Beyond Blind Defense: Gaining Insights from Proactive AppSec

Bryant Zadegan
Director, Application Security
The Advisory Board Company

keybase.io/bryant
@eganist

Beyond Blind Defense

- In a nutshell
  - **Content Security Policy** (+ **CSP2**, + **some CSP3**)
  - **HTTP Public Key Pinning**
- Reporting!
  - **Security, QA,** & **Infrastructure** benefits and considerations
  - **How?** (The easy way)

"Enforcing markup and scripting assumptions client-side"

i.e. "you should never see this kind of code from us"

Content **S**ecurity **P**olicy in a nutshell

Content Security Policy

Quickstart[2]

```
Content-Security-Policy-Report-Only:
default-src 'none';
object-src 'none';
script-src 'self';
connect-src 'self';
img-src 'self';
style-src 'self';
report-uri https://[id].report-uri.io/r/default/csp/[mode]
```

Content Security Policy

- Existing site? Start with Reporting. Refine further.
- New application? Build it in from day one.
- **Does not replace safe input/output**
- w3.org/TR/CSP1/
- caniuse.com/contentsecuritypolicy

Content Security Policy

Threat Model (intended)[4]

<XSS />

Cross-Site Scripting

Clickjacking

Mixed Content

Content Security Policy

Threat Model (stretched)

Mismanaged Change

Internal Threat

Content Security Policy

Directives

- `default-src` (applies to)
- `connect-src`
- `font-src`
- `img-src`
- `media-src`
- `object-src`
- `script-src`
- `style-src`

(does not apply to)

- `frame-src`
- `report-uri`
- `sandbox` - specifies an HTML sandbox policy that the user agent applies to the protected resource.

Content Security Policy 2

Updates CSP with new directives. E.g.:

- `base-uri`, `child-src`, `form-action`, `plugin-types`
  - `frame-ancestors` *supplants* the `x-frame-options` header.
  - `form-action` and `plugin-types` restrict forms and plugins.
- **For unsafe directives, Nonces and Hashes can now validate inline resources.**

Content Security Policy 2

Updated Reporting:

- `effectiveDirective`, `statusCode`, `sourceFile`, `lineNumber`, `columnNumber`
- Also exposed through a `SecurityPolicyViolationEvent`
- Aids XSS triage specifically.

- caniuse.com/contentsecuritypolicy2

You're probably doing it wrong

Allowing
`unsafe-inline`
unbounded

Missing
`object-src`
but permitting
`default-src`

Allowing
`unsafe-eval`

Content Security Policy 2

```
content-security-policy: default-src 'none';
script-src 'sha256-
BOHH2w65dTag9u/qv3W+TOprNupZC7kCtCjUgCviuKU='

[...]

<!-- Hash-Source-->
<script>
    alert(123);
</script>
```

Content Security Policy 2

```
content-security-policy: default-src 'none';
script-src 'nonce-2726c7f26c'


[...]

<!-- Nonce-Source-->
<script nonce="2726c7f26c">
    alert(123);
</script>
```

Content **S**ecurity **P**olicy **2**

Nonce- and Hash-source **will not protect you**:

- If you drop untrusted data into a JS context.
- If you're being stupid with `eval`.
- If you're *literally* hashing or noncing every resource on a page as a post-processing step.

But they're still better than whitelists.

Content Security Policy 2

Considerations for refactoring:

- Hash-source **needs a hash for every script**.
- Nonces do not carry over to new scripts.
  - Fix by Google: "`strict-dynamic`"[1]
- Whitelists are very hard to do correctly.[3]
  - Hashes and Nonces statistically more effective[4]

Content Security Policy 3

- Working Draft!
- Changes to brace for:
  - CSP 3 rewritten with FETCH in mind (fetch.spec.whatwg.org/)
  - Reporting slated for overhaul. "`report-uri`" deprecated in favor of "`report-to`" (w3c.github.io/reporting/)

Content **S**ecurity **P**olicy **3**

- Changes to enjoy:
  - "`strict-dynamic`" (allows new scripts to inherit authorization from a nonced script)
  - Sub-Resource Integrity matching work-in-progress (github.com/w3c/webappsec-csp/issues/78)
- [w3.org/TR/CSP3/](w3.org/TR/CSP3/)

"Trust on first use for https connections"

i.e. "if you don't see *this* key, we shouldn't speak."

Http **P**ublic **K**ey **P**inning in a nutshell

Http Public Key Pinning

This can ~~break~~ brick your site. Use Reporting!

- Have **multiple** keys!
- Have **multiple** backups!
- **Use Certificate Authority Authorization.** (https://tools.ietf.org/html/rfc6844)

Http Public Key Pinning

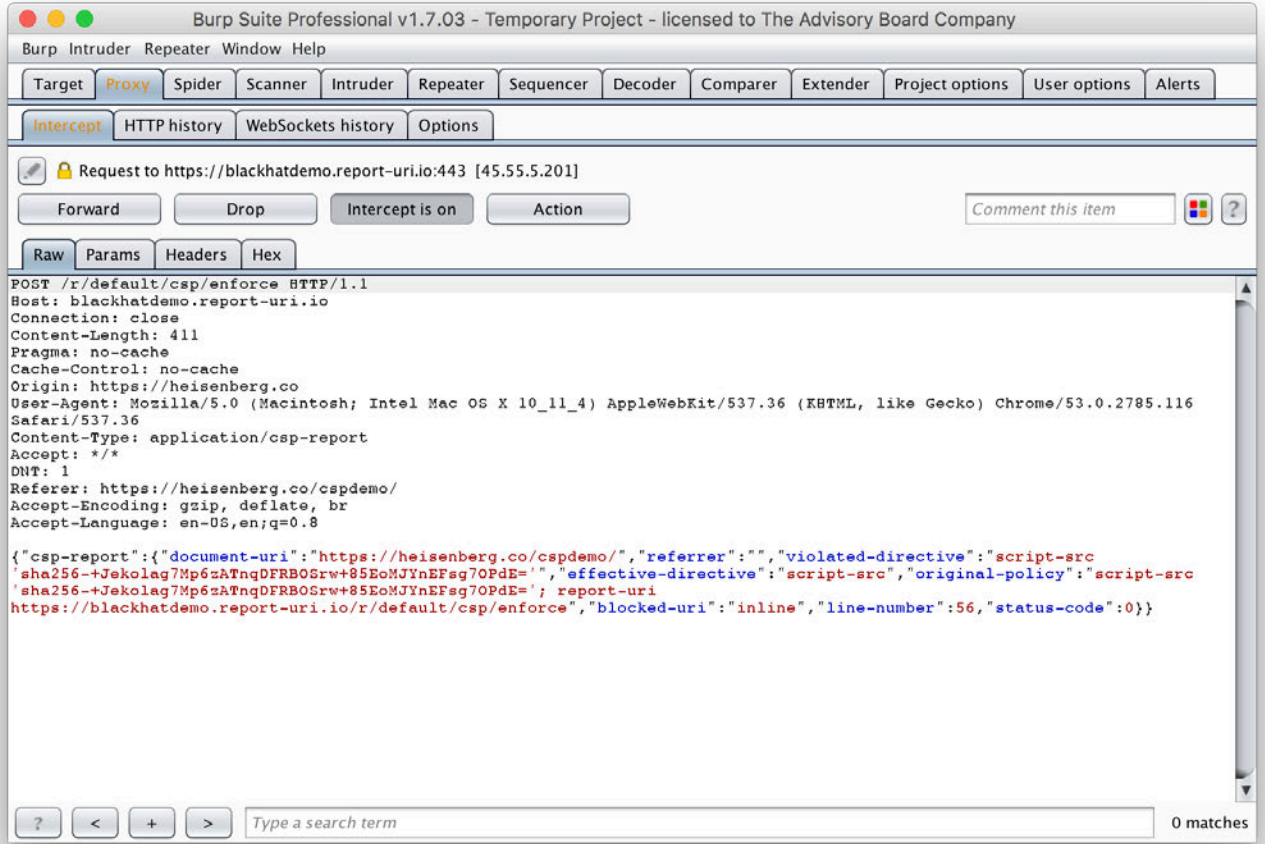
Quickstart

```
Public-Key-Pins-Report-Only:
max-age=5184000; includeSubdomains;
pin-sha256="BAD+HASH/0000000000000000000000000000000000=";
pin-sha256="BAD+HASH/0000000000000000000000000000000001=";
report-uri="https://[id].report-uri.io/r/default/hpkp/[mode]"
```

- caniuse.com/hpkp

Reporting

Why?



Burp Suite Professional v1.7.03 - Temporary Project - licensed to The Advisory Board Company
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to https://blackhatdemo.report-uri.io:443 [45.55.5.201]
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex
?
<
+
>
Type a search term
0 matches

```
POST /r/default/csp/enforce HTTP/1.1
Host: blackhatdemo.report-uri.io
Connection: close
Content-Length: 411
Pragma: no-cache
Cache-Control: no-cache
Origin: https://heisenberg.co
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.116
Safari/537.36
Content-Type: application/csp-report
Accept: */*
DNT: 1
Referer: https://heisenberg.co/cspdemo/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.8

{"csp-report":{"document-uri":"https://heisenberg.co/cspdemo/","referrer":"","violated-directive":"script-src
'sha256-+Jekolag7Mp6zATnqDFRBOSrw+85EoMJYnEFsg7OPdE='","effective-directive":"script-src","original-policy":"script-src
'sha256-+Jekolag7Mp6zATnqDFRBOSrw+85EoMJYnEFsg7OPdE='; report-uri
https://blackhatdemo.report-uri.io/r/default/csp/enforce","blocked-uri":"inline","line-number":56,"status-code":0}}
```

Reporting (CSP)

Security

- Your final layer of defense!
  - *Not your only defense!*
- What gets through your main defenses?
  - ...but is stopped in browser?

Considerations

- Absence of reports is not a report of absence (of issues)
- **Validate the reports.**
  - *Literally* do input validation. Reports are **untrusted.**

Reporting (CSP)

Quality Assurance

- Confirm expectations live.
- What gets through?
  - ...but goes against policy?

- Reports speak to application quality!

Considerations

- Run CSP in QA.
  - **i.e. not just in production.**

- New to CSP?
  Expect **heavy** reports.
  - Reports approach zero as codebase aligns with policy.

Reporting (HPKP)

Security

- *Are your connections to users trusted?*
- Why not?
  - Compromised clients?
  - ...networks?
  - ......servers?
- How do you know?

Infrastructure

- Certificate management
  - Enforce expectations.
  - Gain insight into certificate management practices.

Reporting (HPKP)

Considerations

- Chrome 46+ only; no reporting in Firefox 😐
- Use a different domain!
  - If you brick your site, don't brick your reporting.

Reporting

The easy way

- report-uri.io
  (It's free! Thanks, Scott!)

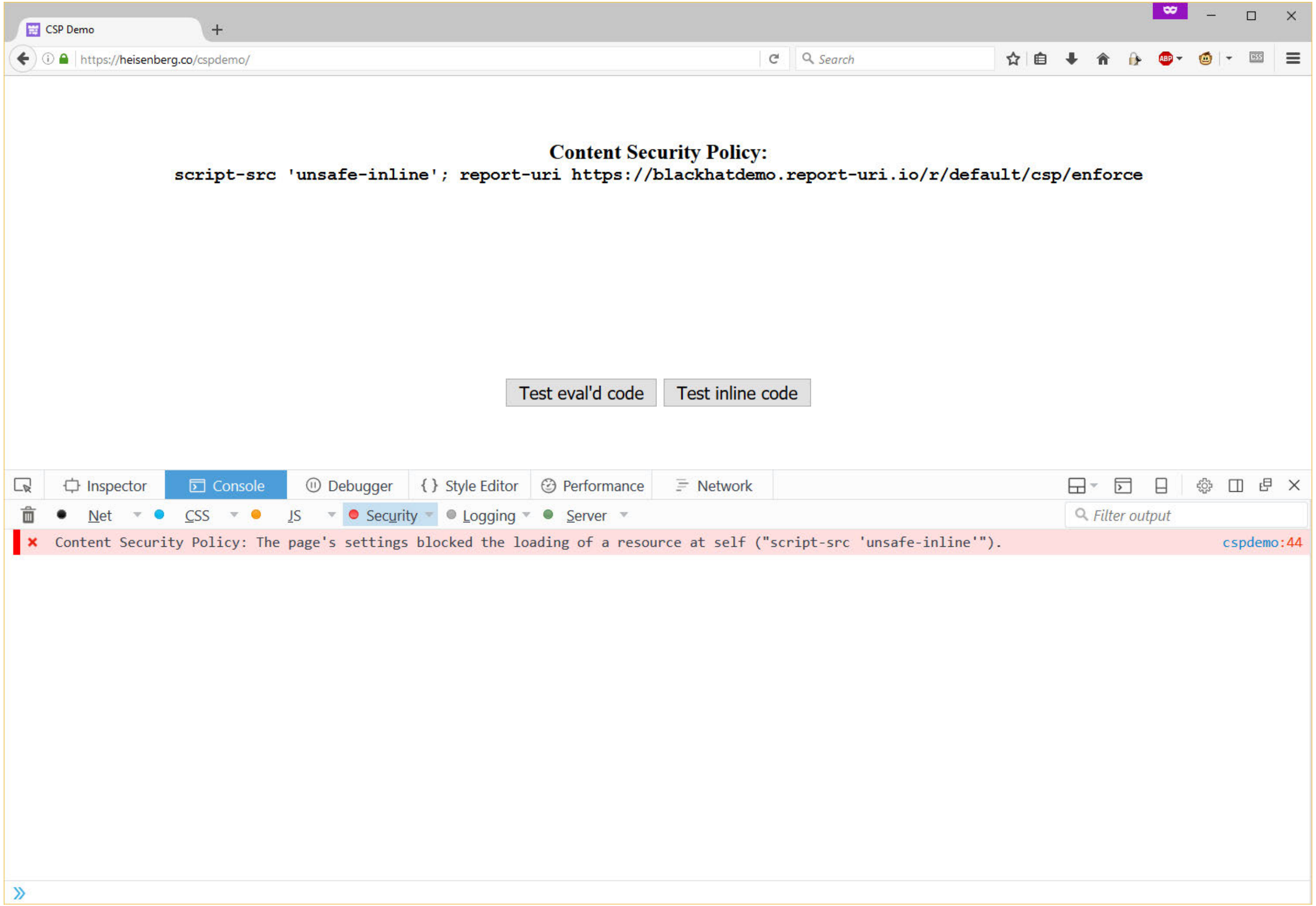
A bit harder

- Build your own aggregator
  mathiasbynens.be/notes/csp-reports

- **Validate the reports.**
  - *Literally* do input validation. Reports are **untrusted.**

Demo (CSP)

heisenberg.co/cspdemo/



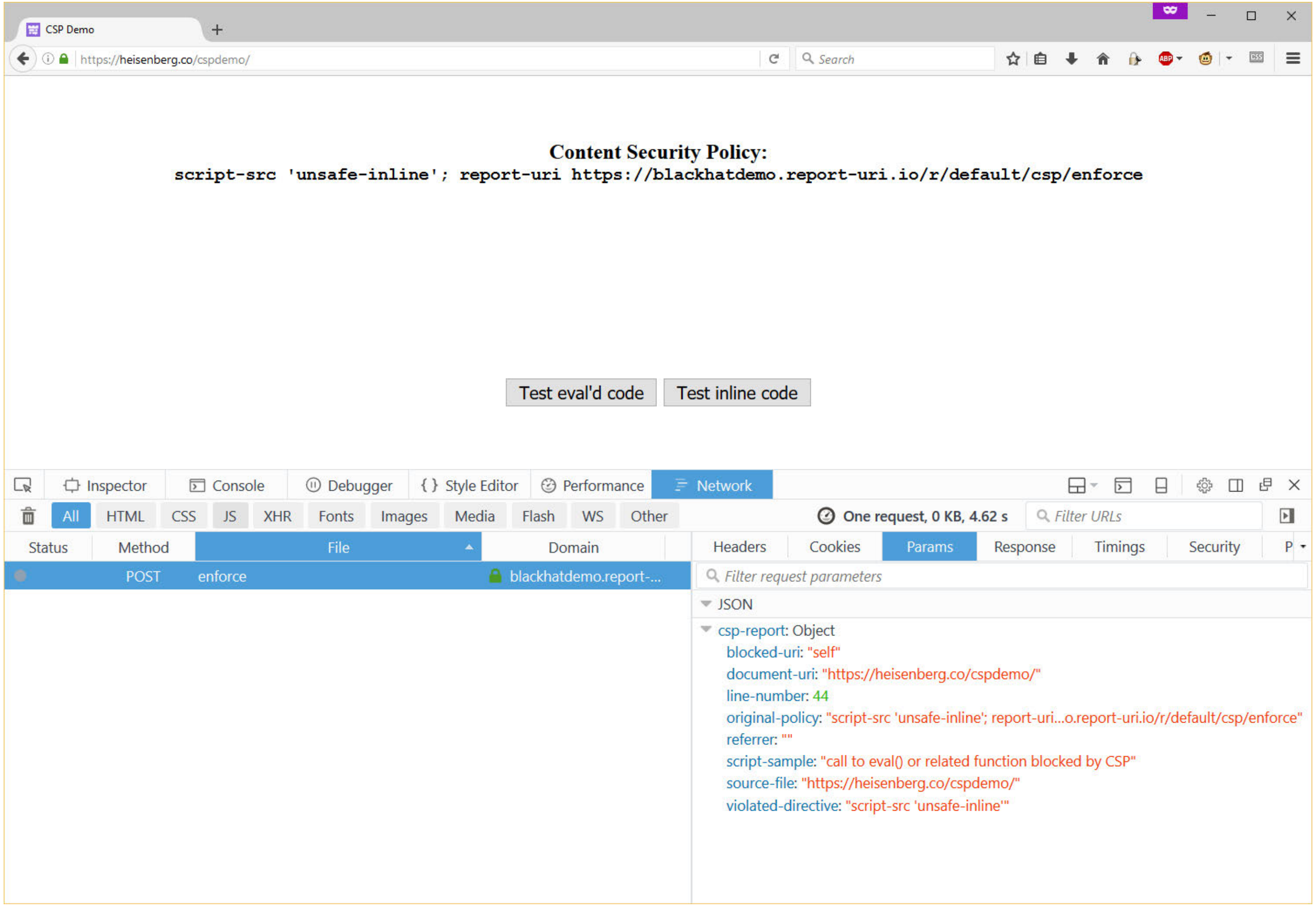
Content Security Policy:

```
script-src 'unsafe-inline'; report-uri https://blackhatdemo.report-uri.io/r/default/csp/enforce
```

Test eval'd code

Test inline code

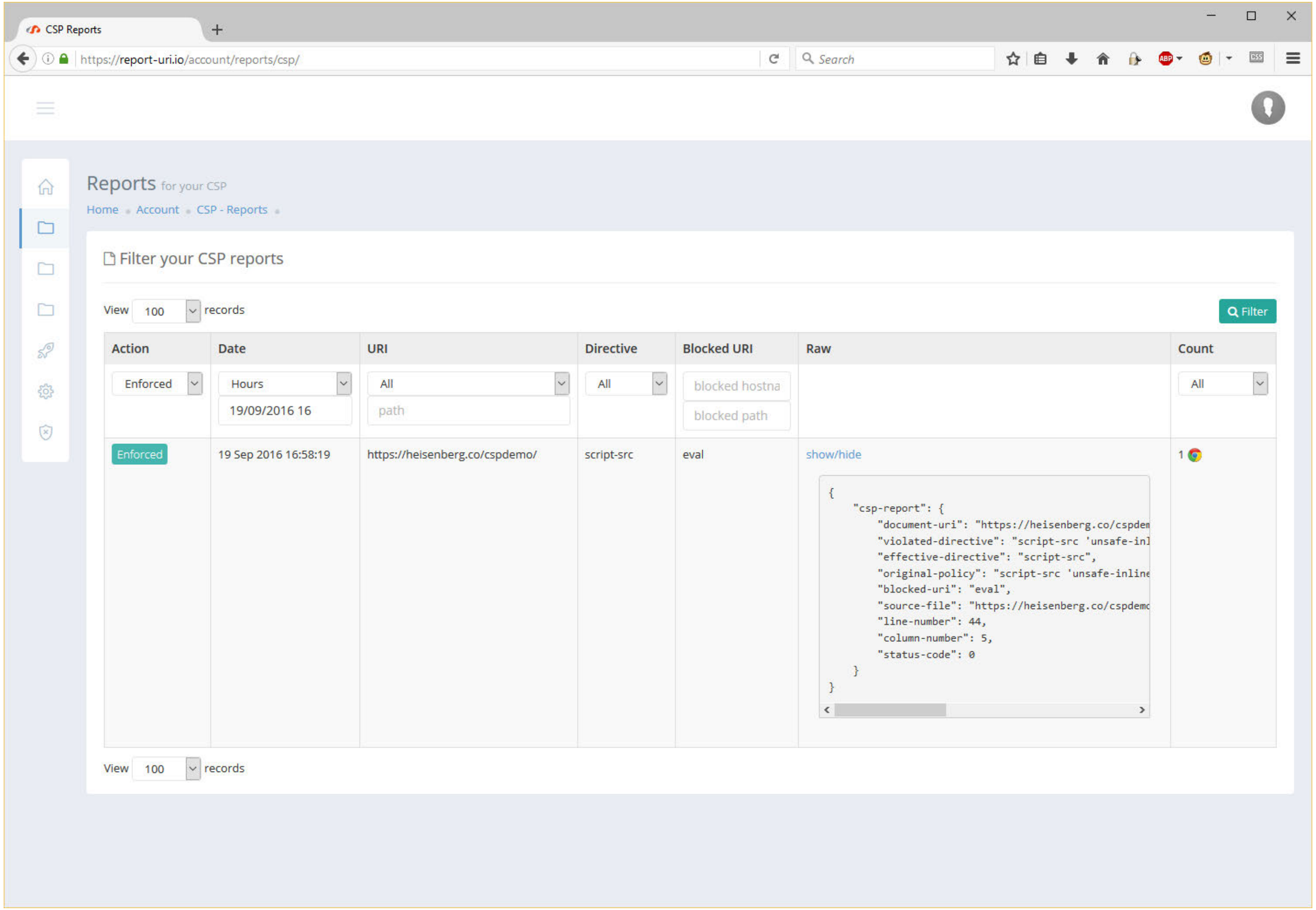
```
✕ Content Security Policy: The page's settings blocked the loading of a resource at self ("script-src 'unsafe-inline'").    cspdemo:44
```



Content Security Policy:

`script-src 'unsafe-inline'; report-uri https://blackhatdemo.report-uri.io/r/default/csp/enforce`

```
JSON
csp-report: Object
  blocked-uri: "self"
  document-uri: "https://heisenberg.co/cspdemo/"
  line-number: 44
  original-policy: "script-src 'unsafe-inline'; report-uri...o.report-uri.io/r/default/csp/enforce"
  referrer: ""
  script-sample: "call to eval() or related function blocked by CSP"
  source-file: "https://heisenberg.co/cspdemo/"
  violated-directive: "script-src 'unsafe-inline'"
```



Reports for your CSP

Home • Account • CSP - Reports •

Filter your CSP reports

View 100 records

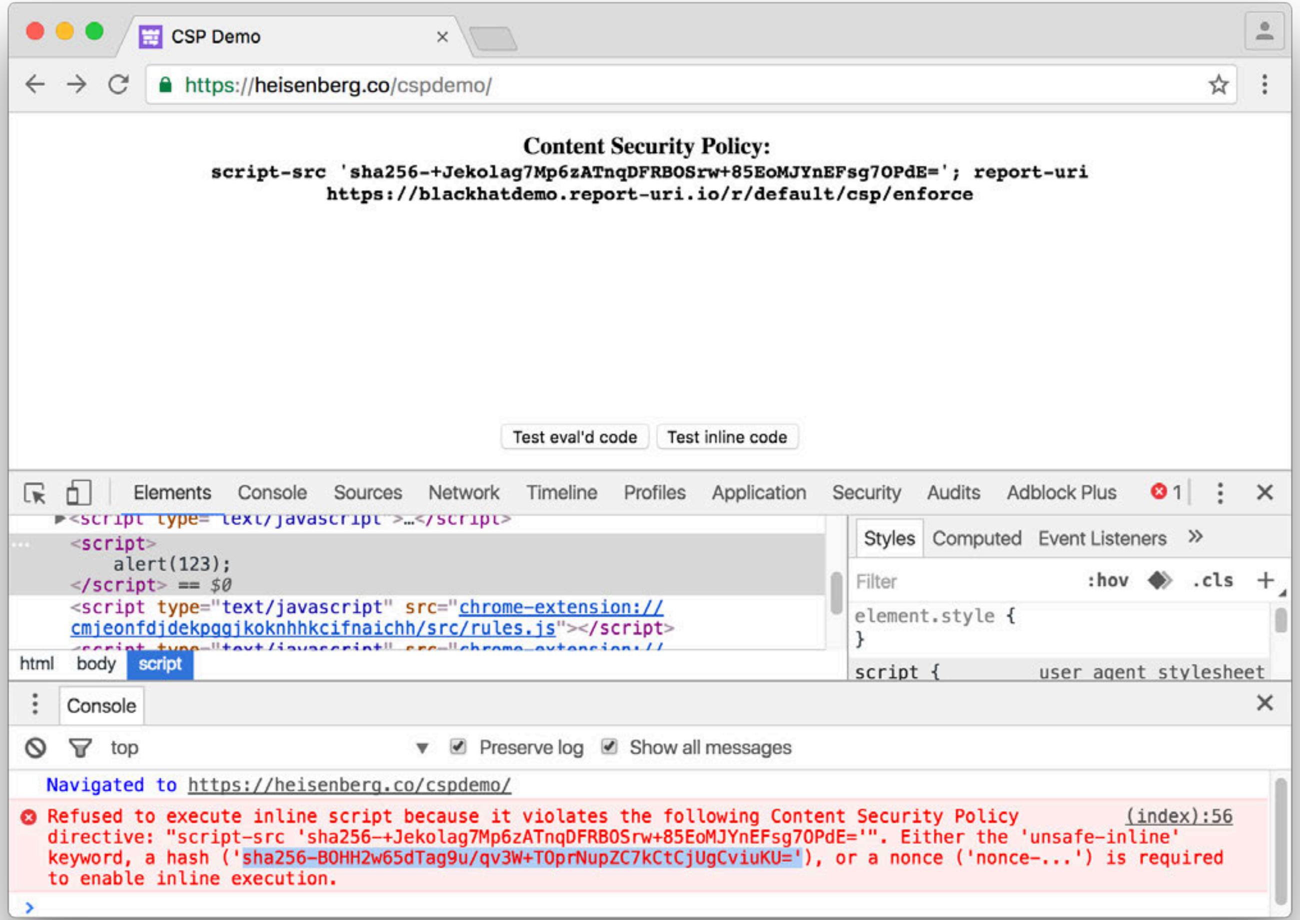
Action	Date	URI	Directive	Blocked URI	Raw	Count
Enforced	Hours 19/09/2016 16	All path	All	blocked hostna blocked path		All
Enforced	19 Sep 2016 16:58:19	https://heisenberg.co/cspdemo/	script-src	eval	show/hide	1

```
{
    "csp-report": {
        "document-uri": "https://heisenberg.co/cspdem
        "violated-directive": "script-src 'unsafe-inl
        "effective-directive": "script-src",
        "original-policy": "script-src 'unsafe-inline
        "blocked-uri": "eval",
        "source-file": "https://heisenberg.co/cspdemo
        "line-number": 44,
        "column-number": 5,
        "status-code": 0
    }
}
```

View 100 records

Easter egg (CSP hashing)

heisenberg.co/cspdemo/



Content Security Policy:
`script-src 'sha256-+Jekolag7Mp6zATnqDFRBOSrw+85EoMJYnEFsg7OPdE='; report-uri https://blackhatdemo.report-uri.io/r/default/csp/enforce`

```
▶<script type="text/javascript">…</script>
  <script>
      alert(123);
  </script> == $0
  <script type="text/javascript" src="chrome-extension://
  cmjeonfdjdekpggjkoknhhkcifnaichh/src/rules.js"></script>
```

```
element.style {
}
script {                user agent stylesheet
```

```
Navigated to https://heisenberg.co/cspdemo/
Refused to execute inline script because it violates the following Content Security Policy     (index):56
directive: "script-src 'sha256-+Jekolag7Mp6zATnqDFRBOSrw+85EoMJYnEFsg7OPdE='". Either the 'unsafe-inline'
keyword, a hash ('sha256-BOHH2w65dTag9u/qv3W+TOprNupZC7kCtCjUgCviuKU='), or a nonce ('nonce-...') is required
to enable inline execution.
```

Demo (HPKP)

redskins.io

Reporting Caveats

"It's about trust."

In the end, who *sends* the reports?

Hat Tip

Demos by Ryan Lester and Bryant Zadegan. Free use of report-uri.io as well as feedback by Scott Helme. Thanks to Rami Essaid and Distil Networks for sponsoring the talk.

Questions? (Have Some Links)

CSP	(old)	w3.org/TR/CSP1/
	(current)	w3.org/TR/CSP2/
	(draft)	w3.org/TR/CSP3/
HPKP		RFC 7469
Report-uri.io		report-uri.io

[1] "Content Security Policy 3" https://www.w3.org/TR/CSP3/#intro

[2] "Content Security Policy Quick Reference Guide"https://content-security-policy.com/, with changes.

[3] "Sh*t!,It's CSP!" https://github.com/cure53/XSSChallengeWiki/wiki/H5SC-Minichallenge-3:-"Sh*t,-it%27s-CSP!"

[4] "CSP is dead!" https://research.google.com/pubs/pub45542.html

Thank You!

Bryant Zadegan
Director, Application Security
The Advisory Board Company

keybase.io/bryant
@eganist