

A CDN that can not XSS you

Using Subresource Integrity



about:frederik

Frederik Braun

Security Engineer at Mozilla

fbraun@mozilla.com

<https://frederik-braun.com>

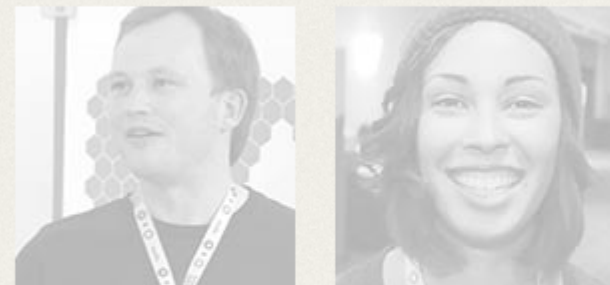
[@freddyb](#)



Why am I here?



02 *The Internet is a global public resource that must remain open and accessible.*



03 *The Internet must enrich the lives of individual human beings.*



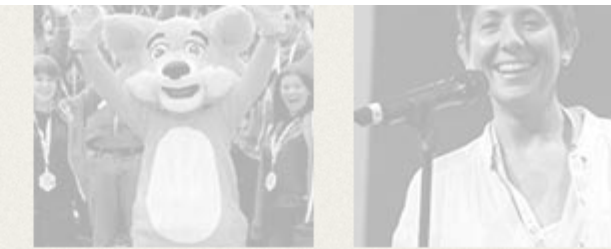
04 *Individuals' security and privacy on the Internet are fundamental and must not be treated as optional.*



05 *Individuals must have the ability to shape the Internet and their own experiences on it.*



06 *The effectiveness of the Internet as a public resource depends upon interoperability (protocols, data formats, content), innovation and decentralized participation worldwide.*



Content Delivery Networks

Who has seen code like this?

```
<script src="https://code.jquery.com/jquery-2.1.4.min.js"></script>
```

```
<link href='http://fonts.googleapis.com/css?family=PT+Sans...'
      rel='stylesheet' type='text/css'>
```

What does it do?

```
<script src="https://code.jquery.com/jquery-2.1.3.min.js"></script>
```

The Same-Origin Policy

Origins Explained

http: / /	www.example.com	:80
------------------	------------------------	------------

Can execute but most not read?

```
<script src="https://code.jquery.com/jquery-2.1.4.min.js"></script>
```

The Same Origin Policy

The Same Origin Policy

XMLHttpRequest

DOM Access

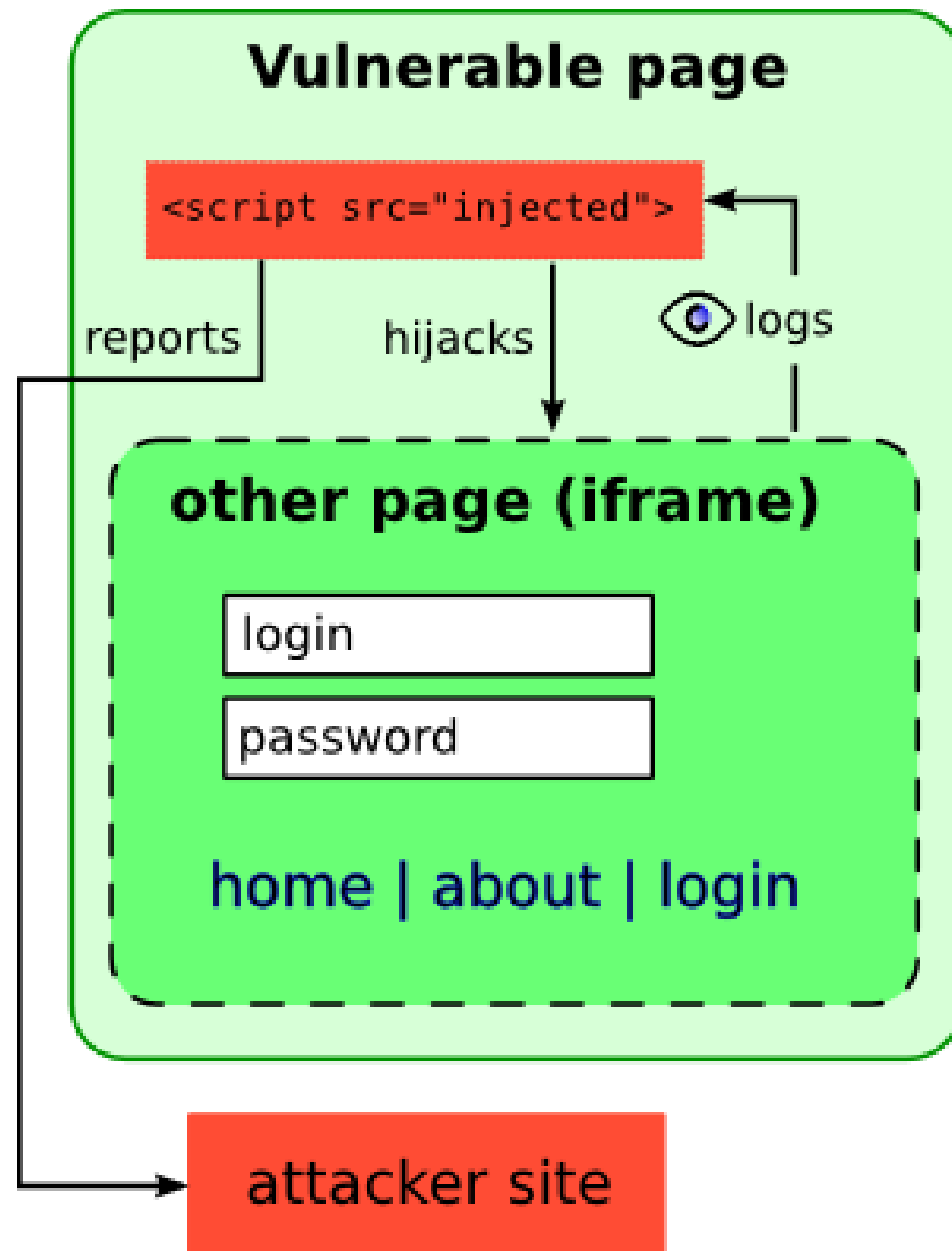
Cookies

Permissions

kotowicz's XSS-Track



kotowicz's XSS-Track



one vulnerability is enough



jQuery Confirms Website Hacked Again

By [Eduard Kovacs](#) on September 25, 2014

[Tweet](#)



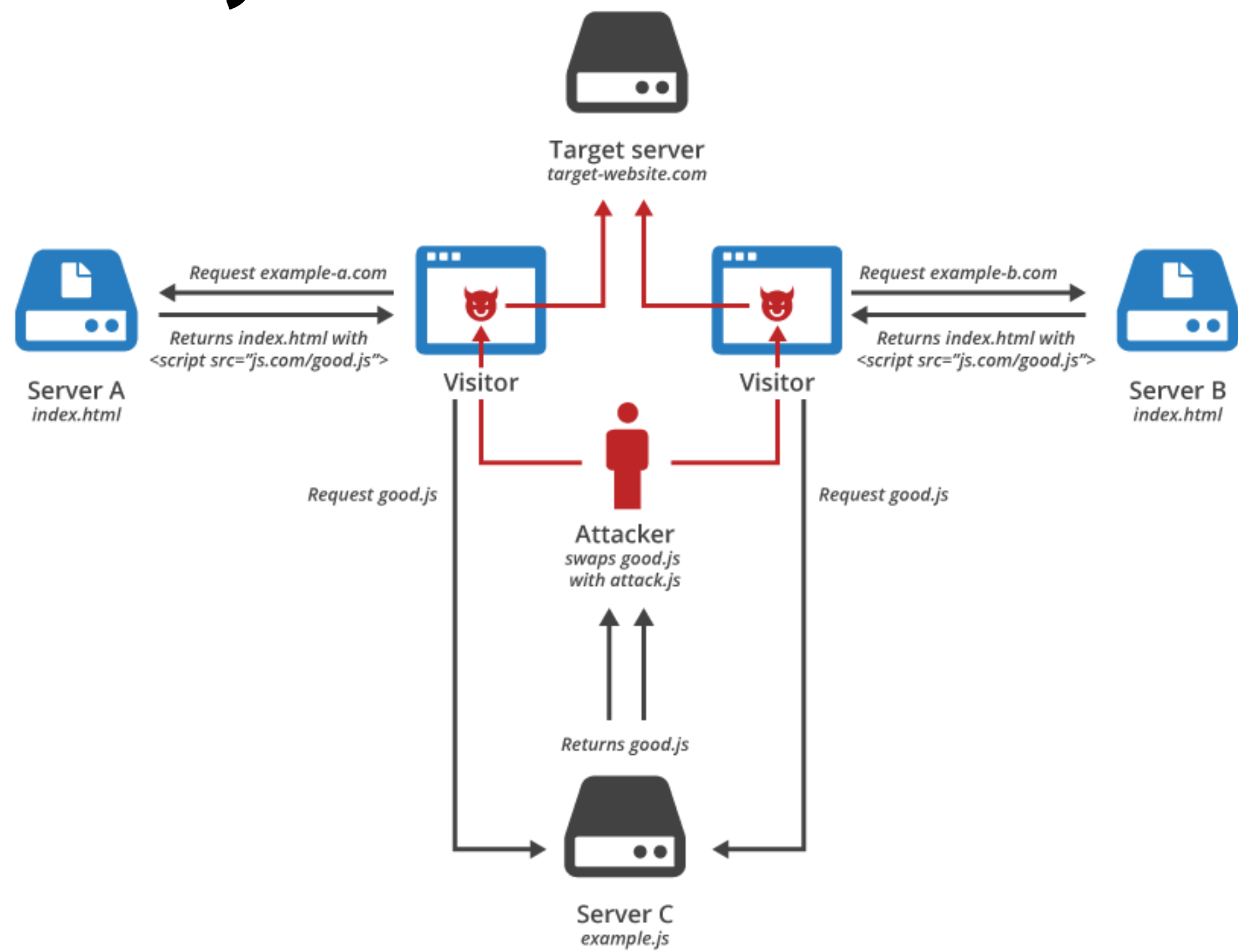
jQuery.com, the official website for the popular JavaScript library, has been compromised for a [second time](#) in less than a week, the organization admitted on Wednesday.

On Tuesday, security firm RiskIQ [reported](#) that jQuery.com had been abused in a drive-by download attack leveraging the RIG exploit kit since September 18. While there was no evidence that the jQuery library itself was compromised, researchers discovered a malicious script designed to load an iframe, which redirected the site's visitors to a page hosting the exploit kit.

James Pleger, RiskIQ director of research, told SecurityWeek that the attackers attempted to distribute the Andromeda malware. Pleger revealed that companies in sectors like banking, technology and defense were affected by the attack.

The redirector domain used in the attack, [jquery-cdn\[.\]com](#), is hosted in Russia and it was registered on September 18, RiskIQ said.

Popular JS libraries used for DDoS



**Dear burglar,
here's the combination to our safe.
Please do not wake us up.**

Subresource Integrity to the Rescue



Subresource Integrity

W3C Working Draft 09 April 2015

Latest published version:

<http://www.w3.org/TR/SRI/>

Latest editor's draft:

<http://w3c.github.io/webappsec/specs/subresourceintegrity/>

Editors:

[Frederik Braun](#), [Mozilla](#)

[Francois Marier](#), [Mozilla](#)

[Devdatta Akhawe](#), [Dropbox, Inc.](#)

[Joel Weinberger](#), [Google, Inc.](#)

Copyright © 2014-2015 W3C® ([MIT](#), [ERCIM](#), [Keio](#), [Beihang](#)). [W3C liability](#), [trademark](#) and [document use](#) rules apply.

```
<script src="https://code.jquery.com/jquery-1.10.2.min.js"  
    integrity="sha256-C6CB9UYIS9UJeqinPHWTHVqh/E1uhG5Twh+Y5qFQmYg="  
    crossorigin="anonymous"></script>
```

```
<script src="https://code.jquery.com/jquery-1.10.2.min.js"  
  integrity="sha256-C6CB9UYIS9UJeqinPHWTHVqh/E1uhG5Twh+Y5qFQmYg="  
  crossorigin="anonymous"></script>
```

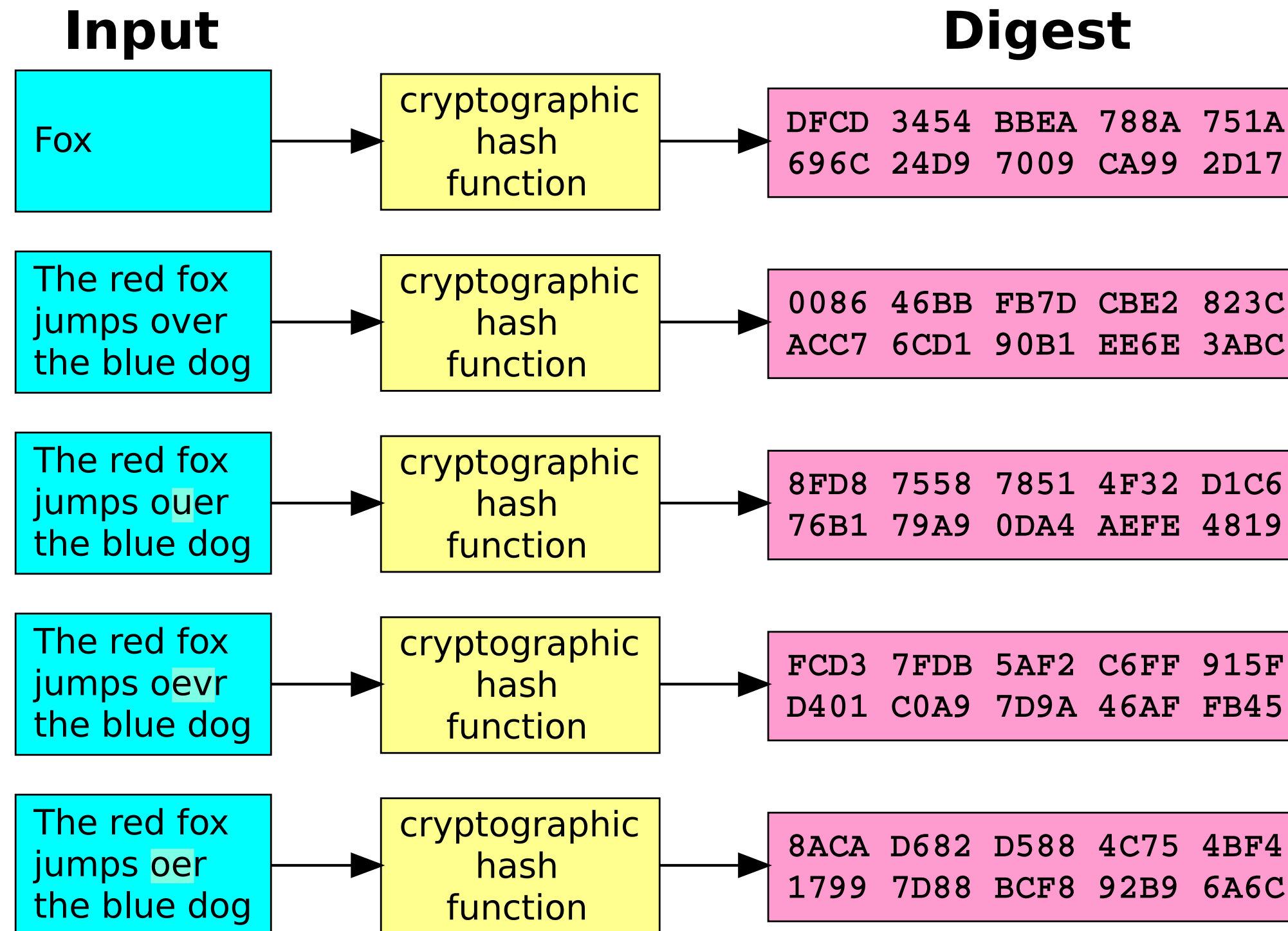
Integrity

Cryptographic Hash Functions

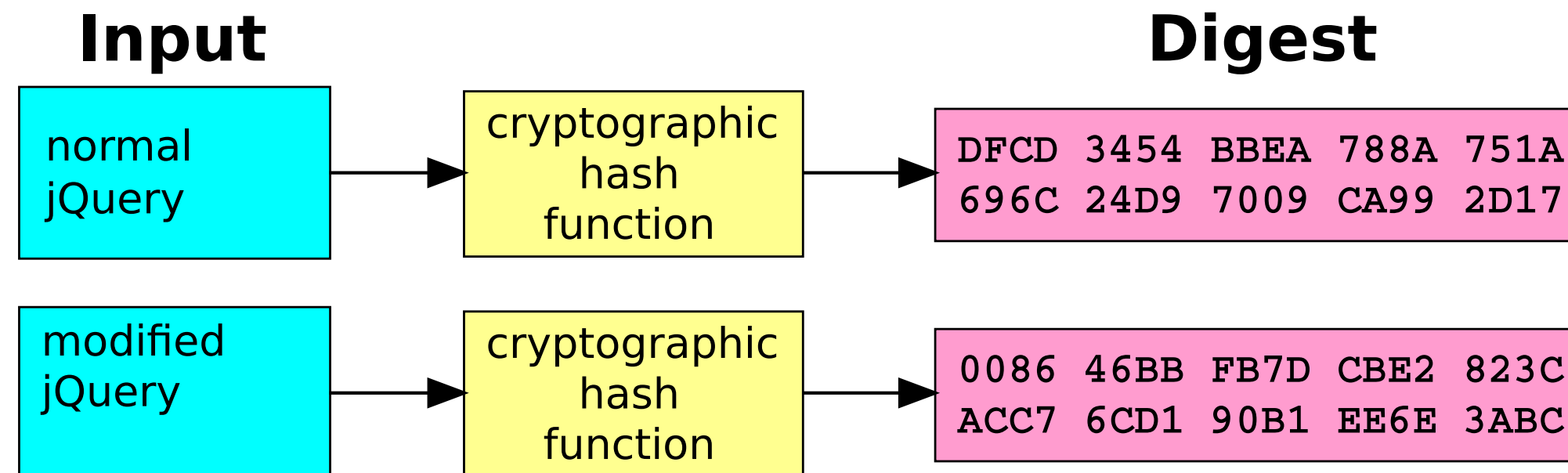
```
$ sha256sum ubuntu-15.04-desktop-amd64.iso
```

```
b970b014b3a2ea216fcf077328bfe32  
18ed5c2f923fe2d9dfd2b41df9d735a5
```

Cryptographic Hash Functions



Cryptographic Hash Functions



Reading Cross-Origin Data?

http://victim.example.com/status.json

```
{  
  'status': 'authenticated',  
  'username': 'Alice'  
}
```

Let's attack!

```
<script src="https://victim.example.com/status.json"  
      integrity="{ hash for Bob }"></script>
```

```
<script src="https://victim.example.com/status.json"  
      integrity="{ hash for Alice }"></script>
```

http://192.168.1.1/config.js

HTTP/1.1 200 OK

Accept-Ranges: bytes

Cache-Control: max-age=604800

Content-Type: text/html

Date: Wed, 29 Apr 2015 09:33:56 GMT

Etag: "359670651"

Server: ...

Content-Length: ...

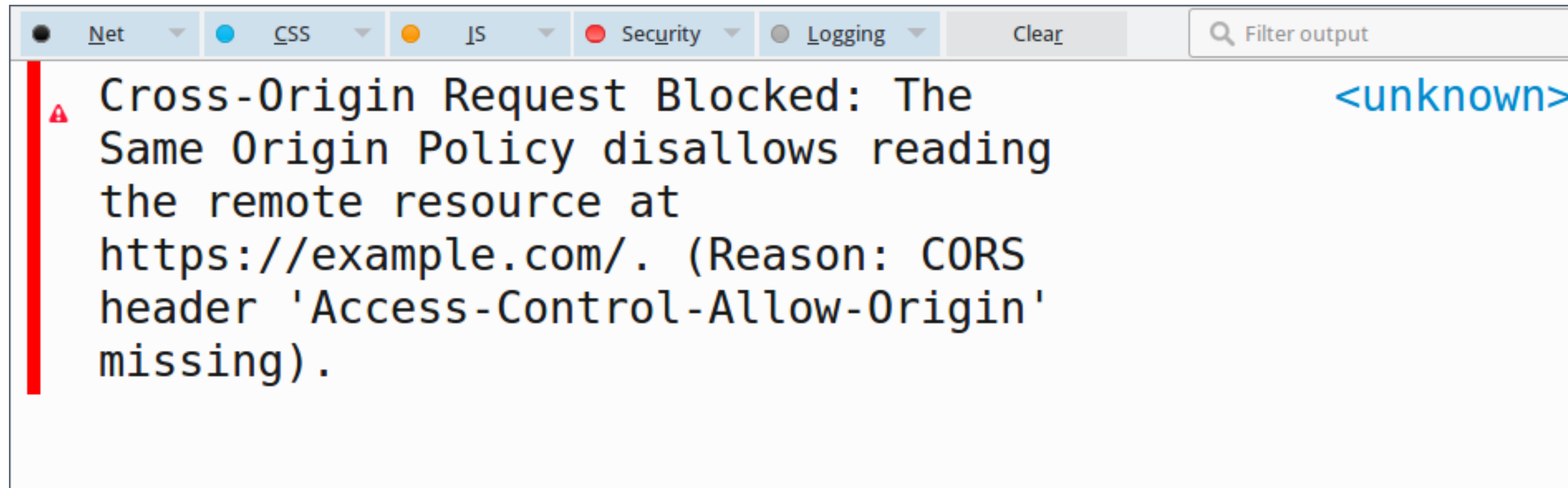
```
{'wifi_enabled': true, ..., 'password': 'admin'}
```

Cross Origin Resource Sharing (CORS)

Recap

```
1 var xhr = new XMLHttpRequest();  
2 xhr.open("GET", "https://example.com")  
3 xhr.send();  
4 xhr.onload = function() { console.log(xhr.response); }
```

CORS Required



Using CORS

HTTP/1.1 200 OK

Accept-Ranges: bytes

Cache-Control: max-age=604800

Content-Type: text/html

Date: Wed, 29 Apr 2015 09:33:56 GMT

Etag: "359670651"

Server: ...

Access-Control-Allow-Origin: *

Content-Length: ...

```
<script src="https://code.jquery.com/jquery.min.js"  
    integrity="sha256-C6CB9UYIS9UJeqinPHWTHVqh/E1uhG5Twh+Y5qFQmYg="   
    crossorigin="anonymous"></script>
```

The Fineprint

integrity Syntax

```
<script src="https://code.jquery.com/jquery.min.js"  
  integrity="sha256-C6CB9U...qFQmYg=" "  
  crossorigin="anonymous"></script>
```

integrity Syntax

sha256-C6CB9U...qFQmYg=

Multiple Hash Functions

```
<script src="https://code.jquery.com/jquery.min.js"  
  integrity="sha256-C6CB9U...qFQmYg=  
    sha384-H8BRh8j4809oYatfu5AZz...t1FLm52t+eX6x0"  
  crossorigin="anonymous"></script>
```

Multiple Hashes

```
<script src="https://code.jquery.com/jquery.min.js"  
  integrity="sha256-C6CB9UYIS9UJeqinPHWTHVqh/E1uhG5Twh+Y5qFQmYg=  
    sha256-qznLcsR0x4GACP2dm0UCKCzCG+HiZ1guq6ZZDob/Tng="  
  crossorigin="anonymous"></script>
```

Multiple Hashes

```
<script src="https://code.jquery.com/jquery.min.js"  
  integrity="sha256-C6CB9UYIS9UJeqinPHWTH...5qFQmYg=  
    sha256-qznLcsR0x4GACP2dm0UCK...Dob/Tng=  
    sha384-H8BRh8j4809oYatfu5AZz...t1FLm52t+eX6x0  
    sha384-Vqh/E1uhG5Twh+YCzCG+H...LznqHiZ1guq6ZZ"  
  crossorigin="anonymous"></script>
```

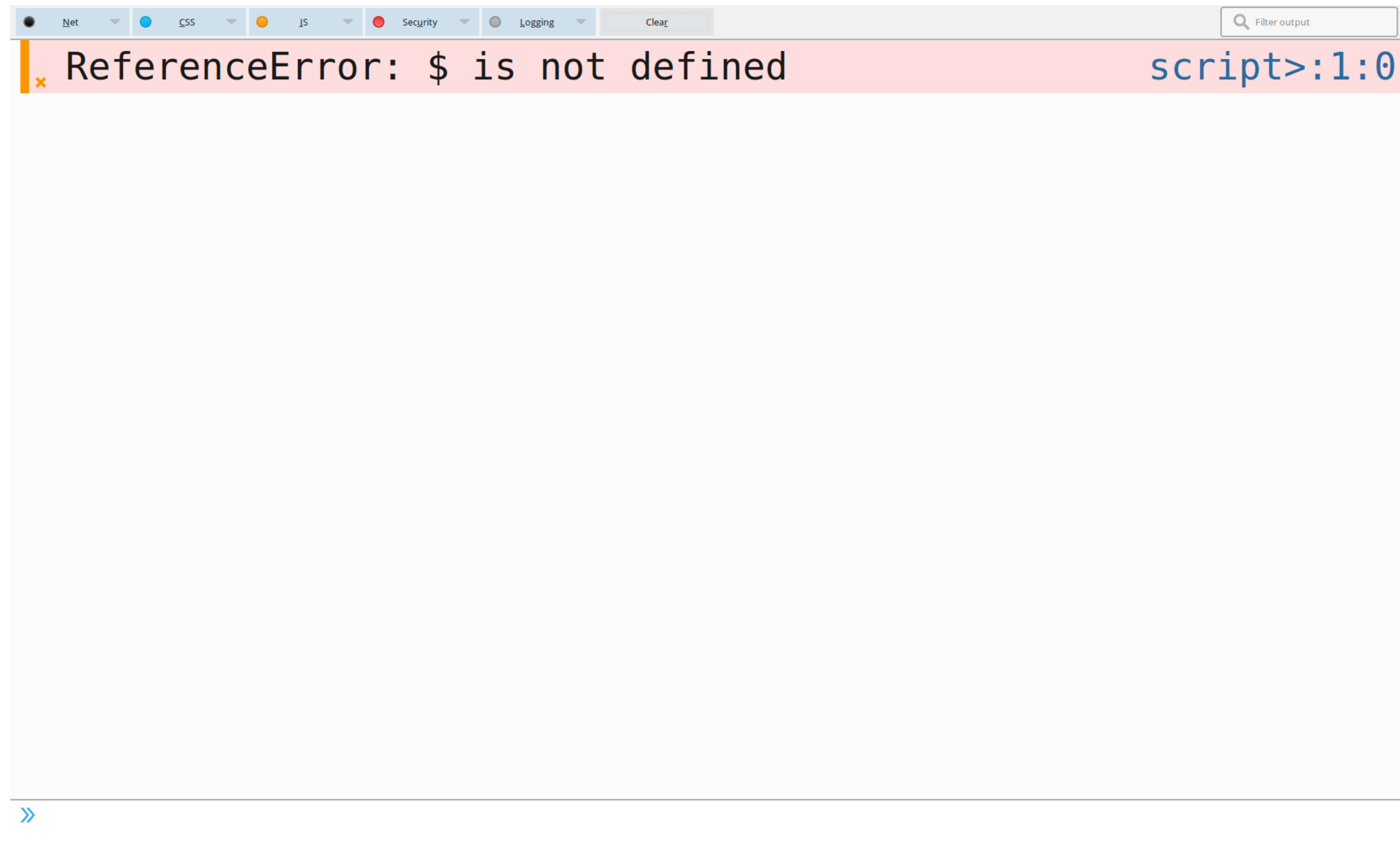
Outdated Hash Function

```
<script src="https://code.jquery.com/jquery.min.js"  
  integrity="brokenAlgo-C6CB9UYIS9UJeqinPHWh/E1uhG5Twh+Y5qFQmYg="  
  crossorigin="anonymous"></script>
```

...over HTTP or HTTPS?

Failover

An evil script was blocked \o/



Manual Error Recovery

```
<script src="https://code.jquery.com/jquery.min.js"  
    integrity="sha256-C6CB9UYIS9UJeqinPHWTHVq..."  
    crossorigin="anonymous"></script>
```

```
<script>window.jQuery || document.write('<script  
src="/jquery-.min.js"><\script>')</script>
```

Future Work

Built-in Error Recovery?

```
<script src="https://code.jquery.com/jquery.min.js"  
  integrity="sha256-C6CB9UYIS9UJeqinPHWTHVq..."  
  crossorigin="anonymous"  
  fallbacksrc="/jquery.min.js">  
</script>
```

NOT IN SPEC

Integrity Policies & Error Reporting

Content-Security-Policy:

```
integrity-policy: ("block" / "report" / "fallback") ["require-for-all"]
```

NOT IN SPEC

More Use Cases

```
<link rel="stylesheet" href="https://site53.cdn.net/style.css"  
      integrity="sha256-SdfwewFAE...wefjijfE"/>
```

Integrity and videos



NOT IN SPEC

Integrity and videos



NOT IN SPEC

We need your help!

Editor's Draft

<http://w3c.github.io/webappsec/specs/subresourceintegrity/>

Tool Support Needed



GRUNT



Enable CORS!

Send `Access-Control-Allow-Origin: *` now!

Conclusion

**You can soon add *integrity* to
secure your script loads.**

Extending the Web is non-trivial

**Browser Security needs to step up
(and will)**

Thank you for listening!

Frederik Braun

fbraun@mozilla.com

[@freddyb](#)

#security on [irc.mozilla.org](#)

