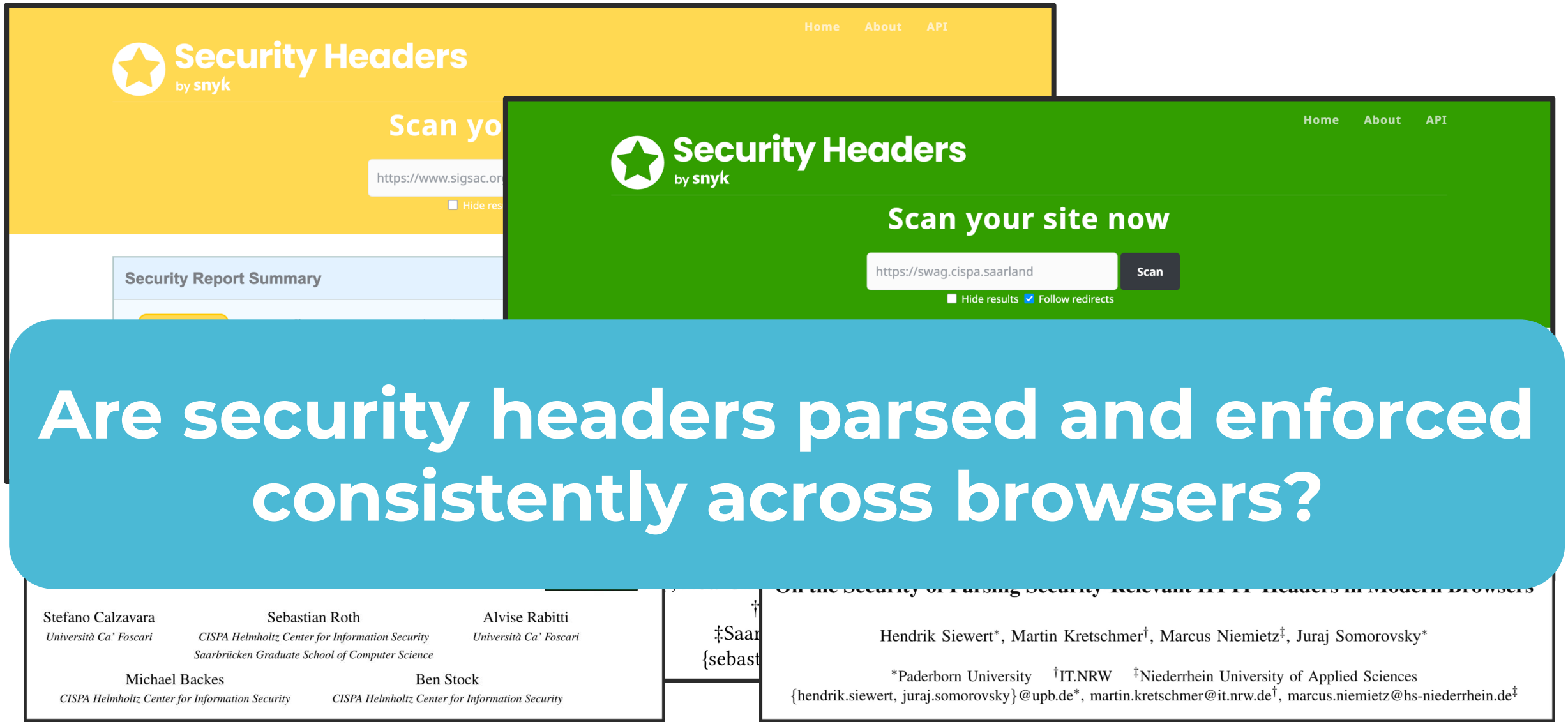
CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

Head(er)s Up! Detecting Security Header Inconsistencies in Browsers

Jannis Rautenstrauch, Trung Tin Nguyen, Karthik Ramakrishnan, Ben Stock

The 32nd ACM Conference on Computer and Communications Security



Are security headers parsed and enforced consistently across browsers?

Stefano Calzavara
Università Ca' Foscari

Sebastian Roth
CISPA Helmholtz Center for Information Security
Saarbrücken Graduate School of Computer Science

Alvise Rabitti
Università Ca' Foscari

Michael Backes
CISPA Helmholtz Center for Information Security

Ben Stock
CISPA Helmholtz Center for Information Security

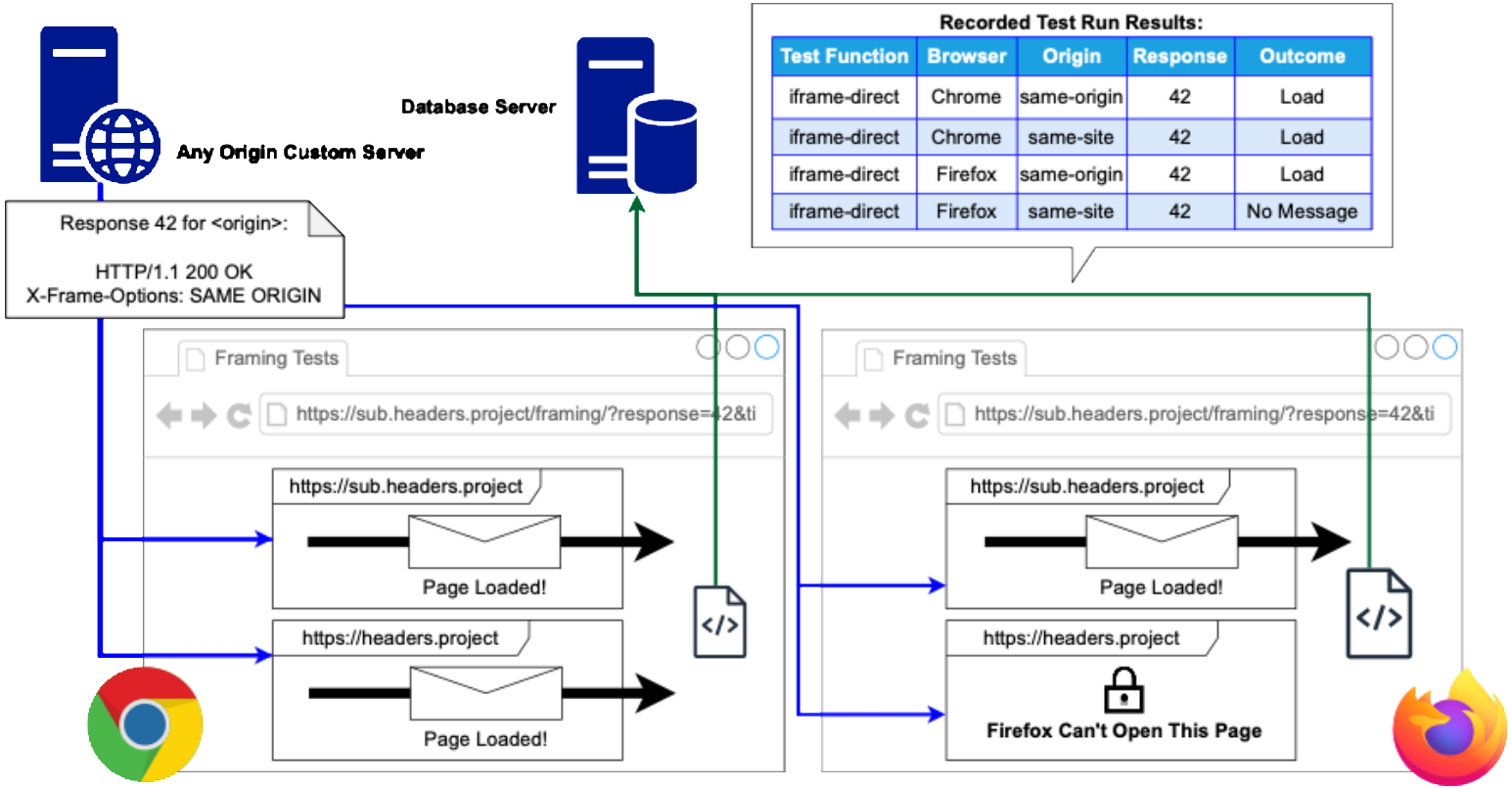
Hendrik Siewert*, Martin Kretschmer†, Marcus Niemietz‡, Juraj Somorovsky*

*Paderborn University †IT.NRW ‡Niederrhein University of Applied Sciences
{hendrik.siewert, juraj.somorovsky}@upb.de*, martin.kretschmer@it.nrw.de†, marcus.niemietz@hs-niederrhein.de‡

Key Idea: Differential Testing

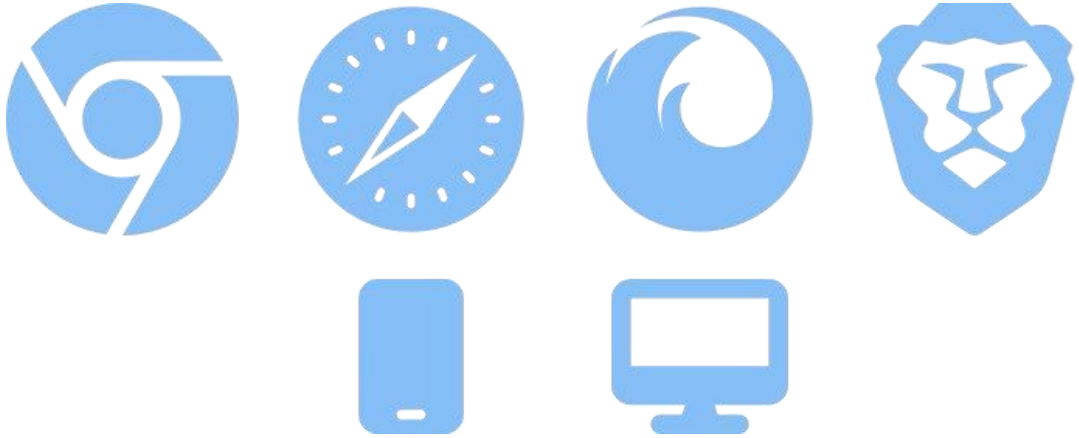
- Widely used test by browser: Web Platform Test (**Expected Outcome Tests**)
  - What about incomplete or ambiguous specification?
- We rely on **Differential Testing**: run the same tests in different browsers
- Compare outcomes across browsers directly
- Any difference = potential bug or spec ambiguity

Example Test Execution



Test Subjects

- Four browsing engines in desktop, Android, and iOS versions
  - 4 versions of Chrome Desktop
  - 4 versions of Firefox Desktop
  - 2 version of Brave Desktop
  - 2 versions of Safari
  - One each of Chrome, Firefox, Brave on Android
  - One Chrome iOS
- In total **16** browser configurations, some with almost one year gap in between



Experimental Setup

- 12 tested features (Framing Control, Permissions, Scriping Restrictions, …)
  - Some of them controlled by multiple headers (e.g., XFO/CSP)
- 43.604 responses across 16 security headers
  - Inspired by WPT, real-world headers, prior work + various mutations
  - Varying status codes, content types, etc.
- Various origin relations: same-origin, same-site (parent + child), HTTP/HTTPS

- In total, **177,146** tests executed at least five times to ensure stable results
  - ~15M test executions, 134 runs failed

Key Results

- 5,606 (~3%) inconsistent tests in total

	Android						Ubun				macOS	
	Brave 1.62.165	Chrome 121	Firefox Beta 123	Brave 1.62.156	Brave 1.73.101	Chrome 120	Chro 121-				Safari 17.3.1	Safari 18.2
Android Brave (1.62.165)	-	88	2854	18	304	122					2570	4011
Android Chrome (121)	88	-	2917	106	392	34					2634	4074
Android Firefox Beta (123)	2854	2917	-	2872	2588	2951	29				2626	3275
Ubuntu Brave (1.62.156)	18	106	2872	-	286	104	88		2858		2584	4029
Ubuntu Brave (1.73.101)	304	392	2588	286	-	390	374	88	2574		2754	3749
Ubuntu Chrome (120)	122	34	2951	104	390	-	16	302	2937		2664	4108
Ubuntu Chrome (121-122)	106	18	2935	88	374	16	-	286	2921		2648	4092
Ubuntu Chrome (131)	392	304	2651	374	88	302	286	-	2637	2571	2818	3812
Ubuntu Firefox (121-123)	2868	2931	14	2858	2574	2937	2921	2637	-	129	2636	3289
Ubuntu Firefox (133)	2785	2849	127	2791	2507	2871	2855	2571	129	-	2567	3214
iPadOS Chrome (122/17.3.1)	2525	2589	2683	2531	2701	2611	2595	2765	2685	2598	-	1754
macOS Safari (17.3.1)	2570	2634	2626	2584	2754	2664	2648	2818	2636	2567	61	-	1799
macOS Safari (18.2)	4011	4074	3275	4029	3749	4108	4092	3812	3289	3214	1754	1799	-

Mostly stable code across versions for Firefox and Chrome (except our bug reports)

More variance in Safari tests

Key Results

- 5,606 (~3%) inconsistent tests in total

	Android			Ubuntu							iPadOS	macOS	
	Brave 1.62.165	Chrome 121	Firefox Beta 123	Brave 1.62.156	Brave 1.73.101	Chrome 120	Chrome 121-122	Chrome 131	Firefox 121-123	Firefox 133	Chrome 122/17.3.1	Safari 17.3.1	Safari 18.2
Android Brave (1.62.165)	-	88	2854	18	304	122	106	392	2868	2785	2525	2570	4011
Android Chrome (121)	88	-	2917	106	392	34	18	304	2931	2849	2589	2634	4074
Android Firefox Beta (123)	2854	2917	-	2588	2951	2935	2651	14	127	2683	2626	3275	
Ubuntu Brave (1.62.156)	18	106	2588	-	54	88	374	2858	2791	2531	2584	4029	
Ubuntu Brave (1.73.101)	304	392	2951	54	-	390	374	88	2574	2507	2701	2754	3749
Ubuntu Chrome (120)	122	34	2935	88	390	-	16	302	2937	2871	2611	2664	4108
Ubuntu Chrome (121-122)	106	18	2651	374	374	16	-	86	2921	2855	2595	2648	4092
Ubuntu Chrome (131)	392	304	14	2858	88	302	286	-	2637	2571	2765	2818	3812
Ubuntu Firefox (121-123)	2868	2931	127	2791	2574	2937	2921	2637	-	129	2685	2636	3289
Ubuntu Firefox (133)	2785	2849	2683	2531	2507	2871	2855	2571	129	-	2598	2567	3214
iPadOS Chrome (122/17.3.1)	2525	2589	2626	2584	2701	2611	2595	2765	2685	2598	-	61	1754
macOS Safari (17.3.1)	2570	2634	2584	2754	2664	2648	2818	2636	2567	61	-	1799	
macOS Safari (18.2)	4011	4074	3275	4029	3749	4108	4092	3812	3289	3214	1754	1799	-

Mobile and Desktop versions highly similar

Key Results

- 5,606 (~3%) inconsistent tests in total

Only Referrer-Policy difference

	Brave 1.62.165	Chrome 121	Firefox 123	Brave 1.62.156	Brave 1.73.101	Chrome 120	Chrome 121-122	Chrome 131	Firefox 121-123	Firefox 133	iPadOS Chrome 122/17.3.1	macOS Safari 17.3.1	Safari 18.2
Android Brave (1.62.165)	-	88	2854	18	304	122	106	392	2868	2785	2525	2570	4011
Android Chrome (121)	88	-	2917	106	392	34	18	304	2931	2849	2589	2634	4074
Android Firefox Beta (123)	2854	2917	-	2872	2588	2951	2935	2651	14	127	2683	2626	3275
Ubuntu Brave (1.62.156)	18	106	2872	-	286	104	88	374	2858	2791	2531	2584	4029
Ubuntu Brave (1.73.101)	304	392	2588	286	-	390	374	88	2574	2507	2701	2754	3749
Ubuntu Chrome (120)	122	34	2951	104	390	-	16	302	2937	2871	2611	2664	4108
Ubuntu Chrome (121-122)	106	18	2935	88	374	16	-	286	2921	2855	2595	2648	4092
Ubuntu Chrome (131)	392	304	2651	374	88	302	286	-	2637	2571	2765	2818	3812
Ubuntu Firefox (121-123)	2868	2931	14	2858	2574	2937	2921	2637	-	129	2685	2636	3289
Ubuntu Firefox (133)	2785	2849	127	2791	2507	2871	2855	2571	129	-	2598	2567	3214
iPadOS Chrome (122/17.3.1)	2525	2589	2683	2531	2701	2611	2595	2765	2685	2598	-	61	1754
macOS Safari (17.3.1)	2570	2634	2626	2584	2754	2664	2648	2818	2636	2567	61	-	1799
macOS Safari (18.2)	4011	4074	3275	4029	3749	4108	4092	3812	3289	3214	1754	1799	-

Key Results

- 5,606 (~3%) inconsistent tests in total

Major differences between the different engines

	Android												
	Brave 1.62.165	Chrome 121	Firefox Beta 123	Brave 1.62.156	Brave 1.73.101	Chrome 120	U… C… 121-122	131	121-123	13…	…1	17.3.1	cOS Safari 18.2
Android Brave (1.62.165)	-	88	2854	18	304	122	106	392	2868	2785	…25	2570	4011
Android Chrome (121)	88	-	2917	106	392	34	18	304	2931	2849	…589	2634	4074
Android Firefox Beta (123)	2854	2917	-	2872	2588	2951	2935	2651	14	127	…2683	2626	3275
Ubuntu Brave (1.62.156)	18	106	2872	-	286	104	88	374	2858	2791	2531	2584	4029
Ubuntu Brave (1.73.101)	304	392	2588	286	-	390	374	88	2574	2507	2701	2754	3749
Ubuntu Chrome (120)	122	34	2951	104	390	-	16	302	2937	2871	2611	2664	4108
Ubuntu Chrome (121-122)	106	18	2935	88	374	16	-	286	2921	2855	2595	2648	4092
Ubuntu Chrome (131)	392	304	2651	374	88	302	286	-	2637	2571	2765	2818	3812
Ubuntu Firefox (121-123)	2868	2931	14	2858	2574	2937	2921	2637	-	129	2685	2636	3289
Ubuntu Firefox (133)	2785	2849	127	2791	2507	2871	2855	2571	129	-	2598	2567	3214
iPadOS Chrome (122/17.3.1)	2525	2589	2683	2531	2701	2611	2595	2765	2685	2598	-	61	1754
macOS Safari (17.3.1)	2570	2634	2626	2584	2754	2664	2648	2818	2636	2567	61	-	1799
macOS Safari (18.2)	4011	4074	3275	4029	3749	4108	4092	3812	3289	3214	1754	1799	-

Root Cause Clustering (XFO example)

- First step: cluster tests by outcome and browser
  - Example: XFO tests which send postmessage to cross-origin parent

Message received: {Chrome, Safari}, No message: {Firefox}	{"DE\tNY", "DE NY", "SAME ORIGIN", ...}
Message received: {Firefox, Safari}, No message: {Chrome}	{"X-Frame\x00-Options: DENY", ...}

- Second step: manually identify patterns in the tests and attribute them to root causes
- Here: Firefox strips whitespaces in header values, Chrome does not allow NULL bytes in header names

Root Causes

- Identify 42 root causes
  - 12 general, i.e., affect all features
  - 30 feature-specific
- 31 previously unknown

#	Title	Type	Affected Party*	Status with Hyperlinks (as of 2025-08-31)
	General Differences			
Related to header parsing				
1	LF in Header Block	Compat.		Confirmed
2	NULL in Header Name	Compat.	Fetch Standard	Confirmed
3	CR in Header Block	Compat.	Fetch Standard	Confirmed; Partially known
4	Whitespace Colon	Compat.	Fetch Standard	Confirmed
5	VT in Header Values	Compat.	,	Confirmed (), Confirmed ()
6	Empty + Non-Empty Header	Compat.		Confirmed
7+	Leading Colon	Compat.		Confirmed
8+	Leading Whitespace	Compat.		Confirmed
Not related to header parsing				
9	Status Code 300	Compat.		Known + unintended; Fixed
10	Mixed Content Images	Security	,	Known + unintended (), Known + unintended (); Fixed
11	HTTP Upgrade	Security	,	Known + intended (), Known + intended ()
12	Embed/Object URL Reliance	Compat.		Confirmed
	Feature-Specific Differences			
Related to header parsing				
13	CSP: Uppercase Scheme	Compat.		Fixed
14	CSP: Invalid Bytes	Compat.		Fixed
15	CSP: */	Compat.		Confirmed + Spec changed
16	CSP: Path in Frame-Ancestors	Security		Confirmed
17	XFO: Whitespace Everywhere	Compat.		Fixed
18	HSTS: Various Issues	Security	, ,	Fixed (), Fixed (), Confirmed ()
19	RP: FF and VT allowed	Compat.		Confirmed
20	LF in Fetch	Compat.	,	Confirmed (), Confirmed ()
21	PerformanceAPI and NULL	Compat.		Confirmed
22	NULL in Header Values (Fetch)	Compat.		Fixed
23	XCTO: Various Issues	Compat.		Known + unintended; Fixed
24+	XFO: FF allowed	Compat.	,	New (), Confirmed ()
Not related to header parsing				
25	Code 300 Cached (HSTS)	Compat.	,	Confirmed (), Fixed ()
26	CSP: Sandboxed Frames FA	Security		Confirmed
27	CSP: Sandboxed Frames 'self' Bypass	Security		Confirmed
28	CSP: Sandboxed Frames *.origin	Security		Confirmed
29	FP Header not supported	Compat.	,	Known + intended
30	PP Header not supported	Security	,	Known + intended
31	TAO and 302	Compat.		Fixed
32	Mixed-Content performanceAPI	Compat.		Confirmed
33	CORP and Object	Compat.		Known + unintended
34	RP Safer-Defaults	Privacy	, ,	Known + intended (,), Known + intended ()
35	RP Safer-Defaults Exception Top-Level	Privacy		Known + intended; Missing documentation
36	RP Safer-Defaults Exception Same-Site	Privacy	,	Known + intended (), Known + intended (); Might change
37	COEP Secure-Context	Security		Confirmed
38	CORP Random Caching	Security		Confirmed
39	Download Window Reference	Compat.	All	Different default settings for download behavior
40	Download Behavior Difference	Compat.	(Mobile only)	Confirmed
41	204 Not About:Blank	Compat.	(Mobile only)	Confirmed
42+	HSTS Race Condition	Security		Confirmed

+ Root cause discovered in the second run with the four new browser configurations

* All root causes affecting Chrome also affect Brave

Table 4: Identified root causes across two dimensions discovered in the initial run and the second run.

Case Studies

15	CSP: */	Compat.		Confirmed + Spec changed

- Reported as a bug to Chrome
  - */ was treated as any origin, any path (same as *)
- Assignee was Mike West, co-author of the CSP spec
- Resulted in specification change

Case Studies

18	HSTS: Various Issues	Security	, ,	Fixed ( ), Fixed ( ), Confirmed ( )

- Deployed header: max-age=20; includeSubdomains=
- Three browsers, three outcomes
  - Firefox: "it's OK, we know what you meant". – will set HSTS for all subdomains
  - Chrome: "Invalid HSTS header" – will ignore it altogether
  - Safari: "Part of it is valid" – will set max-age for the domain, not for subdomains

Towards Better Security Header Parsing

- Security headers are often implemented **inconsistently**
  - Poses risks for developers and users
- Through **differential testing**, we discovered **42 root causes**, 31 of which were previously unknown
  - Led to various bug fixes and specification adjustments
- Open-source tool: Available, Functional, Reproduced

Happy to take your questions!

Attribution

- This presentation uses icons from Font Awesome, which is licensed under the Creative Commons Attribution 4.0 International License.
  Font Awesome icons can be found at: https://fontawesome.com/