

## Session 6

### (Third party cookies, super cookies)

#### HTTP Protocol

HTTP (Hypertext Transfer Protocol) a protocol on application-level. HTTP is designed for distributed, collaborative, and hypermedia systems. HTTP is used for data communication on the Internet. HTTP is based on TCP/IP. TCP/IP consists of TCP (Transmission Control Protocol) and IP (Internet Protocol). These two protocols are distinct network protocols. Protocol is a set of procedures and rules. Protocols allow computers to understand each other and exchanging data. Web browsers and web servers communicate with TCP/IP. Messages or files that are transmitted over Internet, are divided into packets by TCP. The packets are reassembled when the destination is reached. IP takes care that the packets are sent to desired destination. TCP/IP functions on four layers: Datalink layer, Networking layer, Transport layer, and Application layer. Datalink layer includes on a link operating methods and protocols. The link is a network component to interconnect hosts. Networking layer connects network boundaries and independent networks to transport data packets. Communication between hosts is handled by Transport layer.

Flow control, reliability, and multiplexing are Transport layer's responsibilities. Applications' data exchange is standardized on Application layer. Construction and transmission of clients' data is specified in HTTP specification. Also, the way servers respond to clients' requests is specified in HTTP specification. HTTP consists of three features. First, HTTP request is initiated by HTTP client (for an example browser) to a server. The client is disconnected from the server after making the request. The client waits for server's response. The request is processed by the server and the connection between the server and the client is re-established and a response is sent. The disconnection after initiating a request means that HTTP is connectionless. Next, all types of data can be sent by HTTP. Although, it is required that the client and the server can handle the content of the data. This means that HTTP is media independent. HTTP being connectionless results in HTTP being stateless. Awareness between server and client is present during current requests. HTTP is based on request/response. HTTP is based on client/server architecture. Requests are sent to servers by clients over TCP/IP connection. The requests are sent in a form of a request method, URI, and protocol version. This information is followed by message that includes request modifiers, client information, and possible body content. The request is responded by the server. The response includes protocol version of the message, a success or error code, server information message, entity meta information, and possibly content of entity-body. (Tutorials Point.) HTTP identifies resources and establish connections by using URI (Uniform Resource Identifier). HTTP messages are passed after establishing the connection. The messages are client's requests to server and server's responses to client. URIs are strings that include name, location, or other resource identifiers.

## All you need to know about Third-Party Cookies:

Third-party cookies are cookies that are set by a website other than the one you are currently on. For example, you can have a "Like" button on your website which will store a cookie on visitor's computer, that cookie can later be accessed by Facebook to identify visitor and see which websites he visited. Such cookie is considered to be a **third-party cookie**.

Another example would be an advertising service (ex: AdSense) which also creates a third-party cookie to monitor which websites were visited by each user.

Read on to learn more about third-party cookies and why these may soon be disappearing from the web.

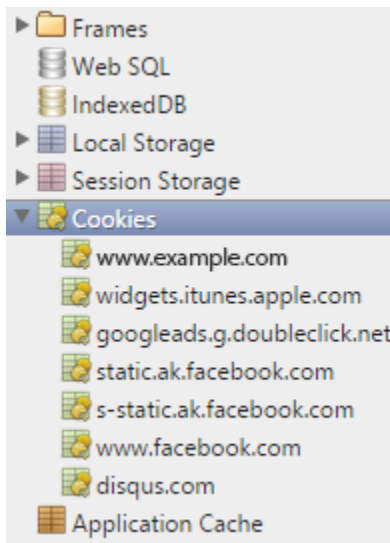
## How to Tell if a Website Uses Third-Party Cookies

You can check if website uses **third-party cookies** in any modern browser. Instructions vary in different browsers.

In Google Chrome, do the following:

- Press F12 to open Developer Tools (or right-click on the page and choose Inspect Element)
- In Developer Tools choose the Application tab
- On the left, double-click the Cookies section to unfold it

You should see current website domain (or subdomain) here. If you see any other domains in this list it means the website uses third-party cookies:



## Blocking Third-Party Cookies

Learn how to prevent third-party cookies from running on your site until users consent to your cookie policy with these helpful instructions from Cookie Script.

## How Third-Party Cookies Work

Third-party cookies are — you guessed it — cookies that are tracked by websites other than the one you are currently visiting. The most common third-party entities are advertisers, marketers, and social media platforms.

**Third-party cookies... one common example.** Let's say earlier in the week you looked up some vacation rentals in Cancun. You browsed a few websites, admired the photos of the sunsets and sandy beaches, but ultimately decided to wait another year before planning your vacation. A few days go by and suddenly it seems like you are seeing ads for Cancun vacations on many of the websites you visit. Is its mere coincidence? Not really. The reason you are now seeing these ads on vacationing in Cancun is that your web browser stored a third-party cookie and is using this information to send you targeted advertisements.

**You're unintentionally creating a "trail of crumbs."** Most web users don't realize that a browser window with multiple tabs open constitutes a single "session." As you move from tab to tab, you are unwittingly relaying information about your web visit history to other websites and parties. And, closing the web browser doesn't always eliminate the cookies your computer stores following the session. Depending on the browser you use, you may have to activate this manually.

**Dump your cookies after each session.** If you want to dump your cookies at the end of each session, select one of the following in your browser's preferences:

- **Chrome:** 'Keep local data only until you quit your browser'
- **Firefox:** 'Clear history when Firefox closes'
- **Internet Explorer:** Delete browsing history on exit

If you do not select one these preferences your browser will preserve cookie data from session to session. In other words, those ads tempting you into a vacation in Cancun will not disappear so quickly.

**That seemingly random email isn't so random.** Let's say you've visited a website where you have created a login ID. They likely have your name, email address, and possibly even your telephone number and street address. If the website uses third-party cookies, or you have other tabs open during your session, your cookies may be revealing your contact information to other parties in order to send you SPAM.

**You may be on a website with third-party cookies and not even know it.** One of the failings of cookie notices is that they don't often specify what types of cookies are being used on the site. They could be first-party, third-party, or both. But, if the website has advertisements (which many do), then you can reasonably expect the website to be generating both first- and third-party cookies.

To see if a particular website is using third-party cookies you can try the method mentioned at the start of this article, or visit [cookie-script.com](http://cookie-script.com) and enter the web address into the bar on the home page.

### **But, are Third-Party Cookies Actually Useful?**

Since the late 1990s, online marketers have built their businesses on the ability to track online users and then target them with advertisements, and much of this has been through the use of third-party cookies. Let's play "devil's advocate" for a moment. Could third-party cookies actually be useful for users? In a way, yes. The two largest online advertising firms, Google Ads and AdSense, make a valid point that third-party cookies are useful to consumers as they create advertisements that are in line with individual interests.

What happens after third-party cookies are eliminated? Once third-party cookies disappear, there's a likelihood that online advertisements will revert to contextual advertisements. That is, advertisements that are targeted to certain populations based on the website being visited, much like how magazines operate.

### **The Crackdown of Third-Party Cookies**

With the passage of [CCPA](#), [ePR](#), and [GDPR](#), governments are seeking to protect the privacy rights of website users. These laws and regulations create civil and/or criminal penalties for those that fail to notify web users of the presence of cookies. These regulations also require website operators to let users know what information is being collected and to whom this information is shared, along with a way to opt-out at any time.

**Third-party cookies' days are numbered.** Pressure from regulators and consumers has led many within the tech industry to declare third-party cookies (and the targeted ads fueled by them) will soon come to an end. Apple's Safari and Mozilla's Firefox now block third-party cookies by default. One notable holdout is Google Chrome, which has a commanding 67% of browser market share.

**Google has a major stake in third-party cookies.** Nearly 90% of Google's revenue is generated through advertising. Without third-party cookies, their advertising prowess could be negatively affected. This is one of the suspected reasons that the company is delaying a default block on third-party cookies until 2022. Until then, the company is taking steps to curtail some of the more invasive aspects of third-party cookies with their SameSite tool.

We have created a separate article which explains how **SameSite cookie attribute** works.

### **Why You Should Be Using Cookie Script on Your Website**

Keeping up with the latest cookie regulations and making sure your website is in compliance is a job in itself. Cookie Script keeps you compliant with GDPR, CCPA, ePR, and other regulations that are surely on the horizon. And, it's super-easy to use.

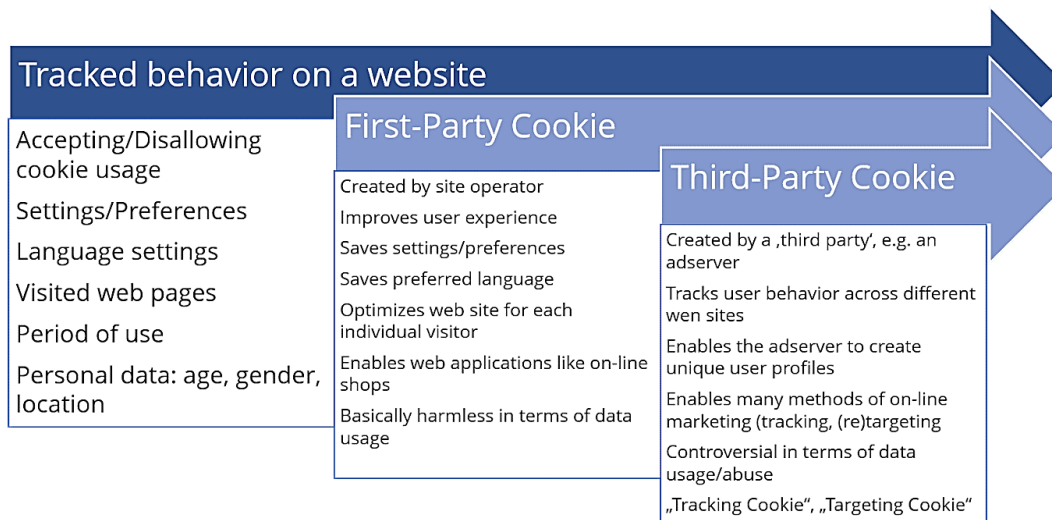
## How it Works

Cookie Script automatically does the following:

- Scans your website for cookies
- Categorizes and adds descriptions to your cookies
- Maintains a full history of user consents (as required by GDPR)
- Allows users to withdraw consent at any time
- Blocks cookies until users agree to privacy policy
- Block cookies until visitor consents (GDPR and CCPA)

**Block third-party cookies by default.** Cookie Script also gives you the option to prevent third-party cookies from running on your website.

Cookie Script makes the web a friendlier, more transparent experience for businesses and users. Getting started is free — today, or check out the to see how Cookie Script will work on your website.



## Super Cookie

A super cookie is a type of browser cookie that is designed to be permanently stored on a user's computer. Super cookies are generally more difficult for users to detect and remove from their devices because they cannot be deleted in the same fashion as regular cookies. Super cookies serve the same function as regular cookies in that they can contain just about any information including browsing history, authentication details or ad-targeting data.

There is some debate as to the precise definition of a super cookie. Originally, super cookies were synonymous with flash cookies as this was the first type of tracking mechanism beyond a basic cookie that could be used on the majority of browsers. As technology has progressed, it is possible to track users via other techniques such as HTML5 session storage. Given that browser technology will continue to change it is advantageous to think of super cookies in terms of their characteristics (permanent storage and difficulty in removal) as opposed to the mechanics of how they are stored

on a computer. Due to privacy concerns, many users and advocacy groups frown on the use of super cookies. However, the potential wealth of data and its use in online advertising have prompted more than a few ad organizations and websites to experiment with these more robust cookies.

**What makes a super cookie super? Are they more delicious than regular cookies? Not for Internet users that cherish their privacy. Continue reading to find out what tracking cookies are, what they mean for your privacy, and how to block them.**

## **What are cookies?**

An HTTP cookie is a small piece of code that is left in your web browser by a website you visited. The cookie places information on your device so that the website could later identify you as a returning user.

They're not necessarily a bad thing, as cookies can improve your online experience. The cookie contains a small text file that has information about you. This could be the last time you visited the website, your login details, or what you left in your shopping cart. The next time you visit the website, the information you previously provided will already be there.

However, cookies can also be used to learn your interests and target you for advertising purposes. You may not like them if you want to keep your online activity to yourself. It's important to note that due to the GDPR and many US state and federal laws, most websites are obligated to notify you that they use cookies. They need your consent to do so. It's your choice whether you are happy to use them or not.

Some cookies can crawl and track you to the websites you visit next, identifying your behavior patterns, and more. So, what do super cookies do?

## **Cookies vs. Super cookies**

The name is rather misleading because supercookies are not actually cookies:

- **Supercookies don't use local storage** as regular cookies do. Instead, they are injected at the network level as Unique Identifier Headers (UIDH).
- **Supercookies are inserted by your Internet Service Provider (ISP)** rather than the website itself.
- **You may not be aware of their existence** as the ISP might use them in secret.
- **UIDH personal data can be revealed to any website** and potentially sold to third parties. Verizon has previously told their partners that they use this type of tracking and have received a \$1.35 million fine from the Federal Communications Commission (FCC).
- **Supercookies allow third parties to track you too.** They can independently identify tracking headers themselves and use the data to serve you targeted ads across the web.
- **Supercookies can restore the data of your deleted cookies** and link the data with new ones. They can access your login credentials, image and file caches, and plug-in data.
- **Ad blockers can't block them**, and you can't clear them by deleting your browser history and cache data.

- **You can't simply delete supercookies.** You only opt-out if your ISP allows you to.

### **Are tracking cookies bad?**

Tracking cookies aren't harmful to your computer in the way that viruses and malware are. However, cookies threaten something more important than your device – your privacy.

ISPs can inject supercookies to improve their advertising revenue and share your data with other companies. The worst part is that internet users have no control over this threat to their privacy. Supercookies could lead to the leaking of private data, government surveillance, and exploits by cybercriminals.

### **How to block tracking cookies**

Supercookies are mysterious yet powerful creatures – detecting and deleting them is close to impossible. The traditional cookie clean-up won't make them go away, and neither will be setting 'Do not track' in your browser or browsing in private mode.

Supercookies depend on HTTP connections, so making an encrypted connection with a website stops tracking headers from functioning. Visiting only HTTPS websites (those that use SSL or TLS certificates) should help you avoid supercookies tracking you or catching them in the first place.

Alternatively, you can reroute your internet traffic through a secure network. Sounds like rocket science? It's not – all you need is a virtual private network, or VPN. NordVPN encrypts your internet connection, making it impossible for the ISP to apply tracking headers and for supercookies to follow you wherever you go.

## **Session 7**

### **CSRF, Command Injection**

#### **Cross-site request forgery (CSRF)**

In this section, we'll explain what cross-site request forgery is, describe some examples of common CSRF vulnerabilities, and explain how to prevent CSRF attacks.

#### **What is CSRF?**

Cross-site request forgery (also known as CSRF) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform. It allows an attacker to partly circumvent the same origin policy, which is designed to prevent different websites from interfering with each other.