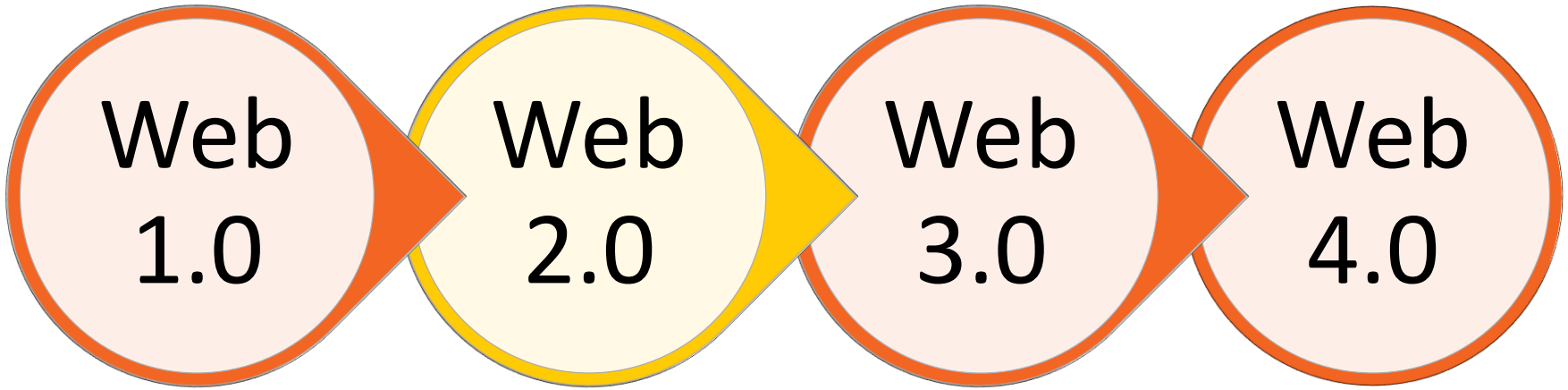
SRK

# COOKIE SECURITY

## HUNCERT WOKRSHOP -2019

R. KISS SÁNDOR

# INTRODUCTION




CONCEPT / BUSINESS MODEL / TECHNOLOGY

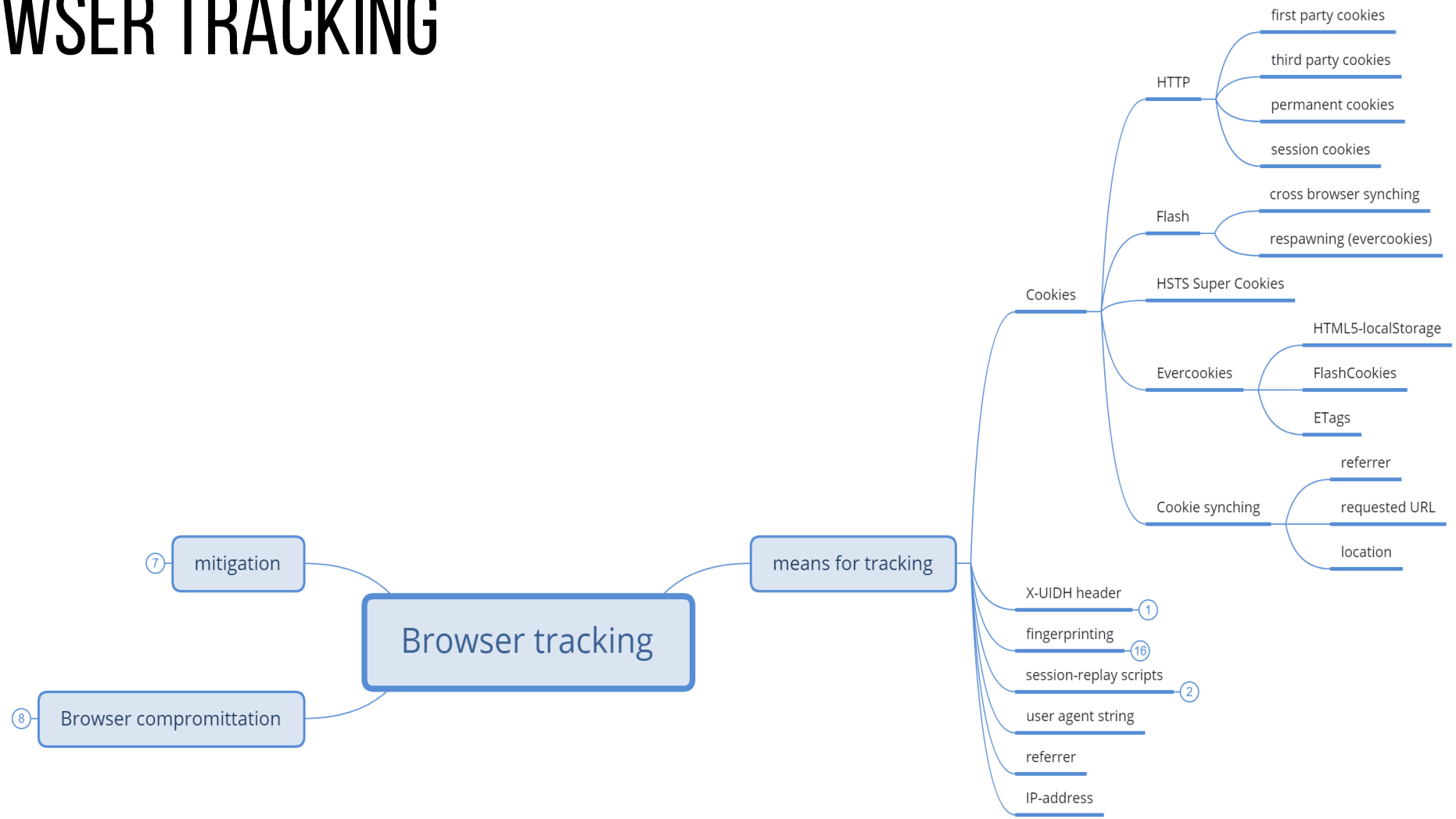
# INTRODUCTION

- HTTP cookie / web cookie / internet cookie / browser cookie
- stateless vs stateful
- session cookie
  - authentication cookies
- persistent cookie
  - tracking cookies
- 3rd party cookie
  - tracking cookies

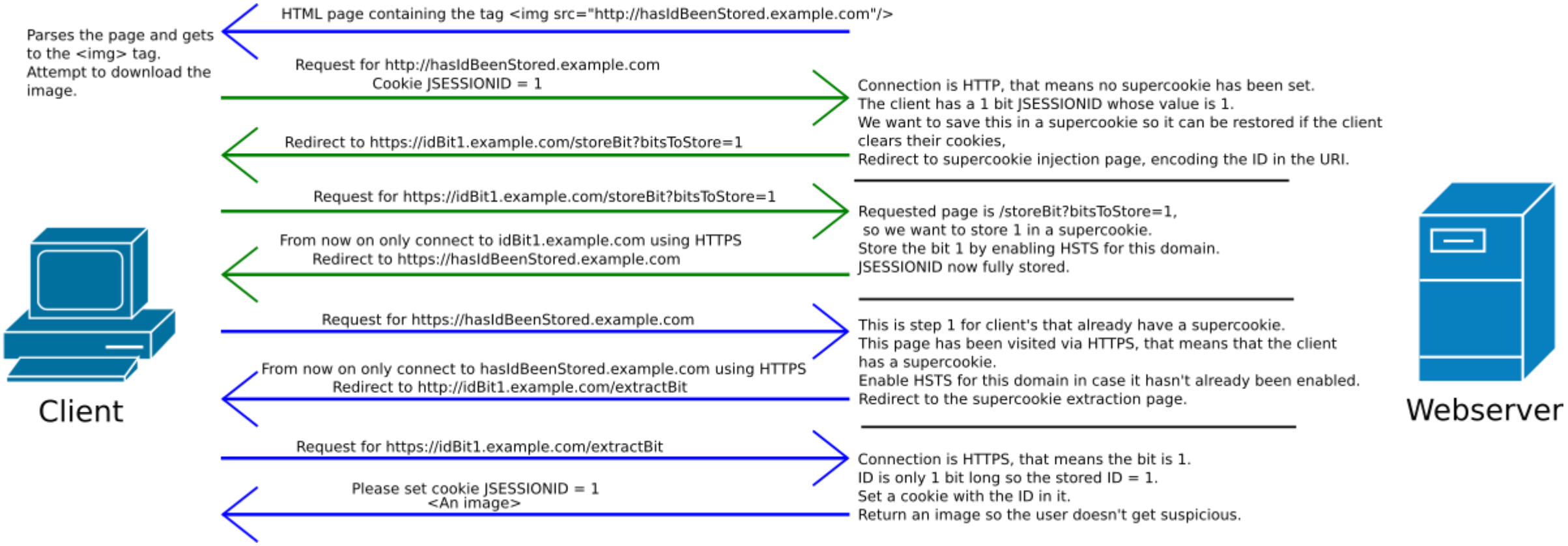
# COOKIE ATTRIBUTES

```
Set-Cookie: <cookie-name>=<cookie-value>
Set-Cookie: <cookie-name>=<cookie-value>; Expires=<date>
Set-Cookie: <cookie-name>=<cookie-value>; Max-Age=<non-zero-digit>
Set-Cookie: <cookie-name>=<cookie-value>; Domain=<domain-value>
Set-Cookie: <cookie-name>=<cookie-value>; Path=<path-value>
Set-Cookie: <cookie-name>=<cookie-value>; Secure=<true> or <false>
Set-Cookie: <cookie-name>=<cookie-value>; HttpOnly=<true> or <false>
Set-Cookie: <cookie-name>=<cookie-value>; SameSite=Strict
Set-Cookie: <cookie-name>=<cookie-value>; SameSite=Lax
```

# BROWSER TRACKING



# HSTS SUPER COOKIES



# THREATS

- Confidentiality, Integrity aren’t provided by default
- Attack vectors
  - Cookie poisoning
  - Cookie hijacking / stealing
    - Network eavesdropping
    - DNS poisoning
    - XSS
    - CSRF
  - Information leakage

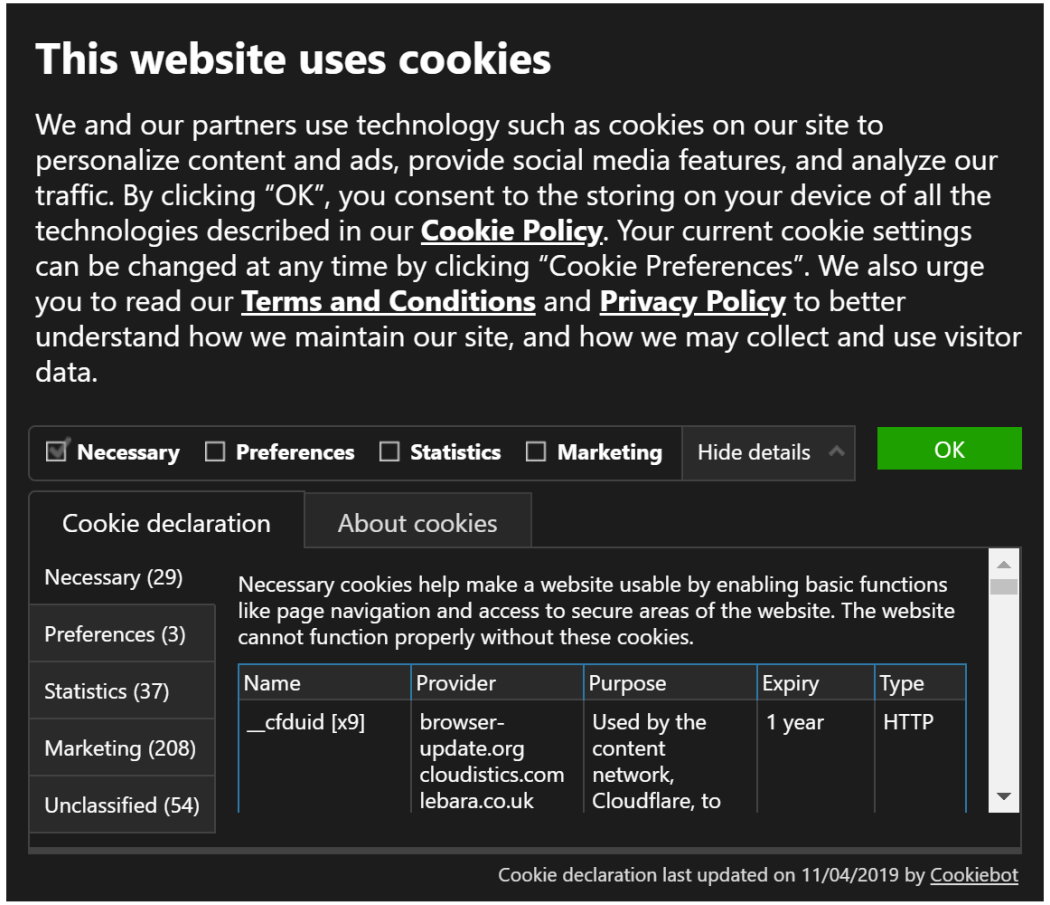
# MITIGATION

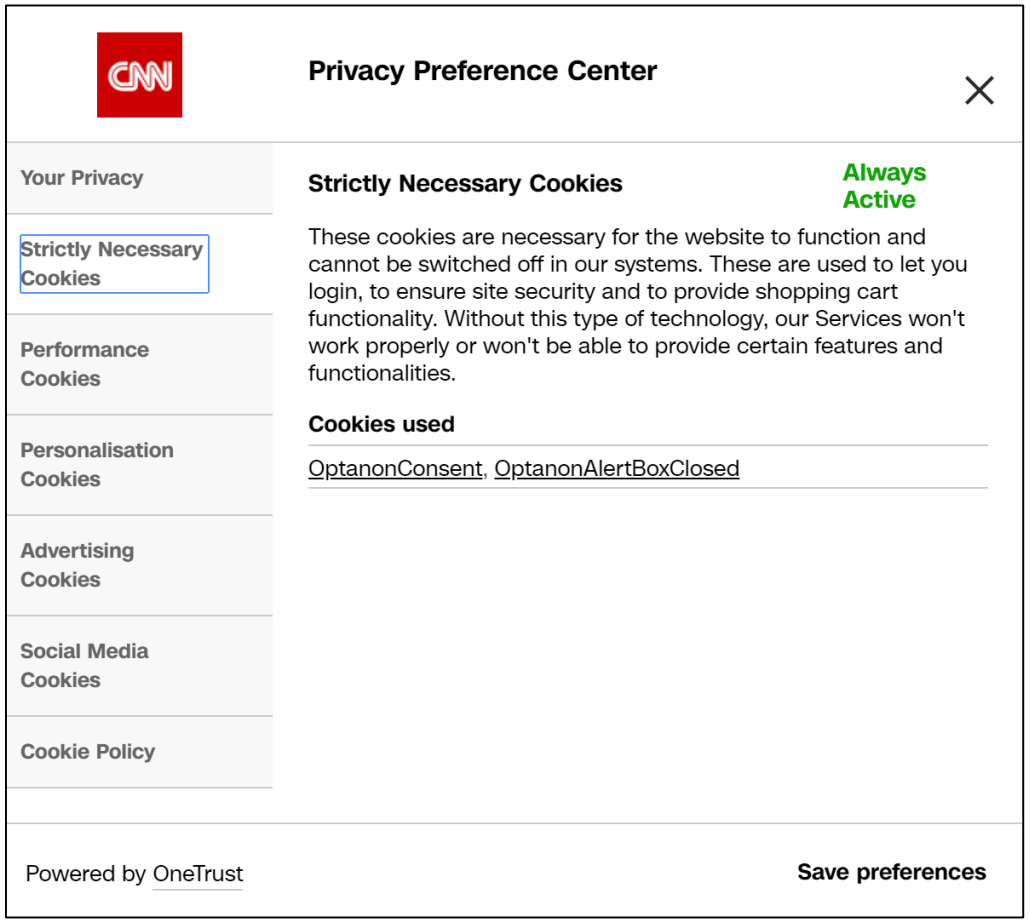
- ‘Secure’ flag
- HttpOnly flag
- Scope limitation
  - Domain attribute
  - Path attribute
  - Samesite attribute
- SessionID: high entropy

# COOKIES VS GDPR & EPR

- If individual can be identified by data → personal data
- Requirements:
  - Informing individual
  - Consent
    - Obtaining consent is prior to data processing
    - Withdrawable
    - Documented
  - Right to be forgotten
- https://www.cookiebot.com/en/

# EXAMPLES


This website uses cookies
We and our partners use technology such as cookies on our site to personalize content and ads, provide social media features, and analyze our traffic. By clicking "OK", you consent to the storing on your device of all the technologies described in our Cookie Policy. Your current cookie settings can be changed at any time by clicking "Cookie Preferences". We also urge you to read our Terms and Conditions and Privacy Policy to better understand how we maintain our site, and how we may collect and use visitor data.
Necessary
Preferences
Statistics
Marketing
Hide details
OK
Cookie declaration
About cookies
Necessary (29)
Preferences (3)
Statistics (37)
Marketing (208)
Unclassified (54)
Necessary cookies help make a website usable by enabling basic functions like page navigation and access to secure areas of the website. The website cannot function properly without these cookies.
Name
Provider
Purpose
Expiry
Type
__cfduid [x9]
browser-update.org cloudistics.com lebara.co.uk
Used by the content network, Cloudflare, to
1 year
HTTP
Cookie declaration last updated on 11/04/2019 by Cookiebot


Privacy Preference Center
Your Privacy
Strictly Necessary Cookies
Performance Cookies
Personalisation Cookies
Advertising Cookies
Social Media Cookies
Cookie Policy
Strictly Necessary Cookies
Always Active
These cookies are necessary for the website to function and cannot be switched off in our systems. These are used to let you login, to ensure site security and to provide shopping cart functionality. Without this type of technology, our Services won't work properly or won't be able to provide certain features and functionalities.
Cookies used
OptanonConsent, OptanonAlertBoxClosed
Powered by OneTrust
Save preferences

# SOURCES


- Takács Gergely – Browser Tracking presentation
- https://flatworldbusiness.wordpress.com/flat-education/previously/web-1-0-vs-web-2-0-vs-web-3-0-a-bird-eye-on-the-definition/
- https://jyx.jyu.fi/bitstream/handle/123456789/59084/1/URN%3ANBN%3Afi%3Ajyu-201808023720.pdf
- https://nakedsecurity.sophos.com/2018/03/20/apple-burns-the-hsts-super-cookie/
- http://www.e2college.com/blogs/web_security/cookie_related_security_threats.html
- https://www.troyhunt.com/understanding-http-strict-transport/
- https://nakedsecurity.sophos.com/2015/02/02/anatomy-of-a-browser-dilemma-how-hsts-supercookies-make-you-choose-between-privacy-or-security/
- https://github.com/ben174/hsts-cookie
- https://www.owasp.org/images/a/a0/OWASPLondon20171130_Cookie_Security_Myths_Misconceptions_David_Johansson.pdf