



Who left open the cookie jar?

A comprehensive evaluation of third-party cookie policies

Gertjan Franken, Tom Van Goethem, Wouter Joosen

August 15th 2018

DistrINet

Third-party policies are highly relevant today

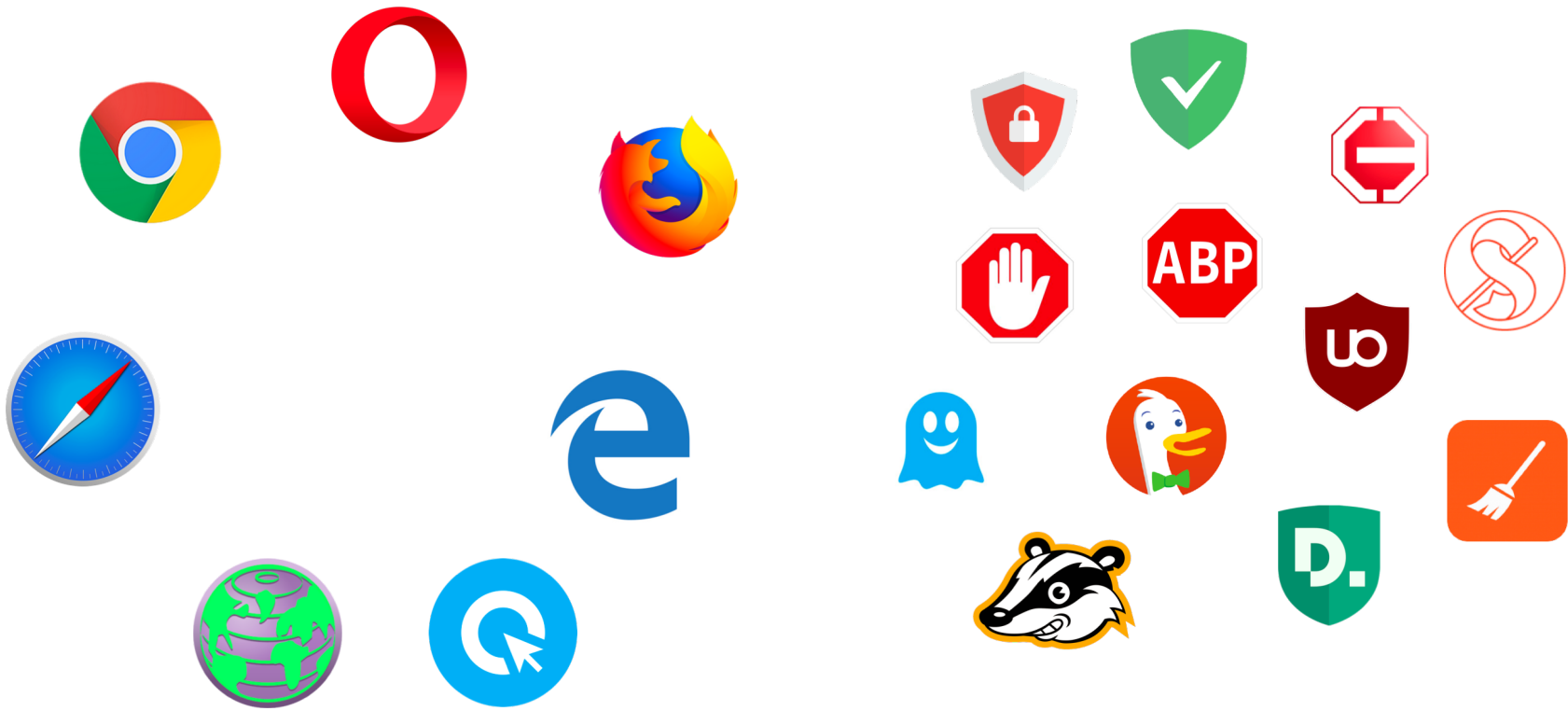
OpenEMR security flaws could have exposed millions of patient records [1]

Over 20 severe bugs were found using only manual methods by a single cybersecurity group.

- › Online tracking study (200,000 users) [2]
 - › 95% of visited pages initiated cross-site request to potential trackers
 - › Of which 78% attempted to transfer potentially identifying data

[1] <https://www.zdnet.com/article/openemr-security-flaws-left-millions-of-patient-records-open-to-attack/>

[2] YU, Z., MACBETH, S., MODI, K., ANDPUJOL, J.M. Tracking the trackers. In *Proceedings of the 25th International Conference on World Wide Web* (Republic and Canton of Geneva, Switzerland, 2016)





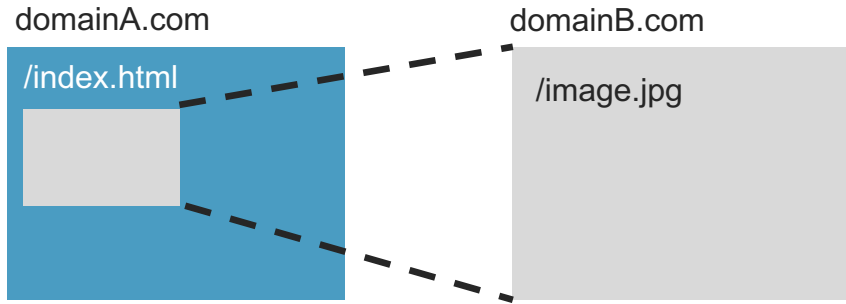
Outline

- › Why you should keep an eye on your cookies
- › The comprehensive evaluation
- › What's wrong with your browser's third-party cookie policies
- › Conclusion



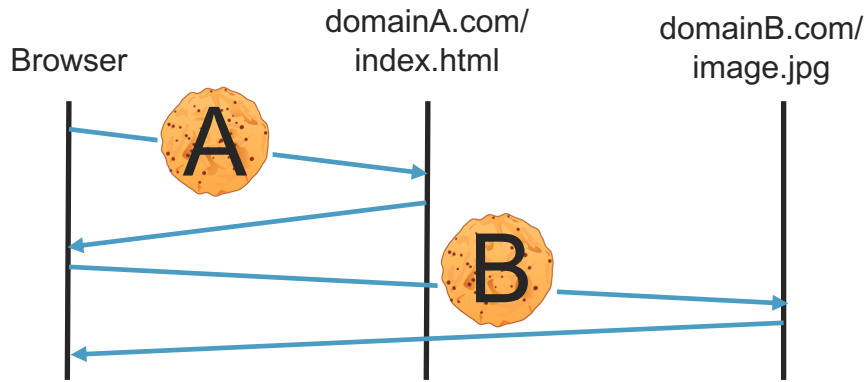
Why you should keep an eye
on your cookies

Web Fundamentals



HTTP cookies [1]

- › Implicit inclusion
- › Authentication / identification
- › Same-Origin Policy



Domain A

Domain B



[1] Barth, A., "HTTP State Management Mechanism", RFC 6265, DOI 10.17487/RFC6265, April 2011.

Exploitation of implicit authentication

Cross-site attacks

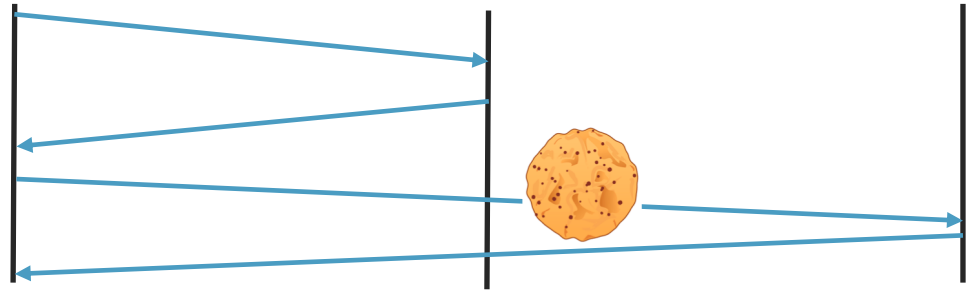
- › CSRF
- › XSSI
- › Cross-site timing attacks



victim

cute-kittens.com

doggo-bank.com



```

```

Exploitation of implicit authentication

Cross-site attacks

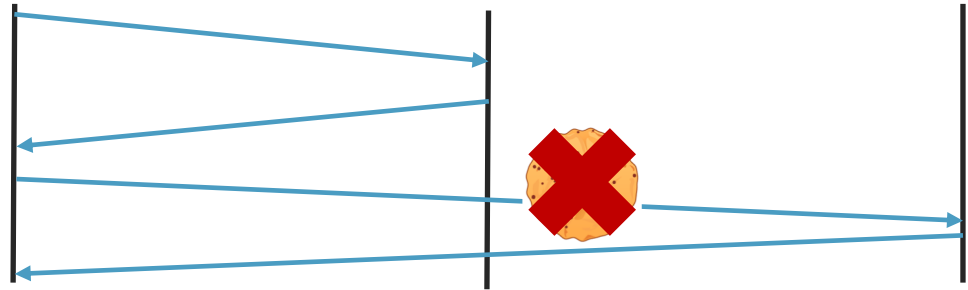


victim

cute-kittens.com

doggo-bank.com

THIRD-PARTY
COOKIE
POLICIES



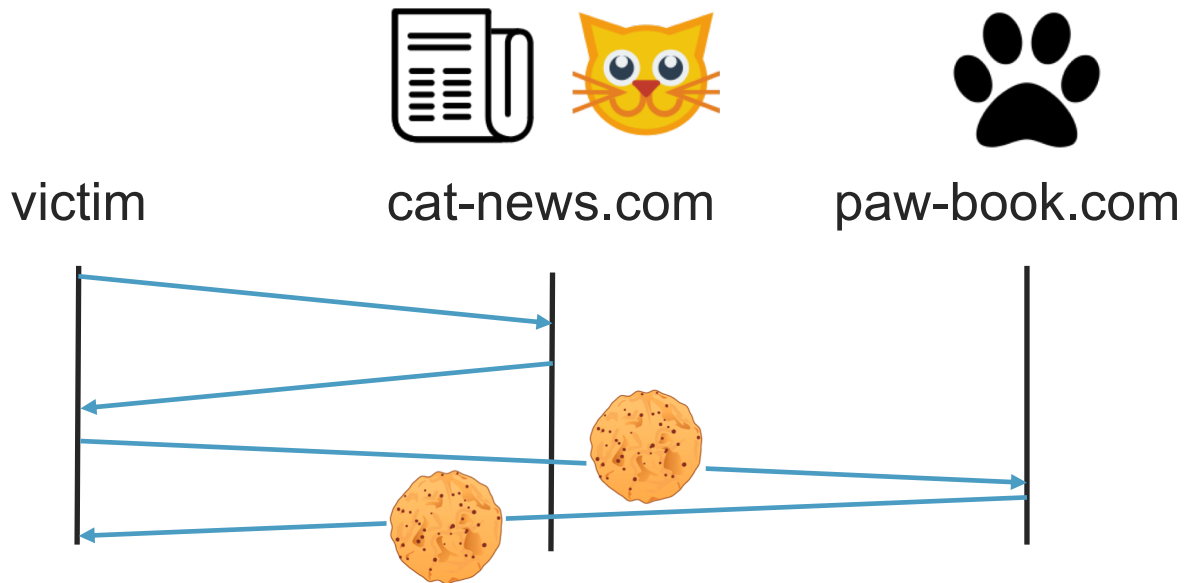
```

```

Exploitation of implicit identification

Tracking

- › Advertising
- › Social media
- › Web analytics



```
<script src="https://paw-book.com/widget.js  
?url=cat-news.com/catnip.html"></script>
```

Exploitation of implicit identification

Tracking

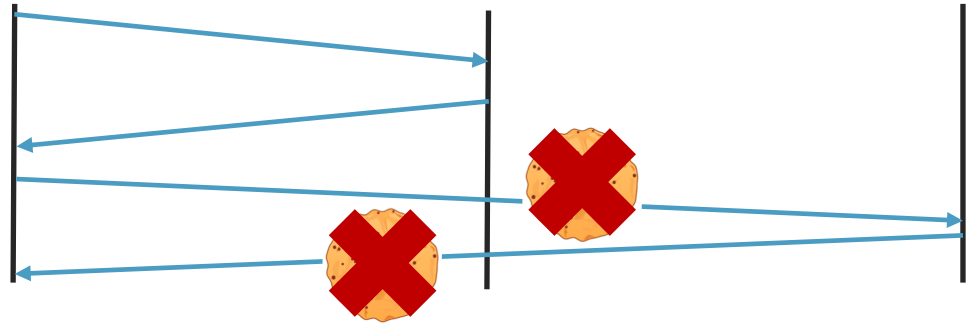


victim

cat-news.com

paw-book.com

THIRD-PARTY
COOKIE
POLICIES



```
<script src="https://paw-book.com/widget.js?url=cat-news.com/catnip.html"></script>
```

Existing third-party cookie policies

- › Built-in browser options

- › Block third-party cookies
- › Firefox Tracking Protection
- › Opera Ad Blocker
- › Safari Intelligent Tracking Prevention

- › Extensions

- › Ad blocking
- › Privacy protection

- › Same-site cookies

Same-site cookie [1]

- › Cookie with extra attribute 'SameSite'
 - ›› SameSite=strict → NO CROSS-SITE REQUESTS!
 - ›› SameSite=lax → exceptions: top-level GET, prerender

[1] West, M., Goodwin, M. Same-site cookies. Internet- Draft draft-ietf-httpbis-cookie-same-site-00, IETF Secretariat, June 2016.

Use of same-site cookies

against cross-site attacks

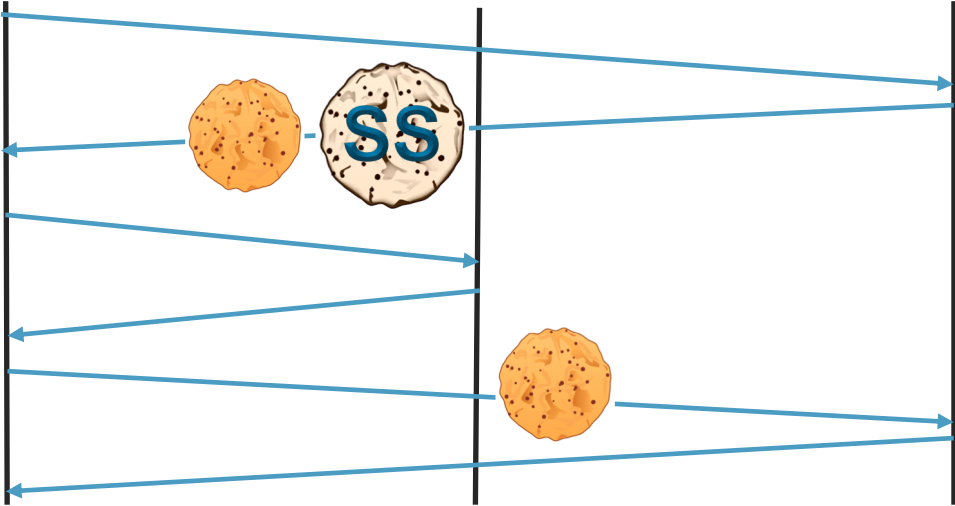


doggo-bank.com

victim

cute-kittens.com

doggo-bank.com



```
Set-Cookie: auth=ekSd2lksq090pQDs; SameSite=strict
```

Why evaluate third-party cookie policies?

- › Browsers are known to exhibit inconsistent behavior
 - › Interference from different standards
 - › Unintended side-effects by code modification
- › Extensions have been actively bypassed in the past [1]

Comprehensive evaluation of effectiveness

[1] <https://blog.bugreplay.com/2016/11/pornhub-bypasses-ad-blockers-with.html>



The comprehensive evaluation

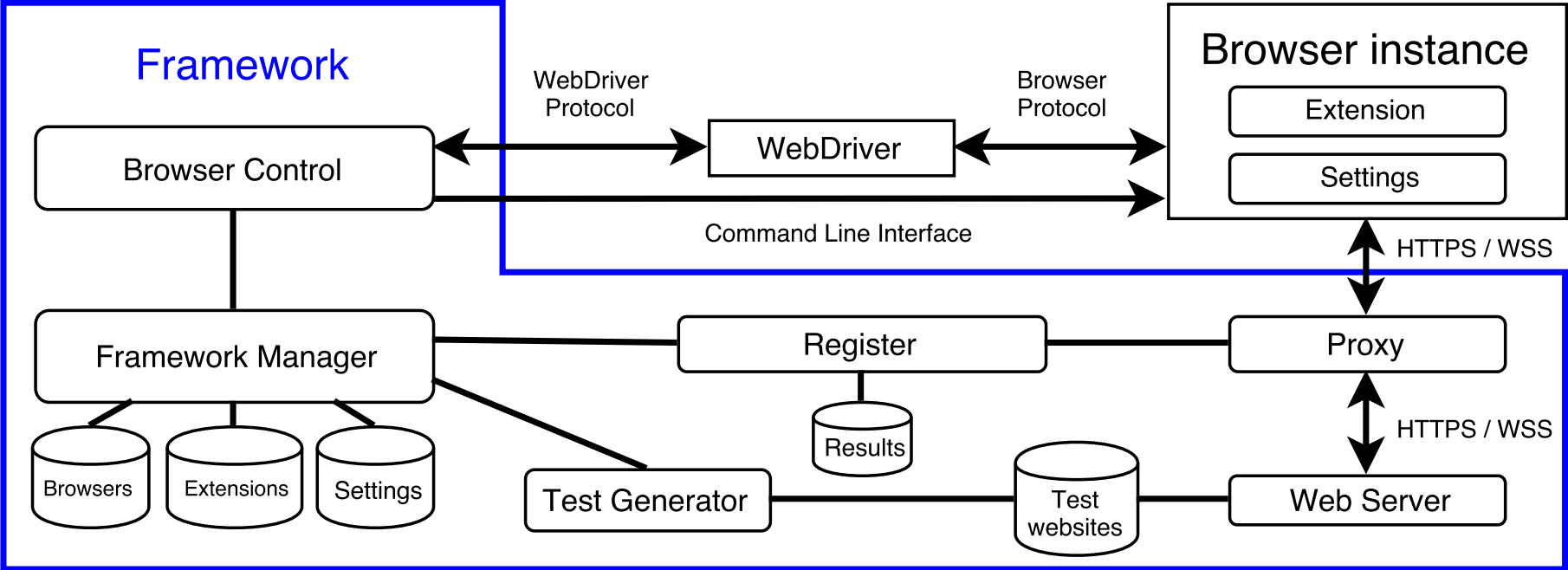
Black box approach

- › No code review!
 - ›› Browsers consist of millions of lines of code
 - ››› Source code not always available
 - ›› Many interesting extensions



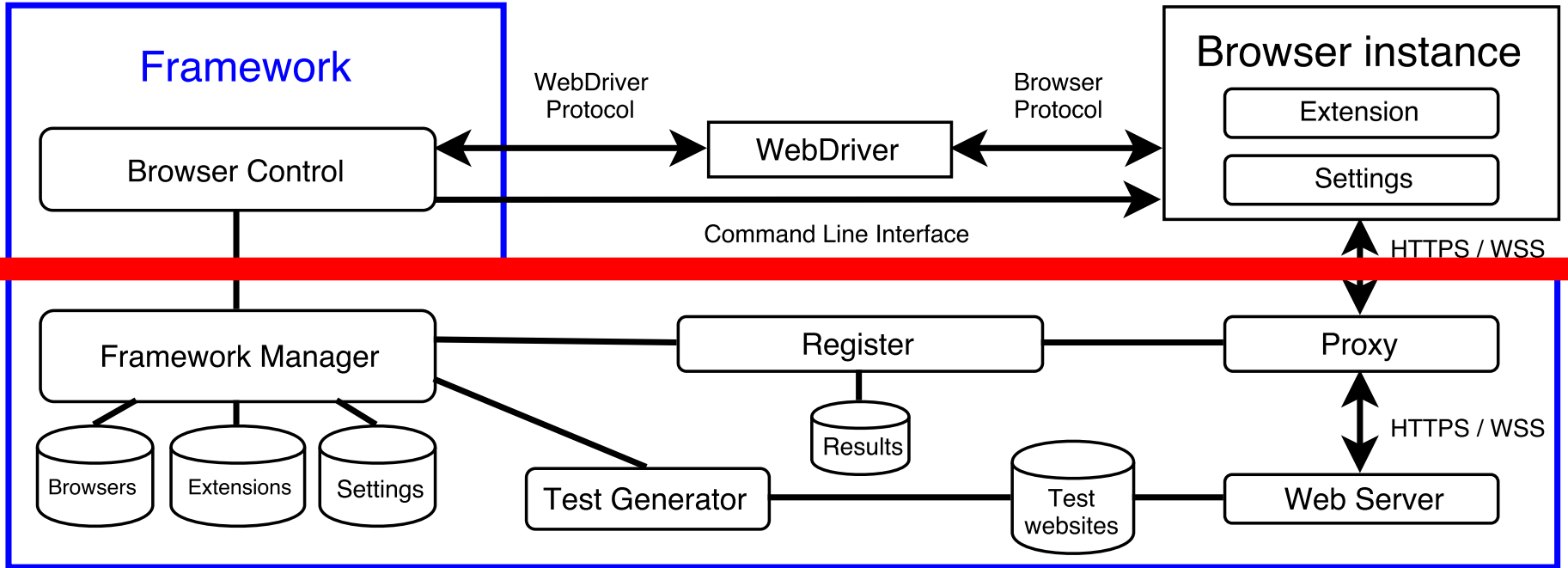
Framework

Design



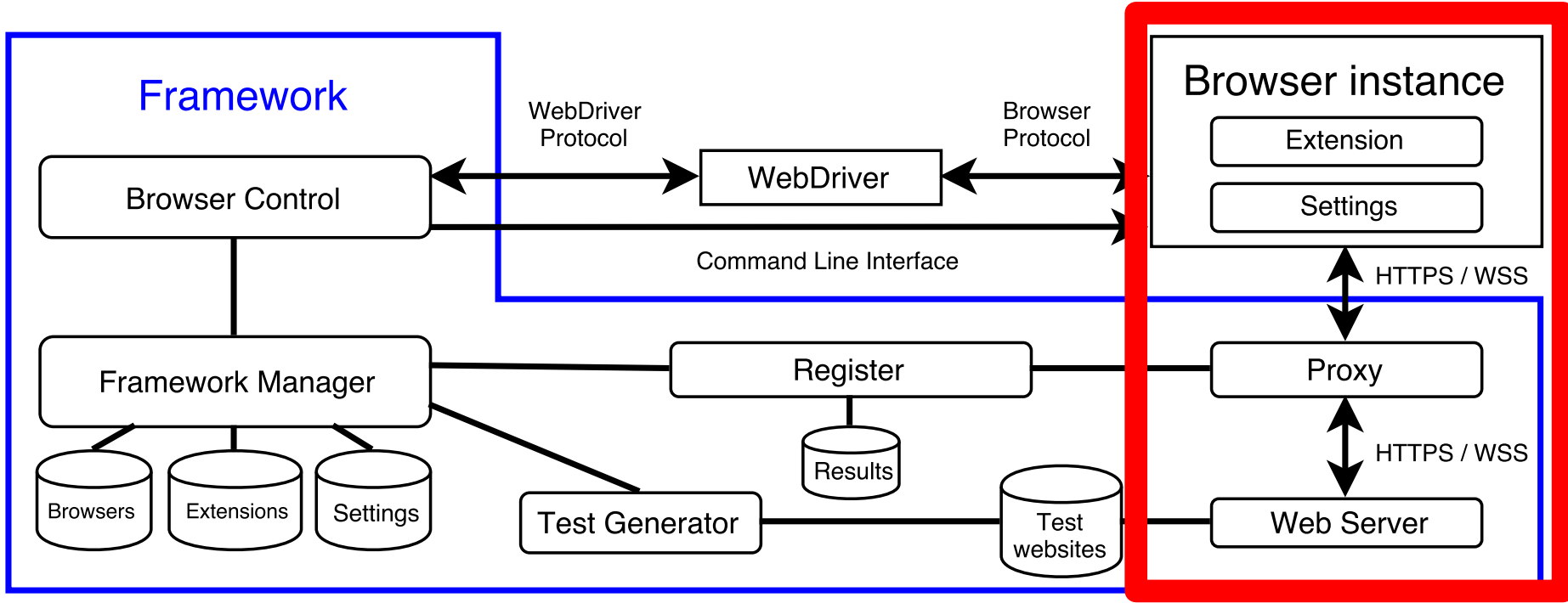
Framework

Design



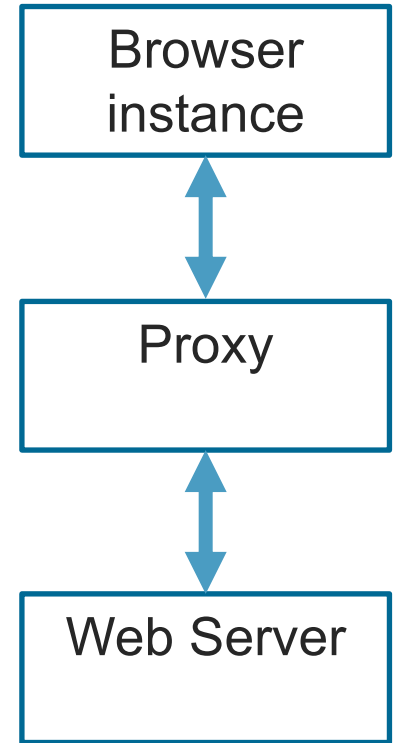
Framework

Design



Inside the framework

- › Browser control
 - › Selenium / Command line interface
- › Web server
 - › Initiate cross-site requests to blacklisted domain
 - › Proxy intercepts all requests



Initiating cross-site requests












- › AppCache API
 - › Caching cross-site pages
- › HTML-tags
 - › `<script>`, ``, `<link>`, etc.
- › Headers
 - › Link, CSP headers
- › Redirects
- › JavaScript
 - › Fetch, EventSource API, etc.
- › PDF JS
 - › `sendForm()`
- › ServiceWorker API

The background is a solid blue color with several large, semi-transparent, light-blue geometric shapes overlaid. These shapes include a large downward-pointing triangle on the left and a large upward-pointing triangle on the right, which together form a diamond-like shape in the center. There are also some curved, abstract shapes in the upper left and right areas.

What's wrong with your browser's
third-party cookie policies

Overview

› Browsers

- › Chrome  
- › Opera  
- › Firefox  
- › Safari 
- › Edge  
- › Tor Browser 
- › Cliqz 

› Extensions

› Ad blocking (31)



› Tracking protection (15)



	AppCache	HTML	Headers	Redirects	PDF JS	JavaScript	SW
Chrome 63	●	●	●	●	●	●	●
- Block third-party cookies	◐	◐	◐	●	●	◐	◐
Opera 51	●	●	●	●	●	●	●
- Block third-party cookies*	◐	◐	◐	●	●	◐	◐
- Ad Blocker	●	●	○	●	○	●	●
Firefox 57	●	●	●	●	○	●	●
- Block third-party cookies	◐	◐	◐	●	○	◐	◐
- Tracking Protection	●	●	●	●	○	●	●
Safari 11	○ [†]	◐	○	●	○	◐	N/A
- No Intelligent Tracking Prevention	● [†]	●	○	●	○	●	N/A
- Block third-party cookies [‡]	● [†]	●	◐	●	○	●	N/A
Edge 40	●	●	◐	●	○	●	N/A
- Block third-party cookies	●	●	◐	●	○	●	N/A
Cliqz 1.17*	◐	●	◐	●	○	◐	◐
- Block third-party cookies	◐	◐	◐	●	○	◐	◐
Tor Browser 7	○	◐	◐	●	○	◐	N/A

●: request with cookies

◐: request without cookies

○: no request

* Secure cookies were omitted in all requests.

[†] Safari does not permit cross-domain caching over https (only over http). 25

[‡] Safari 10.1.2

	AppCache	HTML	Headers	Redirects	PDF JS	JavaScript	SW
Chrome 63	●	●	●	●	●	●	●
- Block third-party cookies	☹	☹	☹	●	●	☹	☹
Opera 51	●	●	●	●	●	●	●
- Block third-party cookies*	☹	☹	☹	●	●	☹	☹
- Ad Blocker	●	●	○	●	○	●	●
Firefox 57	●	●	●	●	○	●	●
- Block third-party cookies	☹	☹	☹	●	○	☹	☹
- Tracking Protection	●	●	●	●	○	●	●
Safari 11	○ [†]	☹	○	●	○	☹	N/A
- No Intelligent Tracking Prevention	● [‡]	●	○	●	○	●	N/A
- Block third-party cookies [‡]	● [‡]	●	☹	●	○	●	N/A
Edge 40	●	●	☹	●	○	●	N/A
- Block third-party cookies	●	●	☹	●	○	●	N/A
Cluz 1.17*	☹	●	☹	●	○	☹	☹
- Block third-party cookies	☹	☹	☹	●	○	☹	☹
Tor Browser 7	○	☹	☹	●	○	☹	N/A

●: request with cookies

◐: request without cookies

○: no request

* Secure cookies were omitted in all requests.

† Safari does not permit cross-domain caching over https (only over http). 26

‡ Safari 10.1.2

	AppCache	HTML	Headers	Redirects	PDF JS	JavaScript	SW
Chrome 63	●	●	●	●	●	●	●
- Block third-party cookies	◐	◐	◐	●	●	◐	◐
Opera 51	●	●	●	●	●	●	●
- Block third-party cookies*	◐	◐	◐	●	●	◐	◐
- Ad Blocker	●	●	○	●	○	●	●
Firefox 57	●	●	●	●	○	●	●
- Block third-party cookies	◐	◐	◐	●	○	◐	◐
- Tracking Protection	●	●	●	●	○	●	●
Safari 10	○ [†]	◐	○	●	○	◐	N/A
- No Intelligent Tracking Prevention	● [†]	●	○	●	○	●	N/A
- Block third-party cookies [‡]	● [†]	●	◐	●	○	●	N/A
Edge 40	●	●	◐	●	○	●	N/A
- Block third-party cookies	●	●	◐	●	○	●	N/A
Clash 1.17*	◐	●	◐	●	○	◐	◐
- Block third-party cookies	◐	◐	◐	●	○	◐	◐
Tor Browser 7	○	◐	◐	●	○	◐	N/A

●: request with cookies

◐: request without cookies

○: no request

* Secure cookies were omitted in all requests.

† Safari does not permit cross-domain caching over https (only over http). 27

‡ Safari 10.1.2

	AppCache	HTML	Headers	Redirects	PDF JS	JavaScript	SW
Chrome 63	●	●	●	●	●	●	●
- Block third-party cookies	€	€	€	●	●	€	€
Opera 51	●	●	●	●	●	●	●
- Block third-party cookies [*]	€	€	€	●	●	€	€
- Ad Blocker	●	●	○	●	○	●	●
Firefox 57	●	●	●	●	○	●	●
- Block third-party cookies	€	€	€	●	○	€	€
- Tracking Protection	●	●	●	●	○	●	●
Safari 11	○ [†]	●	○	●	○	●	N/A
- No Intelligent Tracking Prevention	● [‡]	●	○	●	○	●	N/A
- Block third-party cookies [‡]	● [‡]	●	€	●	○	●	N/A
Edge 40	●	●	€	●	○	●	N/A
- Block third-party cookies	●	●	€	●	○	●	N/A
Clash 1.17 [*]	€	●	€	●	○	€	€
- Block third-party cookies	€	€	€	●	○	€	€
Tor Browser 7	○	€	€	●	○	€	N/A

●: request with cookies

●: request without cookies

○: no request

* Secure cookies were omitted in all requests.

† Safari does not permit cross-domain caching over https (only over http). 28

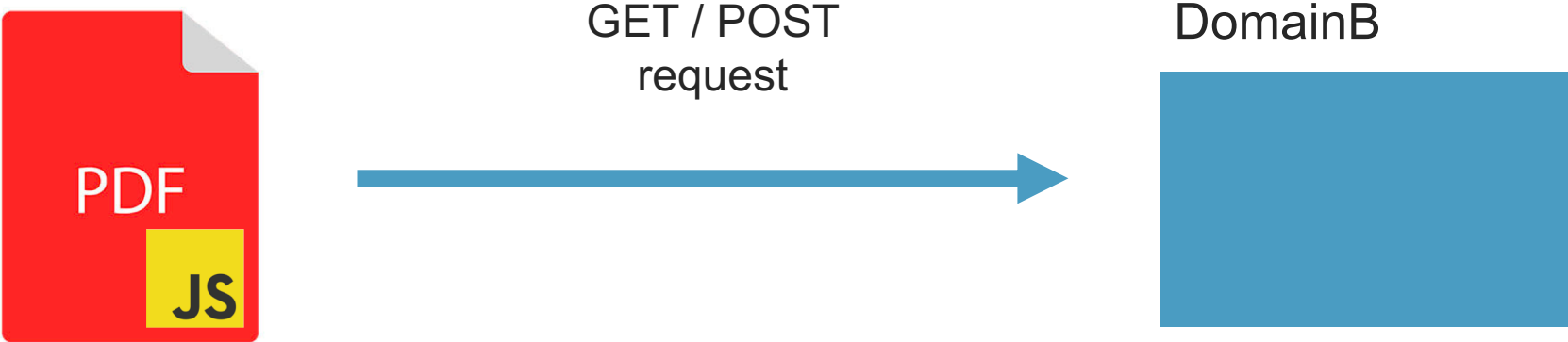
‡ Safari 10.1.2

Extensions

- › No extension managed to block all third-party cookies to blacklisted domains
- › Insufficient API
 - ›› PDF JS for Chromium, but also Firefox favicon (HTML tags)
- › Unclear API
 - ›› No clear distinction for browser background requests
- › Common mistakes
 - ›› Insufficient permissions to intercept certain requests

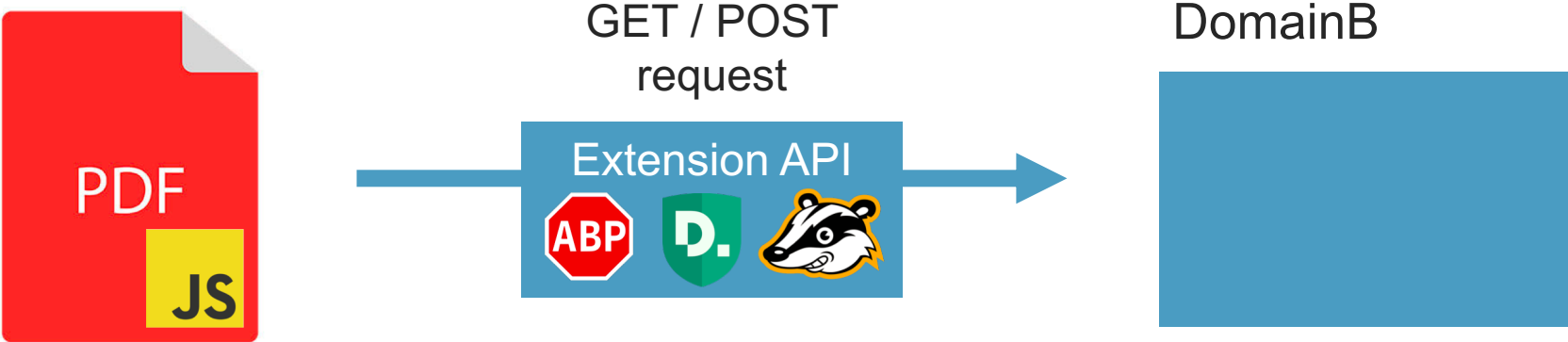
PDFium design flaw

Chrome and Opera



PDFium design flaw

Chrome and Opera

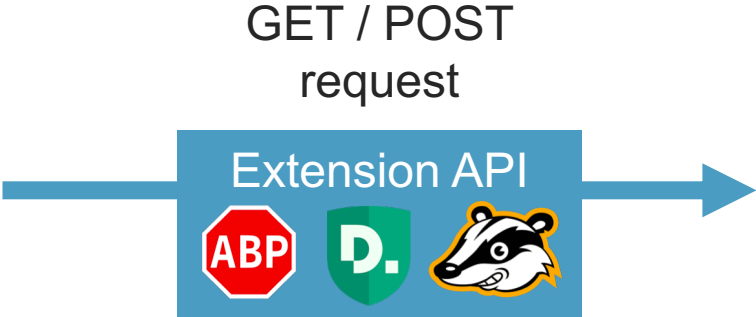


PDFium design flaw

Chrome and Opera



Plugin / Extension



DomainB

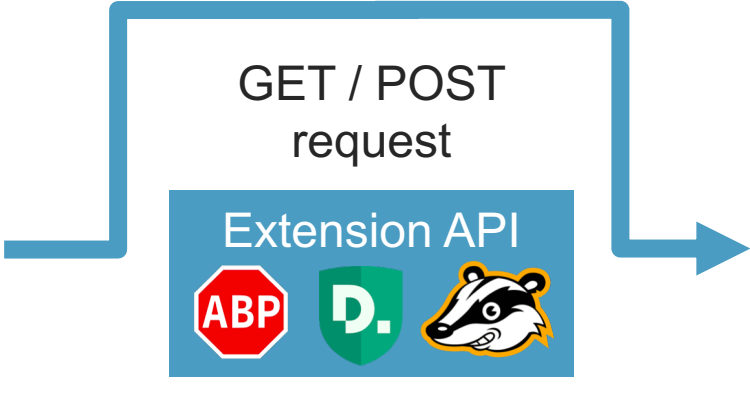


PDFium design flaw

Chrome and Opera



Plugin / Extension



DomainB

PDFium design flaw

Chrome and Opera



Plugin / Extension



DomainB



Same-site cookie policy

- › Chrome and Opera: prerender functionality
 - ›› Both lax and strict included in cross-site request

- › Edge
 - ›› Lax bypasses: WebSocket API, <embed>, <object>
 - ›› Strict bypasses: WebSocket API, redirects

Exploitation of a bypass

Same-site cookies

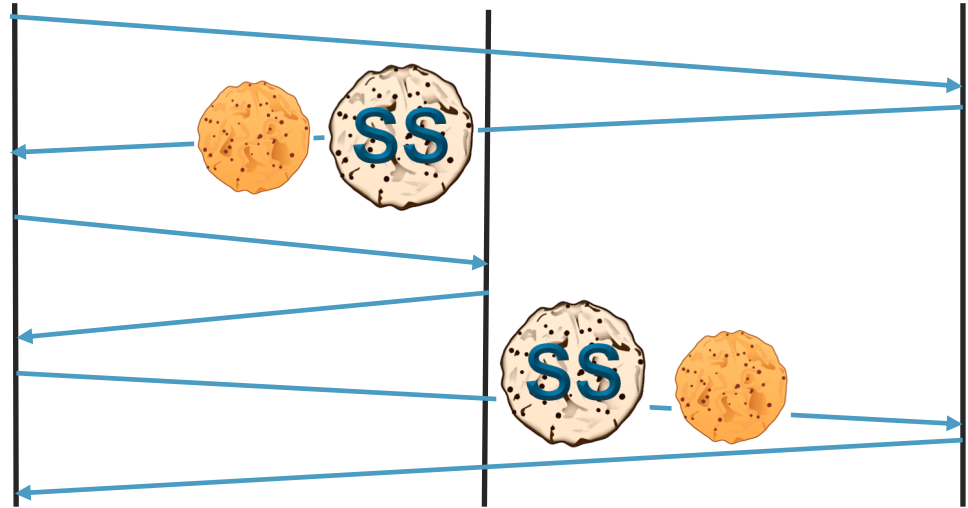


doggo-bank.com

victim

cute-kittens.com

doggo-bank.com



```
<link rel="prerender" href="https://doggo-bank.com/transfer.php?amount=999999&recipient=catboss" />
```


Evaluation of the framework

Completeness and novelty

- › Distributed crawler setup
 - › Interception of headless Chrome network traffic (using linux network namespaces)
 - › Analysis of intercepted HTTP requests
- › Alexa Top 10,000
 - › Up to 20 pages on each website
 - › 160,059 pages visited



Conclusion

Conclusion

What did we find?

- › Built-in browser policies can be bypassed
 - › Same-site cookie, third-party cookie policies
 - › Advanced options (e.g. Opera AdBlocker, Firefox Tracking Protection)
- › All adblocking and privacy extensions can be bypassed
 - › Due to extension API provided by browsers
 - › Due to common mistakes by extension developers

Future work

What about other policies?

- › Expansion of framework

- ›› Policy-wise → private browsing mode, security (e.g. CSP)

- ›› Platform-wise → mobile browsers

- › Goal: tool for comprehensive, automated analysis of security and privacy policy implementations

Illustration of importance

The prerender bug (same-site policy bypass)

- › Originally reported for Chrome 57
- › Present in: 58 59 60 61
- › Fixed in: 62 63 64 65
- › Reintroduced in: 66 67 68

- › Shows importance of a comprehensive evaluation of implemented policies

DistrINet

Thank you!

More info and details:

www.WhoLeftOpenTheCookieJar.com