SUBRESOURCE INTEGRITY

WHEN THE CDN GOES BANANAS

me_irl

- Gabor Szathmari
- Information Security
  ~~Professional~~ ~~Hacker~~
  Freelancer
- Privacy Advocate

I WILL BE TALKING ABOUT

- JavaScript hosted by third-parties
- Some scary bits
- The Solution: Subresource Integrity
  - What it does
  - Tooling

THIRD-PARTY CODE ON MODERN WEBSITES

ANALYTICS

A/B TESTING

HEATMAPS

TAG MANAGERS

PRIVATE CDN

PUBLIC CDN


Google Analytics


CLICKY®
WEB ANALYTICS


JSDELIVR


Taboola


cdnjs


Google
Developers


crazyegg™


Akamai


amazon
web services™
S3


fastly®


amazon
cloudfront


mixpanel


Optimizely


Rollbar


maxCDN

MODERN WEBSITES

- **Third-party JavaScript**
  (heatmaps, user tracking, analytics …)
- **Public CDNs**
  (jsDelivr, ajax.googleapis.com, ajax.aspnetcdn.com …)
- **Private CDNs**
  (S3, Akamai, CloudFront, Fastly …)


"YOU KNOW WHAT THEY SAY:
LOVE* IS BLIND"
* <script src="">"

Capital One Financial Corporation www.capitalone.com

Capital One

Personal Business Commercial Search Locations Sig

Credit Cards Bank Borrow Invest Learn Contact

Sign In

Banking *including Capital One 360*

12345678

Continue

Forgot ID or Customer #?
Enroll in Capital One Bank

F

3 unsafe / 4 tags

Site	https://www.capitalone.com
Scan Date	Today at 12:24 PM
Status Code	HTTP 200 OK
Scripts	*Found **3** unsafe scripts out of **0** script tags*
Stylesheets	*Found **0** unsafe stylesheets out of **1** stylesheet tags*

Results

Scripts 3 issues

Tag	Result
<script type="text/javascript" src="https://assets.cofstatic.com/assets/rwd/js/min/lib.min.js?p=1&v=16.00.02"></script>	✖ Missing SRI hash
<script type="text/javascript" src="https://assets.cofstatic.com/assets/rwd/js/min/cof.min.js?p=1&v=16.00.02"></script>	✖ Missing SRI hash
<script type="text/javascript" src="https://nexus.ensighten.com/capitalone/Bootstrap.js"> </script>	✖ Missing SRI hash

Stylesheets OK

WHAT CAN GO WRONG?

MODERN WEBSITES

- **Third-party JavaScript**
  (heatmaps, user tracking, analytic
- **Public CDNs**
  (jsDelivr, ajax. dn.com …)
- **Private CDNs**
  (S3, Akamai, Clo t, Fastly …)

```
window.location.href =
"https://www.reddit.com/
r/badmemes"
```

WHEN THE CDN GOES BANANAS

- https://www.maxcdn.com/blog/bootstrapcdn-security-post-mortem/
- https://blog.pagefair.com/2015/halloween-security-breach/
- https://citizenlab.org/2015/04/chinas-great-cannon/
- http://securityaffairs.co/wordpress/31480/cyber-crime/afghanistan-cdn-network-hacked.html
- https://medium.com/@FredericJacobs/the-reuters-compromise-by-the-syrian-electronic-army-6bf570e1a85b

www.reuters.com/article/2014/06/22/us-israel-syria-b

REUTERS EDITION: U.S.

HOME BUSINESS MARKETS WORLD POLITICS TECH

Attack from Syria kills teen o occupied Golan, Israel says

JERUSALEM Sun Jun 22, 2014 6:10am EDT

0 COMMENTS | Tweet Share this Email Print

RELATED TOPICS
World »
Syria »
Israel »

(Reuters) - An attack from insid Syria o year-old on the Israeli-occupied on Isra the mil

Israeli tanks fired at Syrian army spokesman described as an inter

Security officials initially said a civilian contractor for Isra Def killed in an explosion. But they later said that a youth, aged 15, wh had died and that two other people were wounded.

A oadside sh fence or th

REUTERS.COM

sea.sy/indexs/

Hacked by Syrian Electronic Army

Stop publishing fake reports and false ar about Syria!

UK government is supporting the terrori Syria to destroy it, Stop spreading its propaganda.

SEA.SY

HTTP://CDN.TABOOLA.COM/LIBTRC/
REUTERS-NETWORK/LOADER.JS

WHAT IS THE DAMAGE?

- Unwanted redirection
- Website defacement
- Click fraud
- Exploit kits (ransomware)
- Cookie stealing, session hijacking
- Keylogging
- UI redressing (password stealing, OTP stealing)

Capital One Financial Corporation www.capitalone.com

Capital One

Personal Business Commercial Search Locations Sig

Credit Cards Bank Borrow Invest Learn Contact

Sign In

Banking *including Capital One 360*

12345678

Continue

Forgot ID or Customer #?
Enroll in Capital One Bank

WHAT CAN WE DO?

SUBRESOURCE INTEGRITY

AKA. SRI

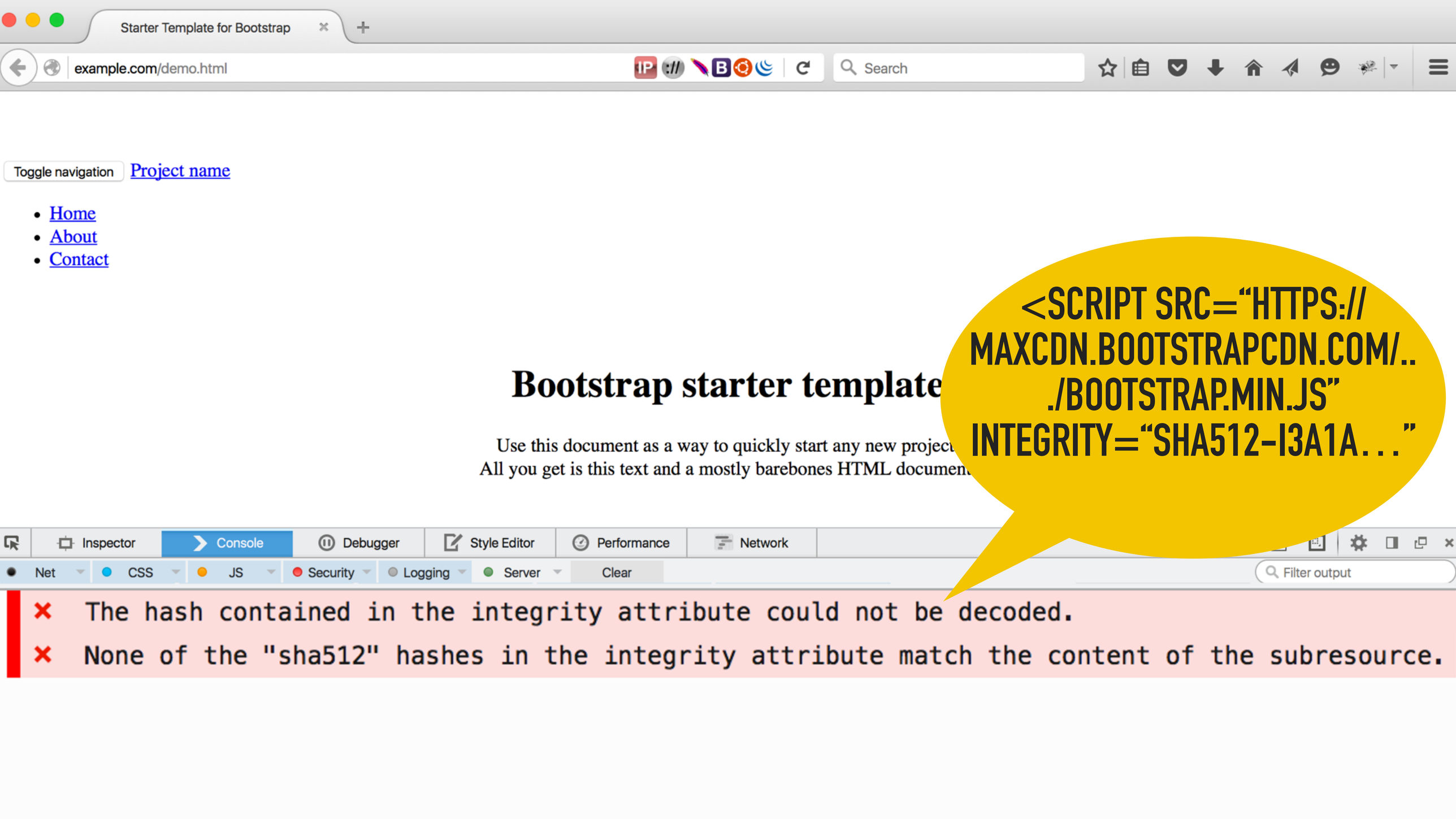
PROTECTS
JAVASCRIPT
INTEGRITY

PROTECTS
CSS
INTEGRITY

```
<script src="https://
cdn.jsdelivr.net/jquery/2.1.4/
jquery.min.js"
integrity="sha256-ImQv...="
crossorigin="anonymous"
></script>
```


"TRUST, BUT VERIFY"

“Я НЕМНОГО ЧАЙНИКА”


Starter Template for Bootstrap
example.com/demo.html
Search
Toggle navigation
Project name
Home
About
Contact
Bootstrap starter template
Use this document as a way to quickly start any new project
All you get is this text and a mostly barebones HTML document
<SCRIPT SRC="HTTPS://MAXCDN.BOOTSTRAPCDN.COM/../BOOTSTRAP.MIN.JS" INTEGRITY="SHA512-I3A1A..."
Inspector
Console
Debugger
Style Editor
Performance
Network
Net
CSS
JS
Security
Logging
Server
Clear
Filter output
The hash contained in the integrity attribute could not be decoded.
None of the "sha512" hashes in the integrity attribute match the content of the subresource.

BROWSER SUPPORT



WHEN THE CDN GOES BANANAS

TOOLING

MANUAL HASHING

OPENSSL

- `openssl dgst -sha256 -binary jquery.min.js | openssl base64 -A`
- `openssl dgst -sha384 -binary jquery.min.js | openssl base64 -A`
- `openssl dgst -sha512 -binary jquery.min.js | openssl base64 -A`

OPENSSL

- $ curl -s https://code.jquery.com/jquery-2.2.3.min.js | openssl dgst -sha512 -binary | openssl base64 -A

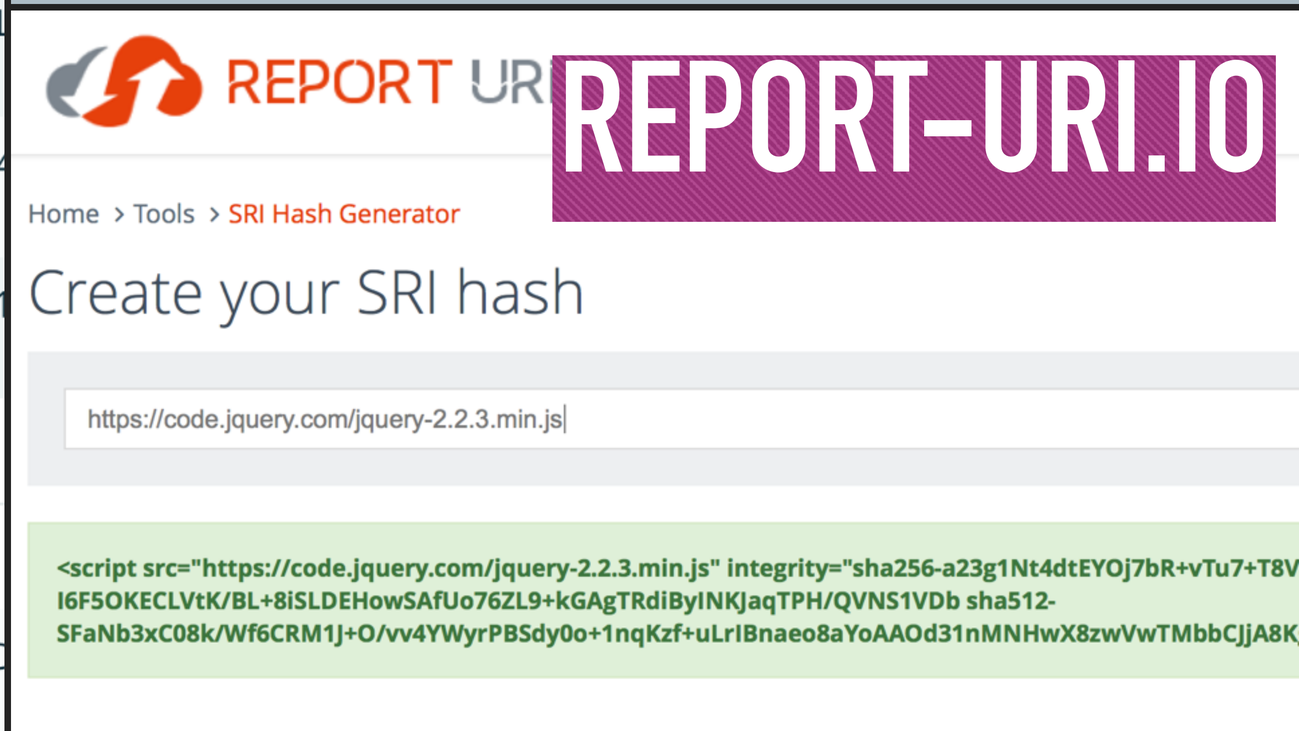
  SFaNb3xC08k/Wf6CRM1J+O/vv4YWyrPBSdy0o+1nqKzf+uLrIBnaeo8aYoAAOd31nMNHwX8zwVwTMbbCJjA8Kg==

- <script src="https://code.jquery.com/jquery-2.2.3.min.js" integrity="sha512-SFaNb3xC08k/Wf…" […]

HOSTED TOOLS


www.jsdelivr.com
Links collection
Add the <script> tag
Enable SRI
JS
6/semantic.min.js" integrity="sha256-BfKqLXxyObYfnwRBAKHj/kHIwJY5yjcIaI
7/semantic.min.js" integrity="sha256-LlwpidR/b83Uo1S+jq1EoxmDjZrP67PL4
ery.min.js" integrity="sha256-ImQvICV38LovIsvIa2zykaCTdEh1Z801Y+DSop91
JSDELIVR.COM


SRI Hash Generato
Enter the URL of the resource you wish to use:
https://code.jquery.com/jquery-2.2.3.min.js
<script src="https://code.jquery.com/jquery-2.2.3.min.js" integrity
diByINKJaqTPH/QVNS1VDb" crossorigin="anonymous"></script>
SRIHASH.ORG


REPORT URI
REPORT-URI.IO
Home › Tools › SRI Hash Generator
Create your SRI hash
https://code.jquery.com/jquery-2.2.3.min.js
<script src="https://code.jquery.com/jquery-2.2.3.min.js" integrity="sha256-a23g1Nt4dtEYOj7bR+vTu7+T8V
I6F5OKECLVtK/BL+8iSLDEHowSAfUo76ZL9+kGAgTRdiByINKJaqTPH/QVNS1VDb sha512-
SFaNb3xC08k/Wf6CRM1J+O/vv4YWyrPBSdy0o+1nqKzf+uLrIBnaeo8aYoAAOd31nMNHwX8zwVwTMbbCJjA8K

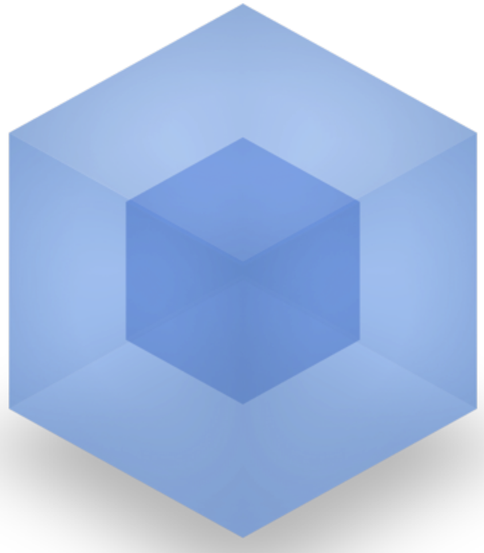
CMS

PLUGINS

- WordPress
  https://wordpress.org/plugins/wp-sri/
- Drupal
  https://www.drupal.org/project/advagg

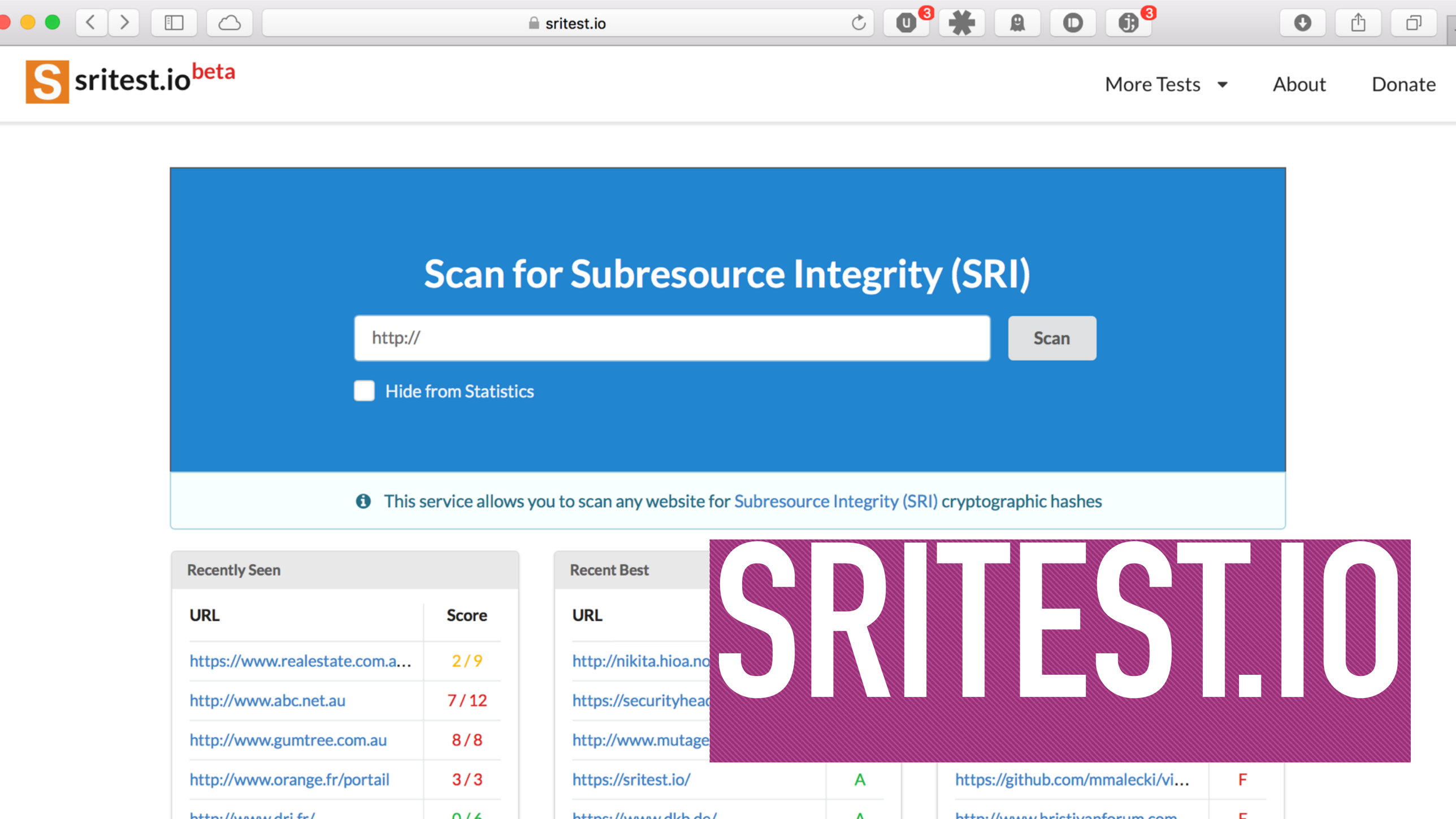
WORKFLOW INTEGRATION

WORKFLOW INTEGRATION



WORKFLOW INTEGRATION

SCAN YOUR WEBSITE FOR SRI USAGE


sritest.io
sritest.io beta
More Tests
About
Donate
Scan for Subresource Integrity (SRI)
http://
Scan
Hide from Statistics
This service allows you to scan any website for Subresource Integrity (SRI) cryptographic hashes
Recently Seen
URL
Score
https://www.realestate.com.a…
2 / 9
http://www.abc.net.au
7 / 12
http://www.gumtree.com.au
8 / 8
http://www.orange.fr/portail
3 / 3
Recent Best
URL
http://nikita.hioa.no
https://securityhead
http://www.mutage
https://sritest.io/
A
https://github.com/mmalecki/vi…
F
SRITEST.IO

Summary

A

Rate: 100.0%

Site	https://sritest.io
Scan Date	Today at 4:36 PM
Status Code	HTTP 200
Scripts	*Found **0** unsafe scripts out of **4** script tags*
Stylesheets	*Found **0** unsafe stylesheets out of **3** stylesheet tags*

Results

Scripts OK

Tag	
<script integrity="sha256-XPAP9JsUJgXWcrZ8veekerjm8XQHkrsolHaXxs src="/js/modernizr-a7845b6804.js"></script>	
<script integrity="sha256-kbpxBK+uCL5nDiFOaeWHsxIEJfRbEPPCAsYyK src="/js/app-eb32ba6f6a.js"></script>	
<script src="https://ajax.googleapis.com/ajax/libs/jquery/2.1.4/jquery.min.js ImQvICV38LovIsvla2zykaCTdEh1Z801Y+DSop91wMU= sha384-8gBf6Y4YYq7Jx97PIqmTwLPin4hxIzQw5aDmUg/DDhul9fFpbbLcLh3nTIIDJKhx sha512-	✔ SRI hash detected

SRITEST.IO

TOOLING

- Manual
- Hosted
- CMS Plugins
- Workflow Integration
- sritest.io

SUMMARY

- Modern websites rely on JS/CSS
- Hosted on CDNs / at third-parties
- SRI protects from unexpected JS/CSS changes
- Tooling is available

FURTHER READING

- https://www.owasp.org/index.php/3rd_Party_Javascript_Management_Cheat_Sheet
- http://j.mp/cdn-goes-bananas
- http://j.mp/new-sri2-features
  - Enforce SRI with CSP
  - Violation Reporting

THANK YOU

- @gszathmari
- PGP: keybase.io/gszathmari