Document Title: Your browser wants you to be secure

Document URL: https://www.appsec.org.nz/conference

Your browser wants you to be secure

Kirk Jackson

@kirkj

RedShield

hack-ed.com

owasp.org.nz

Document Title: Your browser wants you to be secure

Document URL: https://www.appsec.org.nz/conference

Late 1991:

```
<title>          <p>

<a href="">      <h1> <h2> <h3> <h4> <h5> <h6>

<dl><dt></dl>    <ul><li>...</li></ul>
```

"Tags used in HTML". World Wide Web Consortium. November 3, 1992.
http://info.cern.ch/hypertext/WWW/MarkUp/Tags.html


Web browser
URL
sitea.com
HTML
Process
Operating System / Other Applications
DNS Resolvers
Web Server
HTML files
Other Hosts

Document Title: Your browser wants you to be secure

Document URL: https://www.appsec.org.nz/conference

1993 - Mosaic released:

```
<img src="">

<form>
```

File Edit View Go Bookmarks Options Directory Help

Netscape: Version 1.1N

Back Forward Home Reload Images Open Print Find Stop

Location: about:

What's New? What's Cool? Handbook Net Search Net Directory Newsgroups

Netscape Navigator (TM)

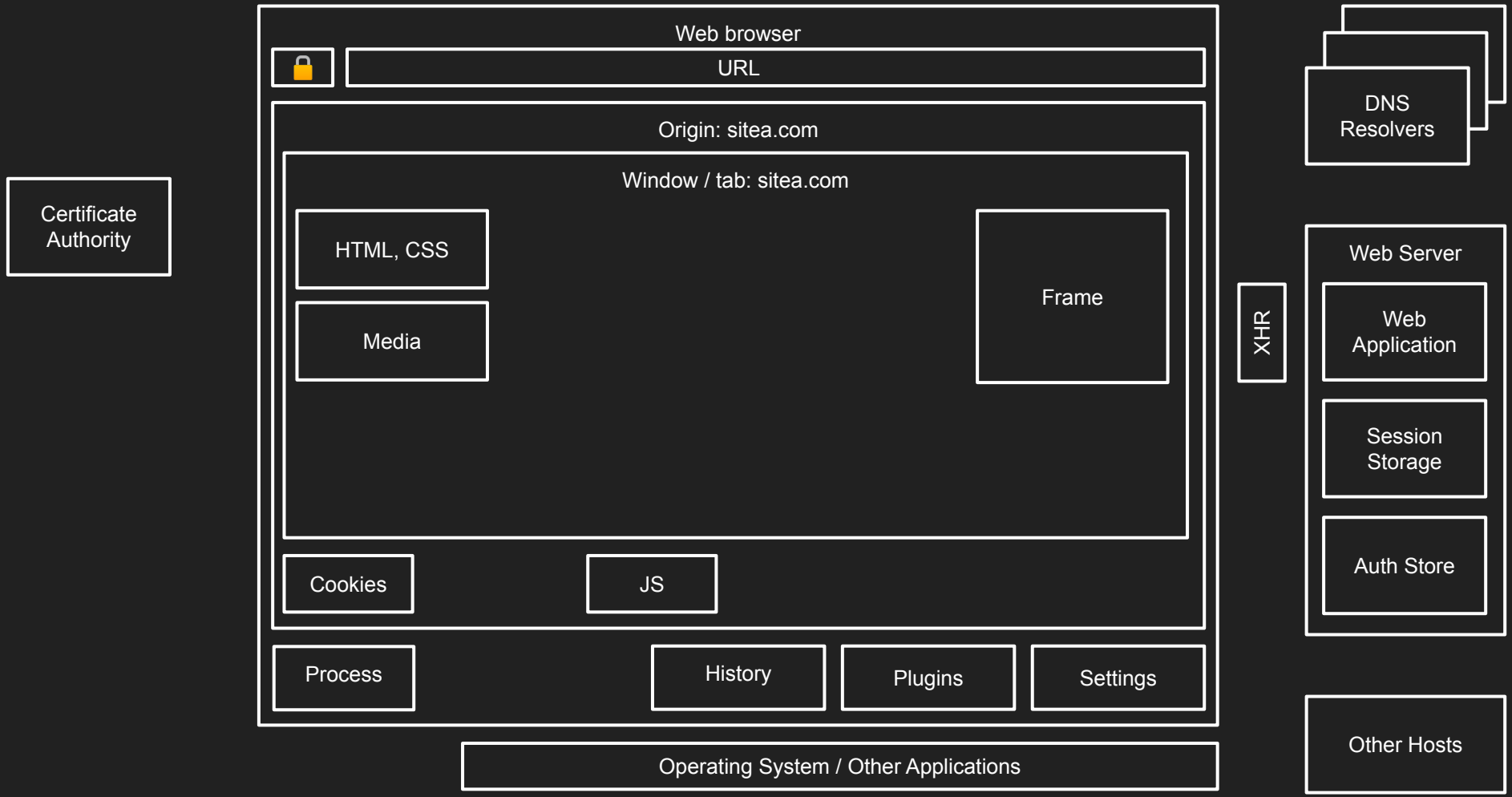
Version 1.1N

This software is subject to the license agreement set forth in the license. Please read and agree to all terms before using this software.

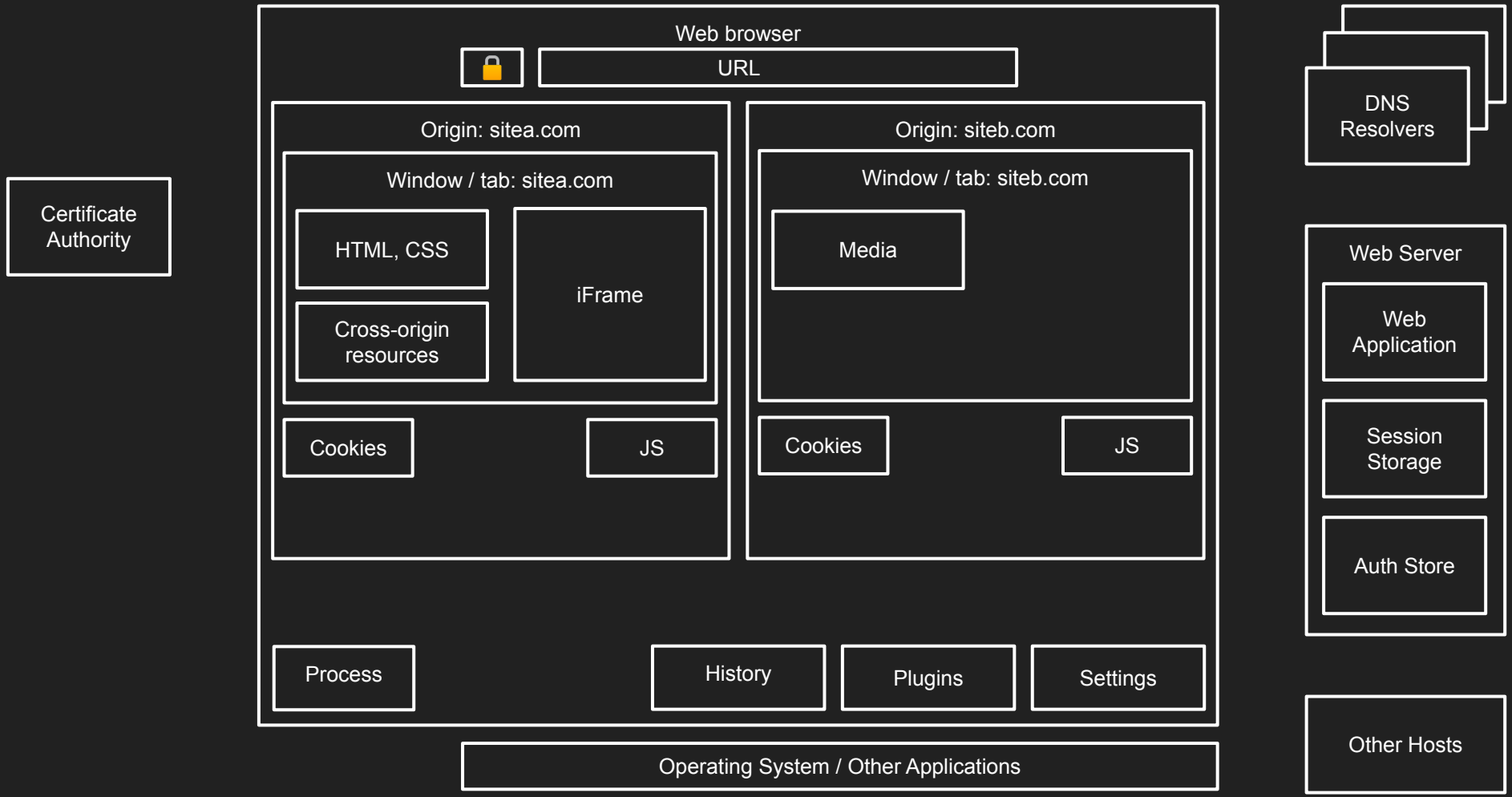
Report any problems through the feedback page.

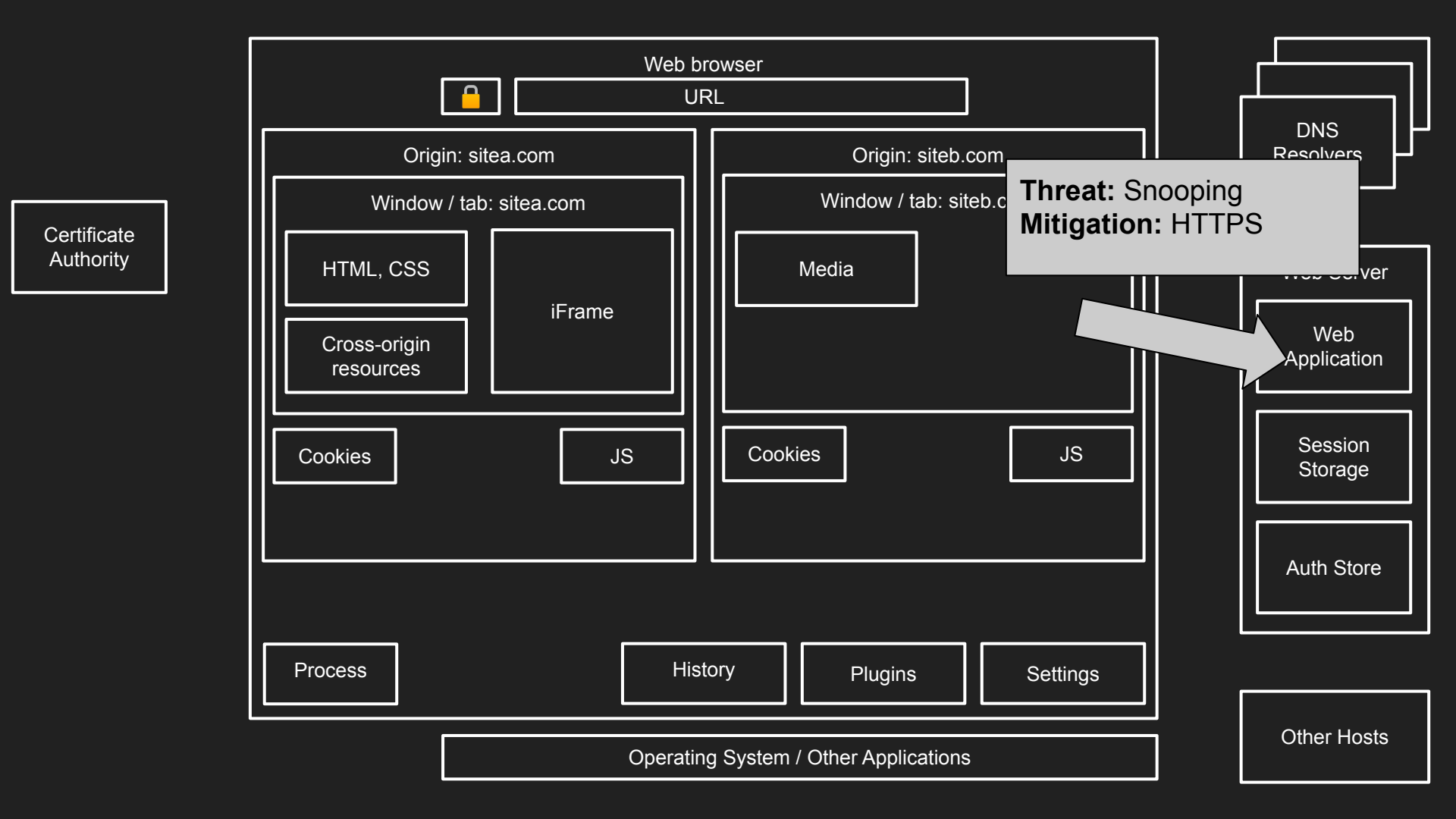
NETSCAPE

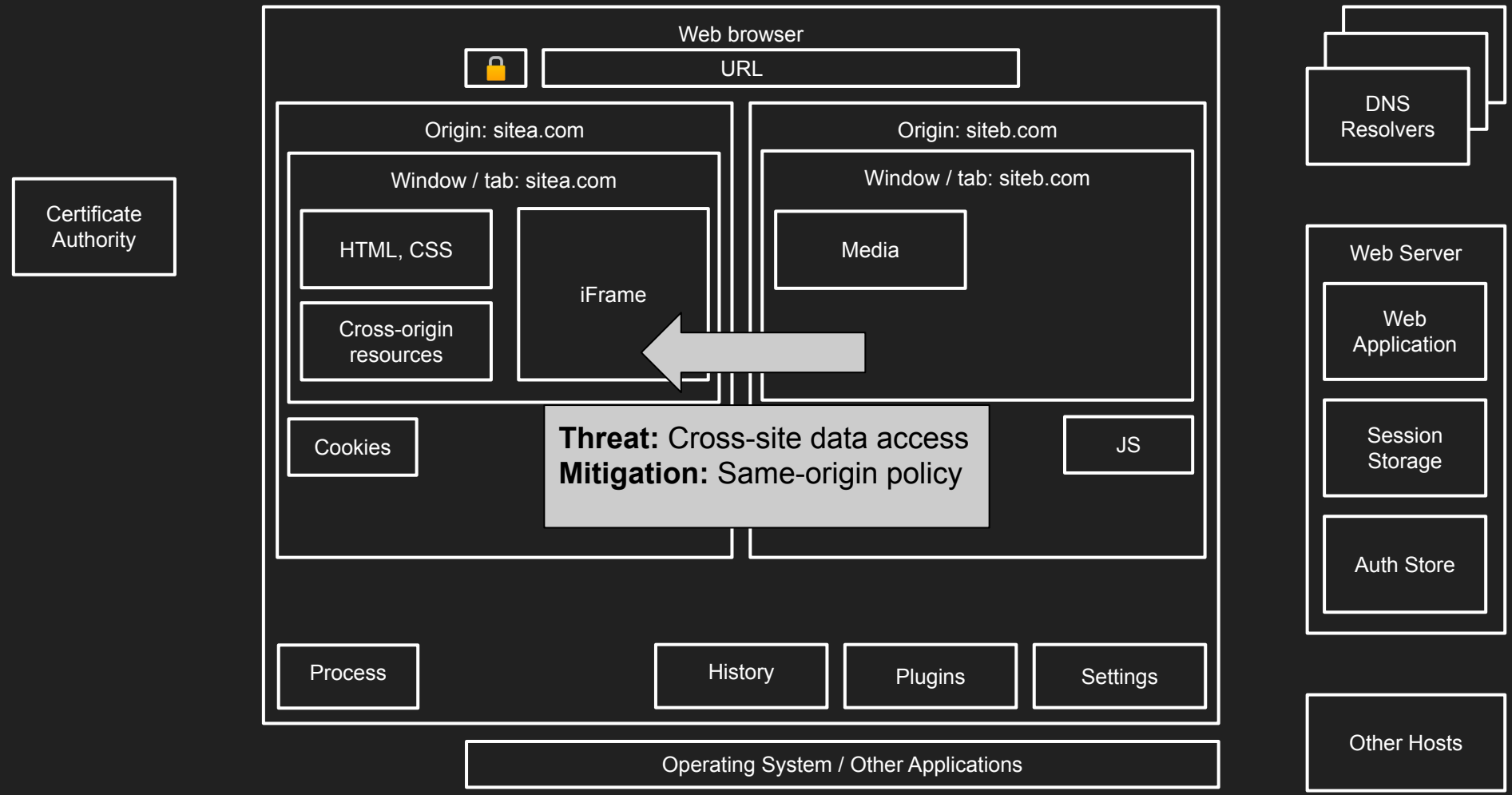

File Edit View Go Bookmarks Options Directory Help
Netscape: Version 1.1N
Back
Forward
Home
Reload
Images
Open
Print
Find
Stop
Location : about :
What's New?
What's Cool?
Handbook
Net Search
Net Directory
Newsgroups
1994:
Set-Cookie
https://
1995:
Mocha (Javascript)
DOM
Same-origin policy

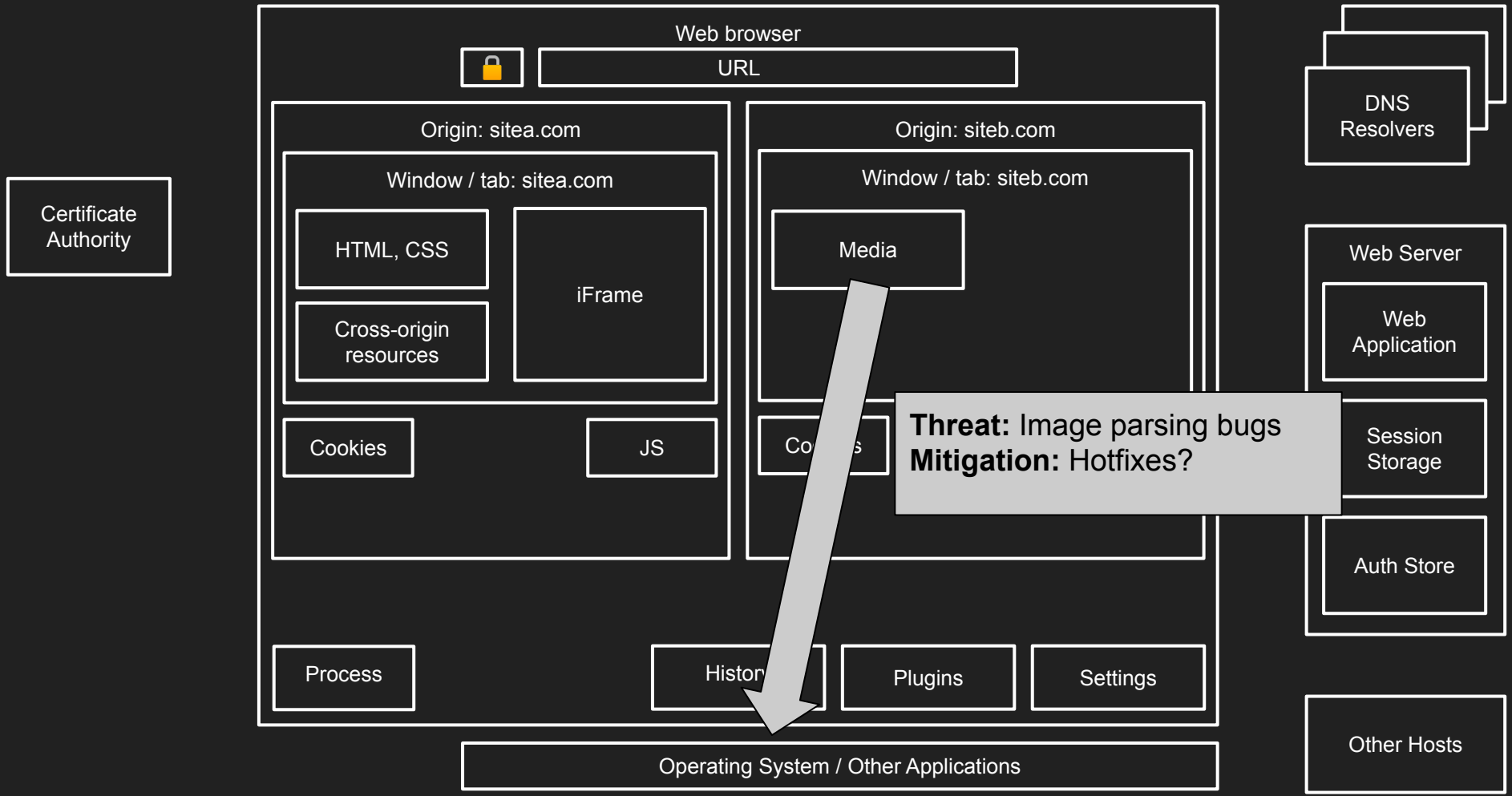

Web browser
URL
Origin: sitea.com
Window / tab: sitea.com
HTML, CSS
Media
Frame
Cookies
JS
Process
History
Plugins
Settings
Operating System / Other Applications
Certificate Authority
XHR
DNS Resolvers
Web Server
Web Application
Session Storage
Auth Store
Other Hosts

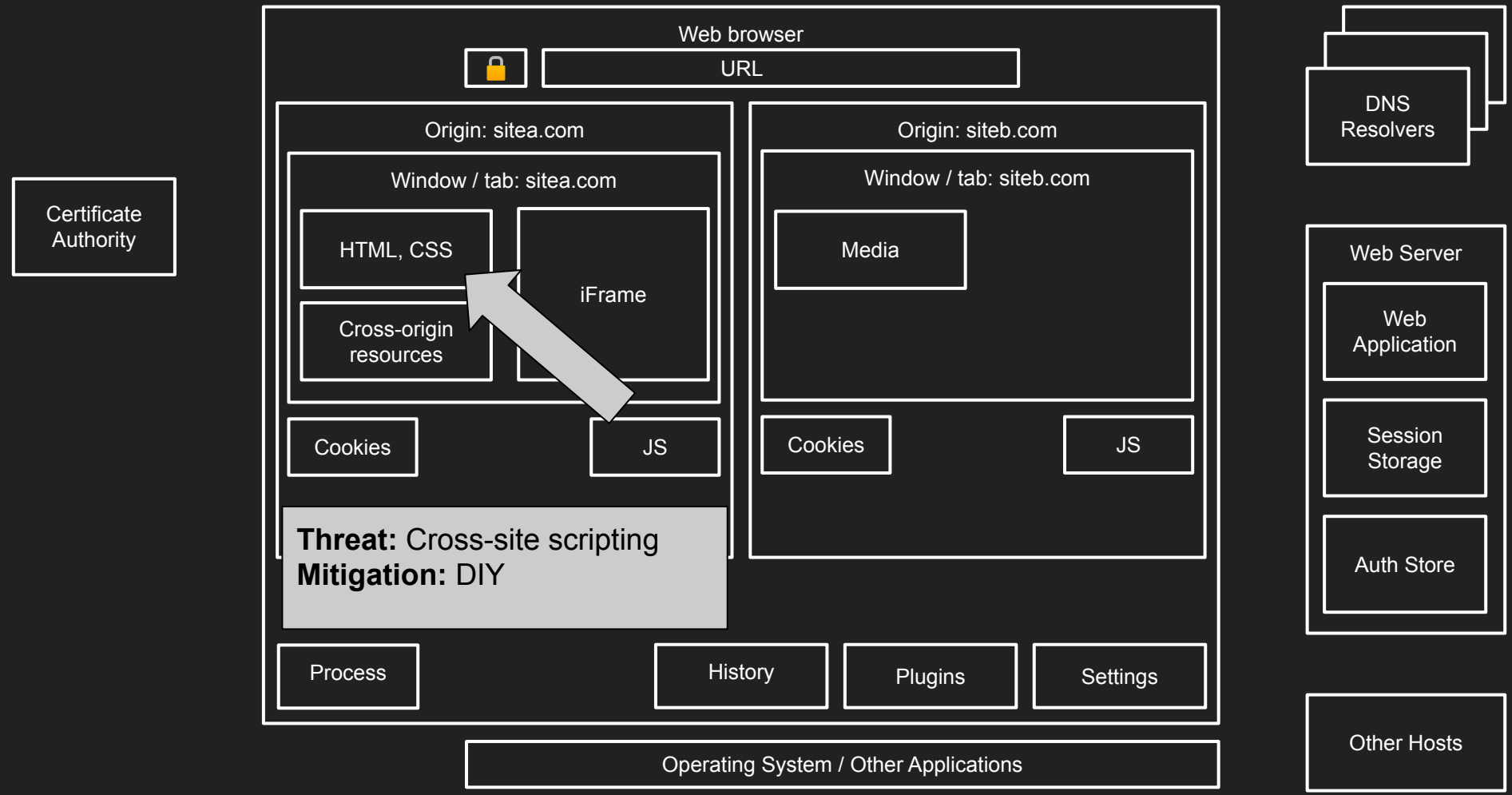
Web 1.0?


Web browser
URL
Origin: sitea.com
Window / tab: sitea.com
HTML, CSS
Cross-origin resources
iFrame
Cookies
JS
Origin: siteb.com
Window / tab: siteb.com
Media
Cookies
JS
Process
History
Plugins
Settings
Operating System / Other Applications
Certificate Authority
DNS Resolvers
Web Server
Web Application
Session Storage
Auth Store
Other Hosts

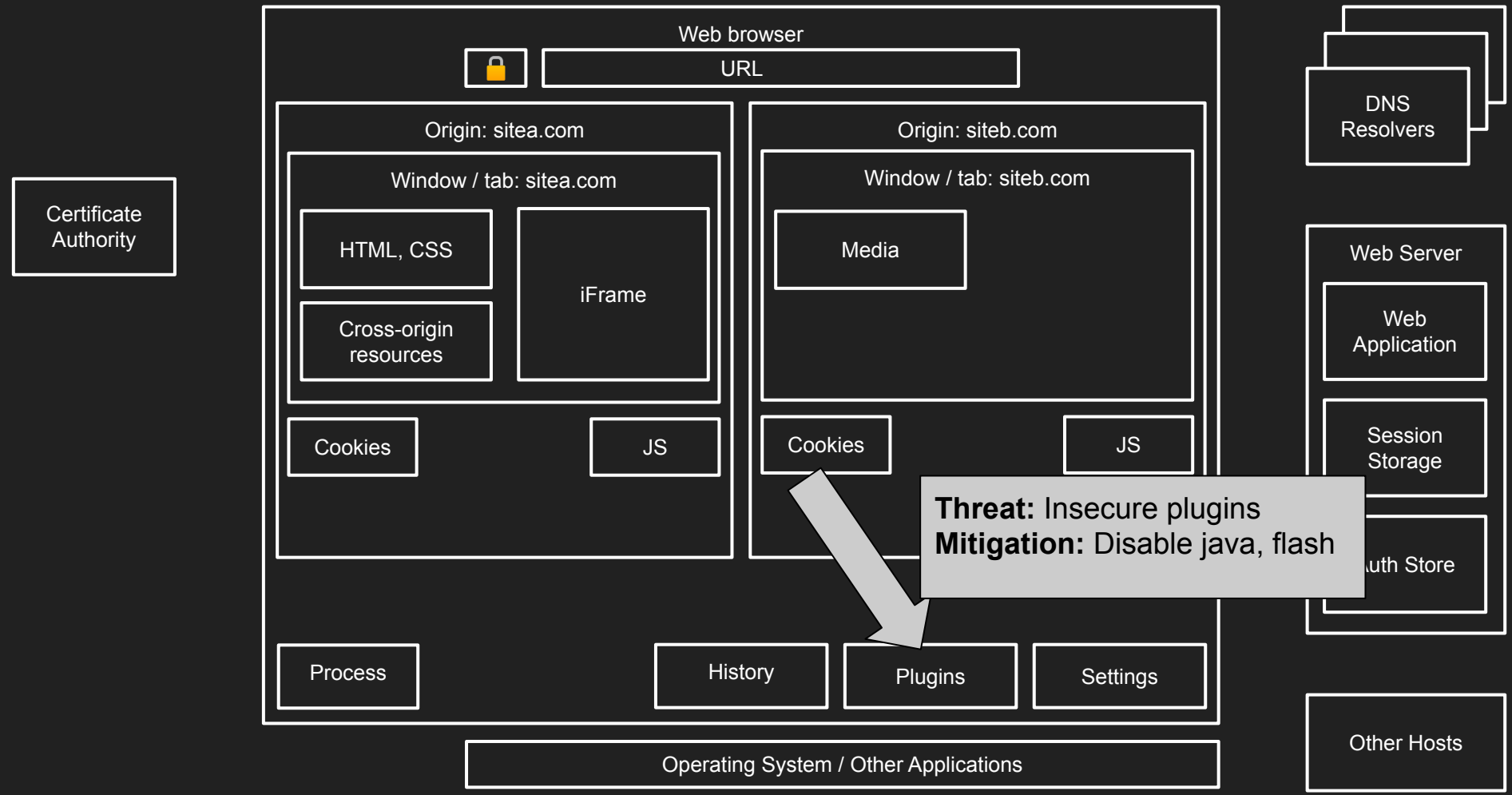

Web browser
URL
Origin: sitea.com
Window / tab: sitea.com
HTML, CSS
iFrame
Cross-origin resources
Cookies
JS
Origin: siteb.com
Window / tab: siteb.c
Media
Cookies
JS
Process
History
Plugins
Settings
Operating System / Other Applications
Certificate Authority
DNS Resolvers
Threat: Snooping
Mitigation: HTTPS
Web Application
Session Storage
Auth Store
Other Hosts


Web browser
URL
Origin: sitea.com
Window / tab: sitea.com
HTML, CSS
Cross-origin resources
iFrame
Origin: siteb.com
Window / tab: siteb.com
Media
Cookies
JS
Threat: Cross-site data access
Mitigation: Same-origin policy
Process
History
Plugins
Settings
Operating System / Other Applications
Certificate Authority
DNS Resolvers
Web Server
Web Application
Session Storage
Auth Store
Other Hosts


Web browser
URL
Origin: sitea.com
Window / tab: sitea.com
HTML, CSS
Cross-origin resources
iFrame
Cookies
JS
Origin: siteb.com
Window / tab: siteb.com
Media
Threat: Image parsing bugs
Mitigation: Hotfixes?
Process
Plugins
Settings
Operating System / Other Applications
Certificate Authority
DNS Resolvers
Web Server
Web Application
Session Storage
Auth Store
Other Hosts


Web browser
URL
Origin: sitea.com
Window / tab: sitea.com
HTML, CSS
iFrame
Cross-origin resources
Cookies
JS
Origin: siteb.com
Window / tab: siteb.com
Media
Cookies
JS
Threat: Cross-site scripting
Mitigation: DIY
Process
History
Plugins
Settings
Operating System / Other Applications
Certificate Authority
DNS Resolvers
Web Server
Web Application
Session Storage
Auth Store
Other Hosts


Web browser
URL
Origin: sitea.com
Window / tab: sitea.com
HTML, CSS
iFrame
Cross-origin resources
Cookies
JS
Origin: siteb.com
Window / tab: siteb.com
Media
Cookies
JS
Threat: Cookies stolen by JS
Mitigation: HTTPOnly flag
Process
History
Plugins
Settings
Operating System / Other Applications
Certificate Authority
DNS Resolvers
Web Server
Web Application
Session Storage
Auth Store
Other Hosts

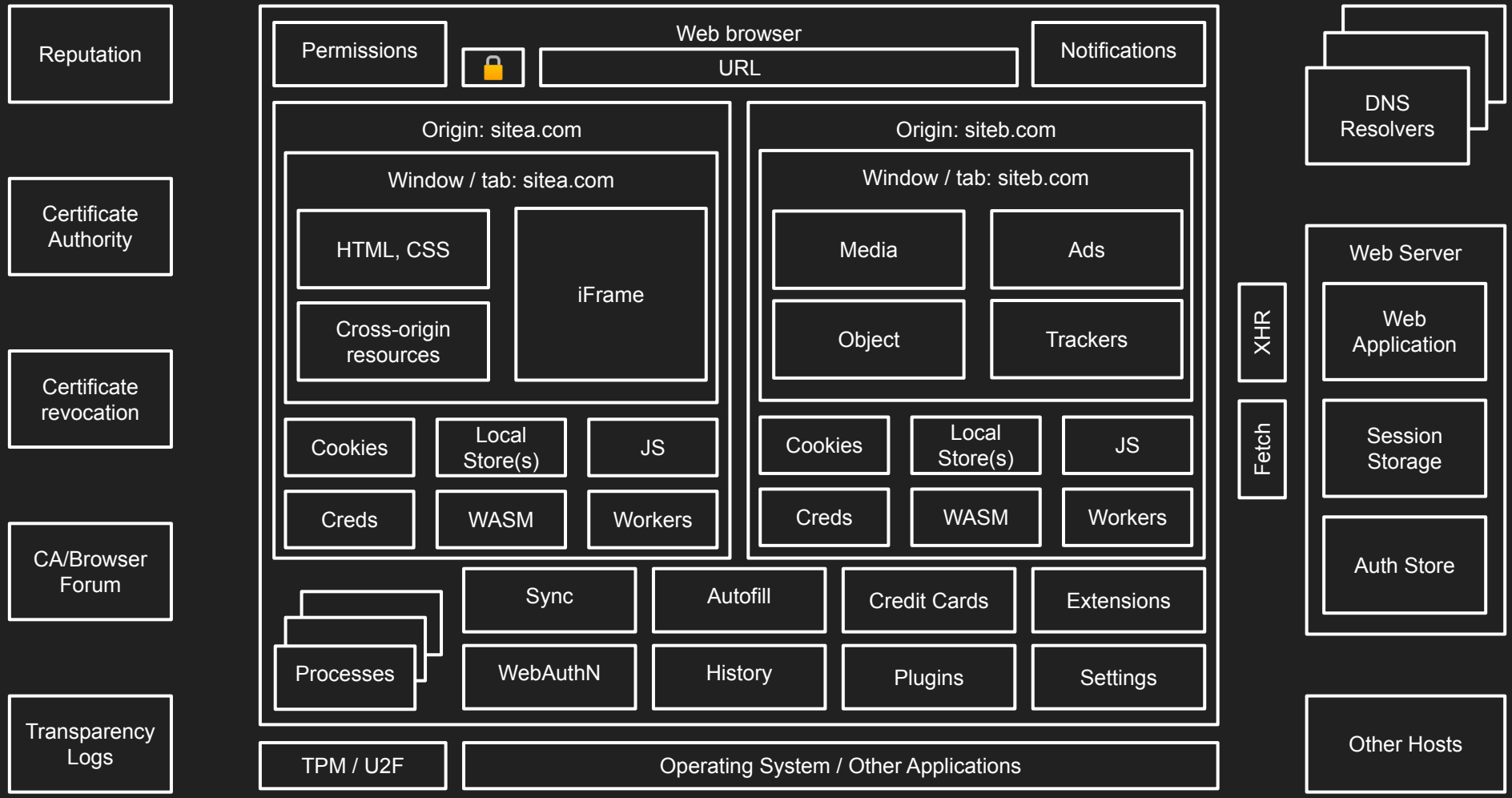

Web browser
URL
Origin: sitea.com
Window / tab: sitea.com
HTML, CSS
iFrame
Cross-origin resources
Cookies
JS
Origin: siteb.com
Window / tab: siteb.com
Media
Cookies
JS
Certificate Authority
DNS Resolvers
Web Server
Web Application
Session Storage
uth Store
Threat: Insecure plugins
Mitigation: Disable java, flash
Process
History
Plugins
Settings
Operating System / Other Applications
Other Hosts

It’s up to you

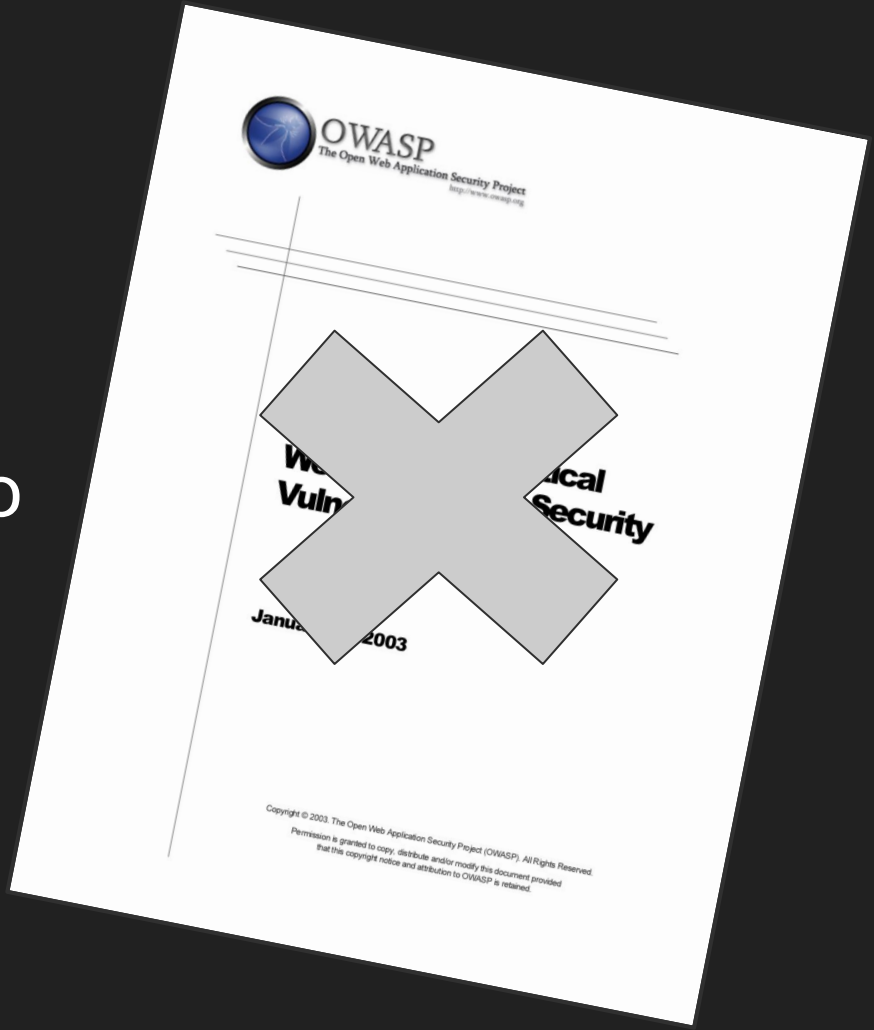

OWASP
The Open Web Application Security Project
The Ten Most Critical Web Application Security Vulnerabilities
January 13, 2003
Copyright © 2003. The Open Web Application Security Project (OWASP). All Rights Reserved.
Permission is granted to copy, distribute and/or modify this document provided that this copyright notice and attribution to OWASP is retained.

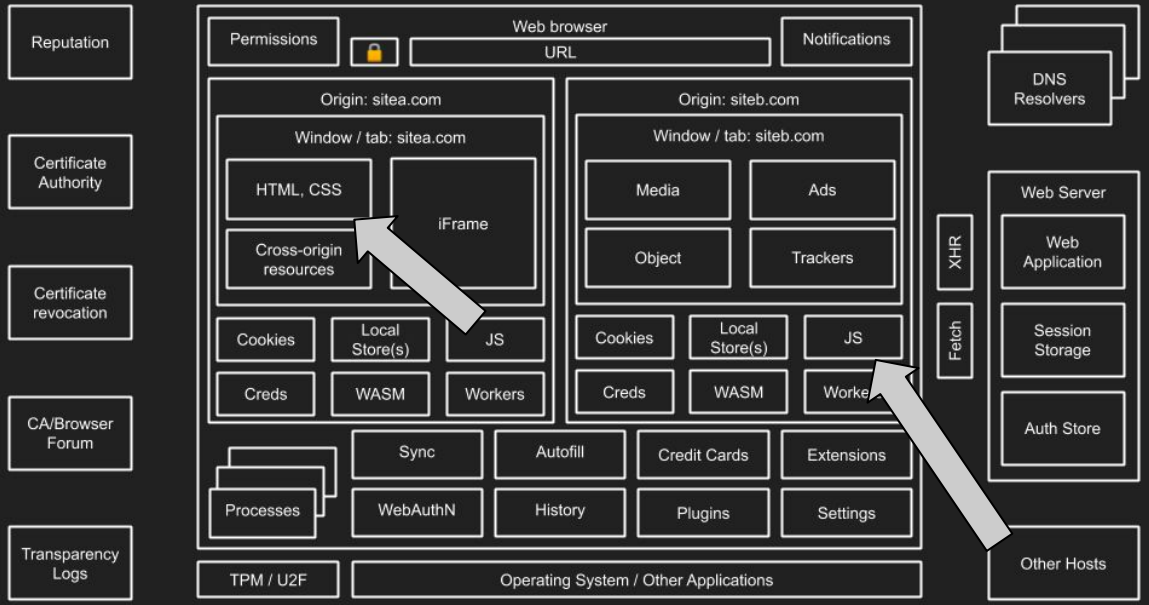
Time passes...

Fast forward to 2021


Reputation
Certificate Authority
Certificate revocation
CA/Browser Forum
Transparency Logs
Permissions
Web browser
URL
Notifications
Origin: sitea.com
Window / tab: sitea.com
HTML, CSS
iFrame
Cross-origin resources
Cookies
Local Store(s)
JS
Creds
WASM
Workers
Origin: siteb.com
Window / tab: siteb.com
Media
Ads
Object
Trackers
Cookies
Local Store(s)
JS
Creds
WASM
Workers
XHR
Fetch
DNS Resolvers
Web Server
Web Application
Session Storage
Auth Store
Processes
Sync
Autofill
Credit Cards
Extensions
WebAuthN
History
Plugins
Settings
TPM / U2F
Operating System / Other Applications
Other Hosts

What can your browser do to stamp out these issues?





XSS

Content Security Policy

- Whitelist of trusted sources
- Strict CSP (nonce-based)

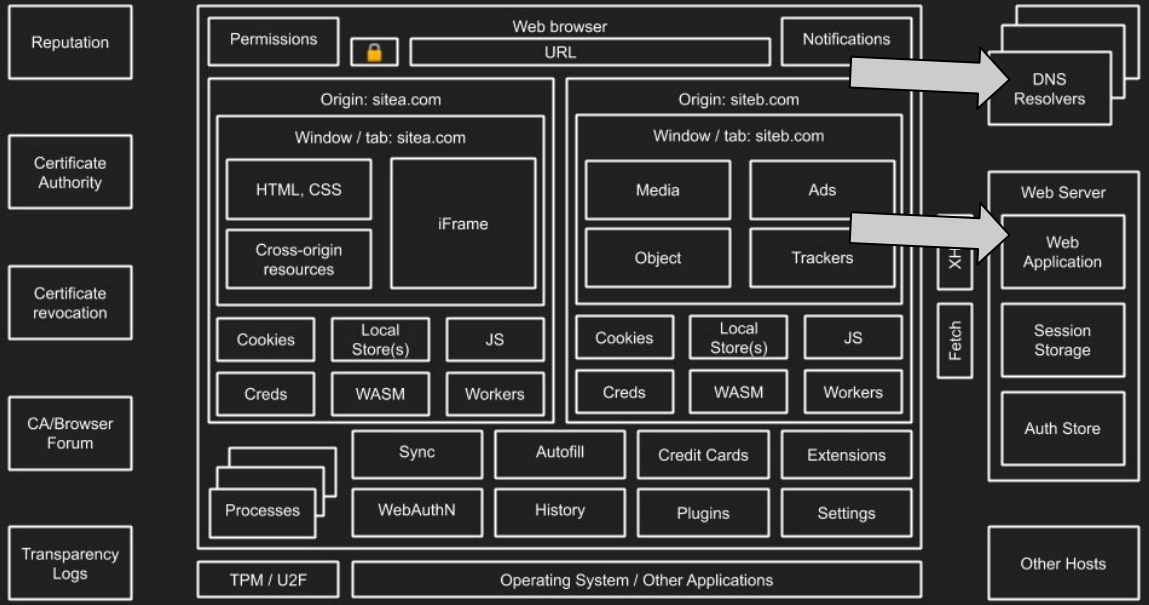
Trusted types:

- Javascript knows which strings are “safe”
- Defence against DOM-XSS

MIME sniffing

Sub-resource integrity

https://security.googleblog.com/2016/09/reshaping-web-defenses-with-strict.html
https://csp.withgoogle.com/docs/index.html
https://web.dev/trusted-types/
https://blog.chromium.org/2020/04/chrome-83-beta-cross-site-scripting.html
https://web.dev/trusted-types/
https://blog.mozilla.org/security/2016/08/26/mitigating-mime-confusion-attacks-in-firefox/
https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity



Encryption

SSL / TLS

- Remove support for legacy TLS, ciphers and certificates

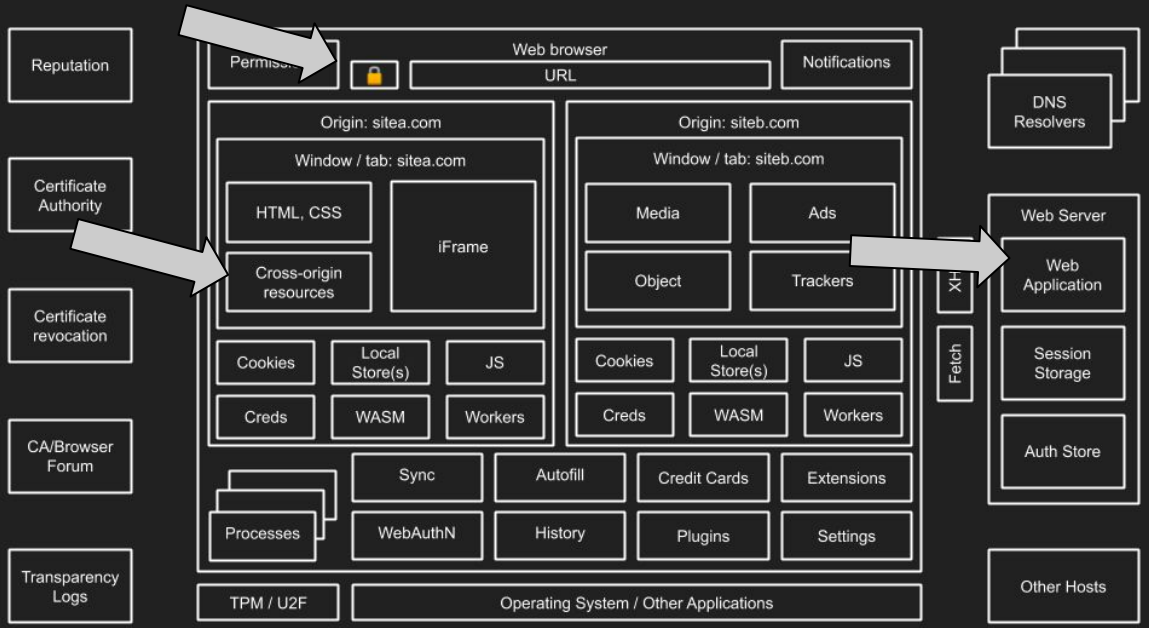
Strict Transport Security

- Enforce HTTPS with

Encrypt the initial connection

- DNS over HTTPS (DoH)
- Encrypted SNI

https://blog.chromium.org/2020/05/a-safer-and-more-private-browsing-DoH.html
https://security.googleblog.com/2019/06/google-public-dns-over-https-doh.html
https://security.googleblog.com/2019/10/chrome-ui-for-deprecating-legacy-tls.html
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
https://security.googleblog.com/2018/10/modernizing-transport-security.html
https://security.googleblog.com/2016/11/sha-1-certificates-in-chrome.html
https://blog.mozilla.org/security/2018/10/18/encrypted-sni-comes-to-firefox-nightly/



Is the site “secure”?

Security indicators (i.e. padlock)

- Improve usability

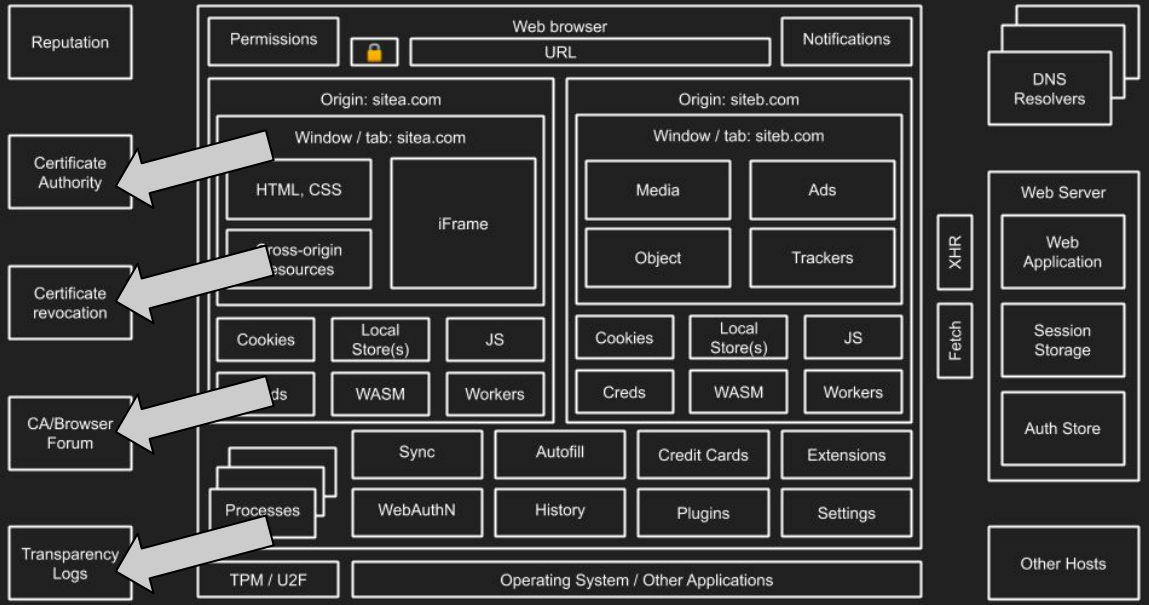
Mixed content blocking

- Block resources, forms, frames over HTTP

Passwords and credit cards

- Only allowed over HTTPS

https://blog.mozilla.org/security/2019/10/15/improved-security-and-privacy-indicators-in-firefox-70/
https://blog.mozilla.org/security/2015/11/03/updated-firefox-security-indicators-2/
https://blog.chromium.org/2019/10/no-more-mixed-messages-about-https.html
https://security.googleblog.com/2020/02/protecting-users-from-insecure_6.html
https://security.googleblog.com/2017/04/next-steps-toward-more-connection.html



Certificate Ecosystem

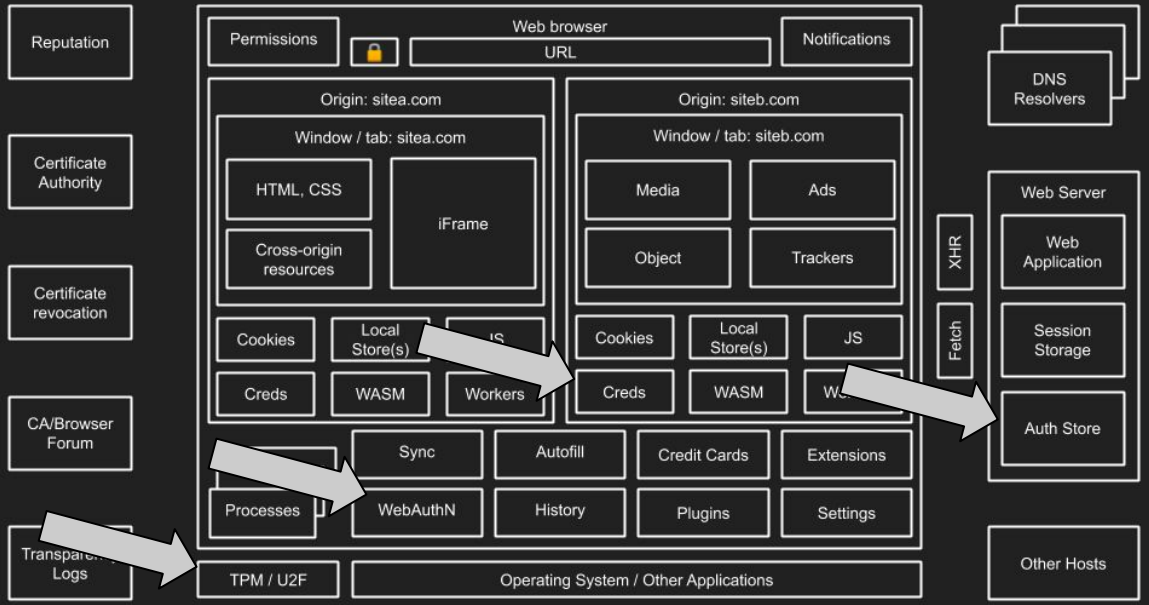
Enforcing standards on certificate authorities

- CA / Browser Forum
- Common CA Database
- Distrusting bad CA's
- Certificate transparency logs

Handling revocation

- Reduce certificate lifetime to 398 days
- CRLite
- OCSP Stapling

https://cabforum.org/
https://blog.mozilla.org/security/2019/04/15/common-ca-database-ccadb/
https://security.googleblog.com/2020/03/how-google-does-certificate-lifecycle.html
https://security.googleblog.com/2017/01/security-through-transparency.html
https://security.googleblog.com/2018/03/distrust-of-symantec-pki-immediate.html
https://security.googleblog.com/2017/07/final-removal-of-trust-in-wosign-and.html
https://blog.mozilla.org/security/2020/07/09/reducing-tls-certificate-lifespans-to-398-days/
https://blog.mozilla.org/security/2020/01/09/crlite-part-1-all-web-pki-revocations-compressed/
https://blog.mozilla.org/security/2013/07/29/ocsp-stapling-in-firefox/



Authentication

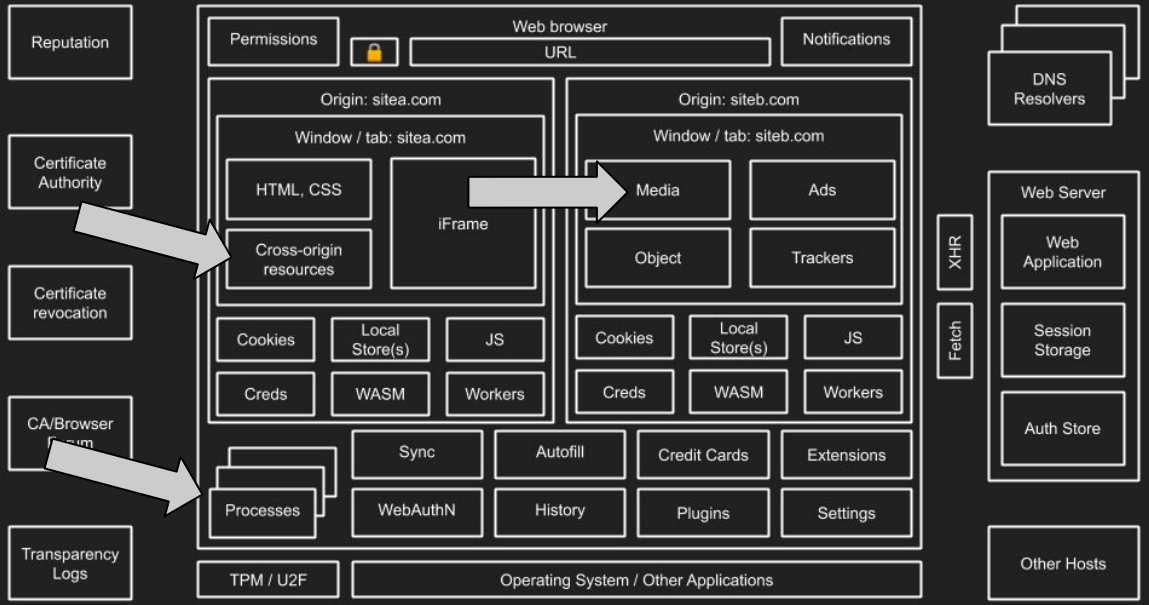
Passwords

- Alert on phishing sites
- Password checkup
- Well-known URL for changing passwords

WebAuthN

- U2F, FIDO
- Credential Management API

https://security.googleblog.com/2015/04/protect-your-google-account-with.html
https://security.googleblog.com/2019/02/protect-your-accounts-from-data.html
https://w3c.github.io/webappsec-change-password-url/
https://webauthn.io/
https://developer.mozilla.org/en-US/docs/Web/API/Web_Authentication_API
https://w3c.github.io/webauthn/
https://security.googleblog.com/2019/11/using-built-in-fido-authenticator-on.html
https://developer.mozilla.org/en-US/docs/Web/API/Credential_Management_API



https://web.dev/same-site-same-origin/
https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe#attr-sandbox
https://www.chromestatus.com/feature/5706745674465280
https://web.dev/why-coop-coep/
https://www.youtube.com/watch?v=D5DLVo_TIEA&feature=youtu.be
https://w3c.github.io/webappsec-permissions-policy/
https://w3c.github.io/webappsec-permissions-policy/document-policy.html
https://www.chromestatus.com/feature/5683766104162304
https://security.googleblog.com/2019/10/improving-site-isolation-for-stronger.html
https://github.com/privacycg/storage-partitioning

Isolating origins

iFrames
- Sandboxing iframes
- Preventing downloads

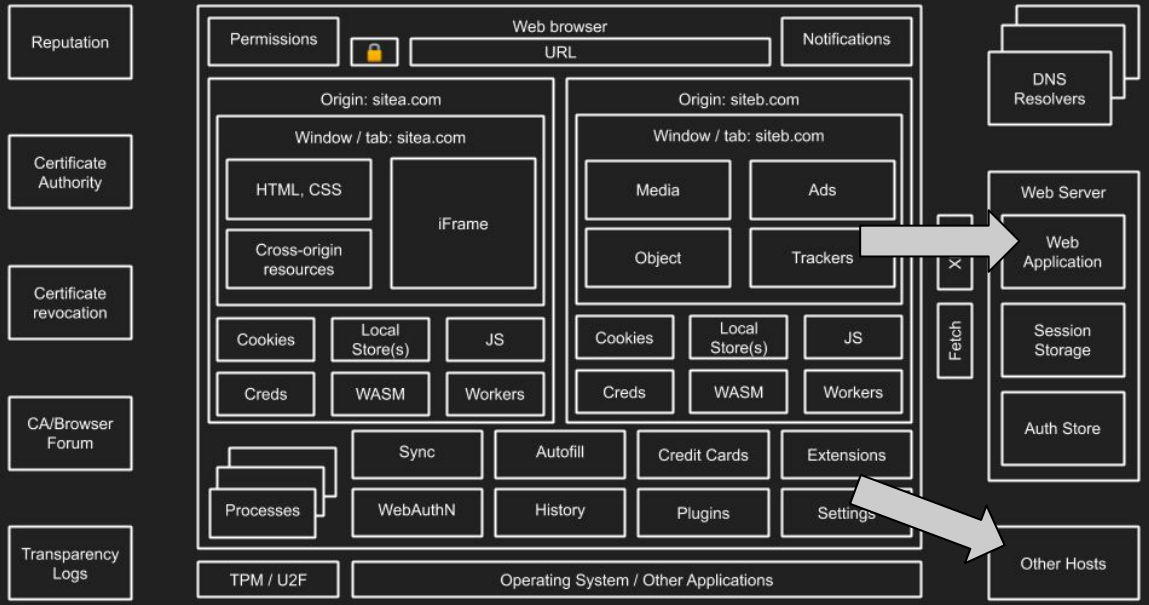
Cross-origin restrictions
- Cross-origin embedder policy
- Cross-origin resource policy

Restrict what documents can do
- Documents & Permissions Policy
- Origin Isolation

Site isolation

Storage partitioning

Network partitioning



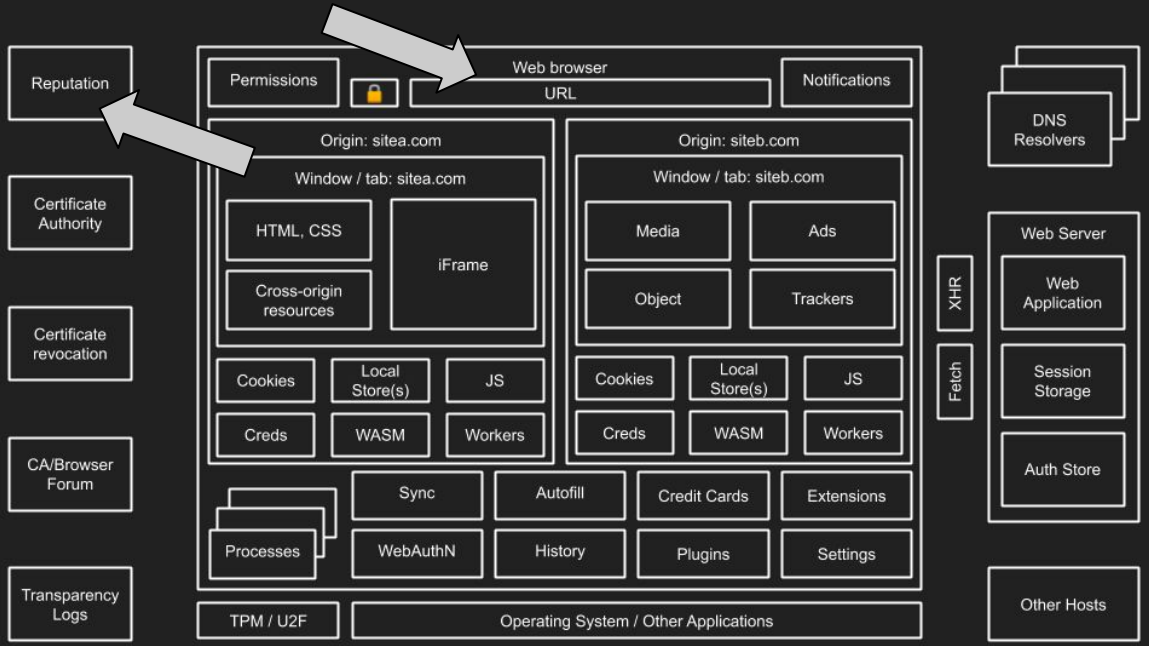
Protocol changes

HTTP protocol
- HTTP/2 and SPDY
- HTTP/3 and QUIC

Removing old protocols
- FTP
- Gopher

Disable dangerous ports

https://blog.chromium.org/2020/10/chrome-is-deploying-http3-and-ietf-quic.html
https://developers.google.com/web/fundamentals/performance/http2
https://www.chromestatus.com/features/6246151319715840
https://developer.mozilla.org/en-US/docs/Mozilla/Firefox/Releases/4#Gopher_support_removed
https://groups.google.com/a/chromium.org/g/blink-dev/c/4Btz5xQ-gXc/m/iPDxYSEgAgAJ



Safely browsing

Checking for dangerous URLs or downloads

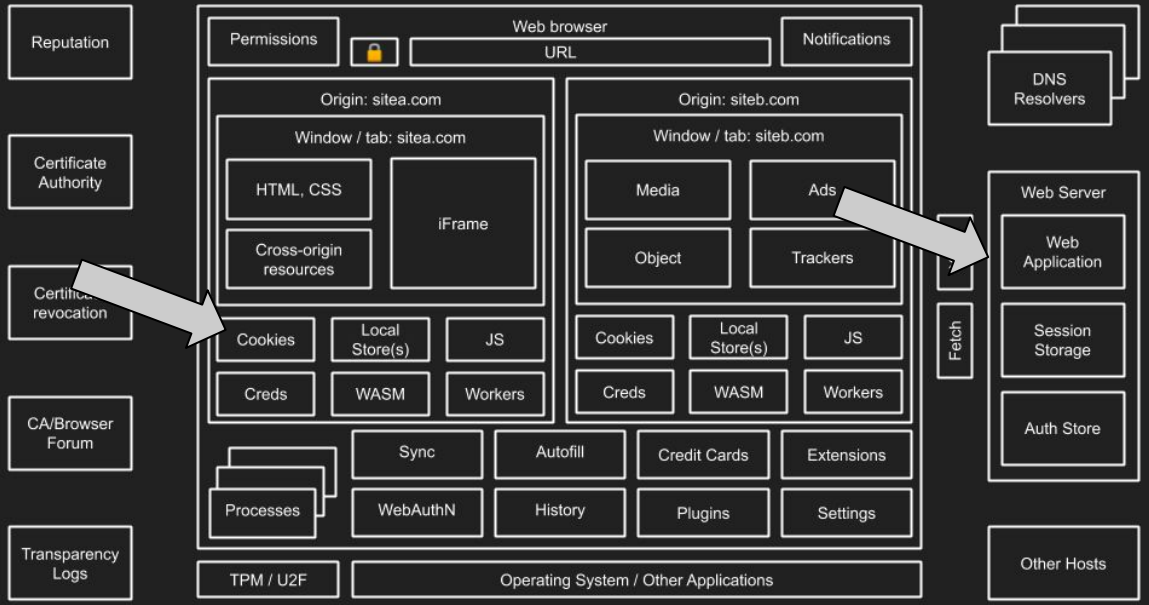
- Safe Browsing
- SmartScreen

Displaying urls safely

- Spoofed URLs
- Internationalised domain homograph attacks

Data urls

https://security.googleblog.com/2020/05/enhanced-safe-browsing-protection-now.html
https://security.googleblog.com/2019/06/new-chrome-protections-from-deception.html
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview
https://blog.chromium.org/2020/08/helping-people-spot-spoofs-url.html
https://en.wikipedia.org/wiki/IDN_homograph_attack#Client-side_mitigation
https://nakedsecurity.sophos.com/2019/02/04/chrome-can-now-detect-lookalike-urls/
https://blog.mozilla.org/security/2017/11/27/blocking-top-level-navigations-data-urls-firefox-59/



Cookies and CSRF

SameSite cookies

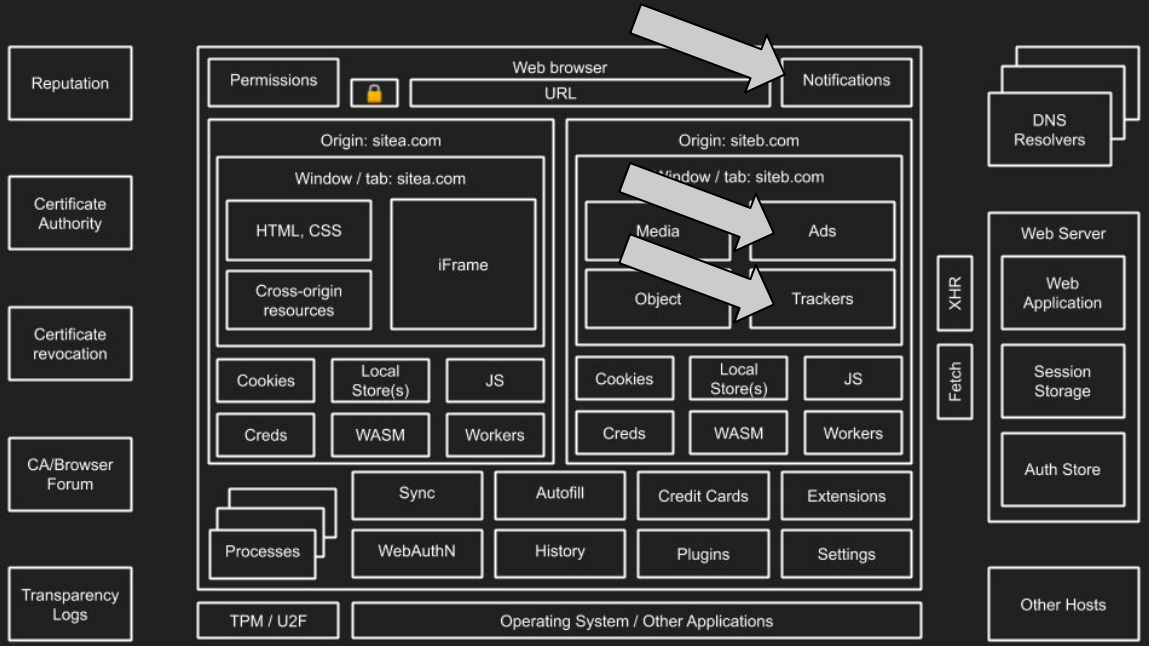
- Preventing CSRF
- Change default cookie behaviour to reduce tracking

Cookie Store API

- Non-blocking access to cookies

First-party sets and SameParty cookies

https://web.dev/samesite-cookies-explained/
https://blog.chromium.org/2019/10/developers-get-ready-for-new.html
https://www.chromestatus.com/feature/5658847691669504
https://groups.google.com/a/chromium.org/g/blink-dev/c/XkWbQKrBzMg/m/dIQckPbZAAAJ



Tracking and abuse

Tracking protection

- Reducing 3rd party tracking via cookies
- Updates to incognito mode
- Private click measurement

Focus on other “ever-cookies”

- HSTS abuse

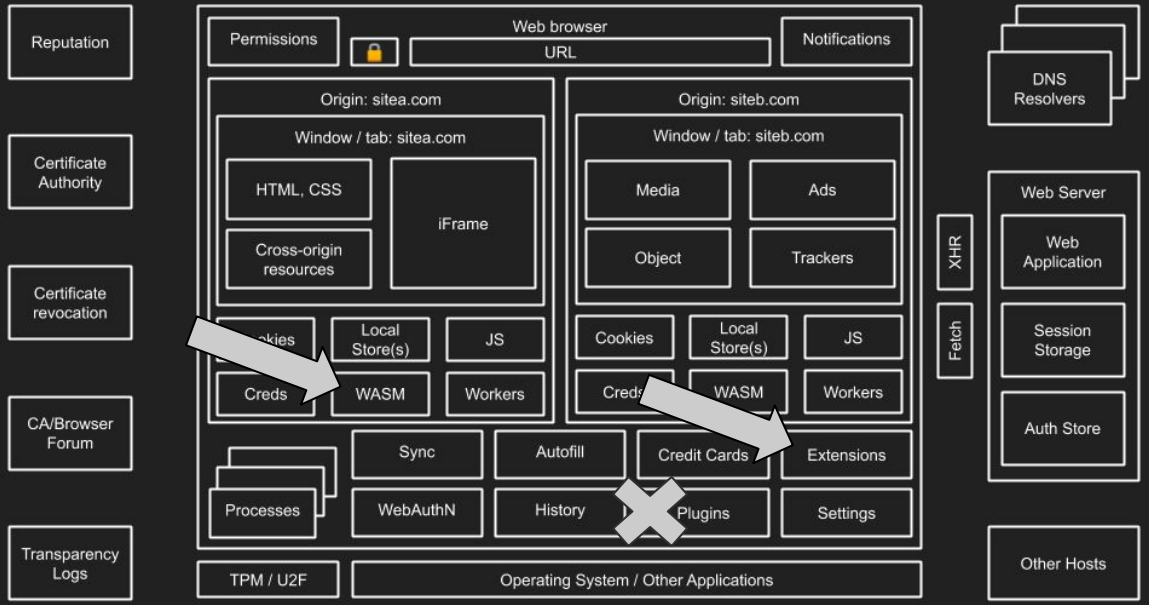
XS-Leaks

Abusive notifications

Resource-heavy advertisements

Referrer policy

https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/
https://blog.mozilla.org/security/2020/01/07/firefox-72-fingerprinting/
https://blog.chromium.org/2020/10/progress-on-privacy-sandbox-and.html
https://blog.google/products/chrome/more-intuitive-privacy-and-security-controls-chrome/
https://webkit.org/blog/8146/protecting-against-hsts-abuse/
https://xsleaks.dev/
https://blog.chromium.org/2020/05/protecting-chrome-users-from-abusive.html
https://blog.chromium.org/2020/05/resource-heavy-ads-in-chrome.html
https://blog.mozilla.org/security/2018/10/02/supporting-referrer-policy-for-css-in-firefox-64/



Plugins and extensions

Removing unsafe plugins

- No more Java
- No more Flash
- No more NPAPI

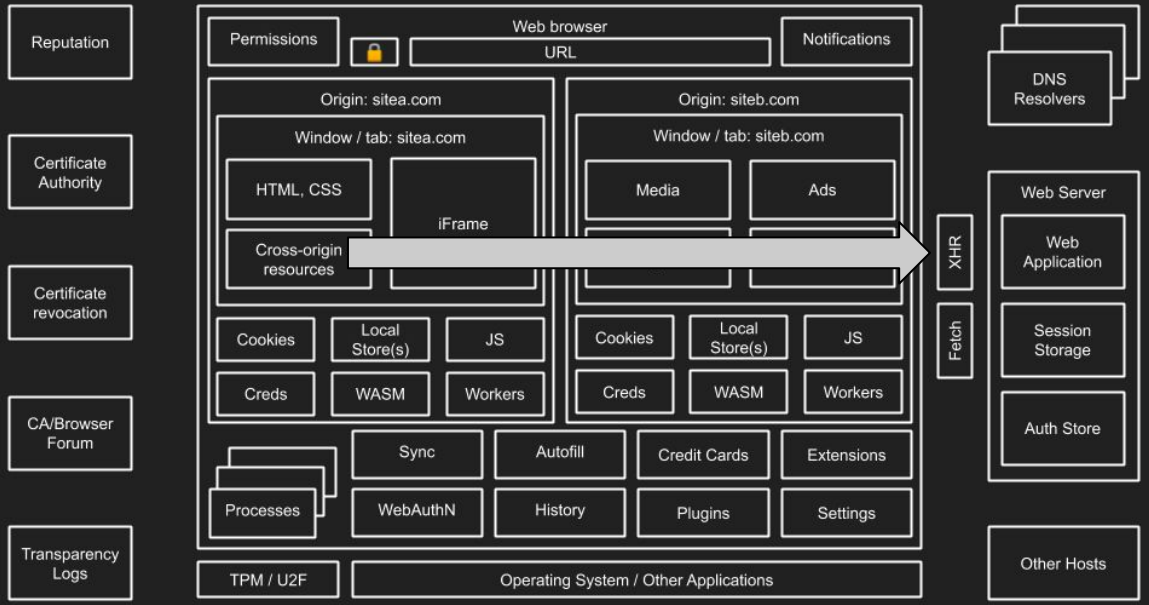
Extensions

- Spam and malicious extensions
- Reducing permissions

Web Assembly

- Sandboxed execution

https://www.blog.google/products/chrome/saying-goodbye-flash-chrome/
https://blog.chromium.org/2014/11/the-final-countdown-for-npapi.html
https://blog.chromium.org/2020/04/keeping-spam-off-chrome-web-store.html
https://security.googleblog.com/2019/06/improving-security-and-privacy-for.html
https://security.googleblog.com/2018/10/trustworthy-chrome-extensions-by-default.html
https://webassembly.org/



Fetching Data

Three ways to request data

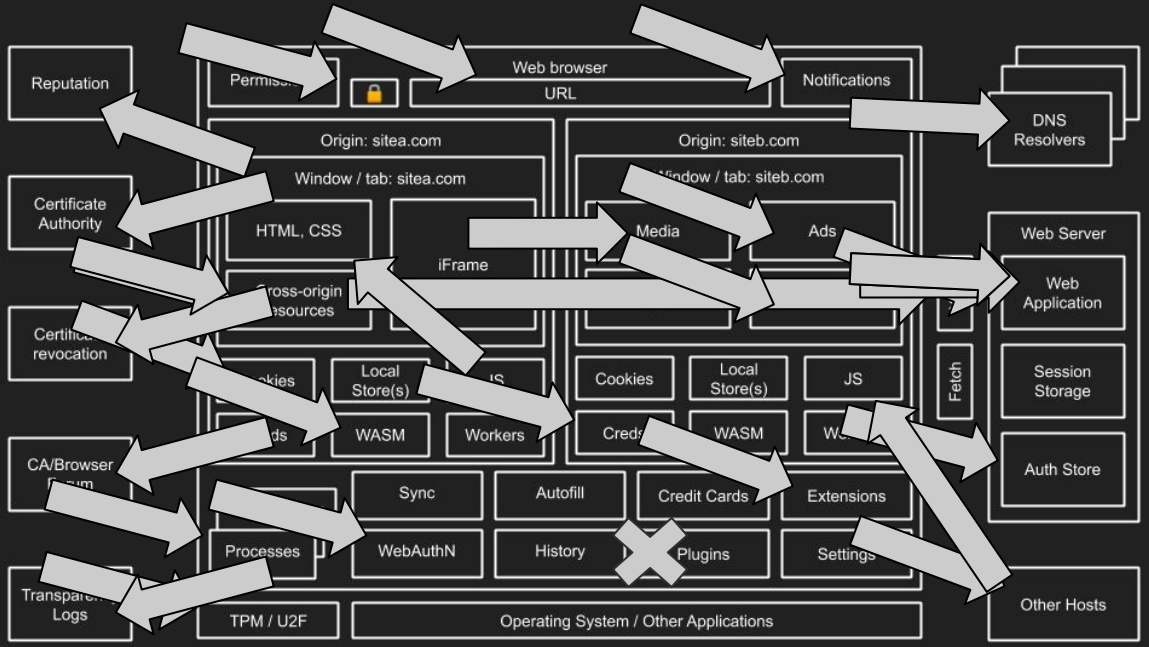
- Regular HTTP
- XMLHttpRequest
- Fetch

SOP limits reading results

- Cross-origin resource sharing allows the server to opt-in

Fetch metadata headers let server restrict where their content is used

https://developer.mozilla.org/en-US/docs/Web/API/Fetch_API
https://web.dev/cross-origin-resource-sharing/
https://web.dev/fetch-metadata/
https://w3c.github.io/webappsec-fetch-metadata/



Summary

Every new web browser feature ~~complicates~~ improves the security model.

Browsers are the operating system of the web.

Browser vendors are working hard to improve the security posture of the web.

How can we make sure we're doing everything we can in our own applications?

Threat modelling all of this is hard!

References

Chrome

- Chromium Blog
- Google Security Blog
- Adrienne Porter Felt
- Lukas Weichselbaum
- Emily Stark
- Justin Schuh
- Parisa Tabriz
- Mike West

Browser history

- Timeline of web browsers
- The evolution of the web

Edge

- Microsoft Edge Blog
- Eric Lawrence

Firefox

- Mozilla Security Blog
- Anne van Kesteren

Safari

- Webkit Blog
- John Wilander