COOKIE SECURITY

HUNCERT WORKSHOP - 2019
R. KISS SÁNDOR

Except where otherwise noted, this work is licensed under:
http://creativecommons.org/licenses/by/3.0
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

Browser tracking

- means for tracking
  - HTTP
    - first party cookies
    - third party cookies
    - permanent cookies
    - session cookies
    - cross browser synching
    - respawnning (evercookies)
  - Flash
  - HSTS Super Cookies
  - HTML5-localStorage
  - Evercookies
  - FlashCookies
  - ETags
  - referrer
  - requested URL
  - location
- mitigation
  - Browser compromittation
  - X-UIDH header
  - fingerprinting
  - session-replay scripts
  - user agent string
  - referrer
  - IP-address
HSTS SUPER COOKIES

parses the page and gets to the `<img>` tag. Attempt to download the image.

HTML page containing the tag `<img src="http://hasIdBeenStored.example.com"/>`

Request for `http://hasIdBeenStored.example.com`  
Cookie JSESSIONID = 1

Connection is HTTP, that means no supercookie has been set. The client has a 1 bit JSESSIONID whose value is 1.
We want to save this in a supercookie so it can be restored if the client clears their cookies,
Redirect to supercookie injection page, encoding the ID in the URI.

Redirect to `https://idBit1.example.com/storeBit?bitsToStore=1`

Request for `https://idBit1.example.com/storeBit?bitsToStore=1`

Requested page is `/storeBit?bitsToStore=1`, so we want to store 1 in a supercookie. Store the bit 1 by enabling HSTS for this domain. JSESSIONID now fully stored.

From now on only connect to `idBit1.example.com` using HTTPS  
Redirect to `https://hasIdBeenStored.example.com`

This is step 1 for client’s that already have a supercookie. This page has been visited via HTTPS, that means that the client has a supercookie. Enable HSTS for this domain in case it hasn’t already been enabled.
Redirect to the supercookie extraction page.

Request for `https://hasIdBeenStored.example.com`  
From now on only connect to `hasIdBeenStored.example.com` using HTTPS  
Redirect to `http://idBit1.example.com/extractBit`

Connection is HTTPS, that means the bit is 1. ID is only 1 bit long so the stored ID = 1.
Set a cookie with the ID in it.
Return an image so the user doesn’t get suspicious.

Please set cookie JSESSIONID = 1  
<An image>
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/
EXEMPLARY

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.

Privacy Preference Center

Strictly Necessary Cookies

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
• 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