Reducing the Attack Surface with X-Content-Type-Options, Subsource Integrity and By Withholding Version Information

Roland Guijt

MICROSOFT MVP, CONSULTANT, AUTHOR AND SPEAKER

@rolandguijt rolandguijt.com

Module Overview

MIME Sniffing

Subresource Integrity Check

Referrer header and policy

ASP.NET Version Headers

Caching

MIME Type Examples

image/jpeg

text/html

application/json

application/zip

MIME Sniffing Exploitation Example

The attacker uploads a HTML file disguised as a JPG

The site stores the html file

The file is requested intended to be displayed in an HTML element

Browsers with MIME sniffing examine the file and determine the MIME type

That MIME type will then be used to render the file

This allows for another way to do cross-site scripting attacks

X-Content-Type-Options

```
X-Content-Type-Options: nosniff
```

Make sure the Content-Type header is set correctly

CDNs

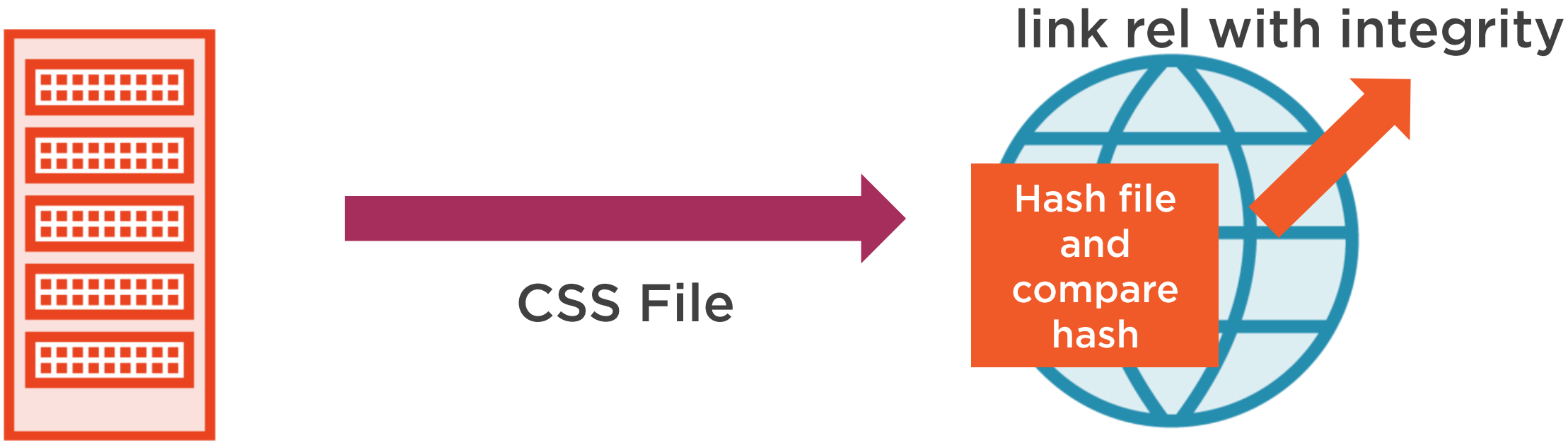
No need to store and updates physical files

No bandwidth charges

Browser caches for a common URI

Can be exploited

Subresource Integrity Check



https://srihash.org

Support in CSP

```
Content-Security-Policy: require-sri-for script style
```

The Referer Header

Misspelled

Contains URL where the user came from

Google Analytics

Privacy issues

Exploits

Controllable by Referrer-Policy header

Referrer Policy

```
Referrer-Policy: no-referrer
```

Referrer-Policy Header Options

- no-referrer
- no-referrer-when-downgrade
- same-origin
- strict-origin
- origin-when-cross-origin
- strict-origin-when-cross-origin
- unsafe-url

Version Header Concerns

Attacker can very easily find out the platform the application is running on

Vulnerabilities are easy to find out and attacks can be targeted at the platform

Caching

Sensitive data sent from server to browser might be cached

Ability to control caching mechanisms

Individual data sources can be attacked

Setting the cache-control header is no guarantee it will be honored

Cache Control Header Options

public

private

no-cache

no-store

Cache Control Header Expiration Options

max-age=<seconds>

max-stale=<seconds>

min-fresh=<seconds>

stale-while-revalidate=<seconds>

stale-if-error=<seconds>

Summary

Browser and platform defaults

Check your sources

Consider referer header