

HTTP security headers

[SAMPLE CONTENT]



Harden all the things



Who this?

- Developer 🧑💻
- DevOps engineer (ex SRE) 🧑💻
- Security engineer 🧑💻
- Hacks on various open source projects 💾
- Runs a 42U rack and K8s PaaS from his living room 🤖
- Worked in IT ~10y 🧑💼
- #improviser #maker #soldier
#blueteamer #bookworm

What this about?

- security headers... what?
- introduction to available security headers
- you, implementing security headers in your projects, hence...
- ...making the web safer

Logistics

- ~1.5h of theory
- <break>
- ~2.5h of lab-work
- questions ad hoc



SECURITY... HEADERS?



HTTP Basics

Request (your browser sends)

GET / HTTP/1.1

Host: improv.ee

User-Agent: Mozilla/5.0 (X11; Linux x86_64)

Cookie: PHPSESSID=a63cce092fa12

Accept: text/html,application/xhtml+xml,application/xml

HTTP Basics

Response (server replies)

```
HTTP/1.1 200 OK
Content-Type: text/html
Referrer-Policy: origin
Server: Apache2
```

HTTP HEADERS (METADATA)

SECURITY HEADER

```
<!doctype html>
<html lang="et">
<head>
<meta charset="utf-8">
...
```

EMPTY LINE

HTTP RESPONSE BODY



OVERVIEW OF HEADERS

HSTS - HTTP Strict Transport Security

— “Always use HTTPS on this domain”

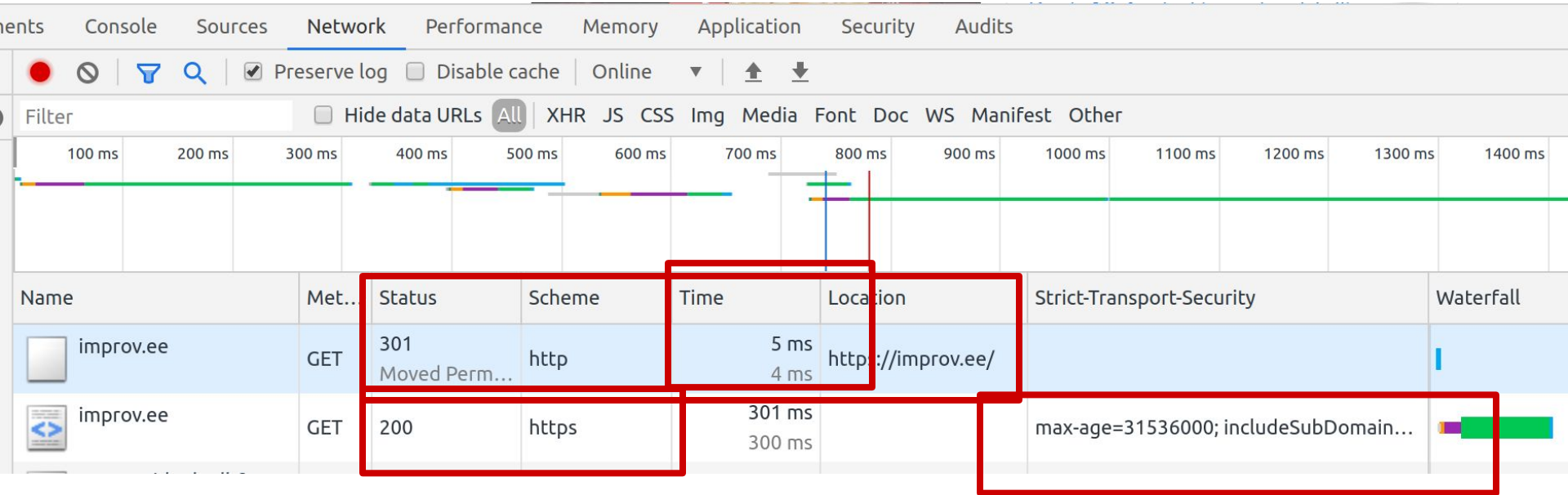


```
Strict-Transport-Security: max-age=31536000;  
                           includeSubDomains;  
                           preload
```

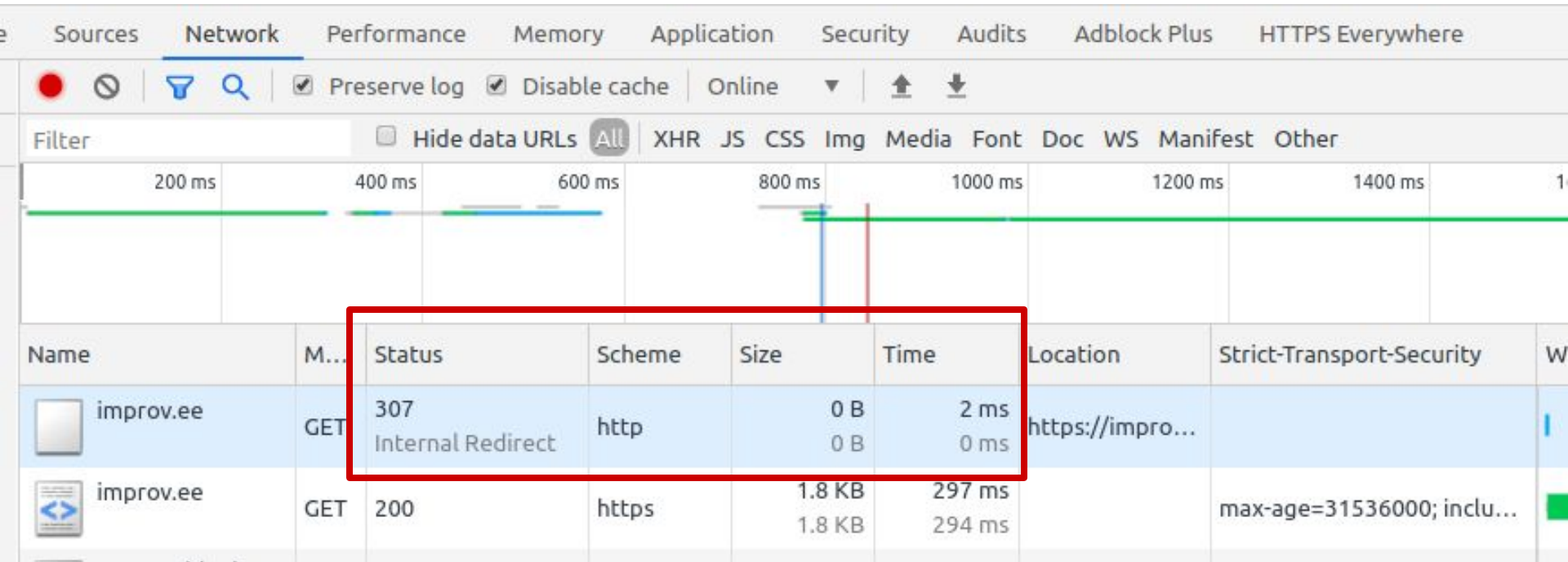
HSTS

- Forces browsers to use only HTTPS (no initial HTTP -> HTTPS redirect)
- Browsers “remember” this setting ^(careful!) for `max-age`
- Can cascade to subdomains
- Browsers today still default to HTTP 😭

HSTS - first visit






HSTS - next visit



HSTS and the TOFU problem

- Q: “How can I enforce HTTPS, when a client does the first ever connection to my domain?”

Name	Method	Status	Scheme	Time	Location	Strict-Transport-Security
 private www.swedbank.ee	GET	302 Found	http	21 ms 19 ms	https://www.swedbank.ee/private	
 private www.swedbank.ee	GET	200 OK	https	132 ms 129 ms		max-age=31536000; includeSubDomains
 shared-styles.min		200		16 ms		

- A: “By hardcoding your domain as HTTPS to the browser itself”



all ▾ (search all code)

[chromium] //src/net/http/transport_security_state_static.json

Files

transport_security_state_static.json

http_security_headers_hsts_fuzzer.cc
http_security_headers_unittest.cc
http_server_properties.cc
http_server_properties.h
http_server_properties_manager.cc
http_server_properties_manager.h
http_server_properties_manager_unittest.cc
http_server_properties_unittest.cc
http_status_code.cc
http_status_code.h
http_status_code_list.h
http_status_code_unittest.cc
http_stream.h
http_stream_factory.cc
http_stream_factory.h
http_stream_factory_job.cc
http_stream_factory_job.h
http_stream_factory_job_controller.cc
http_stream_factory_job_controller.h
http_stream_factory_job_controller_unittest.cc
http_stream_factory_test_util.cc
http_stream_factory_test_util.h
http_stream_factory_unittest.cc
http_stream_properties.cc

```
1 // Copyright (c) 2012 The Chromium Authors. All rights reserved.  
2 // Use of this source code is governed by a BSD-style license that can be  
3 // found in the LICENSE file.  
4  
5 // This file contains the HSTS preloaded list in a machine readable format.  
6  
7 // The top-level element is a dictionary with two keys: "pinsets" maps details  
8 // of certificate pinning to a name and "entries" contains the HSTS details for  
9 // each host.  
10 //  
11 // "pinsets" is a list of objects. Each object has the following members:  
12 //   name: (string) the name of the pinset  
13 //   static_spki_hashes: (list of strings) the set of allowed SPKIs hashes  
14 //   bad_static_spki_hashes: (optional list of strings) the set of forbidden  
15 //     SPKIs hashes  
16 //   report_uri: (optional string) the URI to send violation reports to;  
17 //     reports will be in the format defined in RFC 7469  
18 //  
19 // For a given pinset, a certificate is accepted if at least one of the  
20 // "static_spki_hashes" SPKIs is found in the chain and none of the  
21 // "bad_static_spki_hashes" SPKIs are. SPKIs are specified as names, which must  
22 // match up with the file of certificates.  
23 //  
24 // "entries" is a list of objects. Each object has the following members:  
25 //   name: (string) the DNS name of the host in question.  
26 //   policy: (string) the policy under which the domain is part of the  
27 //     preloaded list. This field is used for list maintenance.  
28 //   test_domain: (string) the domain used for testing.
```



```
{ "name": "memo.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "salon1.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "tiny.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "antraxx.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "reisenbauer.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "kselenia.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "koolitee.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "sisseastumine.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "taskutark.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "arinde.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "bug.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "elevator.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "localhost.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "kooliveeb.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "kovehitus.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "liz.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "smiit.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "kooli.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "daylight-dream.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "digideli.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "seadus.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "tambre.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "improfestival.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "mana.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "toomy.pri.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "gunn.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "prospecto.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "spacebear.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "loli.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "bgp.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
{ "name": "greenpaws.ee", "policy": "bulk-1-year", "mode": "force-https", "include_subdomains": true },
```

Enter a domain:

veriff.com

Check HSTS preload status and eligibility

Status: veriff.com is not preloaded.

Eligibility: In order for veriff.com to be eligible for preloading, the errors below must be resolved:

✖ Error: No HSTS header

Response error: No HSTS header is present on the response.

HSTS preload requirements

- HTTPS supported
- Valid certificate
- Redirect from HTTP -> HTTPS
- All subdomains support HTTPS
- HSTS header on the base domain
 - Max age at least a year
 - Preload and includeSubdomains set (applies to ALL subdomains)
- Requirements must stay satisfied at all times

HSTS and redirections

[HTTP://IMPROV.EE](http://IMPROV.EE)

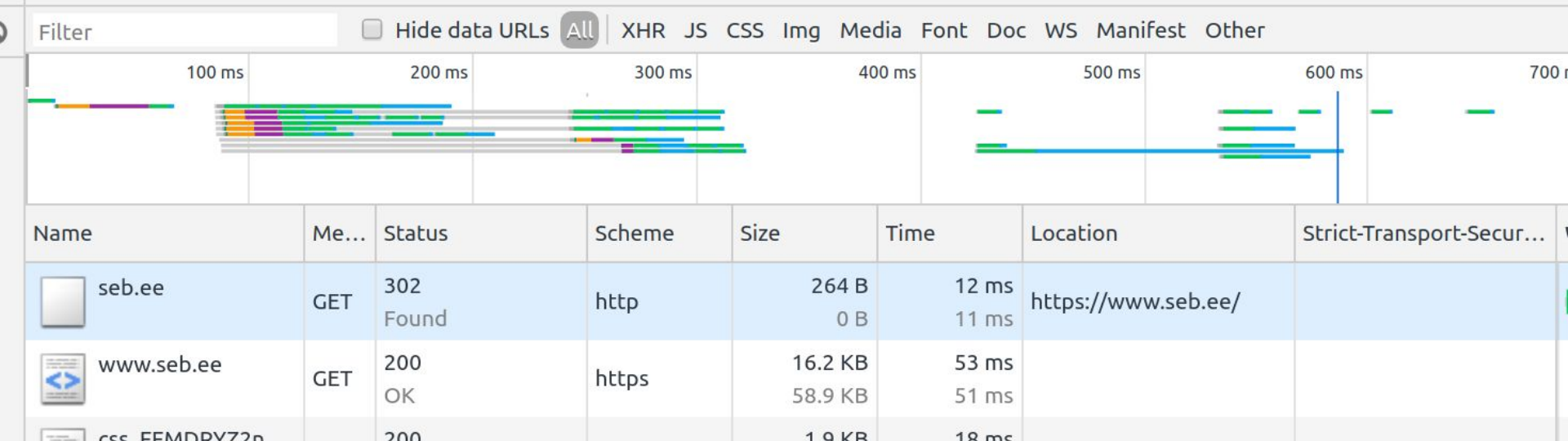


[HTTPS://IMPROV.EE](https://IMPROV.EE) → (SET HSTS FOR IMPROV.EE)



[HTTPS://IMPROV.EU](https://IMPROV.EU) → (SET HSTS FOR IMPROV.EU)




HSTS - what could be better?



No HSTS whatsoever. Why SEB, why?! 🤔

** I am a customer*

HSTS - what could be better?

Name	Method	Status	Scheme	Time	Location	Strict-Transport-Security
 swedbank.ee	GET	302 Found	http	277 ms 275 ms	https://www.swedbank.ee/	
 www.swedbank.ee	GET	302 Found	https	521 ms 520 ms	https://www.swedbank.ee/private	
 private www.swedbank.ee	GET	200 OK	https	123 ms 120 ms		max-age=31536000; includeSubDomains


HSTS is set, but not preloaded. Redirection incorrect. 🙄

** I am a customer*

Why use HSTS

- People won't type https:// into browsers
 - Browsers default to HTTP (no encryption)
 - 1st request will be unencrypted
- Protection against network attacks
 - Attacker in your network path can MitM your redirect
- Performance
 - No 1st redirect - saves load time


(some) cookies are sent with the first request



Väikelaenukuvade galeria

Lisaks tavajärgsele Väikelaenule pakume ka auto või muu mootorsõiduki soetamiseks Autolaenu, kodu remondiks või sisustamiseks Remondilaenu.


[Loen edasi](#)



Rahaasjade ajamiseks pole enam vaja pangakontoris tulla

SEB pakub video teel nii terviknõustamisi kui ka kontode avamist läbisele või ettevõttele.

[Loen edasi](#)



Kindlustuslahendus, mis suurendab Teie pere majanduslikku turvatunnet

Pisava rahapuhvri kogumine ettenägematute sündmuste tarbeks võib võtta oodatust kauem aega. Seevastu elukindlustus annab Teile ja lähedastele keerulises olukorras majandusliku kindlustunde kohe.

[Loen edasi](#)

Logige sisse

Erakliendina

Kasutajatunnus

☐ Smart-ID ☐ Mobiil-ID ☒ ID-kaart ☐ Kood

[Sisenen internetipanka](#)

Kontakt

Klienditugi

Elements Console Sources Network Performance Memory Application Security Audits

Search x [red] [blue] [magnifying glass] [checkbox] Preserve log [checked] Disable cache Online [up] [down]

Aa .* [refresh] [back] Filter [checkbox] Hide data URLs [All] XHR JS CSS Img Media Font Doc WS Manifest Other

Name	Headers	Preview	Response	Cookies	Timing
seb.ee	Response Headers (8)				
www.seb.ee	Request Headers				
css_FFMDRYZ2nSV6HGDyDVPm9...	/sites/default/files/css				
css_NOF5k04fomYwgxL1Y-h6w0v...	/sites/default/files/css				
css_T5FpHa12-tChU448_v_8A7I68...	/sites/default/files/css				
css_y6gHrpgNJCYaMb_J8YF1dPQ...	/sites/default/files/css				
styles_content_desktop.css?08740...					

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9,et;q=0.8,en-GB;q=0.7

Cache-Control: no-cache

Connection: keep-alive

Cookie: responsive=default; s_fid=7925A3B3EE130791-05AD46C4422C261D; s_cc=true

DNT: 1

Host: seb.ee

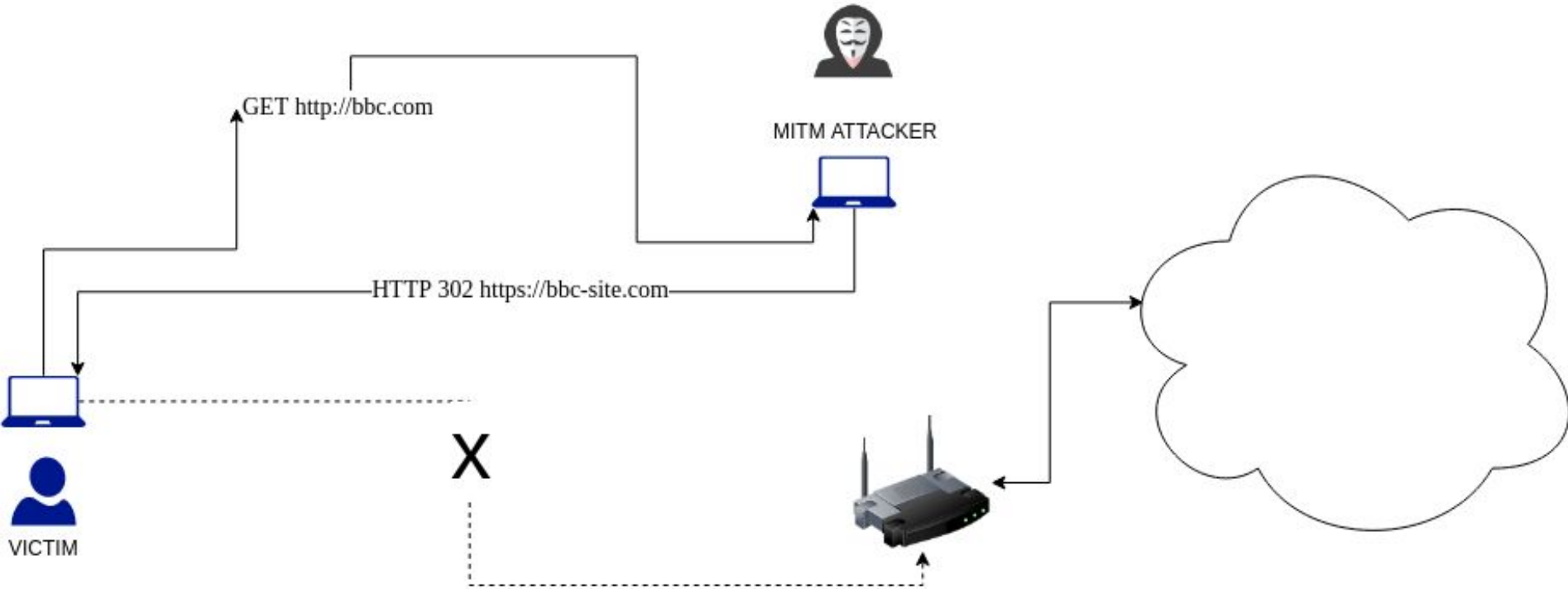
Pragma: no-cache

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36

56 requests 2.1 MB transferred 3.7 M

attacker in network path can hijack the page



HSTS





CAN I USE?

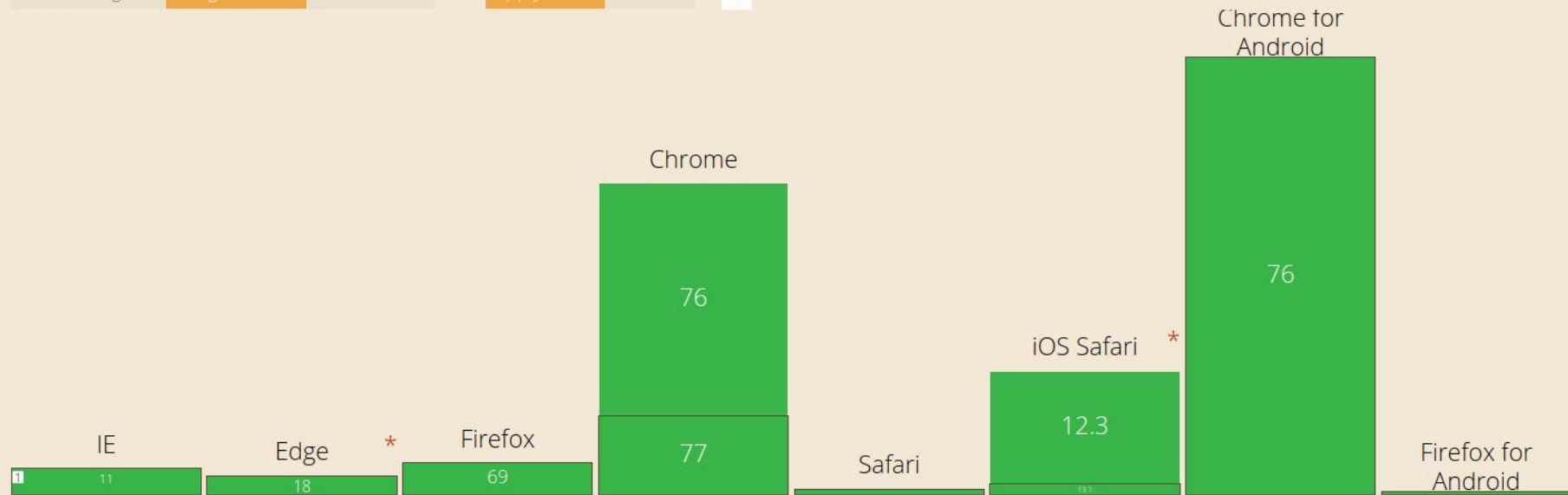
Strict Transport Security - OTHER

Usage % of all users

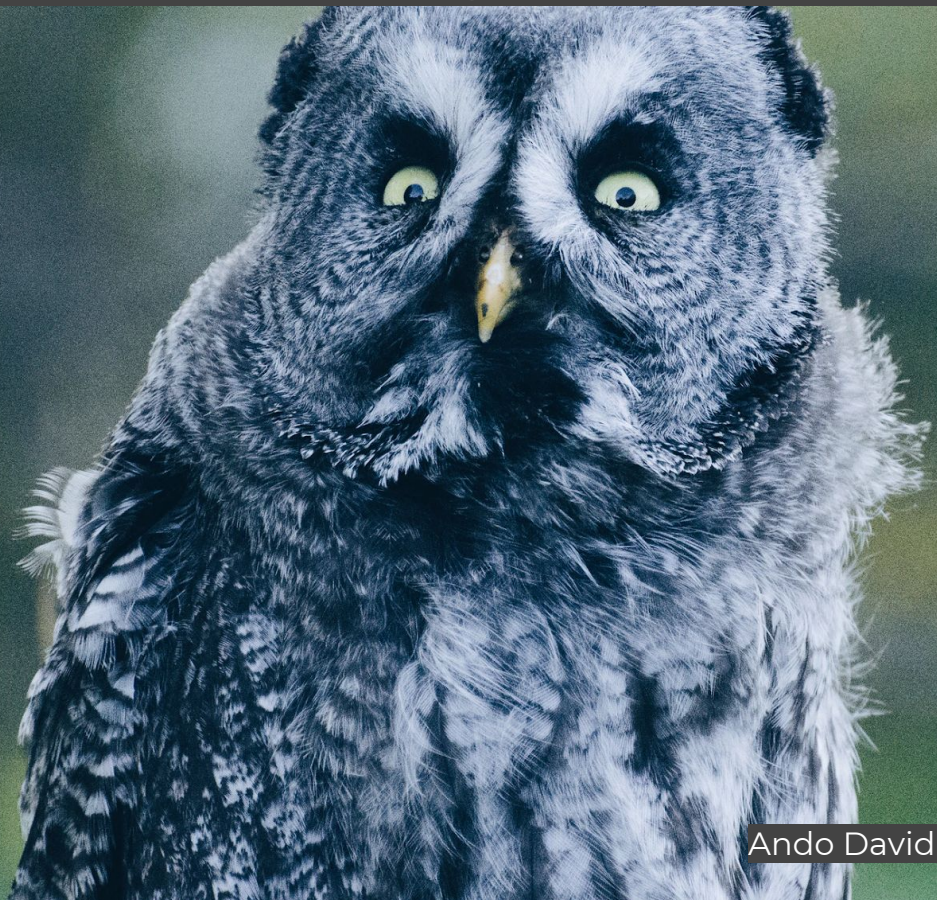
Global 95.54%

Declare that a website is only accessible over a secure connection (HTTPS).

Current aligned Usage relative Date relative Apply filters Show all ?



HTTP security headers



Questions?

Ando David Roots | @SQRooted | sqroot.eu

Credits

- Images
 - Unsplash
 - Mozilla
 - CanIUse
 - <https://carbon.now.sh>