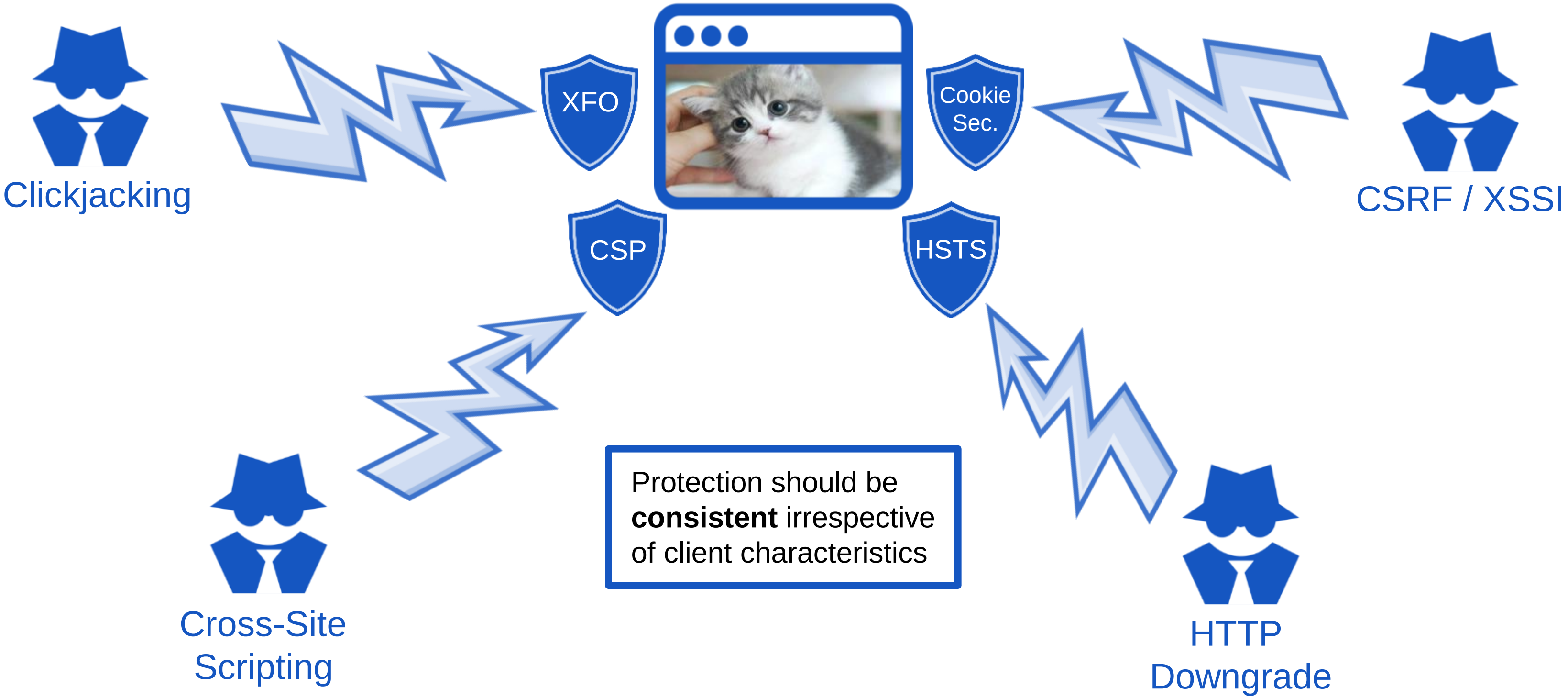
The Security Lottery:
Measuring Client-Side Web Security Inconsistencies

Sebastian Roth*, Stefano Calzavara+, Moritz Wilhelm*, Alvise Rabitti+, and Ben Stock*

*CISPA Helmholtz Center for Information Security +Università Ca' Foscari Venezia

USENIX Security Symposium 2022

Motivation



Clickjacking

XFO

Cookie Sec.

CSRF / XSSI

CSP

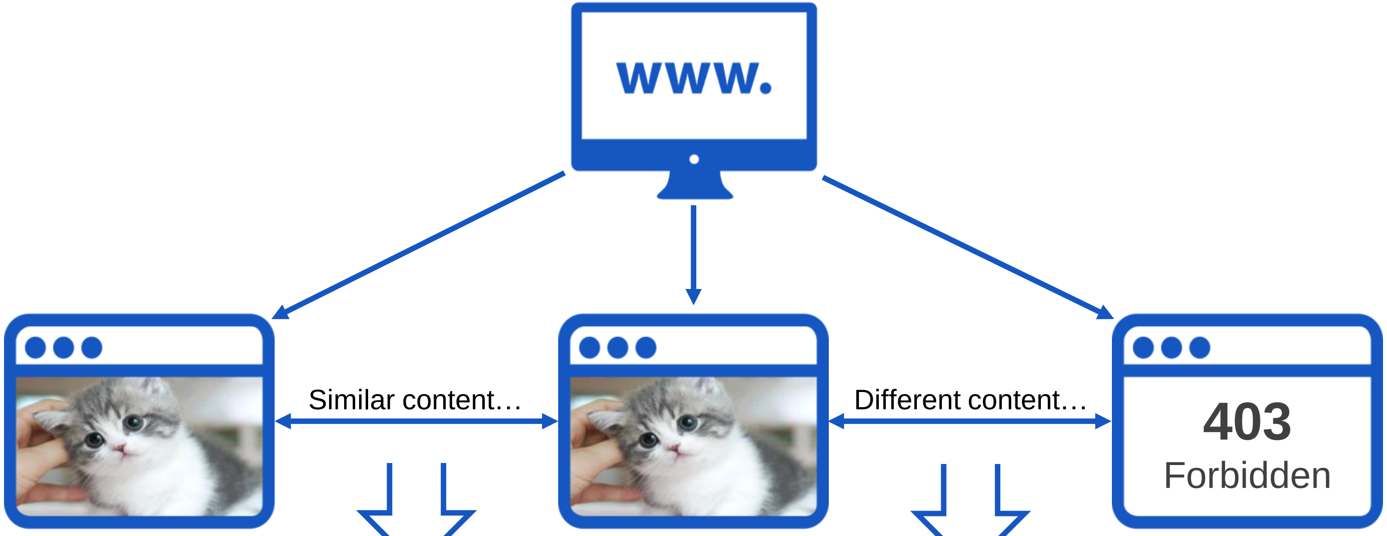
HSTS

Cross-Site Scripting

HTTP Downgrade

Protection should be **consistent** irrespective of client characteristics

What is an Inconsistency?



Similar content…

Different content…

```
CSP:
script-src *
```

```
CSP:
script-src ‘none‘
```

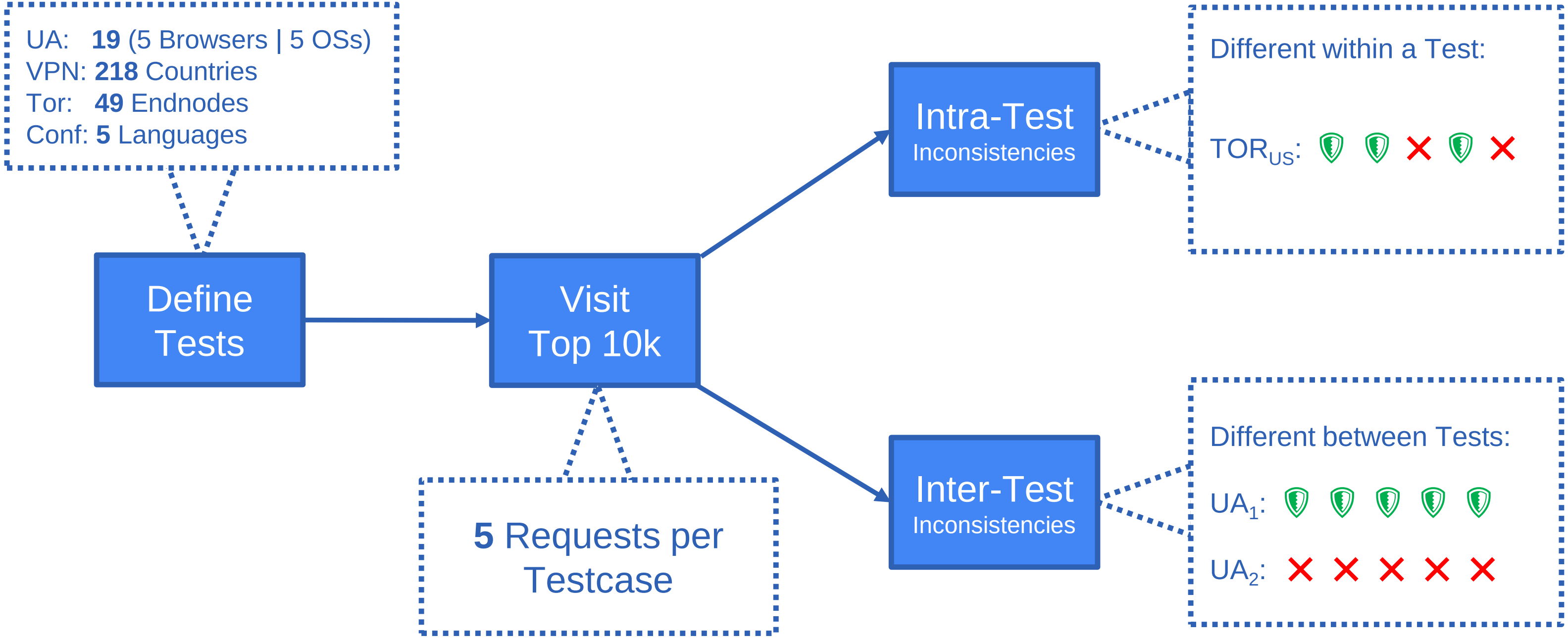
```
CSP:
*not set*
```

...but different security headers

⇒ **Inconsistent**

… not compareable

Methodology



UA: **19** (5 Browsers | 5 OSs)
VPN: **218** Countries
Tor: **49** Endnodes
Conf: **5** Languages

Define Tests

Visit Top 10k

5 Requests per Testcase

Intra-Test Inconsistencies

Different within a Test:

TOR_{US}: 🛡 🛡 ✗ 🛡 ✗

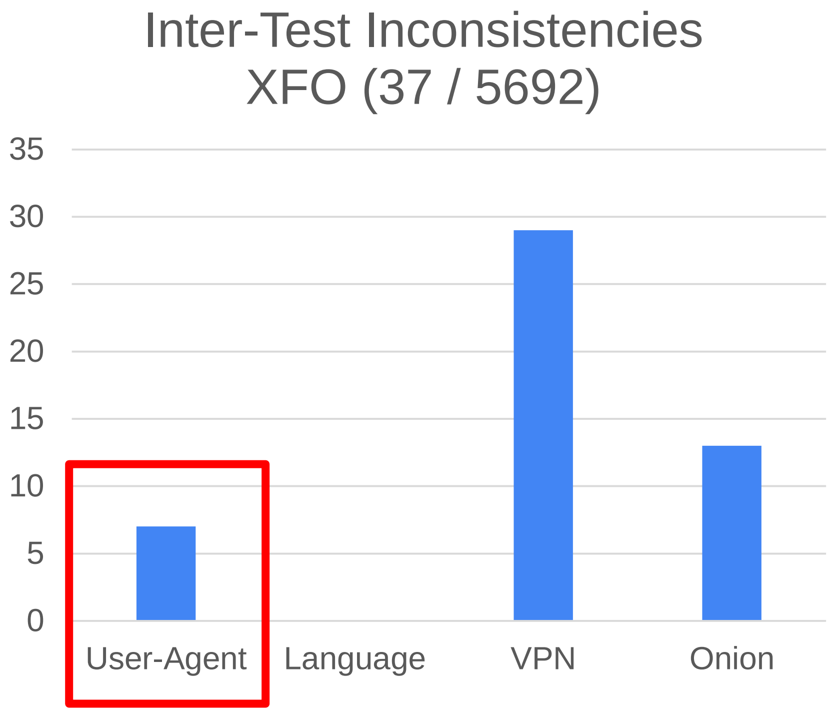
Inter-Test Inconsistencies

Different between Tests:

UA_1: 🛡 🛡 🛡 🛡 🛡

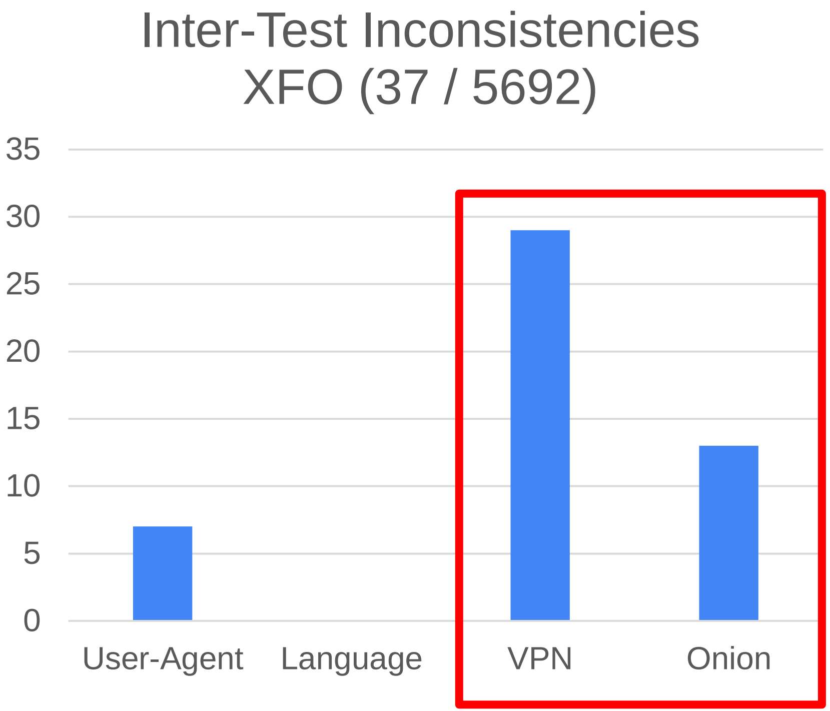
UA_2: ✗ ✗ ✗ ✗ ✗

Inter-Test Inconsistencies (XFO)



- 7 Sites discriminate specific User-Agents (Browser / OS).

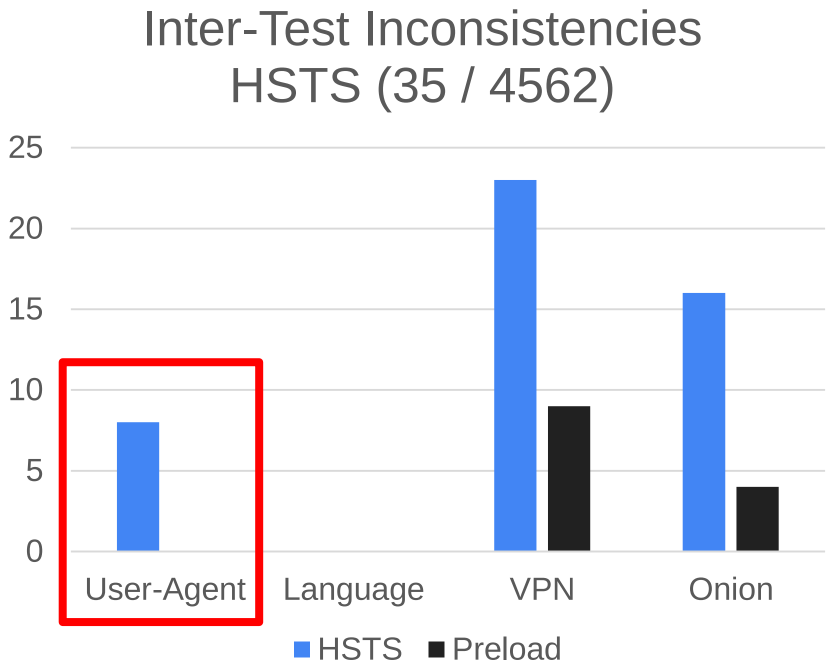
Inter-Test Inconsistencies (XFO)



- 7 Sites discriminate specific User-Agents (Browser / OS).
- 13 sites (Onion) and 29 sites (VPN) exclude specific geolocations.

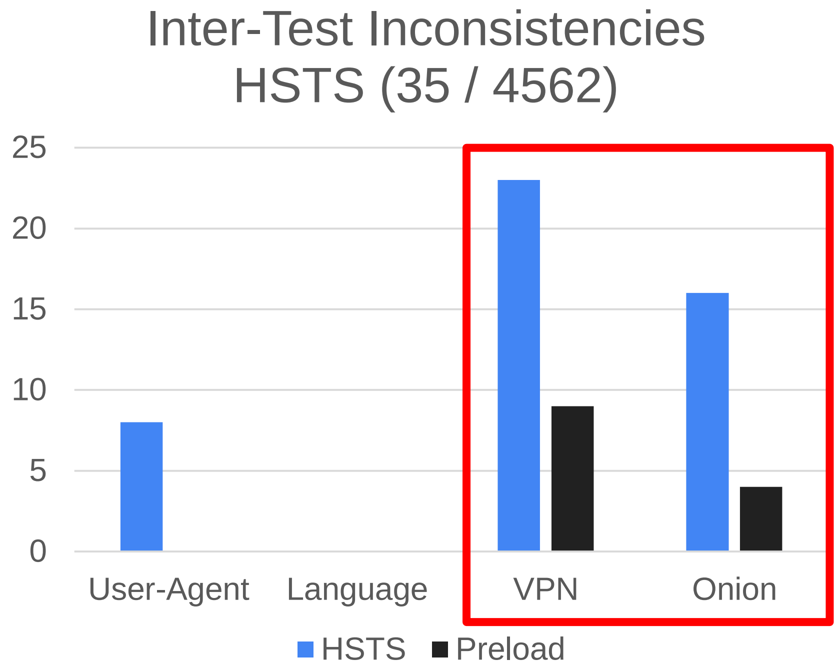
Inter-Test Inconsistencies (HSTS)

- 8 Sites discriminate specific User-Agents.

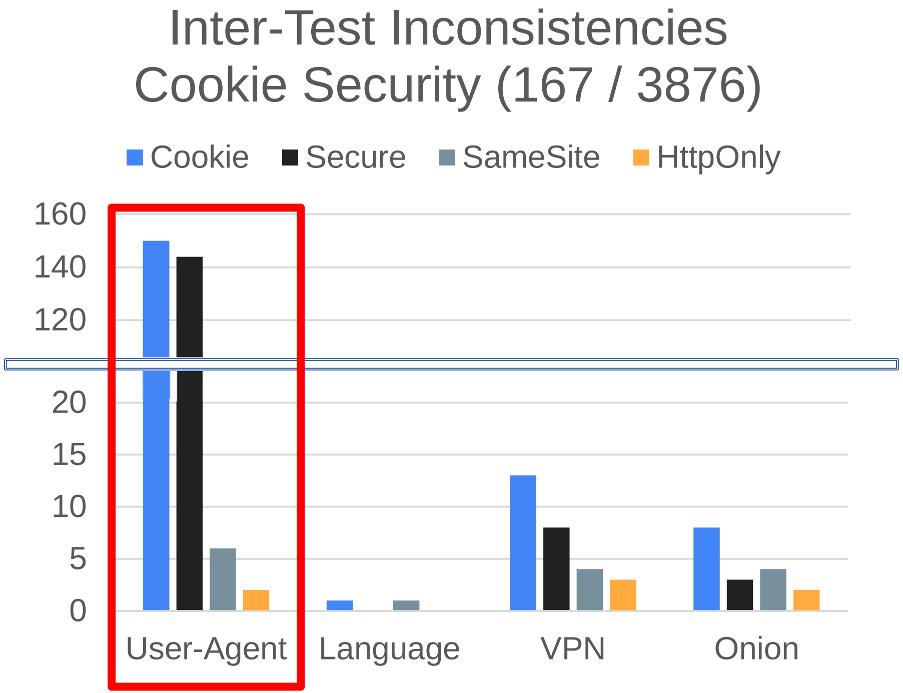


Inter-Test Inconsistencies (HSTS)

- 8 Sites discriminate specific User-Agents.
- 30 sites exclude specific geolocations.

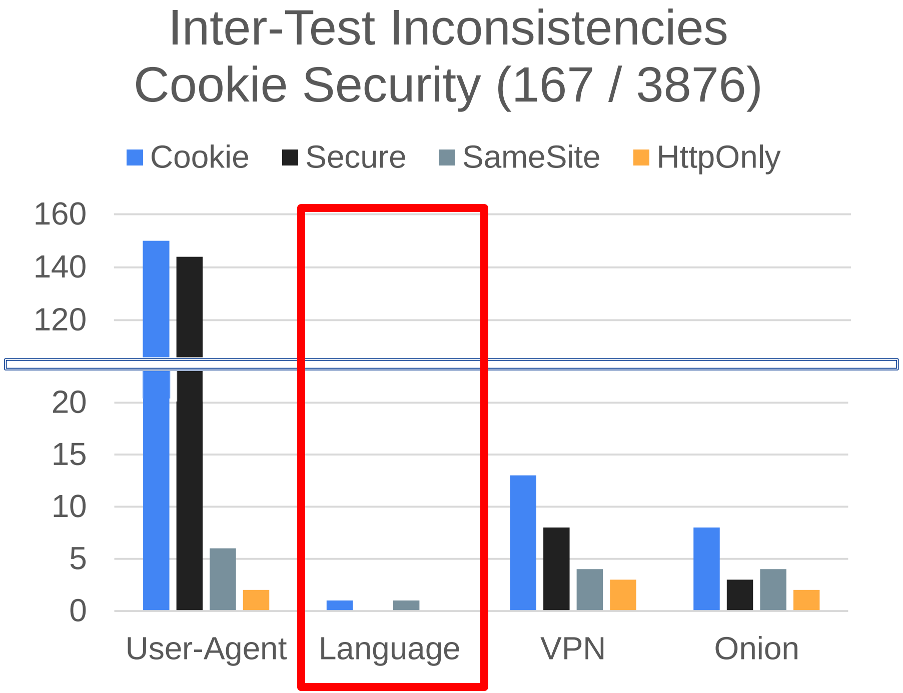

Inter-Test Inconsistencies
HSTS (35 / 4562)

Inter-Test Inconsistencies (Cookies)



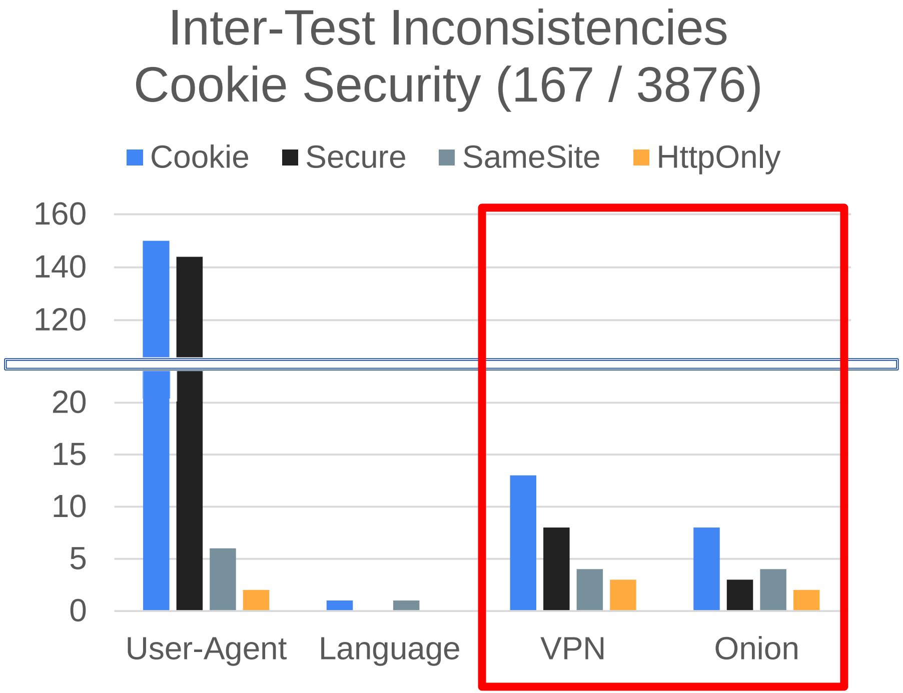
- 144 gave non-secure cookies to specific User-Agents; 130 of those due to Firefox on iOS.

Inter-Test Inconsistencies (Cookies)



- 144 gave non-secure cookies to specific User-Agents; 130 of those due to Firefox on iOS.
- Found langauage-based inconsistency

Inter-Test Inconsistencies (Cookies)

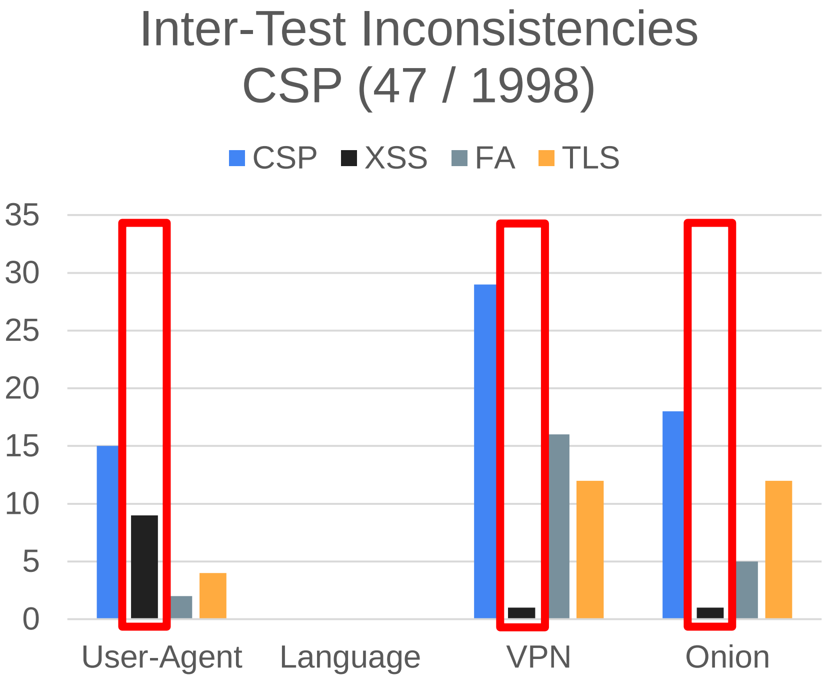


- 144 gave non-secure cookies to specific User-Agents; 130 of those due to Firefox on iOS.
- Found langauage-based inconsistency
- Still we also detected geolocation-based inconsistencies for cookies.

Inter-Test Inconsistencies (CSP)

- For XSS Mitigation Browser-based inconsistencies are dominant.

➢ Discrimination of Safari.

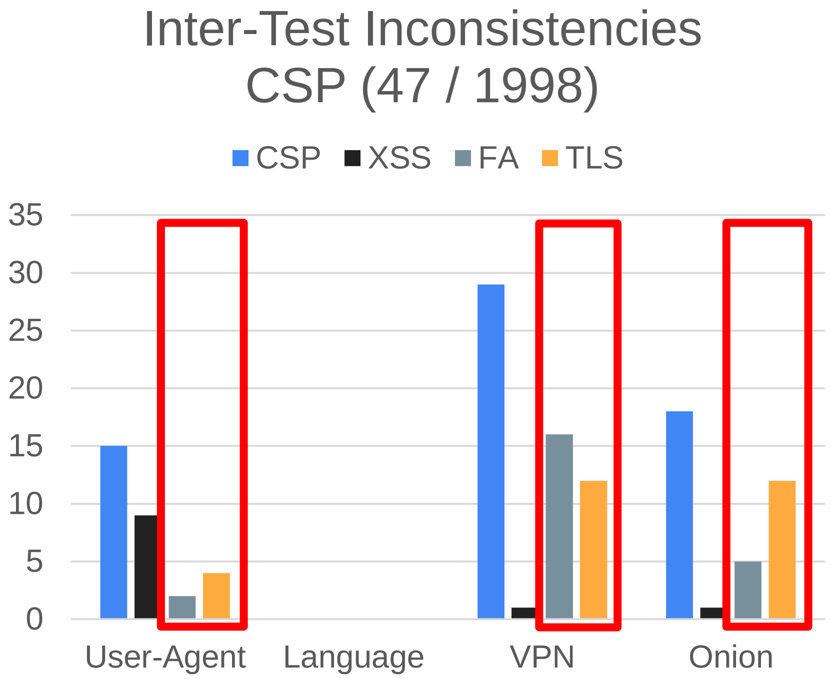


Inter-Test Inconsistencies (CSP)

- For XSS Mitigation Browser-based inconsistencies are dominant.

➢ Discrimination of Safari.

- For Framing / TLS geolocation based changes are dominating.

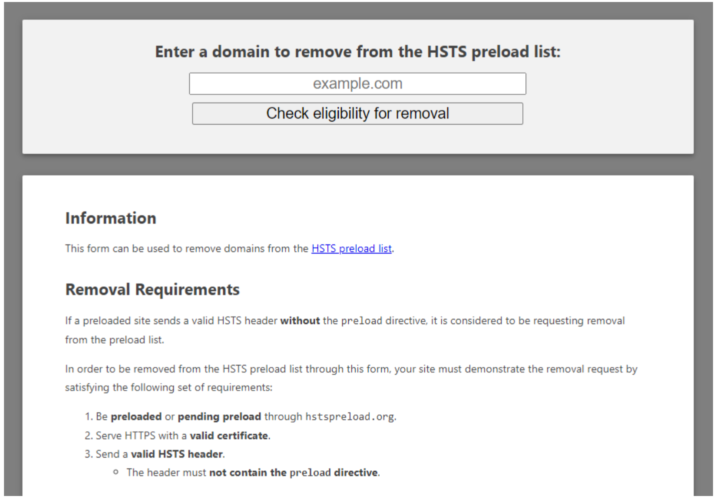


Intra-Test Inconsistencies

Mechanism	Intra-Test Incon.
CSP	36
XFO	50
Cookies	16
HSTS	38
-> Preload	10

⇒ Attackers can opportunistically attack a victim until the attack succeeds.

Special Case: HSTS Preload



Enter a domain to remove from the HSTS preload list:

Information

This form can be used to remove domains from the HSTS preload list.

Removal Requirements

If a preloaded site sends a valid HSTS header **without** the preload directive, it is considered to be requesting removal from the preload list.

In order to be removed from the HSTS preload list through this form, your site must demonstrate the removal request by satisfying the following set of requirements:

1. Be **preloaded** or **pending preload** through `hstspreload.org`.
2. Serve HTTPS with a **valid certificate**.
3. Send a **valid HSTS header**.
   - The header must **not contain the `preload` directive**.

`https://hstspreload.org/removal/`

Reasons for Inconsistencies

- We disclosured the issue to the affected parties and asked them what caused the inconsistency.

- Intra-Test Inconsistencies:
  - (multiple) Misconfigured origin servers
  - Old / weird caching practices
  - …

- Inter-Test Inconsistencies:
  - UA parsing / UA traps based on feature support
  - Misconfigured servers for specific countries
  - …

Conclusion

- Client-side security is not equally delivered to all clients!
  - ➢ 321 Sites had some security inconsistencies!
- Misconfigured servers for specific countries and browser traps enable deteministic attacks (inter-test inconsistencies).
- Non-deterministic (intra-test) inconsistencies play into the hands of opportunistic attackers and impact Web measurements.
  - ➢ Always load a page multiple times during a measurement

cispa/the-security-lottery