

PRODUCT SERIES @ FLATIRON

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?



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](#)

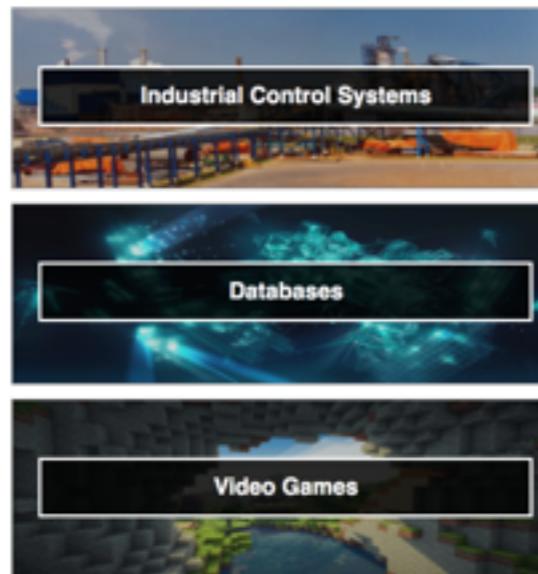




Explore

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. webcam surveillance cams 2010-03-15
4,089	Cams admin admin cam webcam 2012-02-06
2,256	Netcam Netcam netcam 2012-01-13
1,582	default password Finds results with "default password" in the ba... router default password 2010-01-14
1,087	dreambox dreambox dreambox 2010-08-13

More popular searches...

Recently Shared

1	chile 2018-10-08
2	router control panel DD-WRT routeur 2018-10-08
3	1 2018-10-06
1	Logitech Media Server 2018-10-05
3	sushi 2018-10-05

More recent searches...



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!

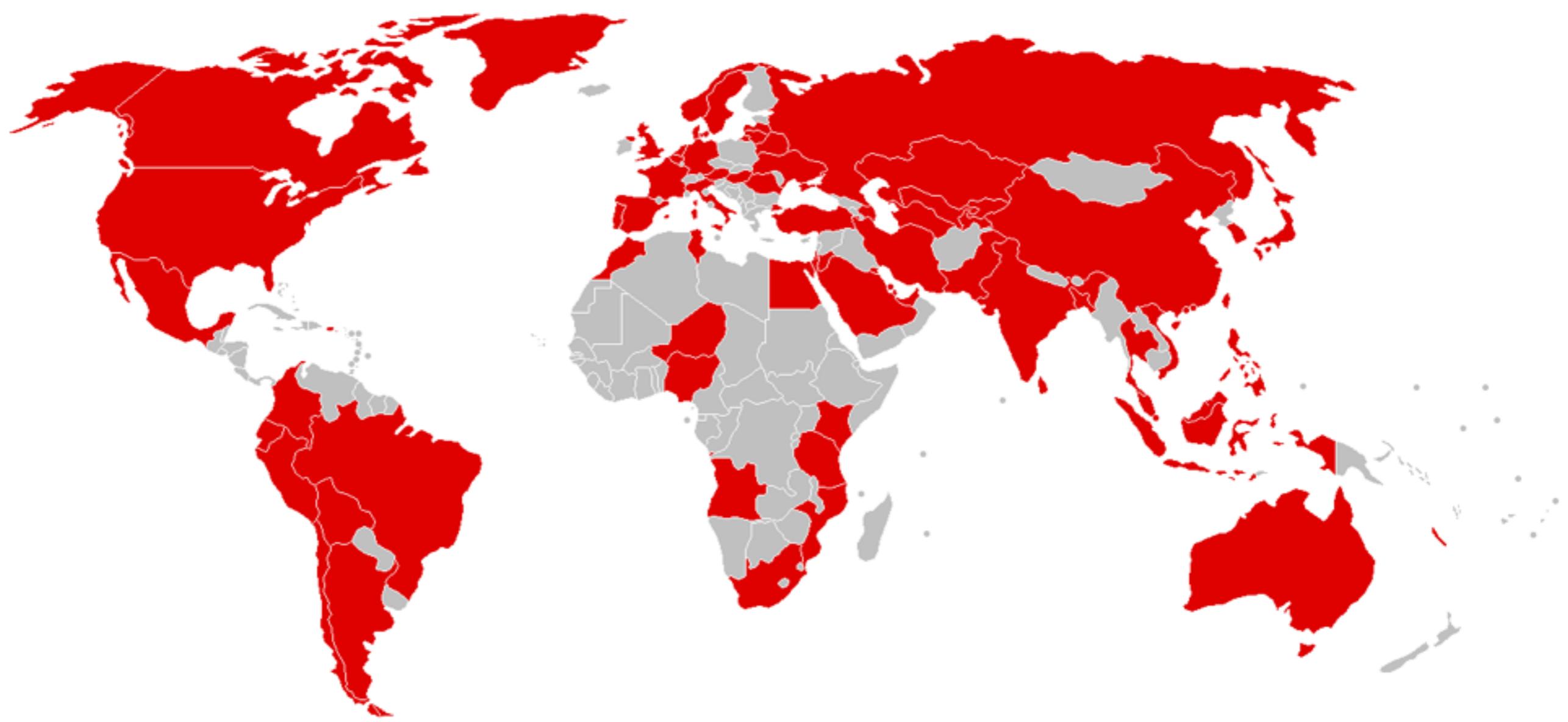


Send \$600 worth of bitcoin to this address:

Copy

[Check Payment](#)

[Decrypt](#)



[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

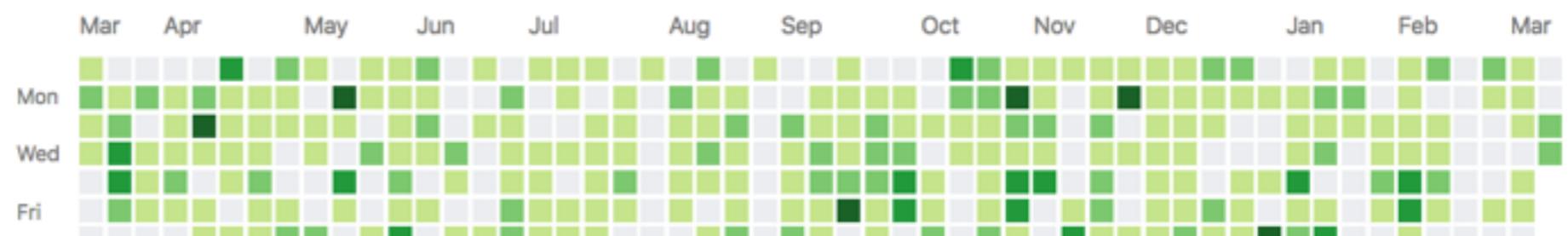
New Zealand

<http://protozoa.nz>

Organizations



2,485 contributions in the last year



[Learn how we count contributions.](#)

Less More

EVENT STREAM POST MORTEM

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



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

The Secure, Shared Bitcoin Wallet

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

[GET COPAY](#)



WHAT IS THE EVENT-STREAM PACKAGE?

- It's a toolkit that provides utilities to create and manage streams
- Authored by Dominic Tarr (dominictarr on npmjs)
- One of the 432 packages he owns on npmjs
- Received contributions from 33 different contributors
- 2000 stars

SOCIAL ENGINEERING DEVS



devinus commented on Jul 31, 2015

...

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



devinus commented on Jul 31, 2015

...

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



dominictarr commented on Jul 31, 2015

Owner

...

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

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

TIMELINE OF EVENTS



December 7, 2011
event-stream package created

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

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

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

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

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

November 26, 2018
HackerNews post appears

November 26, 2018
flatmap-stream package removed from npm

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

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



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

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

 dominictarr / event-stream

 Watch ▾ 72  Star 2,044  Fork 146

 Code

 Issues 7

 Pull requests 0

 Projects 0

 Wiki

 Insights

EventStream is like functional programming meets IO

 322 commits

 1 branch

 13 releases

 34 contributors

 MIT

Branch: master ▾

Create new file

Upload files

Find File

Clone or download ▾

 **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

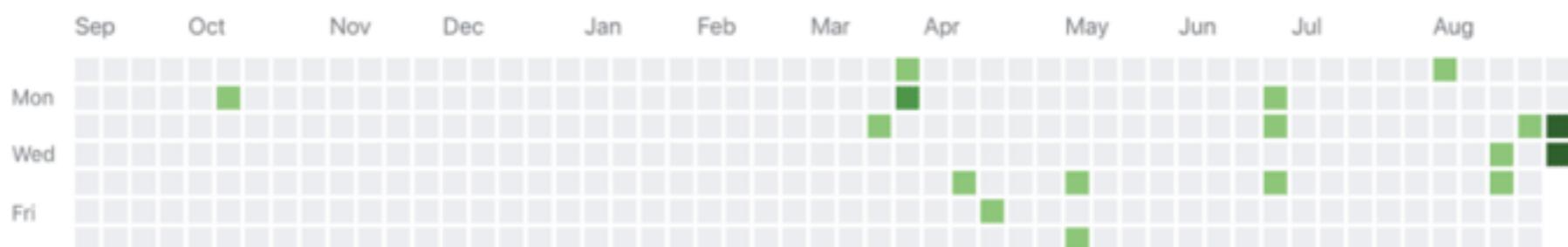
right9ctrl

[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](#)

	@@	-86,7	+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 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 IN THE SYSTEM
- .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



DONATE
OWASP DONATION PORTAL



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

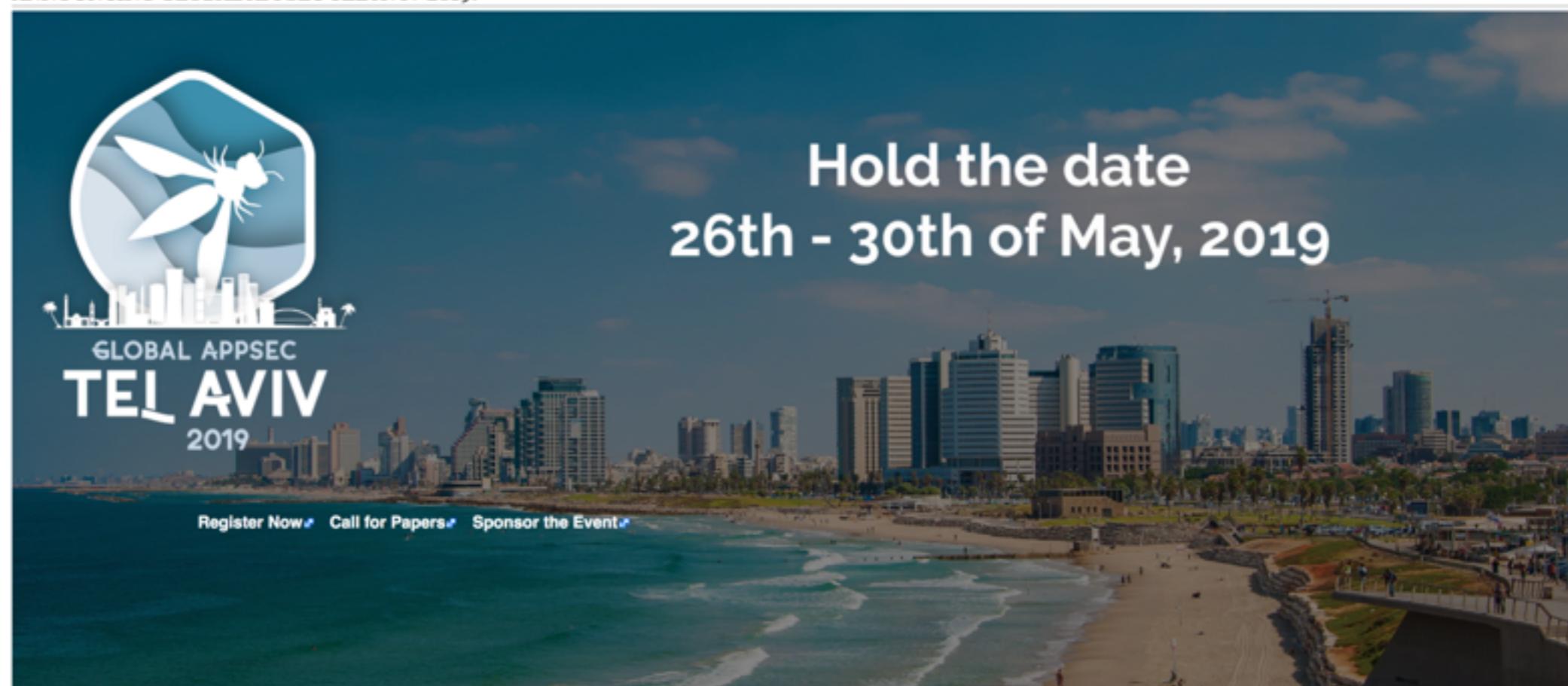
Reference
Activities
Attacks
Code Snippets
Controls
Glossary
How To...
Java Project
.NET Project
Principles
Technologies
Threat Agents
Vulnerabilities

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

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

[Statistics](#) • [Recent Changes](#)

ANNOUNCING GLOBAL APPSEC TEL AVIV 2019!



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



OWASP 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

A6:2017-Security Misconfiguration

Epic:

Attackers will often attempt to exploit unpatched flaws or access default accounts, unused pages, unprotected files and directories, etc to gain unauthorized access or knowledge of the system.

Abuse Case:

As an attacker, I find and exploit missing appropriate security hardening configurations on any part of the application stack, or improperly configured permissions on cloud services.

Abuse Case:

As an attacker, I find unnecessary features which are enabled or installed (e.g. unnecessary ports, services, pages, accounts, or privileges) and attack or exploit the weakness.

Abuse Case:

As an attacker, I use default accounts and their passwords to access systems, interfaces, or perform actions on components which I should not be able to.

Abuse Case:

As an attacker, I find areas of the application where error handling reveals stack traces or other overly informative error messages I can use for further exploitation.

Abuse Case:

As an attacker, I find areas where upgraded systems, latest security features are disabled or not configured securely.

Abuse Case:

As an attacker, I find security settings in the application servers, application frameworks (e.g. Struts, Spring, ASP.NET), libraries, databases, etc. not set to secure values.

Abuse Case:

As an attacker, I find the server does not send security headers or directives or they are not set to secure values.

C2. LEVERAGE SECURITY FRAMEWORKS AND LIBRARIES

- Secure coding libraries and software frameworks with embedded security help software developers guard against security-related design and implementation flaws
- A developer writing an application from scratch might not have sufficient knowledge, time, or budget to properly implement or maintain security features. Leveraging security frameworks helps accomplish security goals more efficiently and accurately

IMPLEMENTING BEST PRACTICES

- Use libraries and frameworks from trusted sources that are actively maintained and widely used by many applications
- Create and maintain an inventory catalog of all the third party libraries and components
- Proactively keep libraries and components up to date

[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



jest

24.5.0 • Public • Published 5 days ago

Readme

2 Dependencies

4,379 Dependents

216 Versions

Jest

Delightful JavaScript Testing

- Developer Ready: Complete and ready to set-up JavaScript testing solution. Works out of the box for any React project.
- Instant Feedback: Failed tests run first. Fast interactive mode can switch between running all tests or only test files related to changed files.
- Snapshot Testing: Jest can [capture snapshots](#) of React trees or other serializable values to simplify UI testing.

Read More: <https://jestjs.io/>

Keywords

ava babel coverage easy expect facebook immersive instant jasmine jest
jsdom mocha mocking painless qunit runner sandboxed snapshot tap tape
test testing typescript watch

install

```
> npm i jest
```

weekly downloads

4,681,533



version

24.5.0

license

MIT

open issues

520

pull requests

69

homepage

jestjs.io

repository

[github](#)

last publish

5 days ago

collaborators



gatsby

2.1.37 • Public • Published a day ago

Readme

122 Dependencies

140 Dependents

1,051 Versions



install

```
> npm i gatsby
```

Gatsby v2



:rocket:

Blazing fast modern site generator for React

Go beyond static sites: build blogs, ecommerce sites, full-blown apps, and more with Gatsby.

[license](#) MIT [build](#) [passing](#) [npm](#) v2.1.37 [downloads](#) 2M/m [PRs](#) welcome

[Quickstart](#) · [Tutorial](#) · [Plugins](#) · [Starters](#) · [Showcase](#) · [Contribute](#) · [Support: Spectrum & Discord](#)

Gatsby is a modern framework for blazing fast websites.

- **Go Beyond Static Websites.** Get all the benefits of static websites with none of the limitations. Gatsby sites are fully functional React apps, so you can create high-quality, dynamic web apps, from blogs to ecommerce sites to user dashboards.
- **Use a Modern Stack for Every Site.** No matter where the data comes from, Gatsby sites are built using React and GraphQL. Build a uniform workflow for you and your team, regardless of whether the data is coming from the same backend.
- **Load Data From Anywhere.** Gatsby pulls in data from any data source, whether it's Markdown files, a headless CMS like Contentful or WordPress, or a REST or GraphQL API. Use source plugins to load your data, then develop using Gatsby's uniform GraphQL interface.
- **Performance Is Baked In.** Ace your performance audits by default. Gatsby automates code splitting, image optimization, inlining critical styles, lazy-loading and prefetching resources, and more to ensure your site is fast — no manual tuning required.

weekly downloads

406,896



version

2.1.37

license

MIT

open issues

386

pull requests

123

homepage

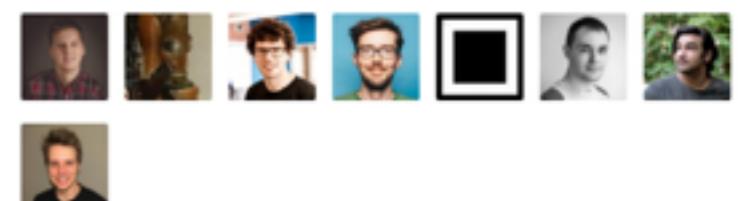
[github.com](#)

repository

[github](#)

last publish
a day ago

collaborators



[Test with RunKit](#)

[Report a vulnerability](#)

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

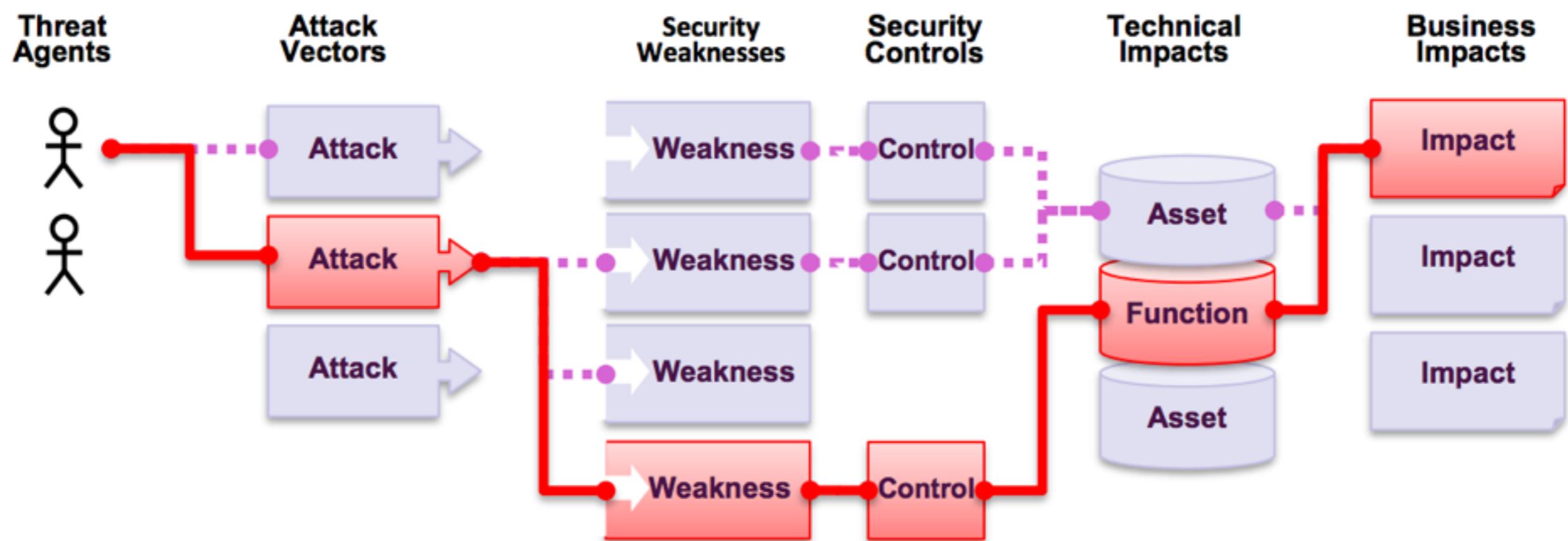
The Ten Most Critical Web Application Security Risks



- . DON'T STOP AT 10
- . CONSTANT CHANGE
- . PUSH LEFT, RIGHT, AND EVERYWHERE

WHAT ARE APPLICATION SECURITY RISKS?

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



WHAT CHANGED FROM 2013 TO 2017?

OWASP TOP 10

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

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





Pride in London

[Repositories 3](#)[People 6](#)[Teams 1](#)[Projects 0](#)[Settings](#)[Type: All ▾](#)[Language: All ▾](#)[Customize pins](#)[New](#)

pride-london-web

Pride In London's New Website

JavaScript MIT Updated 2 hours ago



Top languages

JavaScript

pride-london-web-old

Forked from MarcelCutts/pride-london-web-gatsby

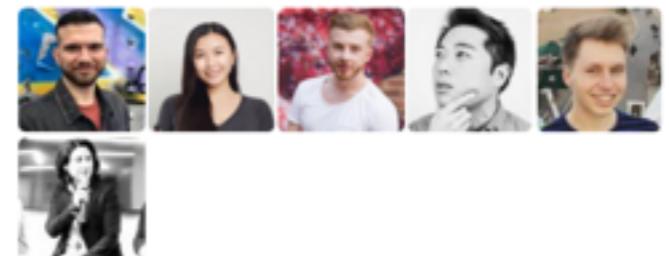
Pride in London's front end web platform

JavaScript 2 MIT Updated 16 days ago



People

6 >

[Invite someone](#)

pride-web-webhook

webhook service to help trigger travis builds from contentful



JavaScript MIT Updated on Jun 19, 2018

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



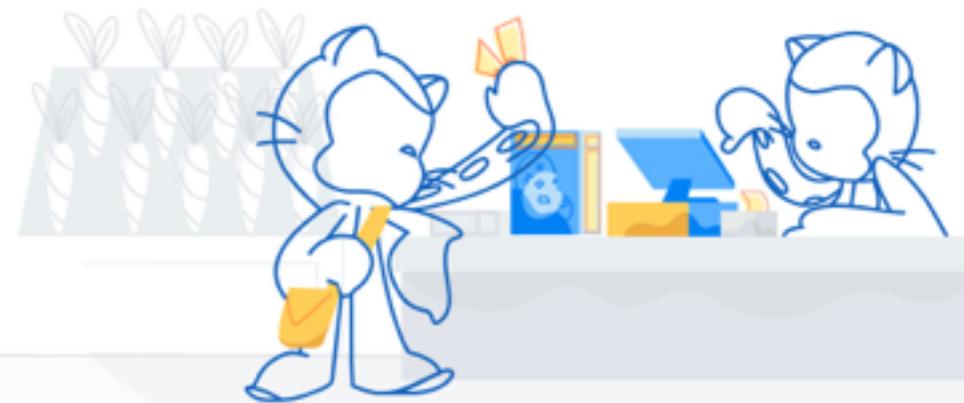
15 – 22 Jun 2018 • 8am – 5.30pm

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

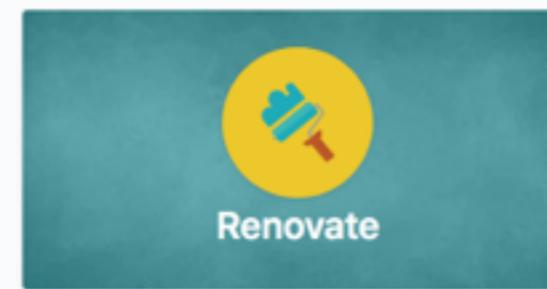
Featured apps



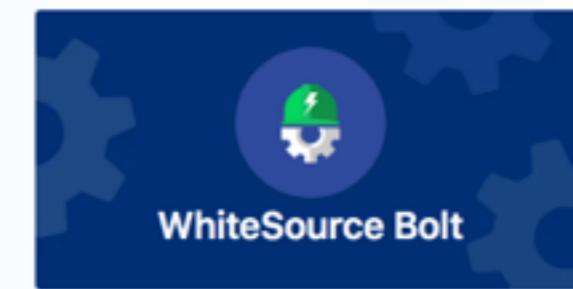
Zube



codebeat



Renovate



WhiteSource Bolt

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

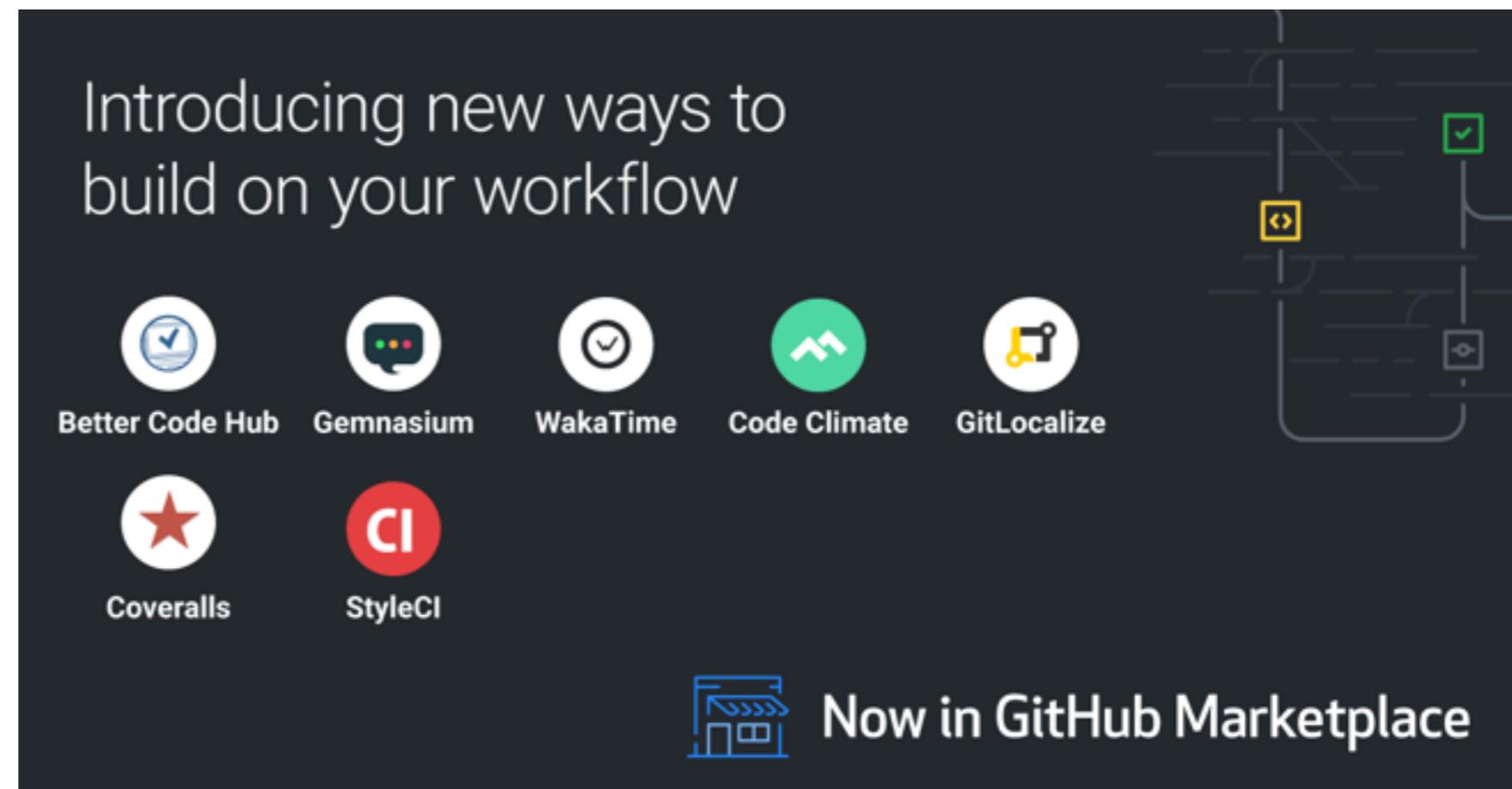


CodeFactor

Automated code review for GitHub

WHAT IS GITHUB MARKETPLACE

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





circleci



PridelnLondon



Updates

Support



Workflows » PridelnLondon » pride-london-web » master



By project

My branches



Showing 1–30

pride-london-web



SUCCEEDED

master / workflow

Add Netlify badge on README file (#87)

1 day ago

00:54

e5d5975

dependabot/npm_and_yarn/dotenv-7.0.0

2 days ago

00:54

e5d5975



dependabot/npm_and_yarn/react-dates-18.0.0

1 day ago

00:54

49de821



feature/blog-page

1 day ago

00:46

49de821



feature/navigation

3 hours ago

00:46

fd9b99e



feature/sponsors

26 days ago

00:49

48da787



master

1 day ago

00:49

48da787



spike/production-release

15 days ago

01:00

1087ff0



task/blog-page-layout

1 day ago

01:00

1087ff0



task/dynamic-blogs

1 day ago

00:49

cb2d455



master / workflow

6 days ago

00:49

cb2d455



master / workflow

1 week ago

00:55

853084b



master / workflow

master / workflow

master / workflow

master / workflow



circleci

Jobs » PrideInLondon » pride-london-web » master » 188 (build)

2.0

C Rerun workflow



SUCCESS

Finished: Previous: Parallelism: Queued: Resources: Workflow: Context:

1 day ago (00:51) 173

1x out of 4x 00:00 waiting + 00:01 in queue

2CPU/4096MB

workflow

N/A

Triggered by:

Janine Luk (pushed e5d5975)

COMMITS (1)

Sonya Moisset Janine Luk -o e5d5975 Add Netlify badge on README file (#87)

Test Summary

Queue (00:01)

Artifacts

Configuration

Timing

Parameters

Set Up Test Summary

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

0
(0:51)



TEST

Spin up Environment

00:01

Checkout code

00:00

Restoring Cache

00:04

Install Dependencies

00:19

Saving Cache

00:11

yarn lint

00:04

yarn test

00:09



circleci

Test Summary

Queue (00:01)

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        keys:
12          - v1-npm-deps-{{ checksum "package-lock.json" }}
13          - v1-npm-deps-
14      - run:
15        name: Install Dependencies
16        command: npm install
17      - save_cache:
18        key: v1-npm-deps-{{ checksum "package-lock.json" }}
19        paths:
20          - ./node_modules
21      - run:
22        command: yarn lint
23      - run:
24        command: yarn test
25 workflows:
26   version: 2
27   workflow:
28     jobs:
29       - build
30
31 # Original config.yml file:
32 # version: 2.1
33 #
34 # orbs:
35 #   codecov: codecov/codecov@1.0.3
36 #
37 # jobs:
38 #   build:
39 #     docker:
40 #       - image: circleci/node:8
41 #     working_directory: ~/repo
42 #
43 #     steps:
44 #       - checkout
45 #
46 #       - restore_cache:
47 #         keys:
48 #           - v1-npm-deps-{{ checksum "package-lock.json" }}
49 #           - v1-npm-deps-
50 #
51 #       - run:
52 #         name: Install Dependencies
53 #         command: npm install
54 #
55 #       - save_cache:
56 #         key: v1-npm-deps-{{ checksum "package-lock.json" }}
```



Environment Variables

Environment Variables for PridelnLondon/pride-london-web

[Import Variables](#)[Add Variable](#)

Add environment variables to the job. You can add sensitive data (e.g. API keys) here, [rather than placing them in the repository](#).

Name	Value	Remove
CODECOV_TOKEN		×
CONTENTFUL_ID		×
CONTENTFUL_TOKEN		×



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.

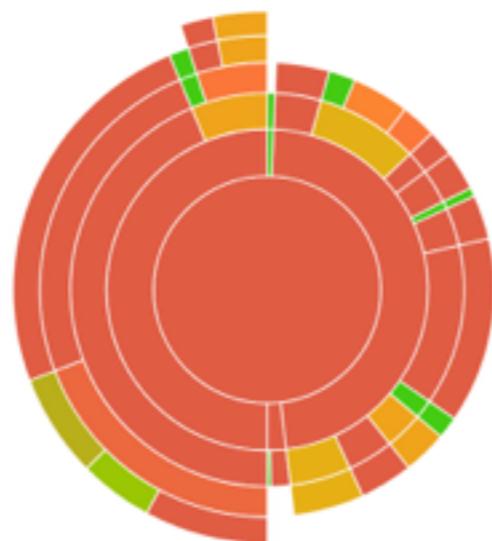
[Overview](#)[Commits](#)[Branches](#)[Pulls](#)[Compare](#)[Settings](#)

Showing min per day coverage for the last 6 months

COVERAGE CHART



COVERAGE SUNBURST



ALL RECENT COMMITS

- | | | | | | |
|--|---|-------------------------------|--------------------|------------|-----------|
| | Fix tests | Browse Report | | | |
| | giancarlo88 | a day ago | task/dynamic-blogs | -> 2e31e63 | CI Passed |
| | remove shortid | Browse Report | | | |
| | laij84 | a day ago | feature/navigation | -> 2efeac1 | CI Passed |
| | remove no-scroll package, finish nav styles | Browse Report | | | |
| | laij84 | a day ago | feature/navigation | -> 40186d5 | CI Passed |
| | Bump react-dates from 16.7.0 to 18.0.0 | Browse Report | | | |
| | dependabot-bot | a day ago | #18 | -> fa7c35f | CI Passed |
| | Add Netlify badge on README file (#87) | Browse Report | | | |
| | SonyaMoisset | a day ago | master | -> e5d5975 | CI Passed |
| | Fix jest-jdom version | Browse Report | | | |
| | giancarlo88 | a day ago | #69 | -> 9e81077 | CI Passed |

[View all recent commits](#)

Files	318	153	28	137	Coverage
src	318	153	28	137	48.11%
Project Totals (23 files)	318	153	28	137	48.11%



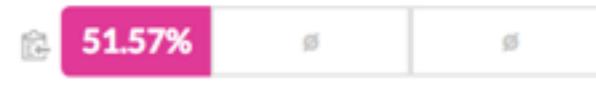
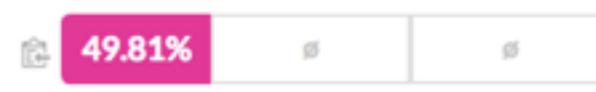
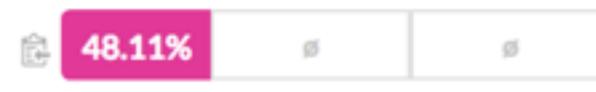
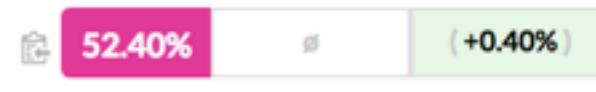
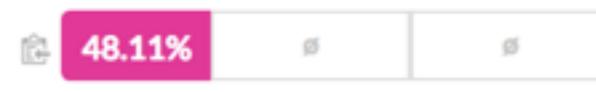
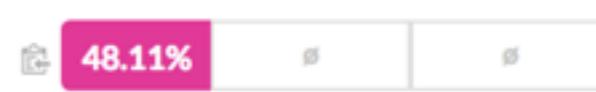
Codecov

Code coverage done right.

[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

[Fix tests](#)**giancarlo88** a day ago task/dynamic-blogs 2e31e63 CI Passed[remove shortid](#)**laij84** a day ago feature/navigation 2efeacl CI Passed[remove no-scroll package, finish nav styles](#)**laij84** a day ago feature/navigation 40186d5 CI Passed[Bump react-dates from 16.7.0 to 18.0.0](#)**dependabot-bot** a day ago #18 fa7c35f CI Passed[Add Netlify badge on README file \(#87\)](#)**SonyaMoisset** a day ago master e5d5975 CI Passed[Fix jest-jdom version](#)**giancarlo88** a day ago #69 9e81077 CI Passed[Implement Rollbar agent](#)**SonyaMoisset** 2 days ago master 77fb7fa CI Passed[Remove deploy:ci script](#)**SonyaMoisset** 2 days ago master 1989363 CI Passed



C O D A C Y

pride-london-web master

Badge

C Project certification

Quality evolution

Issues • ②
190% ▲190%

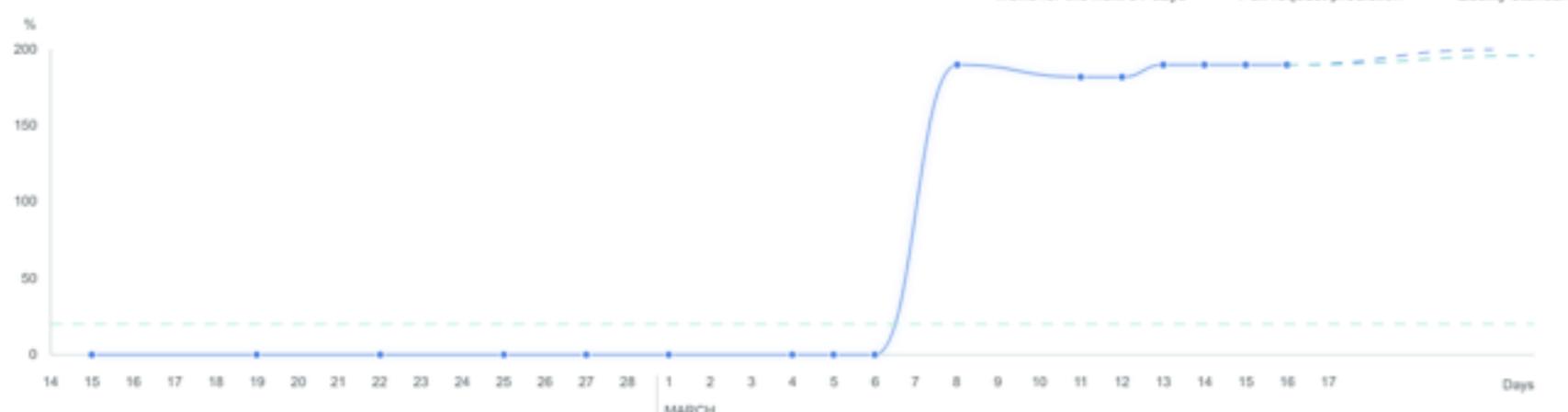
Complex Files ②
-

Duplicated code ④ ②
3% =

Coverage ②

Last 7 days

Last 31 days



Issues breakdown

1487 total issues

Category

	Total
Security	9
Error Prone	1163
Code Style	304
Compatibility	9
Unused Code	0
Performance	2

[See all issues](#)

Coverage



Make sure your code is all tested. Set up your coverage here.

Project ②

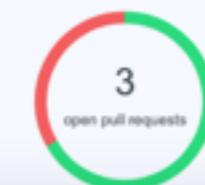
Hotspots

- ⚡ pride-london-web has decreased 37% in quality in the last 7 days.
- ⚠️ Security pattern Prohibit instances of var[var] reported 10 times in pride-london-web
- ❗ pride-london-web has 1 open pull request breaking the standards.

Logs

- 👤 Sonya Moisset ignored pattern "Local Storage". 3 days ago
- 👤 Sonya Moisset ignored pattern "A "return", "break", "continue", or "throw" statement should be the last in a block.". 4 days ago
- 👤 Sonya Moisset ignored pattern "Avoid adjoining classes". 8 days ago
- 👤 Sonya Moisset ignored pattern "Enforce coherent multiline dot". 8 days ago
- 👤 Sonya Moisset ignored pattern "Enforce Dangling Commas". 8 days ago
- 👤 Sonya Moisset disabled JSHint. 20 days ago

Pull requests status



- 🔴 Not up to standards 1
- 🟢 Up to standards 2





C O D A C Y

Code patterns

CSSLint



💡 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](#)

ESLint 5.8.0



JSHint



JacksonLinter



Node Security



PMD 6.4.0



PMD (Legacy) 5.8.1



RemarkLint 6.0.2



Stylelint 9.4.0



Not supported ⓘ

Your rules configuration

Tool pattern list

Select your rules for analysis from the ESLint default pattern list

OR

Configuration file

We will scan for a ESLint configuration file in your project root

ESLint pattern list



Languages

JSON
Javascript

ESLint-angular-angularelement

ESLint-angular-angularelement

[Javascript](#) [JSON](#) [Code Style](#)

ESLint-angular-component-limit

ESLint-angular-component-limit

[Javascript](#) [JSON](#) [Code Style](#)

ESLint-angular-component-name

ESLint-angular-component-name

[Javascript](#) [JSON](#) [Code Style](#)

ESLint-angular-controller-as

ESLint-angular-controller-as

[Javascript](#) [JSON](#) [Code Style](#)

ESLint-angular-controller-as-route

ESLint-angular-controller-as-route

[Javascript](#) [JSON](#) [Code Style](#)

Category

Unused Code	10
Error Prone	141
Compatibility	4
Security	15
Code Style	287

Active

Enabled	300
Disabled	157





C O D A C Y



giancarlo88 wants to merge task/blog-page-layout into feature/blog-page March 16

Task/blog page layout

Current Status: Analysed View logs
View on GitHub

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

+83

Issues



Duplication

Complexity

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)

```
6 const CenterDot = () => <span>-</span>
```

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

```
6 const CenterDot = () => <span>-</span>
```

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

Alert filters

No filter selected

[Export alerts](#)

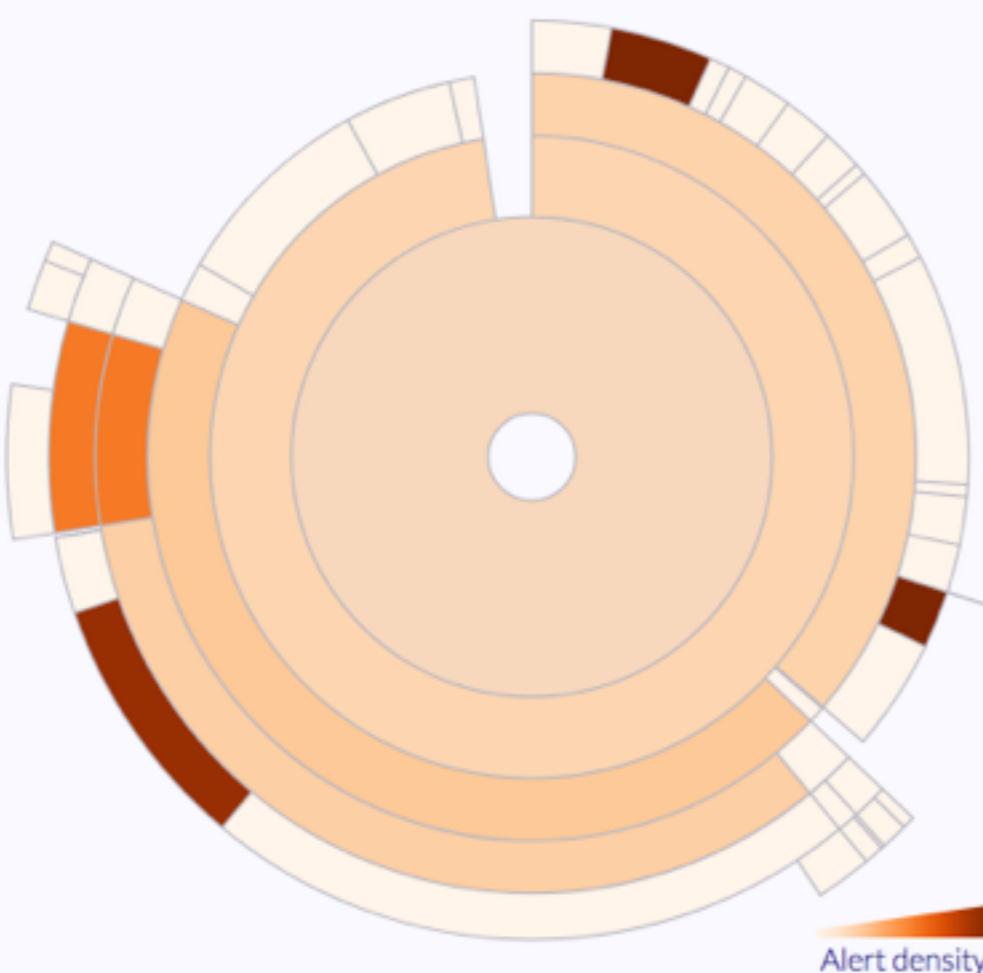
Severity

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   }
```

Component state update uses potentially inconsistent value.



```
145
↓ 146-230
```

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.lgtm/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](#).

PrideInLondon/pride-london-web

JavaScript A

Unfollow

Query this project

Overview

Alerts 5

Files

Contributors 6

Compare

Dependencies

Integrations

A when compared to other JavaScript projects

Language: JavaScript Add a language



[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

severity low

Prototype Pollution

lodash

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

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)

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 +1 ...

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

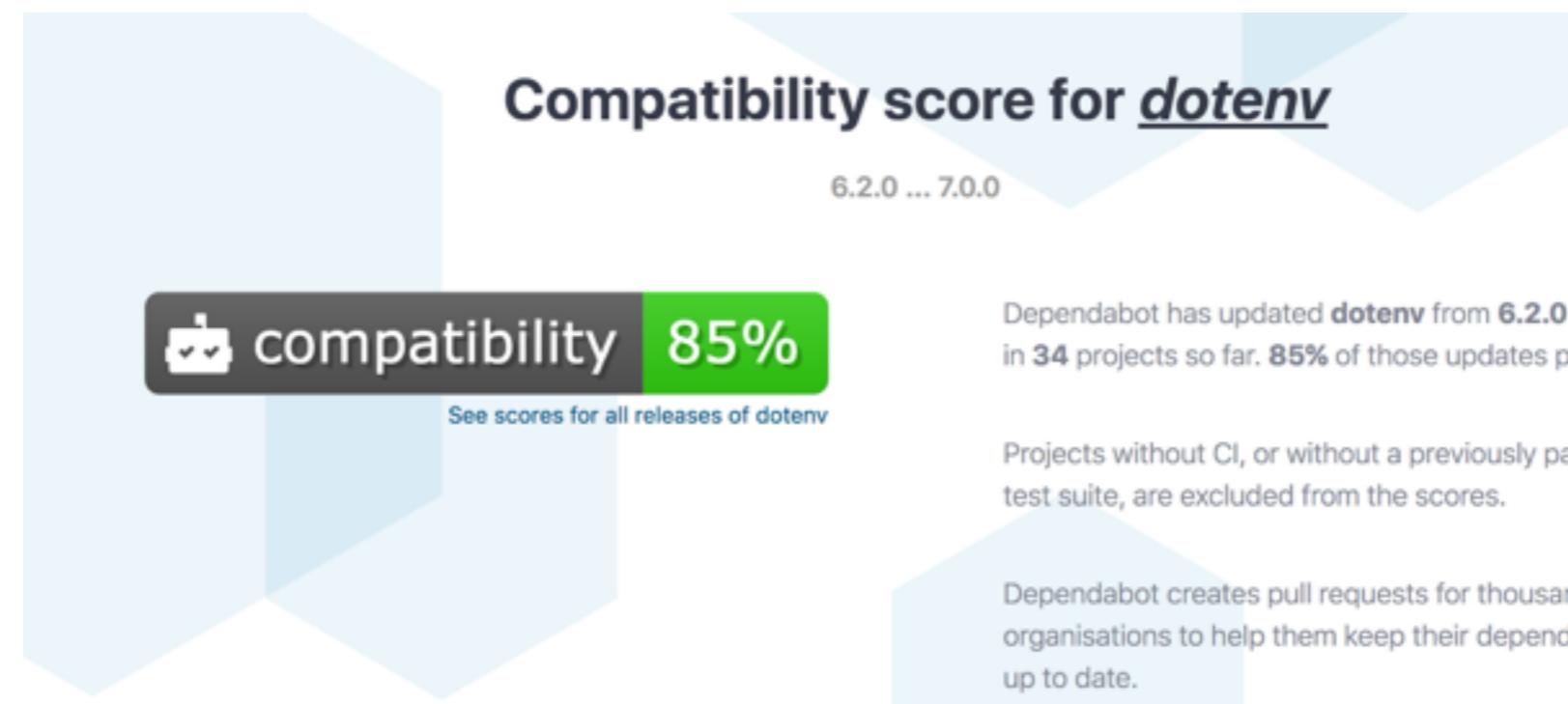
Comments

1

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

All checks have passed

7/7 successful checks



**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

Dependencies 1555

Source [GitHub](#)

Taken by Web

Tested with package-lock.json, package.json

Repository [pride-london-web](#)

Branch master

Manifest [package.json](#)

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



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-printer-fix.z > 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

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

Source control



GitHub

[Add projects](#)



GitHub Enterprise

[Contact us to enable](#)



GitLab

[Connect to GitLab](#)



Bitbucket Server

[Contact us to enable](#)



Bitbucket Cloud

[Coming soon!](#)

Platform as a Service



Heroku

[Connect to Heroku](#)



Cloud Foundry

[Connect to Cloud Foundry](#)



Pivotal Web Services

[Connect to Pivotal](#)



IBM Cloud

[Connect to IBM Cloud](#)

Serverless



AWS Lambda

[Connect to AWS Lambda](#)



Azure Functions BETA

[Connect to Azure Functions](#)



Google Cloud Platform

[Coming soon!](#)

Notifications



Slack

[Edit settings](#)



Jira

[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](#)



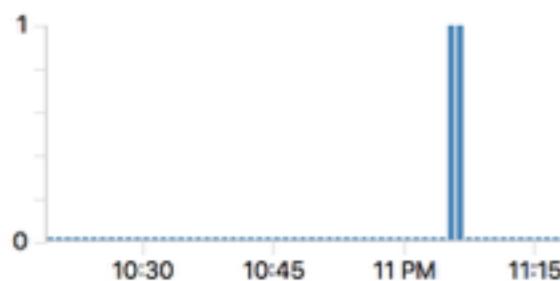
development

#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.rn
2019-03-15 04:06 pm				https://fervent-albattani-72bcb1.netlify.com/		TestError: Hello world	Hello world
2019-03-15 04:05 pm				https://5c8c2f281514740008340117--fervent-albattani-72bcb1.netlify.com/	TestError: Hello world		Hello world



Add Netlify badge on README file #87

[Edit](#)

- Merged ja9-lock merged 10 commits into master from test/deployment a day ago

[Conversation 1](#)[Commits 10](#)[Checks 4](#)[Files changed 7](#)

+1,482 -1,356



SonyaMoisset commented 2 days ago • edited

Member



Testing Netlify deployment settings

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

#1 TestError: Hello world

Level: Error Status: Active [Resolve](#) [Mute](#) [Report wrongdoing](#) [Create GitHub Issue](#)

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

Last 60 Minutes Last 60 Hours Last 60 Days

Timestamps: [Timestamps](#) [Occurrences](#) [People](#) [Milestones](#) [IP Addresses](#) [Suggested Labels](#) [Similar items](#) [Co-Occurring items](#) [Community Initiatives](#)

Timestamp (PDT)	Browser or context requested	trace.exception.description	trace.exception.message	client_ip
2019-03-19 04:08 pm	GET https://www.ubuntutest.123test.netlify.com/	Netlify: Hello world	Hello world	192.168.1.11
2019-03-19 04:09 pm	GET https://86320381914760008320771-testnet-ubuntutest.123test.netlify.com/	Netlify: Hello world	Hello world	192.168.1.10

Reviewers



ja9-lock



Assignees

No one—assign yourself

Labels

[enhancement](#)

Projects

None yet

Milestone

No milestone

Notifications

[Unsubscribe](#)

You're receiving notifications because you authored the thread.

2 participants

[Lock conversation](#)Add Netlify badge on README file [bb9223d](#)

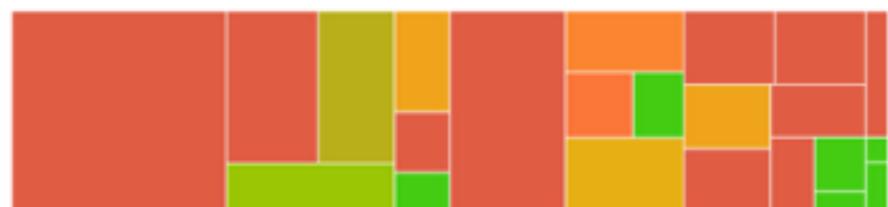
codecov bot commented 2 days ago • edited

Member



Codecov Report

Merging [#87](#) into [master](#) will not change coverage.
The diff coverage is [n/a](#).



##	Coverage	Diff	##
##	master	#87	+/- ##

Coverage	48.11%	48.11%
----------	--------	--------

Files	23	23
-------	----	----

Lines	318	318
-------	-----	-----

Branches	34	34
----------	----	----

Hits	153	153
------	-----	-----

Misses	137	137
--------	-----	-----

Partials	28	28
----------	----	----



PrideInLondon / pride-london-web

Watch 2 ⌂ Star 0 ⌂ Fork 0

Code Issues 2 Pull requests 3 Projects 0 Wiki Insights Settings

Add Netlify badge on README file #87

Merged ja9-look merged 10 commits into master from test/deployment a day ago

Conversation 1 Commits 10 Checks 4 Files changed 7 +1,482 -1,356

-o 77fb7fa + -- Implement Rollbar agent 3 neutral, and 1 successful checks

Netlify Succeeded — 2 days ago

Header rules - fervent-albattani-72bcb1 Success ran 2 days ago in 2 minutes
-o 77fb7fa by @SonyaMoisset
p test/deployment

Mixed content - fervent-albattani-72bcb1 Success All content is secure!

Sonatype DepShield Queued 2 days ago

Re-run all checks Re-run failed checks

Codecov Queued 2 days ago

Re-run all checks Re-run failed checks

[View more details on Netlify](#)



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](#).



ja9-look approved these changes a day ago

[View changes](#)



ja9-look merged commit `e5d5975` into `master` a day ago

[Hide details](#)

[Revert](#)

8 checks passed

✓ **AccessLint** Review complete

✓ **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 49de821...77fb7fa [Details](#)

✓ **codecov/project** 48.11% remains the same compared to 49de821 [Details](#)

✓ **netlify/fervent-albattani-72bcb1/deploy-preview** Deploy preview ready! [Details](#)

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



ja9-look deleted the `test/deployment` branch a day 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...@faeef84

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**

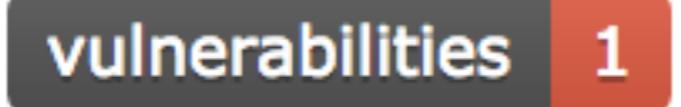
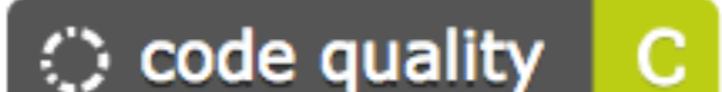
Add Netlify badge on README file (#87)

- * 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



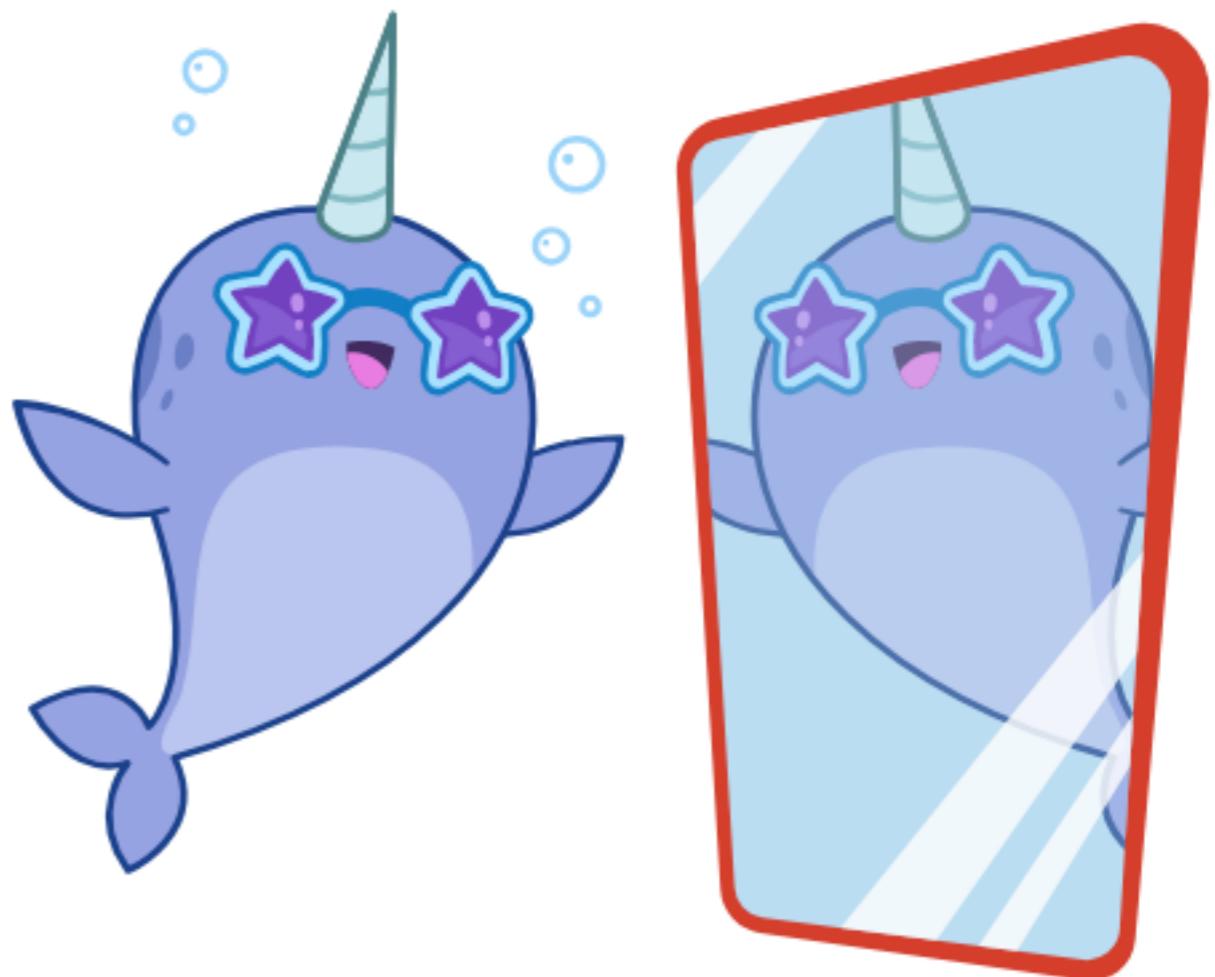
MORE TOOLS

ONLINE SCAN



WEBHINT

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



SCANNING 100%

SCAN TIME: 03:00

HINTS

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

HINTS
1PASSED
0/1

Compatibility

expand all

content-type: 17 hints

HINTS
3PASSED
4/7

highest-available-document-mode: 1 hints

HINTS
1PASSED
3/4

meta charset utf-8: 1 hints

HINTS
4PASSED
3/7

PWA

expand all

apple-touch-icons: 1 hints

HINTS
0PASSED
0/0HINTS
5PASSED
5/10



44

55

60

69

90

Performance

44

Performance

Progressive Web App

55

Progressive Web App

Accessibility

60

Accessibility

Best Practices

69

Best Practices

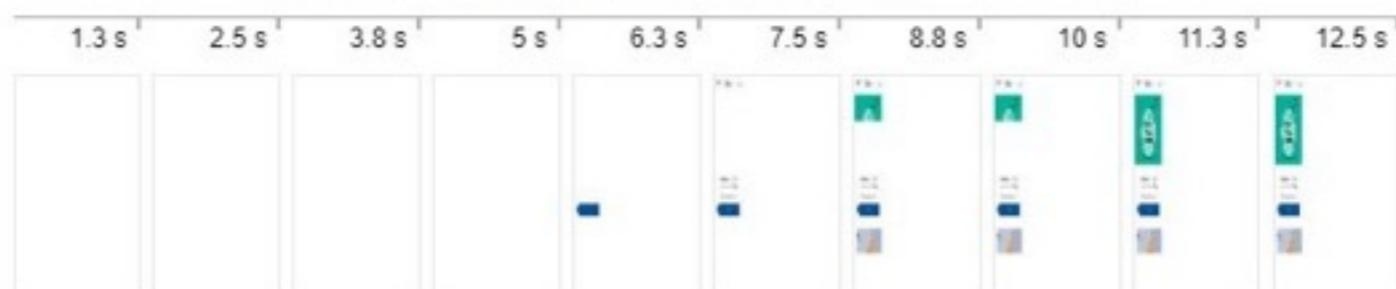
SEO

90

44

Performance

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



▶ First meaningful paint 6,640 ms

▶ First Interactive (beta) 6,640 ms

▶ Consistently Interactive (beta) 12,510 ms

▶ Perceptual Speed Index: 8,136

29

▶ Estimated Input Latency: 16 ms

100

Opportunities

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

▶ Serve images in next-gen formats  2,070 ms
429 KB

▶ Reduce render-blocking stylesheets  1,920 ms

▶ Reduce render-blocking scripts  1,460 ms

▶ Unused CSS rules  1,260 ms
261 KB

Scan your site now

<https://facebook.com>

Scan

Hide results Follow redirects

Security Report Summary



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

Raw Headers

HTTP/1.1	200 OK
X-XSS-Protection	0
Pragma	no-cache
content-security-policy	default-src * data: blob:; script-src * facebook.com *.fbcn.net *.facebook.net *.google-analytics.com *.virtualearth.net *.google.com 127.0.0.1: * *.spotilocal.com: * 'unsafe-inline' 'unsafe-eval' *.atlassolutions.com blob: data: 'self'; style-src data: blob: 'unsafe-inline' *; connect-src *.facebook.com facebook.com *.fbcn.net *.facebook.net *.spotilocal.com: * wss://*.facebook.com: * https://fb.scanandcleanlocal.com: * *.atlassolutions.com attachment.fbsbx.com ws://localhost: * blob: *.cdninstagram.com 'self' chrome-extension://boadgeojelhgndaghlijhdicfkmlpafdf chrome-extension://dllochdbjfkdbacpmhlcpmleaejidimm;
Cache-Control	private, no-cache, no-store, must-revalidate
X-Frame-Options	DENY
Strict-Transport-Security	max-age=15552000; preload
X-Content-Type-Options	nosniff
Expires	Sat, 01 Jan 2000 00:00:00 GMT
Set-Cookie	fr=1wkGGucUxIWFrzfy3F..Bbu-In.pD.AAA.0.0.Bbu-In.AWX6X0CU; expires=Sun, 06-Jan-2019 23:03:03 GMT; Max-Age=7776000; path=/; domain=.facebook.com; secure; httponly
Set-Cookie	sb=j-K7W2EWdZ47v6zcJUflge-y; expires=Wed, 07-Oct-2020 23:03:03 GMT; Max-Age=63072000; path=/; domain=.facebook.com; secure; httponly
Vary	Accept-Encoding
Content-Type	text/html; charset="utf-8"
X-FB-Debug	6I9wPmZxPR1sQZM0sln8HEM3IPpp1dGlLwpRtrXkkjm2hjCO9pRQwIm+Zen4XbSMhFG8mMW/0mpgHXFQW4787Q==
Date	Mon, 08 Oct 2018 23:03:03 GMT
Transfer-Encoding	chunked
Connection	keep-alive

WHAT'S NEXT?

SECURITY CHAMPIONS



Security Champions playbook

Identify teams

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

Define the role

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

Nominate champions

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

Comm channels

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





Life is too short. AppSec is tough. Cheat!

CIS Controls™

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

V7

ATT&CK Matrix for Enterprise										
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Keyboard Intercepting Application	Assembly	Identify, profile and exploit	Access Point Interception	Access Point Interception	Account Takeover	Account Discovery	Application Whining	Automated Collection	Automated Collection	Automatically read their communication through removable media
Hardware Pollution	GASDP	Accessibility Features	Accessibility Features	BTUJ-Java	Bad History	Application Whining	Application Deployment Software	Data Compromised	Data Compromised	Communication Propagator
Application Through Removable Media	Command Line Interface	Access Manipulation	AppCntr-SLs	Drive Padding	Drive Truncation	Device Shadow Documents	Device Configuration Object Store	Device Data	Device Decrypted	Device Delivered and Delisted Protocol
Assumeering Environment	Configured VMs, File	AppDef-RCE	AppDef-RCE	Before User Account Control	Clipboard Dumping	File and Directory Discovery	File Exploitation of Network Services	File Shred	File Transfer via Links	File Transfer via Links
Assumeering Links	Dynamic DNS Change	Application Shimming	Application Shimming	Installer	Installations in Files	Network Name Tracing	Logon Attacks	New Host Information Acquisition	Network User Observation	Network User Observation Method
Assumeering via Device	Execution through API	Authentication Package	BLU-Breach Order Hijacking	Code Signage	Exploit for Credential Access	Network Drive Discovery	Pass the Hash	Data from Local System	Exploit for Command and Control	Exploit for Command and Control
Apple Chain Components	Execution through Module Load	BTUJ-Java	Drive-Monitoring	Configured VMs, File	Forgot Authentication	Forgot Password	Forgot the Token	Data from Network Shared Drives	Exploit for Other Networks Medium	Exploit for Other Networks Medium
Malicious Relationship	Exploits for Mass Invasion	Blurst	Exploits for Mass Invasion	Exploits for Mass Invasion	Impersonate	Impersonate	Impersonate	Impersonate	Impersonate	Impersonate
File Inclusions	Endpoint User Interface	Browser Extensions	Data Disclosure Recovery Injection	Common Space Abuse Injection	Input Capture	Permission Group Discovery	Remote Beating Monitor	Only Non-Removable Media	Utilization over Physical Medium	Volume Hunting
	Filezilla	Change Default File Association	File System Permissions	File System Permissions	File System Permissions	File System Permissions				
	Log4j	Component Pollution	File System Permissions	File System Permissions	File System Permissions	File System Permissions				
	Locust	Component Impact Replacing	Image File Execution Options	Image File Execution Options	Image File Execution Options	Image File Execution Options				
	Local Job Scheduling	Unsanitised Accounts	Launch Listener	Launch Listener	Launch Listener	Launch Listener				
	None	BLU-Breach Order Hijacking	New Service	Lockdown and File Processing	Lockdown and File Processing	Lockdown and File Processing	Lockdown and File Processing			
	PowerShell	Path Traversing	Path Traversing	Path Traversing	Path Traversing	Path Traversing	Path Traversing	Path Traversing	Path Traversing	Path Traversing
	Regicide	Remote Hostname Resolution	Remote Hostname Resolution	Remote Hostname Resolution	Remote Hostname Resolution	Remote Hostname Resolution	Remote Hostname Resolution	Remote Hostname Resolution	Remote Hostname Resolution	Remote Hostname Resolution
	Report2	File System Permissions Injection	File System Permissions Injection	File System Permissions Injection	File System Permissions Injection	File System Permissions Injection	File System Permissions Injection	File System Permissions Injection	File System Permissions Injection	File System Permissions Injection
	Rundll32	Hidden File and Directories	Process Injection	Process Injection	Process Injection	Process Injection				
	Scheduled Task Triggering	Job Triggers	Service Configuration Modification	Service Configuration Modification	Service Configuration Modification	Service Configuration Modification				
	Service Execution	Image File Execution Options Injection	Service Configuration Modification	Service Configuration Modification	Service Configuration Modification	Service Configuration Modification				
	Signed Driver Process Injection	Kernel Modules and Drivers	Service Configuration Modification	Service Configuration Modification	Service Configuration Modification	Service Configuration Modification				
	Signed Script Process Injection	UCL-2040-2018-Addition	Service Configuration Modification	Service Configuration Modification	Service Configuration Modification	Service Configuration Modification				
	Name	Launch Listener	Task Manager	Task Manager	Task Manager	Task Manager				
	Space-time Persistence	Launch Listener	Task Manager	Task Manager	Task Manager	Task Manager				
	Threading Defenses	Launch Listener	Task Manager	Task Manager	Task Manager	Task Manager				
	Top	Launch Listener	Local Job Scheduling	Local Job Scheduling	Local Job Scheduling	Local Job Scheduling				
	Process Resource Utilisation	Local Job Scheduling	Local Job Scheduling	Local Job Scheduling	Local Job Scheduling	Local Job Scheduling	Local Job Scheduling	Local Job Scheduling	Local Job Scheduling	Local Job Scheduling
	Windows Management Instrumentation	Logon Scripts	Logon Scripts	Logon Scripts	Logon Scripts	Logon Scripts	Logon Scripts	Logon Scripts	Logon Scripts	Logon Scripts



Troy Hunt

Hi, I'm Troy Hunt, I write this blog, create courses for Pluralsight and am a Microsoft Regional Director and MVP who travels the world speaking at events and training technology professionals.

Weekly Update 129

07 March 2020

Hugs of stuff going on this week with all sorts of different bits and pieces. I bought a massive new stash of HIRP stickers (took oughta last... a few weeks?), I'll be giving them out at a heap of upcoming events. I was on the Ducknet Diaries podcast (which is epic!) plus there's more insights into the ShareThis data breach and the ginerous verifications.io incident. Oh - and Udemy is still pirating my content, here's the tweet if you'd like to let them know how you feel about that: Disgusted that @udemy is still pirating courses from @datademerelth and myself. Seriously guys, this has been going on for years, there's obviously no checks on this whatsoever. Here... [\[link\]](#)

WEEKLY UPDATE

Upcoming Events

I usually run [events](#), [workshops](#) around these, here's the upcoming public events I'll be at:

- NDC Melbourne: 12 Mar, Melbourne (Australia)
- SmashR0C: 14 Mar, Denver, USA
- Microsoft MVP Summit: 17 to 22 Mar, Seattle, USA
- ANZAC Security Summit World Tour: 28 Mar, Sydney (Australia)
- NDC Melbourne: 29 Mar, Sydney (Australia)
- NDC Gold Coast: 30 Mar, Gold Coast (Australia)
- NDC Minnesota: 6 to 10 April, Minneapolis, USA



LADIES OF LONDON
HACKING SOCIETY



OWASP LONDON
CHAPTER

GET SECURE, BE SECURE AND STAY SECURE



Thank
you!