

WHAT ARE COOKIES?

In the simplest sense, website cookies are just a small pieces of data sent to the browser by the website you are visiting at the time. They are stored on your system and are attached to requests sent to website servers. Cookies hold useful and sometimes essential information about the user. They can be used to save items in your shopping cart, track website usage, and store information that was previously entered. For example, this may include your name and address when filling out a billing form on a shopping website. Cookies are part of the HTTP/HTTPS protocol and started as information that was added on to the end of a URL. Do to how much information is stored and how many cookies that can be used together, today they are now stored in a separate files. The general form of a cookie file is as follows:

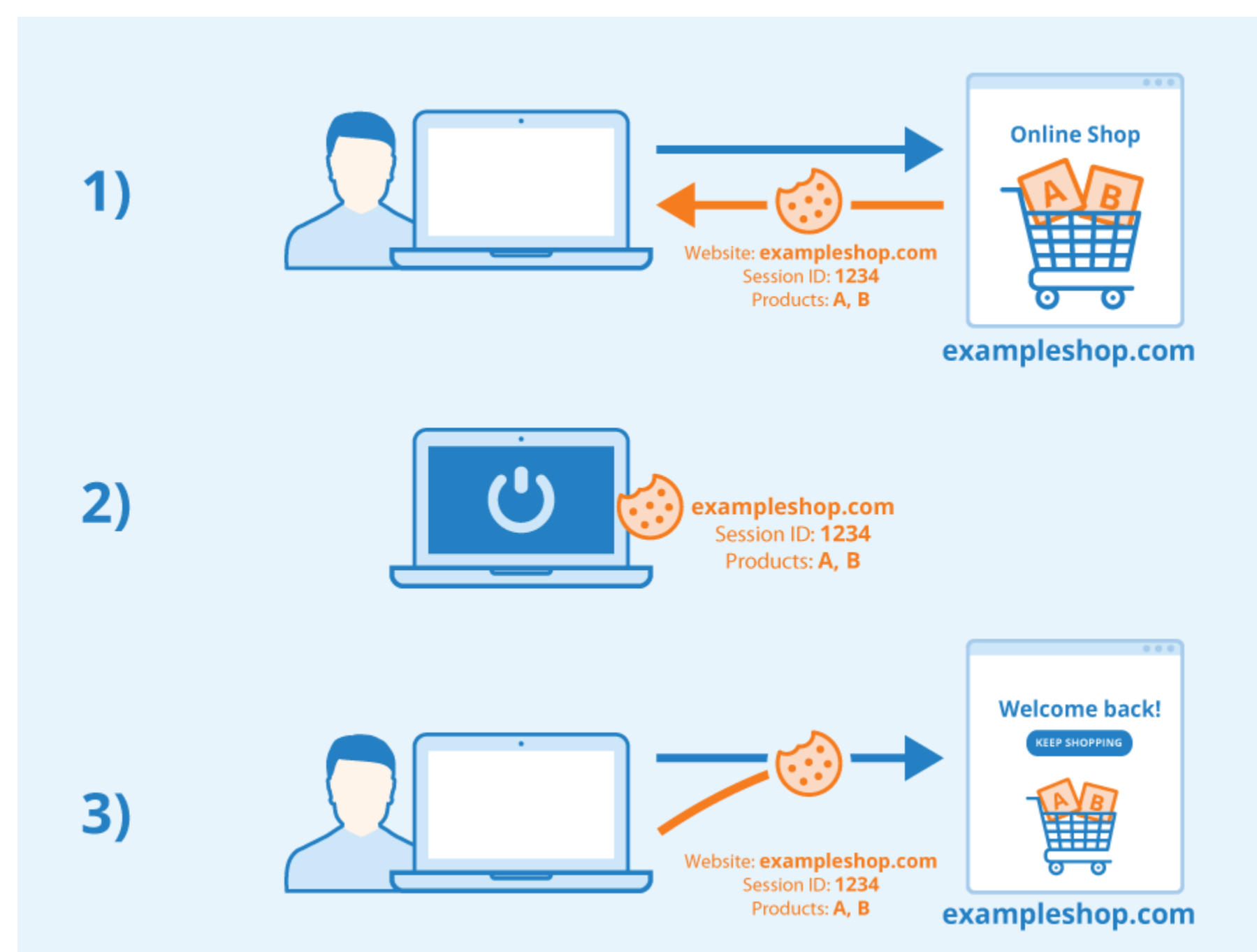
Name
Value
Zero or more attributes.

Attributes store information such as the cookie's expiration, domain, and flags. See the figure 1 below for what this file looks like.

Figure 1.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html
Set-Cookie: PREF=ID=5e66ffd215
TM=1147099841;LM=1147099841;S=
Bs23xeSv0; expires=Sun, 17-Jan-
9:14:07 GMT; path=/; domain=.c
om
```







Figure 2.



The photo above illustrates how a cookie is sent from the user's browser to a remote web server. This also illustrates how cookies are sent back to the user from the web server. This is an example of an authentication cookie.

TYPES OF COOKIES

Below are examples of the different kinds of cookies that are used when we are browsing the web:

-  **User Session/Authentication Cookies:** Cookies that associate website activity to a specific user. They are used to provide sensitive information to the correct user session. They do this with a cookie identifier string. These cookies are deleted after the user has closed the website/user session. These cookies have no expiration date so they need to be deleted after the user has ended their session. For example, if you log into an account the website is able to keep you logged in as you browse the site, sending the cookie along with further requests.
-  **Personalization Cookies:** Cookies that help websites remember user preferences to customize the users experience on said website. For example, a username is stored in a cookie so that when you access a website the username is remembered by the website. The user then only has to provide their password.
-  **Tracking Cookies:** Cookies that track which websites a user visits. This information is sent the next time that a cookies server needs to load content. These cookies can see that a user is shopping for a car and send ads to the user about cars. Some tracking cookies can also be used to anonymously record user activity.
-  **Persistent Cookies:** These cookies contain an expiration date for a predetermined length of time.
-  **Zombie Cookies:** Cookies that regenerate after they are deleted. They create backup versions of themselves outside of a browser's typical cookie storage location, using the backup to regenerate. Zombie cookies are used by ad networks and even cyber attackers.
-  **Third Party Cookies:** Cookies that are not owned by the website that you are currently on. These types of cookies are usually tracking cookies, such as Google AdSense cookies.

RISKS AND MITIGATIONS

Below are some common exploits involving cookies in the HTTP/HTTPS and ways that developers or users can mitigate these issues:

Cookie Capturing (Cookies): Authentication cookies should always be transmitted securely. If they are not an attacker they could steal credentials such as a username and password. Authentication cookies should always be sent using HTTPS which encrypts the cookies. To do this, developers should set the Set-Cookie response header to secure which sends all cookies through HTTPS. (*Malcolm*).

Session fixation (Cookies): This type of attack exploits a web application by grabbing the session ID from a query string in a URL. An attacker might be able to send a malicious link that can give access to a users session. To protect against this, web applications should only store session IDs in secure HTTPS cookies. (*Malcolm*).

Cross-site scripting (XSS) (Cookies): To steal cookies using cross-site scripting an attacker exploits a website that allows users to post unfiltered HTML and JavaScript content. This allows sensitive data to be passed through the code of the website. This can be mitigated by setting the Set-Cookie flag to HttpOnly in the response header so cookies can not be read by malicious JavaScript.

Cross-site request forgery (CSRF) (Cookies): Cross site request exploits a website by running unauthorized commands from a trusted user. Once the request goes through, an attacker is able to place their malicious link inside the page. This can also occur when a victim loads an email which automatically sends a request. This can also be mitigated by only sending the cookie data with the HttpOnly flag on the response header.

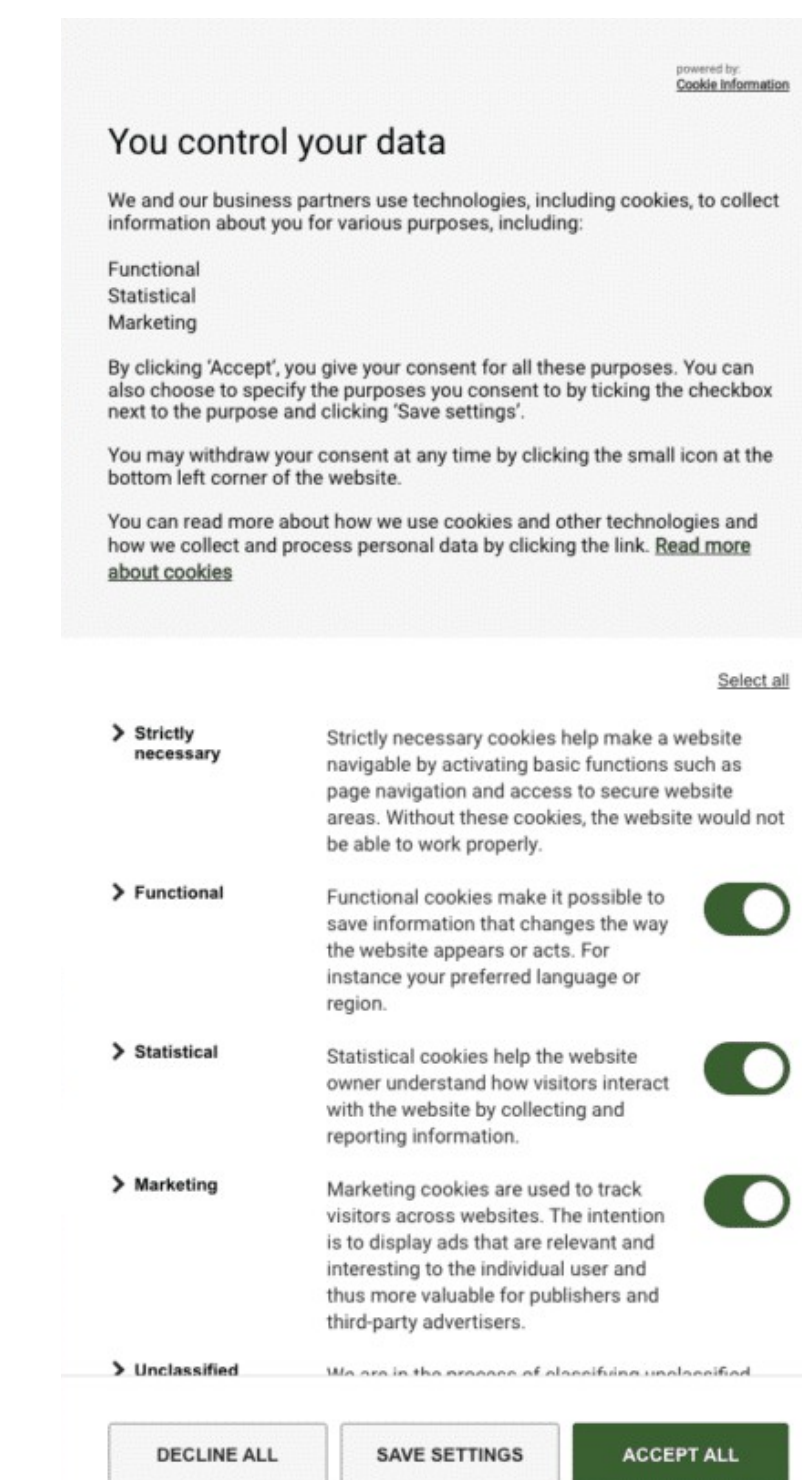
Cookie tossing (Cookies): Cookie tossing is an attack that provides users with malicious cookies. When the victim visits a site, cookies are loaded from the domain and a malicious subdomain. This enables an attacker to set arbitrary values that can be used in CSRF and XSS attacks. Domains should only allow trusted subdomains and monitor their subdomains so that cookie tossing is not possible.

These security concerns should be dealt with on all websites to protect its users user information and personal information stored in their cookies. Other than security concerns with cookies, there are also a number of privacy concerns even if the site is secure. Third party and tracking cookies have evolved exponentially over the years, from simple counting of ad impressions, and views and clicks. These types of cookies are now able to profile users based off there web-traffic that is capture inside of these cookies. The most popular and used on a lot of large scale sites is Google AdSense. They are able to grab enormous amounts of data on a user in the background and report it back to Google. With every website you visit that has third party or tracking cookies, you are leaving a trail of crumbs that these marketing firms are able to build a profile about you. This can be from data about shopping, political affiliations, and religious beliefs. Especially when it comes to Google they are able to combine this with other data that they can collect on, say a smartphone, like location data. Then Google is able to figure out almost everything about you, even things that you might not think of. This is very powerful and even sensitive information that they are able to derive from even just your cookie data.

BEST PRACTICES AND POLICY

With growing concerns about privacy when it pertains to third party and tracking cookies, one might ask how can we limit the amount of information that these cookies are able to capture about us. In 2016, the EU set out to write policy on privacy online for its users including the use of tracking cookies called the GDPR. Effective as of 2018, any website that a member of the EU can visit has to provide a box so that they can opt in or out of cookies being collected. This is why now when you view a website a box pops up that asks you what type of cookies you want to opt in or out of (see the figure below). Though the user has the choice, companies are now losing out on valuable private data about there users and are trying to make it harder for users to opt out of theses cookies. Stated by a report from *TechCrunch* in June 2021, "Sites are choosing to try to wear people down so they can keep grabbing their data by only offering the most cynically asymmetrical "choice" possible" (*Lomas*). This goes against the GDPR and is opening up websites to massive fines under the GDPR. Also according to *TechCrunch*, there are not for profit companies that are working on automating a system so that users can set there privacy choices in the background without the annoying cookies banners (*Lomas*). To truly combat these privacy concerns there needs to be policy written and followed as to protect every user's privacy online. So now that you know about cookies how can you apply this knowledge? Next time a cookie page appears on your screen you are now armed with the knowledge of what each cookie is. You can decide what information you are willing to give up to the website. You should also always keep your browser up to date to protect against cookie vulnerabilities and allow your browser to delete cookies and even block certain tracking cookies. You can even install an ad on that can auto delete cookies when not in use and block advertising cookies to mitigate your own privacy concerns.

Figure 3.



REFERENCES

- cookie. (n.d.). viaggio. Retrieved October 20, 2023, from <https://www.viaggio.co/wp-content/uploads/2022/03/HTTP-Cookie.png>. Title Image
- Cookies: An overview of associated privacy and security risks. Infosec. (n.d.). <https://resources.infosecinstitute.com/topics/general-security/cookies-an-overview-of-associated-privacy-and-security-risks/>
- Cookie Diagram. (n.d.). Seobility. Retrieved October 20, 2023, from <https://www.seobility.net/en/wiki/images/2/2a/Session-id.png>. Figure 2
- cookie info. (n.d.). cookie information. Retrieved October 20, 2023, from <https://cookieinformation.com/wp-content/uploads/Overlay-v3-cookie-banner-example-from-cookie-information-1200x857.png>. Figure 3
- Europe's cookie consent reckoning is coming. Lomas, N. (2021, June 1). Europe's cookie consent reckoning is coming. TechCrunch. <https://techcrunch.com/2021/05/30/europes-cookie-consent-reckoning-is-coming/>
- Http Cookie. (n.d.). Wikimedia. Retrieved October 20, 2023, from <https://upload.wikimedia.org/wikipedia/commons/thumb/8/8b/HTTP-Cookie-Google.svg/300px-HTTP-Cookie-Google.svg.png?20220911184249>. Figure 1
- Location. (n.d.-a). Freerangestock. Retrieved October 20, 2023, from <https://freerangestock.com/sample/119156/location-pin-vector-icon.jpg>
- Lock. (n.d.-b). Freerangestock. Retrieved October 20, 2023, from <https://freerangestock.com/sample/119149/pad-lock-vector-icon.jpg>
- multiple people. (n.d.). open clip art. Retrieved October 20, 2023, from <https://openclipart.org/detail/282576/about-icon>
- Malcolm McDonald - Web Security for Developers. McDonald, M. (2020). Web security for developers: Real threats, practical defense. No Starch Press.
- What are cookies? | cookies definition | cloudflare. (n.d.). <https://www.cloudflare.com/learning/privacy/what-are-cookies/>
- Virus. (n.d.). rawpixel. Retrieved October 20, 2023, from https://images.rawpixel.com/image_800/cHJpdjF0ZS9scj9pbWFnZXMvd2Vlc20ZSByMDIzLTA2L2pvYj2Ni0vODAtMDE5cGc.jpg
- What are cookies? | cookies definition | cloudflare. (n.d.). <https://www.cloudflare.com/learning/privacy/what-are-cookies/>