The Security Lottery: Measuring Client-Side Web Security Inconsistencies

Sebastian Roth Stefano Calzavara Moritz Wilhelm Alvise Rabitti
Ben Stock

Presented by
Ramesh Adhikari
Graduate Research Assistant
School of Computer and Cyber Sciences, Augusta University

November, 2022

AUGUSTA UNIVERSITY

Table of Contents

AUGUSTA UNIVERSITY

Table of Contents

AUGUSTA UNIVERSITY

Introduction

- Web apps are a primary target for attackers because they are one of the main entry points to security-sensitive information and functionality that we use on a regular basis.

AUGUSTA UNIVERSITY

Introduction

- Web apps are a primary target for attackers because they are one of the main entry points to security-sensitive information and functionality that we use on a regular basis.
- To mitigate a variety of Web attacks, modern browsers support client-side security policies shipped through HTTP response headers.

AUGUSTA UNIVERSITY

Introduction

- Web apps are a primary target for attackers because they are one of the main entry points to security-sensitive information and functionality that we use on a regular basis.
- To mitigate a variety of Web attacks, modern browsers support client-side security policies shipped through HTTP response headers.
- To enforce these defenses, the server needs to communicate them to the client, a seemingly straightforward process.

AUGUSTA UNIVERSITY

Introduction

- Web apps are a primary target for attackers because they are one of the main entry points to security-sensitive information and functionality that we use on a regular basis.
- To mitigate a variety of Web attacks, modern browsers support client-side security policies shipped through HTTP response headers.
- To enforce these defenses, the server needs to communicate them to the client, a seemingly straightforward process.
- However, same site can be accessed by users in a variety of ways, such as by utilizing various User-Agents, network access techniques, or language settings.

AUGUSTA UNIVERSITY

Introduction

- Web apps are a primary target for attackers because they are one of the main entry points to security-sensitive information and functionality that we use on a regular basis.
- To mitigate a variety of Web attacks, modern browsers support client-side security policies shipped through HTTP response headers.
- To enforce these defenses, the server needs to communicate them to the client, a seemingly straightforward process.
- However, same site can be accessed by users in a variety of ways, such as by utilizing various User-Agents, network access techniques, or language settings.
- All these usage scenarios should enforce the same security policies, otherwise a **security lottery** would take place.

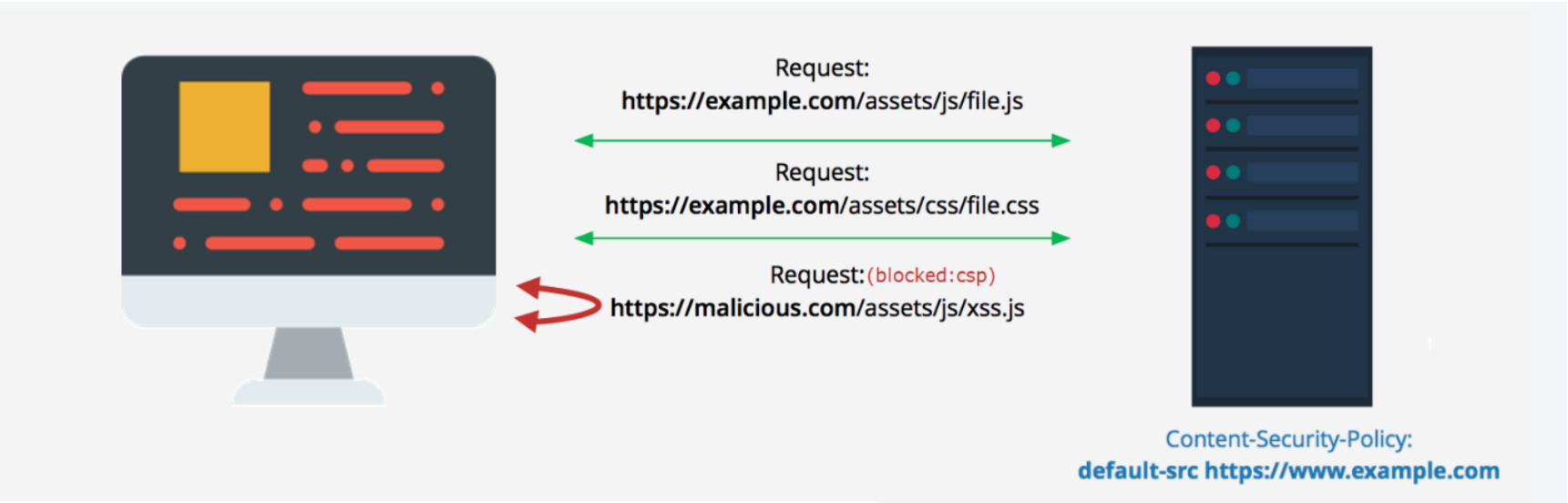
AUGUSTA UNIVERSITY

Table of Contents

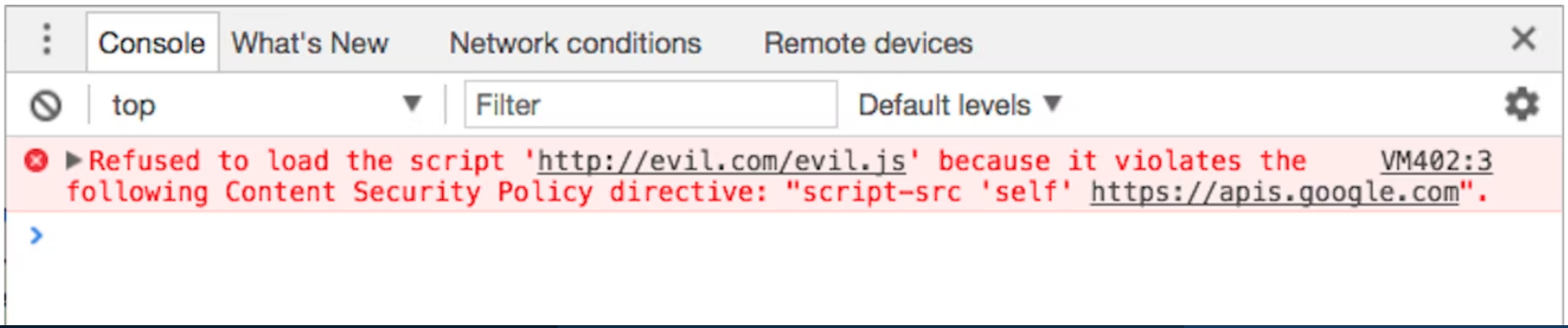
AUGUSTA UNIVERSITY

Technical Preliminaries: Content Security Policy (CSP)

Content Security Policy can significantly reduce the risk and impact of cross-site scripting attacks in modern browsers.




```
Content-Security-Policy: script-src 'self' https://apis.google.com
```



AUGUSTA UNIVERSITY

Technical Preliminaries: X-Frame-Options

- **Allow for Same Origin (Default Action)**

```
Header set X-Frame-Options: "SAMEORIGIN"
```

- **Allow from specific origin**

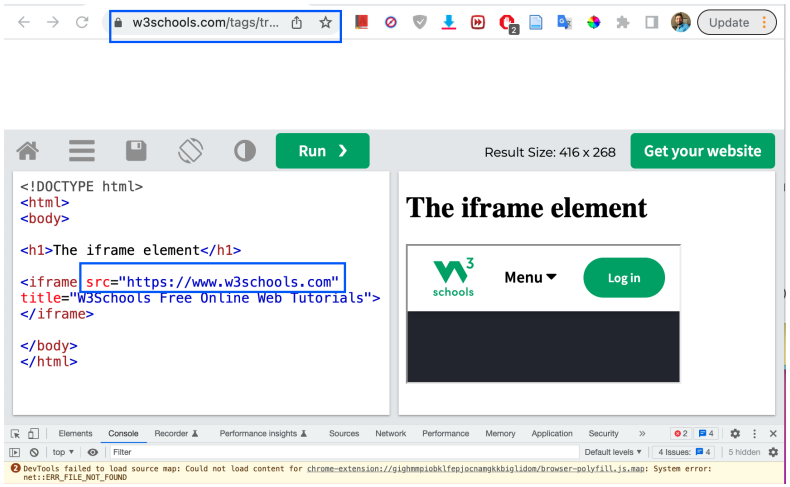
```
Header set X-Frame-Options: "ALLOW-FROM http://example.com/"
Header set X-Frame-Options: "ALLOW-FROM http://www.example.com/"
Header set X-Frame-Options: "ALLOW-FROM https://example.com/"
Header set X-Frame-Options: "ALLOW-FROM https://www.example.com/"
```

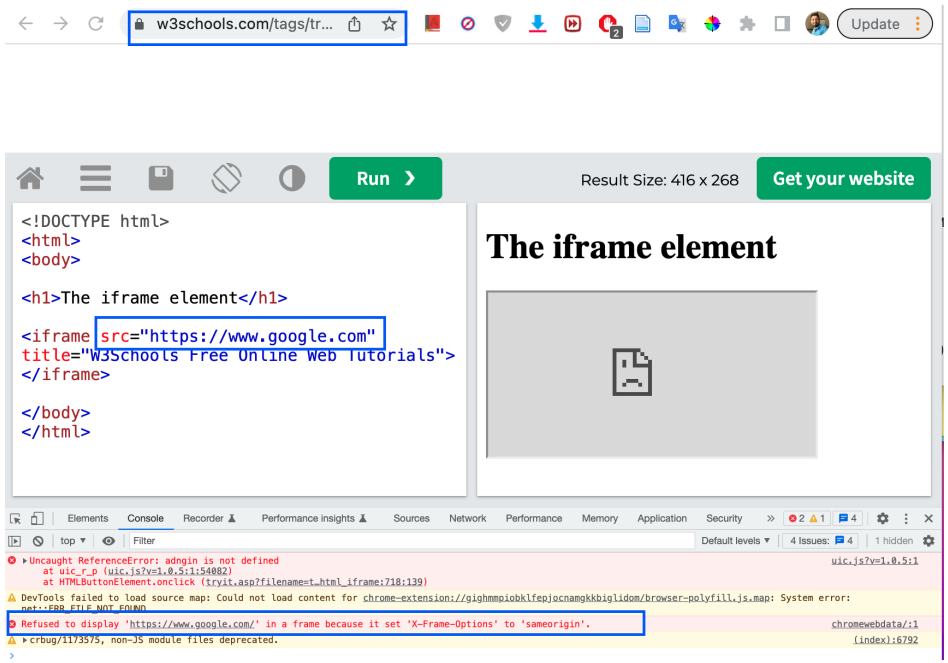
- **Deny to everyone**

```
Header set X-Frame-Options: "DENY"
```

AUGUSTA UNIVERSITY

Technical Preliminaries: X-Frame-Options

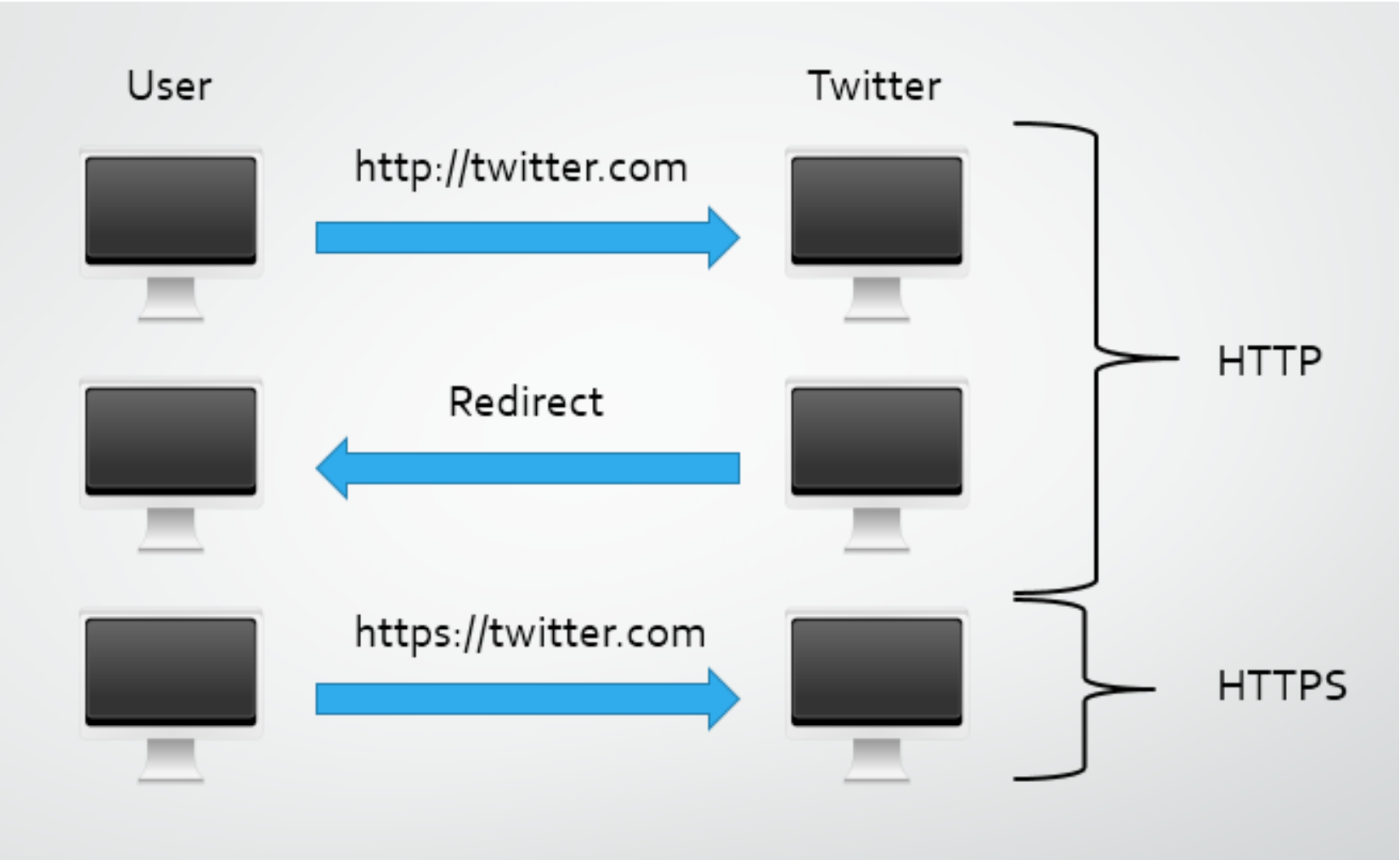




AUGUSTA UNIVERSITY

Technical Preliminaries: Strict Transport Security

HTTP Strict Transport Security (HSTS) is a simple and widely supported standard to protect visitors by ensuring that their browsers always connect to a website over HTTPS



AUGUSTA UNIVERSITY

Table of Contents

AUGUSTA UNIVERSITY

Motivation

- A web site may set the secure attribute on its session cookies when it is accessed using **Chrome**, but may forget the attribute when it is accessed using **Opera**.

AUGUSTA UNIVERSITY

Motivation

- A web site may set the secure attribute on its session cookies when it is accessed using **Chrome**, but may forget the attribute when it is accessed using **Opera**.
  - Opera users vulnerable to cookie

AUGUSTA UNIVERSITY

Motivation

- A web site may set the secure attribute on its session cookies when it is accessed using **Chrome**, but may forget the attribute when it is accessed using **Opera**.
  - Opera users vulnerable to cookie
  - May enable **session hijacking** attacks against a specific user population

AUGUSTA UNIVERSITY

Motivation

- A web site may set the secure attribute on its session cookies when it is accessed using **Chrome**, but may forget the attribute when it is accessed using **Opera**.
  - Opera users vulnerable to cookie
  - May enable **session hijacking** attacks against a specific user population
- A web site may configure its **content security policy (CSP)** differently when accessed from different countries.

AUGUSTA UNIVERSITY

Motivation

- A web site may set the secure attribute on its session cookies when it is accessed using **Chrome**, but may forget the attribute when it is accessed using **Opera**.
  - Opera users vulnerable to cookie
  - May enable **session hijacking** attacks against a specific user population
- A web site may configure its **content security policy (CSP)** differently when accessed from different countries.
  - e.g., due to the use of different ad networks, and there is no guarantee that all these CSPs enjoy the same security guarantees.

AUGUSTA UNIVERSITY

Motivation

- A web site may set the secure attribute on its session cookies when it is accessed using **Chrome**, but may forget the attribute when it is accessed using **Opera**.
  - Opera users vulnerable to cookie
  - May enable **session hijacking** attacks against a specific user population
- A web site may configure its **content security policy (CSP)** differently when accessed from different countries.
  - e.g., due to the use of different ad networks, and there is no guarantee that all these CSPs enjoy the same security guarantees.
- Security mechanisms might change when sites are accessed from different geolocations.

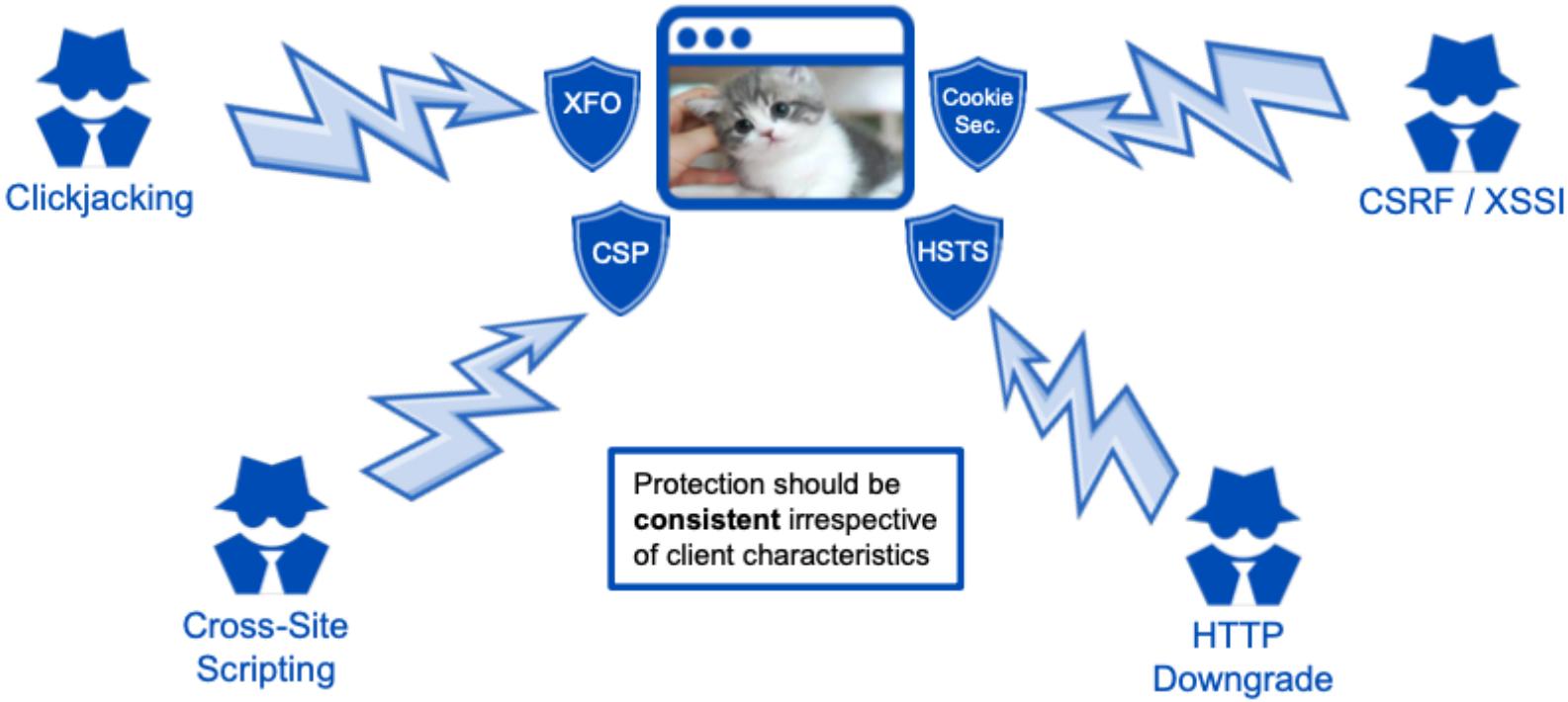
AUGUSTA UNIVERSITY

Motivation

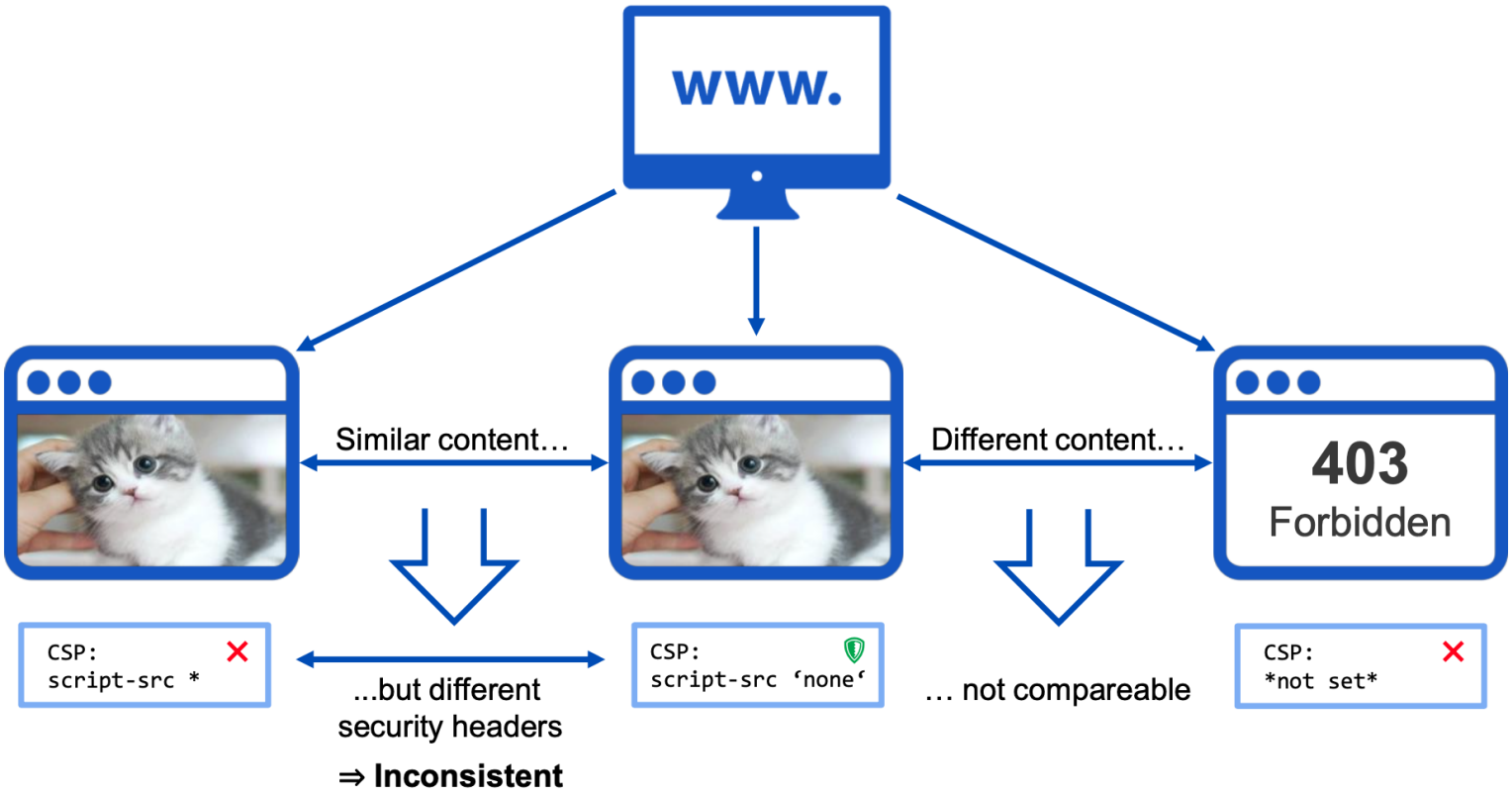
- A web site may set the secure attribute on its session cookies when it is accessed using **Chrome**, but may forget the attribute when it is accessed using **Opera**.
  - Opera users vulnerable to cookie
  - May enable **session hijacking** attacks against a specific user population
- A web site may configure its **content security policy (CSP)** differently when accessed from different countries.
  - e.g., due to the use of different ad networks, and there is no guarantee that all these CSPs enjoy the same security guarantees.
- Security mechanisms might change when sites are accessed from different geolocations.
  - Visitor originates from a specific country or because they rely on a VPN or the Onion network to spoof their **geolocation**

AUGUSTA UNIVERSITY

Motivation


Clickjacking
XFO
Cookie Sec.
CSRF / XSSI
CSP
HSTS
Protection should be **consistent** irrespective of client characteristics
Cross-Site Scripting
HTTP Downgrade

What is an Inconsistency?



AUGUSTA UNIVERSITY

Table of Contents

AUGUSTA UNIVERSITY

Contribution

Authors measured the commonness of inconsistencies in the security policies of top sites across different client characteristics and they quantify their security implications:

- They propose a **data collection methodology**

AUGUSTA UNIVERSITY

Contribution

Authors measured the commonness of inconsistencies in the security policies of top sites across different client characteristics and they quantify their security implications:

- They propose a **data collection methodology**
- They introduce general **definitions of consistency** for clientside security mechanisms

AUGUSTA UNIVERSITY

Contribution

Authors measured the commonness of inconsistencies in the security policies of top sites across different client characteristics and they quantify their security implications:

- They propose a **data collection methodology**
- They introduce general **definitions of consistency** for clientside security mechanisms
- They **apply their definitions to the collected data** and they report on the key findings

AUGUSTA UNIVERSITY

Table of Contents

AUGUSTA UNIVERSITY

Data Collection framework

They propose a data collection methodology to their analysis and they build a dataset of 13,626,145 responses collected from the 10,000 highest-ranking sites by crawling based on the Tranco list of January 1,

1	google.com
2	gtld-servers.net
3	youtube.com
4	facebook.com
5	microsoft.com
6	akamaiedge.net
7	netflix.com
8	twitter.com
9	instagram.com
10	amazonaws.com
11	baidu.com
12	apple.com
13	cloudflare.com
14	a-msedge.net
15	linkedin.com
16	epicgames.com

26	bing.com
27	googletagmanager.com
28	l-msedge.net
29	akadns.net
30	fastly.net
31	wordpress.org
32	cnn.com
33	domaincontrol.com
34	office.com
35	pinterest.com
36	github.com
37	googlevideo.com
38	youtu.be
39	zhihu.com
40	mail.ru
41	whatsapp.com
42	nflxso.net
43	doubleclick.net

55	sharepoint.com
56	wordpress.com
57	goo.gl
58	t-msedge.net
59	googleusercontent.com
60	bit.ly
61	cloudapp.net
62	windows.net
63	apple-dns.net
64	taobao.com
65	edgekey.net
66	myfritz.net
67	csdn.net
68	vk.com
69	blogspot.com
70	aaplimg.com
71	163.com
72	mozilla.org

AUGUSTA UNIVERSITY

Data Collection framework

They identify three factors which users may legitimately manipulate as part of their everyday Web browsing experience, without realizing that they can unintendedly affect Web application security.

Factor	Set of tests	Tests
User-Agent	Windows client	User-Agent header: Chrome 96, Firefox 95, Edge 96, Opera 82
	Linux client	User-Agent header: Chrome 96, Firefox 95, Opera 82
	macOS client	User-Agent header: Chrome 96, Firefox 95, Edge 96, Opera 82, Safari 15.2
	Android client	User-Agent header: Chrome 96, Firefox 95, Opera 96
	iOS client	User-Agent header: Chrome 96, Firefox 95, Edge 86, Safari 15.2
Vantage Point	VPN service	Servers from hidemyass.com - 1 per country (218 countries)
	Onion network	Standard Onion client - 1 end-node per country (49 countries)
Client Configuration	Language	Accept-Language header: en, es, cn, ru, de

Table 1: Selected client conditions that might influence the received security headers

AUGUSTA UNIVERSITY

Table of Contents

AUGUSTA UNIVERSITY

Formalizing Inconsistencies

Authors introduce general definitions of consistency for clientside security mechanisms and they express them to a set of popular defenses available in modern browsers.

- All the responses collected from the **same URL must enforce the same security policies**.

AUGUSTA UNIVERSITY

Formalizing Inconsistencies

Authors introduce general definitions of consistency for clientside security mechanisms and they express them to a set of popular defenses available in modern browsers.

- All the responses collected from the **same URL must enforce the same security policies**.
  - But they consider, two security policies can be syntactically different, yet provide an equivalent level of protection. For example, two syntactically different CSPs may both effectively mitigate the dangers of XSS.

AUGUSTA UNIVERSITY

Formalizing Inconsistencies

Authors introduce general definitions of consistency for clientside security mechanisms and they express them to a set of popular defenses available in modern browsers.

- All the responses collected from the **same URL must enforce the same security policies**.
  - But they consider, two security policies can be syntactically different, yet provide an equivalent level of protection. For example, two syntactically different CSPs may both effectively mitigate the dangers of XSS.
- **Intra-test consistency**: It requires all compatible responses collected within the same test to provide an equivalent level of protection.

AUGUSTA UNIVERSITY

Formalizing Inconsistencies

Authors introduce general definitions of consistency for clientside security mechanisms and they express them to a set of popular defenses available in modern browsers.

- All the responses collected from the **same URL must enforce the same security policies**.
  - But they consider, two security policies can be syntactically different, yet provide an equivalent level of protection. For example, two syntactically different CSPs may both effectively mitigate the dangers of XSS.
- **Intra-test consistency**: It requires all compatible responses collected within the same test to provide an equivalent level of protection.
- **Inter-test consistency**: It requires all compatible responses collected within two different tests (defined for the same factor) to provide an equivalent level of protection.

AUGUSTA UNIVERSITY

Example of consistencies

Consider just two tests for the User-Agent factor: Chrome 96 for Windows and Firefox 95 for Linux. Assume that pages are visited five times for each test and may be classified in two security levels: low (L) and high (H)

Chrome 96	Firefox 95
H,H,H,H,H	H,H,H,H,H
H,H,H,L,H	H,H,H,H,H
H,H,H,H,H	L,L,L,L,L

Table 2: Example observations upon crawling

- First row represents a scenario where Intra-test consistency and inter-test consistency are satisfy.
- Second row represents a scenario where intra-test consistency doesnot hold, hence inter-test consistency is undefined.
- Third row represents a scenario where intra-test consistency is satisfied but inter-test consistency is not.

AUGUSTA UNIVERSITY

Table of Contents

AUGUSTA UNIVERSITY

Measuring Inconsistencies

Authors apply their definitions to the collected data and they report on the key findings. Their measurement shows that a significant fraction of the analyzed Web sites suffers from different types of client-side security inconsistencies.

Mechanism	Usage	# Sites w/ intra-test inconsistencies					# Sites w/ inter-test inconsistencies					# Sites w/ only inter-test inconsistencies				
		UA	Lang.	VPN	Tor	**Any**	UA	Lang.	VPN	Tor	**Any**	UA	Lang.	VPN	Tor	**Any**
Content Security Policy	1,998	12	11	31	23	36	15	-	29	18	47	15	-	11	3	28
- for XSS mitigation	360	1	-	1	1	3	9	-	1	1	10	9	-	1	-	10
- for framing control	1,288	6	5	15	9	16	2	-	16	5	20	2	-	9	1	12
- for TLS enforcement	661	7	7	19	14	22	4	-	12	12	17	4	-	1	2	6
X-Frame-Options	5,692	20	18	43	22	50	7	-	29	13	37	7	-	9	5	20
Strict-Transport-Security	4,562	15	13	28	23	38	8	-	23	16	35	8	-	12	5	22
- w/o page similarity	-	*42*	*33*	*148*	*593*	*693*	*19*	*2*	*576*	*218*	*643*	*17*	*2*	*524*	*20*	*552*
- preload	920	3	3	6	6	10	-	-	9	4	10	-	-	6	-	6
↳ w/o page similarity	-	*5*	*6*	*20*	*113*	*124*	*1*	*1*	*124*	*48*	*137*	*1*	*1*	*117*	*2*	*119*
Cookie Security	3,876	10	9	11	12	16	150	1	13	8	167	149	1	9	2	160
- Secure attribute	2,937	4	4	5	6	8	144	-	8	3	152	144	-	7	1	151
- SameSite attribute	788	5	5	5	6	7	6	1	4	4	14	6	1	2	-	9
- HttpOnly attribute	3,104	1	-	2	2	3	2	-	3	2	6	2	-	2	1	5
Any	8,174	51	44	103	75	127	177	1	82	49	267	174	1	34	12	194
Any (incl. HSTS w/o similarity)	*8,174*	*77*	*64*	*222*	*634*	*765*	*188*	*3*	*631*	*252*	*833*	*183*	*3*	*541*	*26*	*429*

Table 4: Detected intra-test and inter-test inconsistencies by factor (321 sites in total). We present the numbers with and without page similarity for HSTS to highlight the impact of this choice on the measurement.

Measuring Inconsistencies

Overview of overlap with additional snapshots of their analysis.

Mechanism	Usage	# Sites w/ intra-test inconsistencies					# Sites w/ inter-test inconsistencies					# Sites w/ only inter-test inconsistencies				
		UA	Lang.	VPN	Tor	**Any**	UA	Lang.	VPN	Tor	**Any**	UA	Lang.	VPN	Tor	**Any**
Intersection of January 2 and January 6																
Content Security Policy	1,987	7	4	27	18	29	15	-	25	15	43	15	-	8	4	27
- for XSS mitigation	357	1	-	-	1	2	9	-	1	1	10	9	-	1	-	10
- for framing control	1,281	3	3	14	7	14	2	-	13	5	17	2	-	6	2	10
- for TLS enforcement	659	4	1	16	11	17	4	-	11	9	16	4	-	1	2	7
X-Frame-Options	5,662	15	13	35	17	44	7	-	22	7	30	7	-	7	2	15
Strict-Transport-Security	4,553	13	12	23	17	30	8	-	17	9	28	8	-	9	3	19
w/o page similarity	-	*37*	*23*	*75*	*322*	*394*	*18*	*2*	*515*	*145*	*583*	*17*	*2*	*489*	*27*	*520*
- preload	918	3	3	6	6	10	-	-	8	3	9	-	-	6	-	6
↳ w/o page similarity	-	*5*	*4*	*12*	*59*	*67*	*1*	*1*	*115*	*29*	*129*	*1*	*1*	*109*	*4*	*112*
Cookie Security	3,836	9	7	10	11	15	147	1	9	4	158	147	1	8	1	156
- Secure attribute	2,907	4	2	5	6	8	142	-	6	3	148	142	-	6	1	148
- SameSite attribute	777	5	5	5	5	7	5	1	3	1	10	5	1	2	-	8
- HttpOnly attribute	3,069	-	-	1	1	2	2	-	2	1	4	2	-	2	-	4
Any	8,145	39	31	86	59	100	174	1	64	30	244	172	1	26	8	191
Intersection of January 2 and January 10																
Content Security Policy	1,986	9	4	27	18	30	15	-	26	16	43	15	-	10	4	29
- for XSS mitigation	354	-	-	-	1	2	9	-	1	1	10	9	-	1	-	10
- for framing control	1,285	5	3	15	8	15	2	-	14	5	18	2	-	7	1	10
- for TLS enforcement	658	5	1	16	10	18	4	-	11	10	15	4	-	2	3	9
X-Frame-Options	5,654	14	12	35	19	43	7	-	20	12	30	7	-	6	5	17
Strict-Transport-Security	4,549	12	12	21	16	30	8	-	17	9	27	8	-	10	4	20
w/o page similarity	-	*32*	*24*	*77*	*370*	*443*	*18*	*2*	*512*	*139*	*573*	*17*	*2*	*480*	*18*	*503*
- preload	914	2	3	5	5	9	-	-	8	4	9	-	-	6	1	7
↳ w/o page similarity	-	*4*	*4*	*11*	*71*	*81*	*1*	*1*	*114*	*28*	*130*	*1*	*1*	*108*	*3*	*112*
Cookie Security	3,841	10	8	11	10	16	147	1	10	4	159	146	1	7	1	154
- Secure attribute	2,914	4	3	5	5	8	141	-	6	3	147	141	-	5	1	146
- SameSite attribute	781	5	5	5	5	7	6	1	4	1	12	6	1	2	-	9
- HttpOnly attribute	3,075	1	-	2	1	3	2	-	2	1	4	2	-	2	-	4
Any	8,142	39	30	86	58	100	174	1	66	35	244	173	1	29	12	194
Intersection of January 2 and January 14																
Content Security Policy	1,985	8	5	26	20	31	15	-	26	16	43	15	-	10	4	29
- for XSS mitigation	359	-	-	-	1	1	9	-	1	1	10	9	-	1	-	10
- for framing control	1,278	5	2	15	8	16	2	-	13	5	17	2	-	6	2	10
- for TLS enforcement	659	4	3	15	12	18	4	-	12	10	16	4	-	3	2	9
X-Frame-Options	5,654	14	8	32	18	38	6	-	18	11	26	6	-	7	5	15
Strict-Transport-Security	4,548	12	10	19	17	26	7	-	15	7	24	7	-	11	2	19
w/o page similarity	-	*33*	*22*	*65*	*369*	*424*	*17*	*2*	*535*	*136*	*595*	*16*	*2*	*512*	*20*	*535*
- preload	913	3	2	5	6	9	-	-	8	4	9	-	-	6	-	6
↳ w/o page similarity	-	*5*	*5*	*10*	*66*	*73*	*1*	*1*	*119*	*29*	*131*	*1*	*1*	*114*	*2*	*116*
Cookie Security	3,825	10	9	11	11	16	148	1	11	4	161	147	1	9	1	157
- Secure attribute	2,897	4	4	5	6	8	143	-	8	3	151	143	-	7	1	150
- SameSite attribute	778	5	5	5	5	7	5	1	3	1	10	5	1	2	-	8
- HttpOnly attribute	3,066	1	-	2	1	3	2	-	2	1	4	2	-	2	-	4
Any	8,135	38	27	79	61	96	174	1	61	33	239	173	1	31	10	194

Table 6: Overview of overlap with additional snapshots of our analysis

AUGUSTA UNIVERSITY

Disclosure Email

Authors sent email to the respective site operator, contained information about their institutions, as well as a detailed description of the individual inconsistent headers and how they were collected.

```
Hello,

We are a team of security researchers from the CISPA Helmholtz
↪  Center for Information Security located in Saarland, Germany
↪  and Università Ca' Foscari Venezia, Italy. In our current
↪  research project, we investigate inconsistent behavior in the
↪  deployment of security headers for Web applications.

For that, we have visited your site through different vantage
↪  points (VPN and Tor) as well as with different configurations
↪  (User-Agents and Accept-Language request headers).

In our automated tests, we detected both non-deterministic
↪  differences (e.g., we received different levels of security
↪  even with the same user agent) or those differences which
↪  seemed related to the vantage point or configuration.

We would like to raise your attention to one of those
↪  inconsistencies that occurred on <DOMAIN>:
<DETAILS_ABOUT_INCONSISTENCY>

We would appreciate if you can check the reason for the issue,
↪  address it to ensure consistent security, and also let us know
↪  about what such a reason might have been, since this will allow
↪  us to better help others in the future.

If you have any questions or need further information, please do
↪  not hesitate to contact us by answering this email.
```

- In total, they sent out 256 emails.
- They only got 21 response
- Seven operators asked them to provide more details

AUGUSTA UNIVERSITY

Table of Contents

AUGUSTA UNIVERSITY

Conclusion

- This paper investigated the inconsistent configuration of client-side security mechanisms on top sites.
- Client-side security is not equally delivered to all clients!
  - 321 Sites had some security inconsistencies!
- Authors observed that Inter-test inconsistencies across network access methods might arise due to misconfigured origin server for specific geolocations.

AUGUSTA UNIVERSITY

Thank You!

AUGUSTA UNIVERSITY