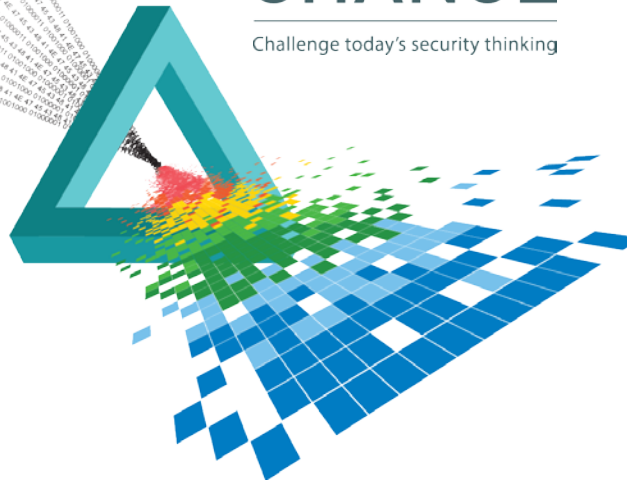
RSAConference2015
Singapore | 22-24 July | Marina Bay Sands

CHANGE
Challenge today's security thinking



SESSION ID: CDS-F03

Know Your Own Risks: Content Security Policy Report Aggregation and Analysis

Ksenia Dmitrieva

Senior Consultant
Cigital, Inc.
@KseniaDmitrieva

Agenda

- What is Content Security Policy (CSP) and why do we need it?
- CSP reporting functionality
- Extracting important information from reports at scale
- CSP support and adoption
- Real world examples of policies

Pop Quiz

Which web application vulnerability was

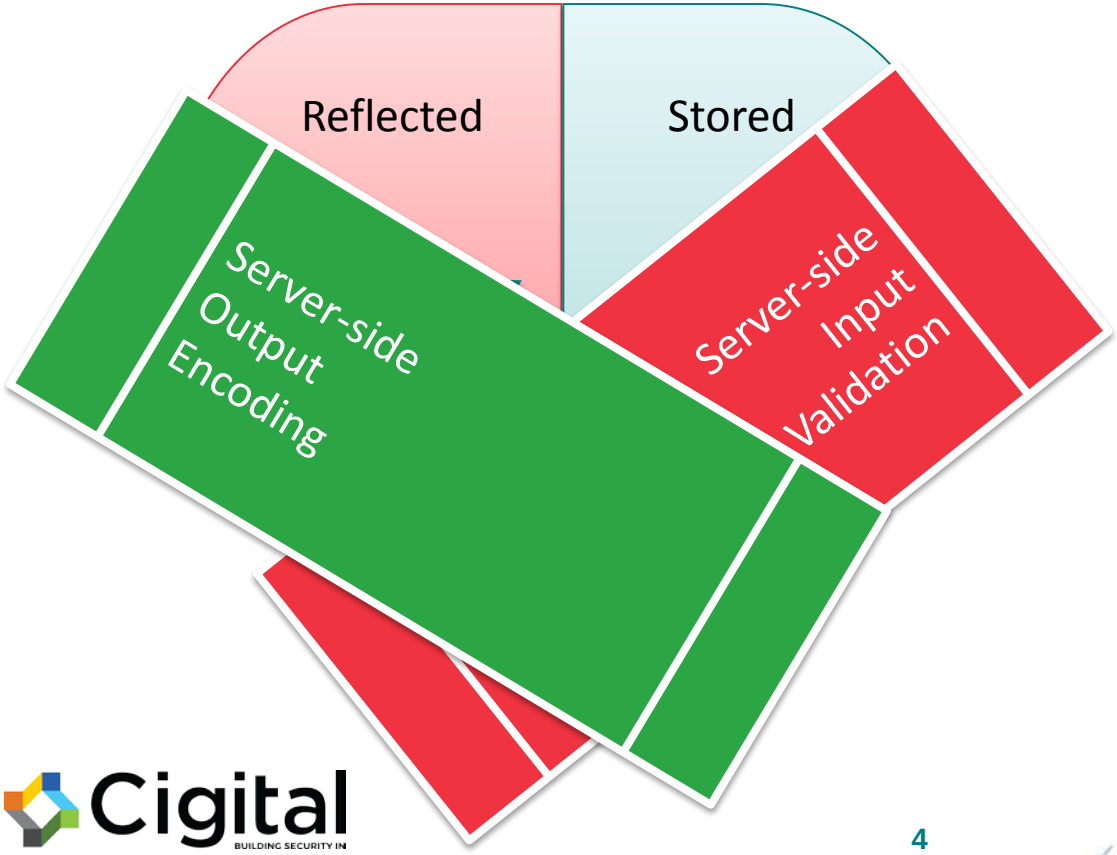
- #4 in OWASP* Top 10 in 2003
- #1 in OWASP Top 10 in 2007
- #2 in OWASP Top 10 in 2010
- #3 in OWASP Top 10 in 2013

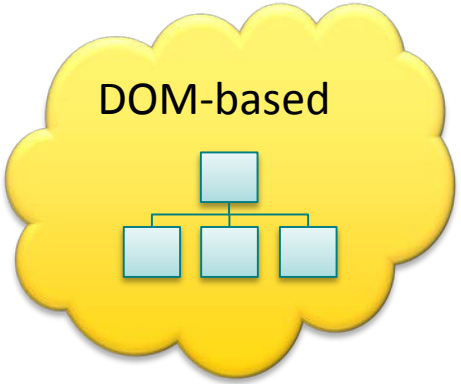
?

CROSS-SITE SCRIPTING

* OWASP – Open Web Application Security Project (https://www.owasp.org/)

Traditional Methods of XSS Protection

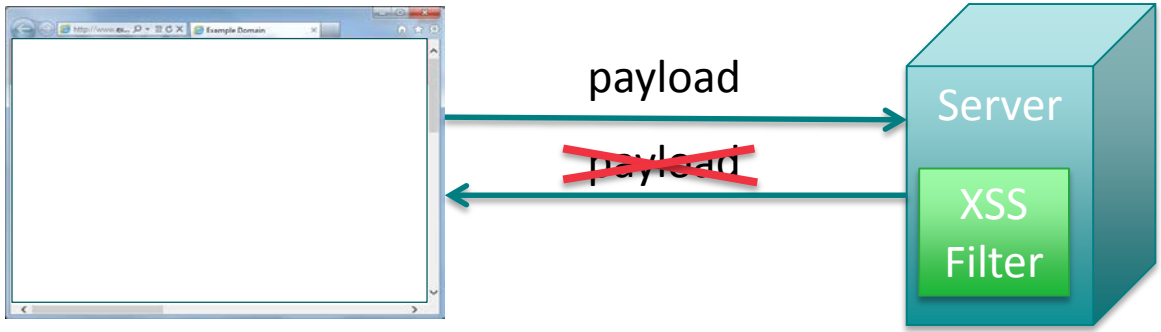




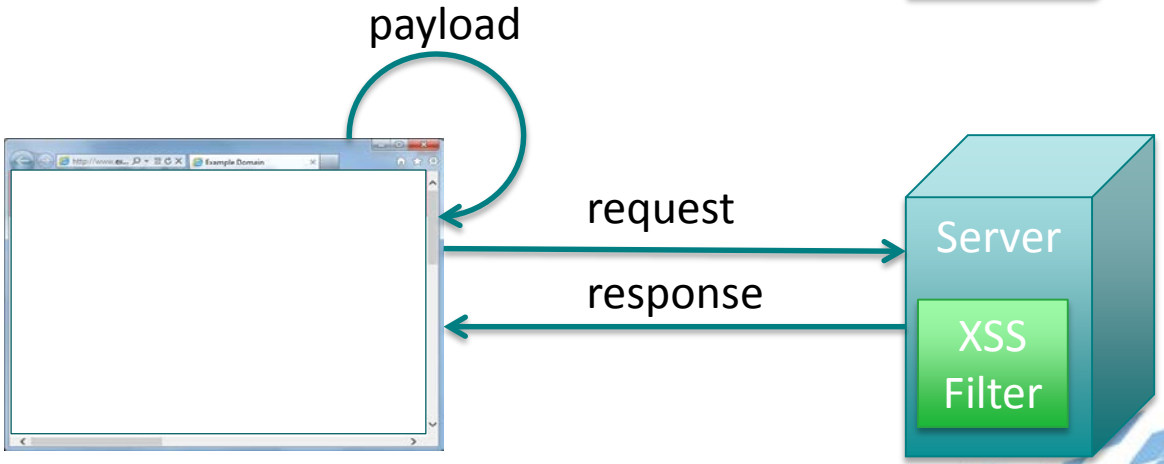
Cigital
BUILDING SECURITY IN

Execution of DOM-based XSS

Traditional XSS

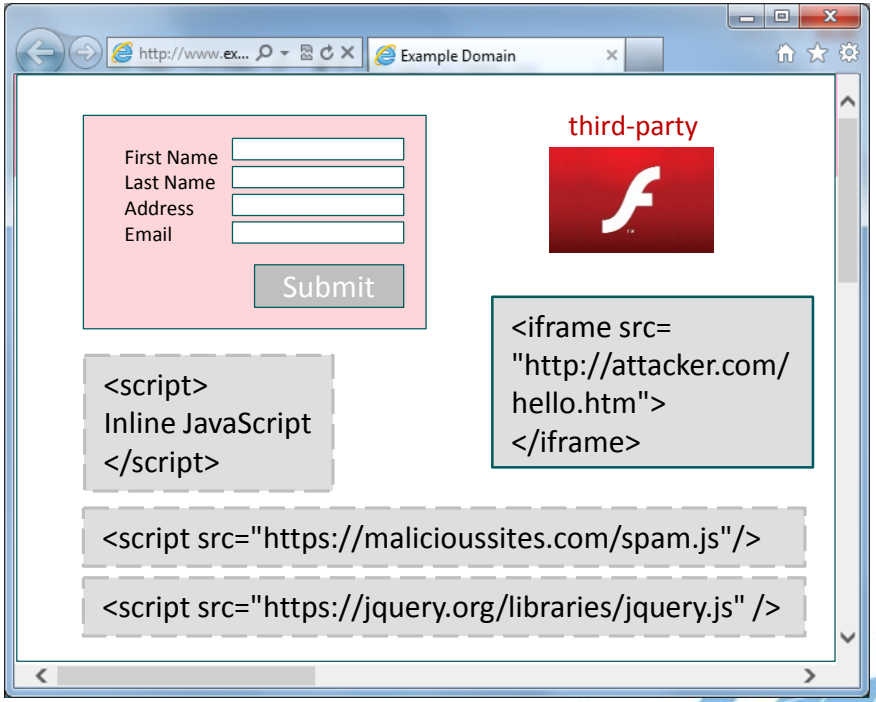


DOM-based XSS



What is Content Security Policy?

- Content Security Policy:
  - Restricts ad-hoc XSS vectors: inline scripts and eval-constructs
  - Imposes restrictions on resources based on their origin
- CSP defines a list of resource directives:
  - script-src
  - object-src
  - frame-src
  - img-src
  - media-src
  - etc.



Sample CSP Policies

- Policy is sent by the server as an HTTP header:

```
Content-Security-Policy: script-src 'self' https://apis.google.com
```

- Any malicious inline scripts or scripts hosted elsewhere will not be executed.

✓ Can a page with the following policy load a CSS style sheet from http://wordpress.org?

```
Content-Security-Policy: script-src 'self'; frame-src 'none';
object-src 'none'
```

CSP Reporting

- Browsers supporting CSP send policy violation reports in JSON format to the server
- Violation report may contain data about the attack

```
{
  "csp-report": {
    "document-uri": "http://example.com/page.html",
    "referrer": "http://evil.example.com/",
    "blocked-uri": "http://evil.example.com/evil.js",
    "violated-directive": "script-src 'self' https://apis.google.com",
    "original-policy": "default-src 'self'; script-src 'self'
https://apis.google.com; report-uri http://example.com/reporting/parser.php"
  }
}
```

Where the violation occurred

Where the attack is coming from

What the attacker is trying to do

Directive controlling the resource

CSP Reporting and Enforcing

- **Content-Security-Policy** header with report-uri enforces the policy
- **Content-Security-Policy-Report-Only** header reports policy violations, but does not enforce the policy

```
Content-Security-Policy-Report-Only: default-src 'self'; script-src 'self'
https://apis.google.com; report-uri http://example.com/reporting/parser.php
```

- Use both headers: one to enforce the old policy and another to test out the new policy

```
Content-Security-Policy: default-src 'self' *.google.com;

Content-Security-Policy-Report-Only: default-src 'self' *.google.com;
script-src 'self' https://apis.google.com; frame-src 'self';
report-uri http://example.com/reporting/parser.php
```

Browser Dependent Report Formats

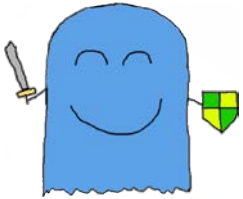
- Browsers use slightly different formats for the reports

Google Chrome	Mozilla Firefox	Windows Edge
document-uri referrer blocked-uri: “” violated-directive original-policy effective-directive status-code	document-uri (with path) referrer blocked-uri (with path): ‘self’ violated-directive original-policy	? Coming soon July 29, 2015

- Special tools are needed to process CSP reports at scale

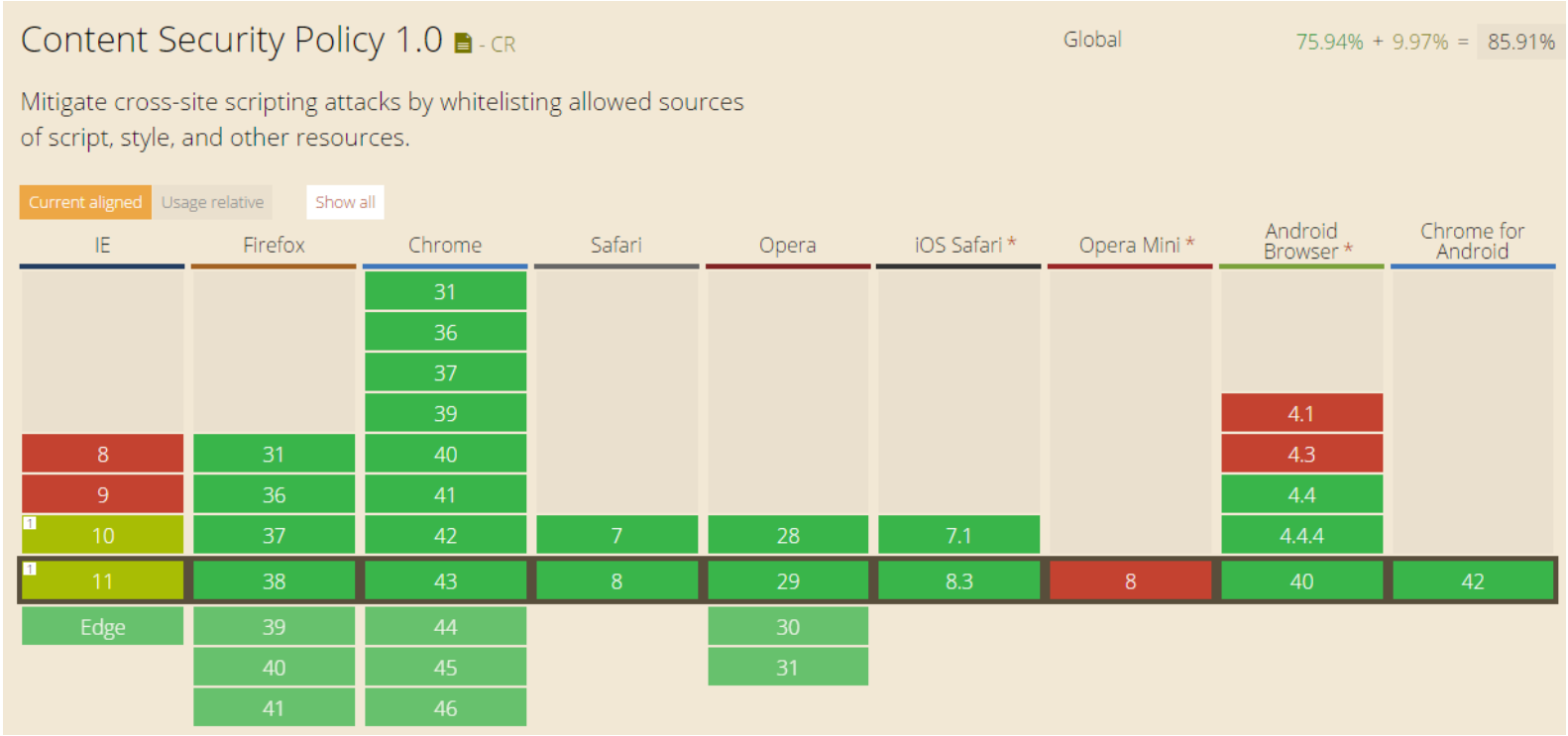
Report Aggregation: Tools

- Aggregate Data
  - Normalize data coming from different browsers
  - Add extra fields: application name, user agent
- Filter
  - According to Twitter, 80% is noise
  - Filter out reports from browser plugins, proxy sites, ISP cache servers
- Graph
  - Twitter created custom CSP report aggregation tool – “highly proprietary and will never be open sourced”
  - Yelp uses Elasticsearch/Logstash/Kibana trio
  - Open source tool Caspr (http://www.caspr.io/)



Source: http://engineeringblog.yelp.com/2014/09/csp_reports_at_scale.html

Yelp's Report Aggregation



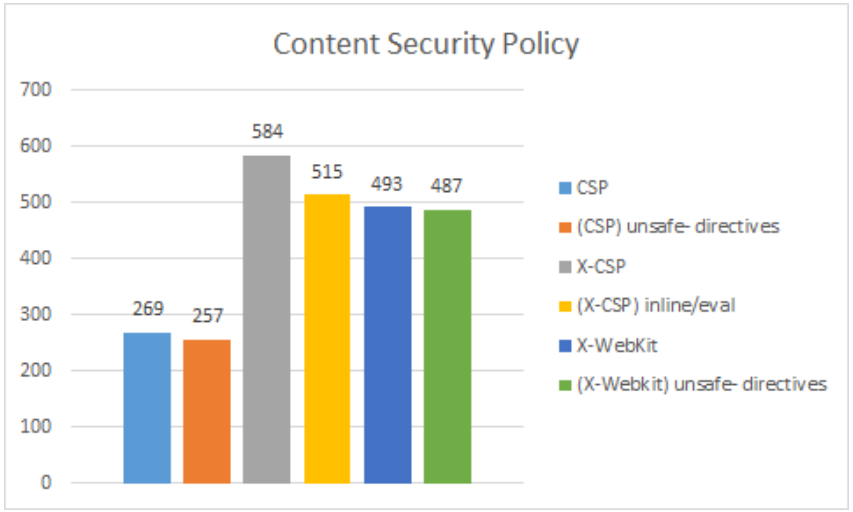
Source: http://caniuse.com/#feat=contentsecuritypolicy

Browser Support of CSP

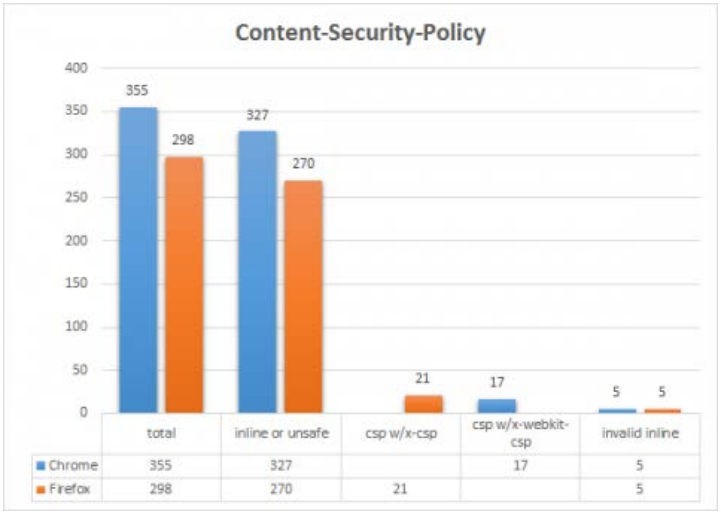
CSP Adoption

Number of sites using CSP out of Alexa Top 1 Million

2013



2014



Sources: https://www.veracode.com/blog/2013/11/security-headers-on-the-top-1000000-websites-november-2013-report/
https://www.veracode.com/blog/2014/03/guidelines-for-setting-security-headers

CSP Level 2

- Problem with CSP 1
  - Using CSP requires re-writing a whole application
  - Frameworks still use inline JavaScript and eval-constructs
- CSP Level 2 (W3C Candidate Recommendation)
  - Protecting inline JavaScript without re-writing an application:
    - Nonce-source directive
    - Hash-source directive
  - Replacing X-Frame-Options with frame-ancestors

Real World CSP Adoption Example: Facebook

Facebook uses CSP on www.facebook.com

```
Content-Security-Policy: default-src *; script-src https://*.facebook.com
http://*.facebook.com https://*.fbcdn.net http://*.fbcdn.net
*.facebook.net *.google-analytics.com *.virtualearth.net *.google.com
127.0.0.1:* *.spotilocal.com:* 'unsafe-inline' 'unsafe-eval'
https://*.akamaihd.net http://*.akamaihd.net *.atlassolutions.com; style-
src * 'unsafe-inline'; connect-src https://*.facebook.com
http://*.facebook.com https://*.fbcdn.net http://*.fbcdn.net
*.facebook.net *.spotilocal.com:* https://*.akamaihd.net
wss://*.facebook.com:* ws://*.facebook.com:* http://*.akamaihd.net
https://fb.scanandcleanlocal.com:* *.atlassolutions.com
http://attachment.fbsbx.com https://attachment.fbsbx.com;
```

Real World CSP Adoption Example: Yelp

Yelp uses CSP on www.yelp.com

```
Content-Security-Policy-Report-Only: report-uri
https://www.yelp.com/csp_report; default-src https:; img-src https: ;
script-src https://*.facebook.com https://*.facebook.net
https://*.googleapis.com https://*.quantserve.com https://*.yelp.com
https://*.yelpcdn.com https://*.yelpassets.com https://*.google-
analytics.com https://*.scorecardresearch.com 'unsafe-inline'
'unsafe-eval'; style-src https: 'unsafe-inline'; connect-src https:;
font-src https: data:; media-src https:; object-src https:; frame-
ancestors 'self'; frame-src yelp-webview://* https://*.facebook.com
```

Real World CSP Adoption Example: Twitter

Twitter uses CSP on all their services

```
Content-Security-Policy: default-src 'none'; connect-src 'self'; font-src
https://abs.twimg.com data:; frame-src 'self' twitter:; frame-ancestors
'none'; img-src https://abs.twimg.com https://*.twimg.com
https://pbs.twimg.com data:; media-src 'none'; object-src 'none';
script-src https://abs.twimg.com https://abs-0.twimg.com; style-src
https://abs.twimg.com https://abs-0.twimg.com; report-uri
https://twitter.com/i/csp_report?a=
NVQWGYLXFVWG6Z3JNY%3D%3D%3D%3D%3D%3D&ro=false;
```

Apply What You Have Learned Today

- If you want to use reporting functionality of CSP, next week answer the two questions:
  - Do any of your applications use CSP?
  - If they do, do you collect and analyze violation reports?
- In the next three months do the following:

Not Using CSP Yet	Already Using CSP
Run a pilot: • Select an application developed from scratch. • Understand technologies used by the application. Are there any that don't support CSP? • Use technologies that support CSP (Angular JS, Django). • Do not use 'unsafe-eval' and 'unsafe-inline'. • Use Report-Only option to test the policy.	Start collecting and analyzing reports: • Add the *report-uri* directive to the policy. • Filter out the noise. • Add extra information to easily identify the application/module. • Provide analysis results to development teams and to the security team. • Use Report-Only option to test a new policy.

Summary

- CSP protects applications from all types of XSS, including DOM-based XSS.
- CSP 1.0 is hard to implement on existing applications, but can be added to the newly developed applications. CSP 1.1 is on its way!
- CSP violation reports provide essential data about the application in the users' browsers. Use it!
- Normalize and filter CSP reports before analyzing and plotting data.

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

Questions?

@KseniaDmitrieva

kdmitrieva@cigital.com