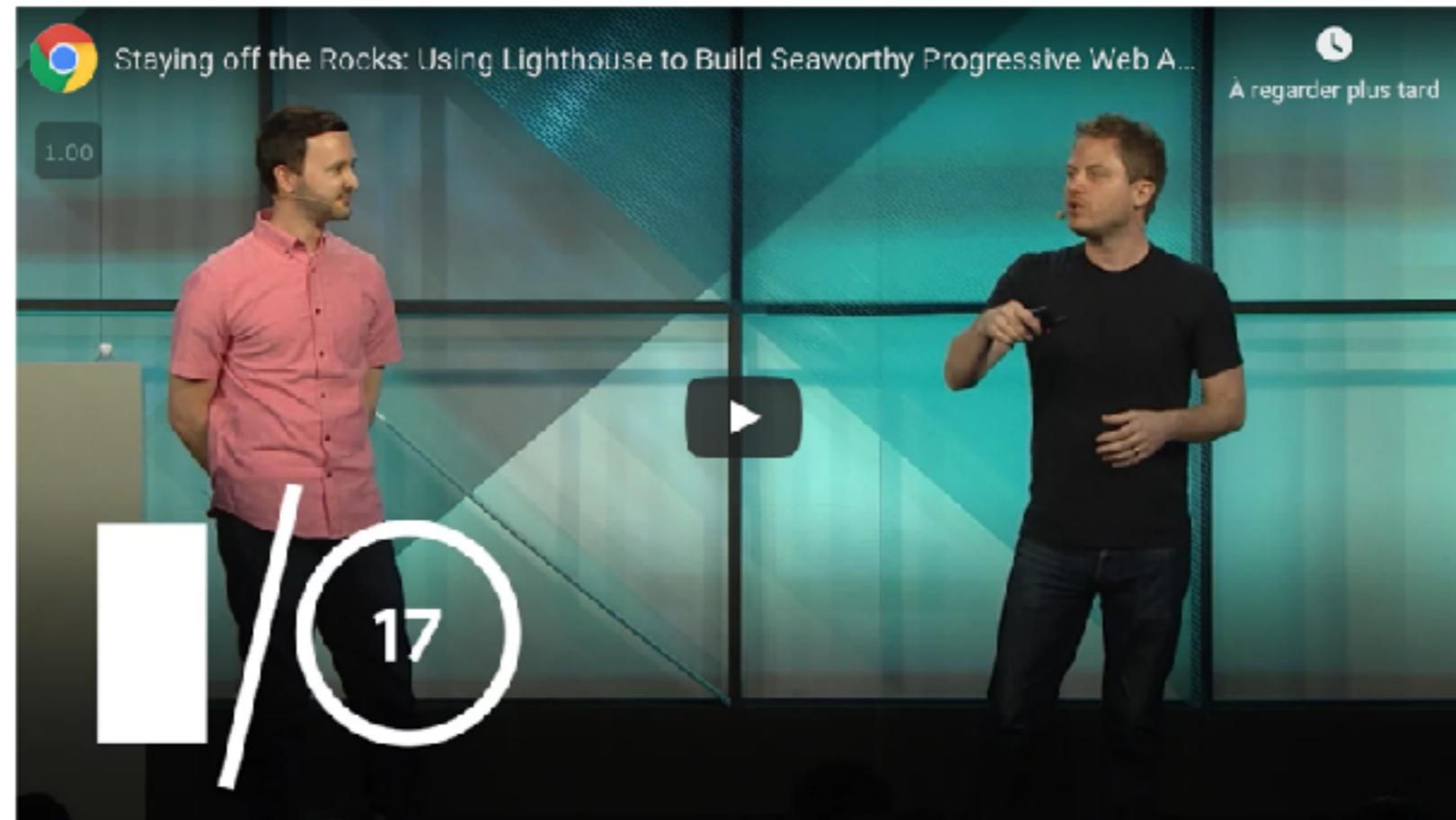


Lighthouse is an [open-source](#), automated tool for improving the quality of web pages. You can run it against any web page, public or requiring authentication. It has audits for performance, accessibility, progressive web apps, and more.

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

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

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

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

The screenshot shows the Polymer Project Shop homepage. At the top, there's a navigation bar with a menu icon, the word "SHOP", and a shopping cart icon. Below the header, there's a large image of a person from behind, wearing a textured jacket. To the right of the image, the text "Men's Outerwear" is displayed, followed by a "SHOP NOW" button.

Audits help you identify and fix common problems that affect your site's performance, accessibility, and user experience. [Learn more](#)

[Perform an audit...](#)

The screenshot shows the Chrome DevTools Audits tab for the URL `shop.polymer-project.org` at 9/26/2017, 4:59:10 P. The tab is currently selected, showing four audit scores:

- Progressive Web App: 100
- Performance: 88
- Accessibility: 100
- Best Practices: 85

Progressive Web App
These audits validate the aspects of a Progressive Web App, as specified by the baseline [PWA Checklist](#). 100

- 0 failed audits
- 11 Passed Audits
- Manual checks to verify

Performance
These encapsulate your app's performance. 88

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

Scan your site now

Scan

Hide results Follow redirects

Grand Totals

A+	706,238
A	5,067,049
B	1,652,057
C	902,875
D	3,079,011
E	2,050,396
F	14,110,812
R	2,832,408
Total	30,400,846

Recent Scans

proline.physics.li...	E
yzthundecoc.tk	F
lakeareahomesandra...	F
wlagency.ru	D
wiki.mk7.jp	F
kasp27.ru	D
officeinvoice.com	F
diepriv.helpforski...	F
www.billfishermans...	F

Hall of Fame

www.aupiedleve.org	A
www.dashlane.com	A
console.dashlane.c...	A
iphonesoft.fr	A
rosiefurniture.com	A
www.instagram.com	A
avalon.skynet-corp...	A
www.patreon.com	A
securityheaders.co...	A+

Hall of Shame

lifewordonline.com	F
www.carmax-blows.n...	F
yzthundecoc.tk	F
lakeareahomesandra...	F
wiki.mk7.jp	F
officeinvoice.com	F
diepriv.helpforski...	F
www.billfishermans...	F
pacho.com	F

Security Report Summary



Site:	https://www.facebook.com/
IP Address:	2a03:2880::131:83:face:00c0:025de
Report Time:	14 Apr 2019 20:04:31 UTC
Headers:	<input checked="" type="checkbox"/> X-Content-Type-Options <input checked="" type="checkbox"/> Strict-Transport-Security <input checked="" type="checkbox"/> Content-Security-Policy <input checked="" type="checkbox"/> X-Frame-Options <input checked="" type="checkbox"/> X-XSS-Protection <input type="checkbox"/> Referrer-Policy <input type="checkbox"/> Feature-Policy
Warning:	Grade capped at A, please see warnings below.

Supported By

Netsparker - security scanner

Go beyond secure http headers and scan your website for critical vulnerabilities malicious hackers can exploit.

[Free Demo](#)

Raw Headers

HTTP/1.1	200 OK
Cache-Control	private, no-cache, no-store, must-revalidate
Expires	Sat, 01 Jan 2000 00:00:00 GMT
Vary	Accept-Encoding
X-Content-Type-Options	nosniff
Pragma	no-cache
Strict-Transport-Security	max-age=15552000; pre load 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-eval' 'unsafe-eval' blob: data: 'self'; style-src data: blob: 'unsafe-inline' *; connect-src *.facebook.com facebook.com *.fbcn.net *.facebook.net *.spotilocal.com: * wss://*.facebook.com: * https://fb.scanandcleanlocal.com: * attachment: fbsbx.com ws://localhost: * blob: *.cdm.instagram.com 'self' chrome-extension://beadgeojelhgndaghlijhdicflkmllpaid chrome-extension://dliochdbjfkdbacpmhlcpmleaejidimm;
content-security-policy	
X-Frame-Options	DENY
expect-ct	max-age=86400, report-uri='https://reports.fb.com/expectct/'
X-XSS-Protection	0
Set-Cookie	fr=1<1qvCBUzgHZcf81..Bcs5jP.c9.AAA.0.0.Bcs5jP.AWUxtF4m; expires=Sat, 13-Jul-2019 20:04:31 GMT; Max-Age=7776000; path=/; domain=.facebook.com; secure; httponly
Set-Cookie	sb=T5KzXB3k41Au8isJ3o1B7KRx; expires=Tuesday, 13-Apr-2021 20:04:31 GMT; Max-Age=63072000; path=/; domain=.facebook.com; secure; httponly
Content-Type	text/html; charset="utf-8"
X-FB-Debug	0CQ0ZIM2Sg3MNjFcpjjU2fwCs0KvhgDHXPQmjKmjjEMULtoNsNr3AA1jAQZY3oK+NqfIRun2xTtKa+2ubSPhvW==
Date	Sun, 14 Apr 2019 20:04:31 GMT
Transfer-Encoding	chunked
Connection	keep-alive

WHAT'S NEXT FOR YOU?

BECOME A
SECURITY
CHAMPION!



Security Champions playbook

Identify teams

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

Define the role

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

Nominate champions

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

Comm channels

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

Knowledge base

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

Maintain interest

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



<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
APRIL 25 - LOGICALIS UK LTD

OWASP LONDON
CHAPTER

GET SECURE, BE SECURE AND STAY SECURE



Thank
you!



IF YOU LIKE WHAT YOU'VE SEEN
WE'RE RECRUITING DEVS & QA
:)

@SONYAMOISSET  
SONYAMOISSET@PRIDEINLONDON.ORG