Cookies

•••

The Non-Edible Ones, Of Course !

Shivani Sethi

1. Overview

Internet cookies are small text files (255 characters or less) that are placed on your web browser or computer by web servers.

2. How this helps ?

A cookie is created when you first visit a site that wants to store information. This text file usually includes a name, an expiration date, a coded number, and the domain name of the visited site.

When you return to a site, the cookie tells the site that a computer with code XYZ has returned and reminds it of your activities and preferences on your previous visits.

3. OMG ! So does it store your private data ?

Cookies, do not store any of your personal information such as your email address or phone number. However, because they allow third-party sites to track you across the web, there can be a downside to cookies , particularly if you are concerned about what some refer to as “targeted advertising” and others as “online spying” or “invasion of privacy.”

4. So what all data can a cookie store ?

Well, cookies typically have 6 fields : Name, Value, Domain ,Path (the “/” means the cookie is valid anywhere on that domain.) ,Expires, Secure (used for cookies that need a SSL connection)

Types of cookies

(Except the chocolate and butter ones)

5. Persistent Cookies

Persistent cookies can exist for an **extended period of time** until expired or until they are deleted. They enable the site to recognize you on a continuous basis. This is done by the web server planting a small text file with a unique ID tag on your computer, while keeping a matching file on the server. On subsequent visits to the site, your browser delivers this cookie over to the site, allowing the site to retrieve the matching file.

Persistent cookies enable websites to remember your preferences and settings (i.e. login information, language selection, font size preference, etc) so that they can offer you a more personalized and convenient access the next time you visit. For security purposes, your login information is generally encrypted by the web server before it gets stored in a cookie.

5. Session Cookies

Session cookies help websites to recognize you and remember the information provided by you as you move from one page to another within the same website. For example, e-commerce sites use session cookies to remember the items you place in your shopping cart as you go from one page to another on the site. Without session cookies, your shopping cart will be empty upon “Checkout” since your shopping activities on prior pages will not be remembered.

Session cookies only retain information about your activities **during your visit to the site**. Once you close the browser, the session cookies are lost and the site will not recognize you the next time you return to the site.

6. Other types of classification - By party

Cookies can come from multiple sources.

First party cookies are sent directly by the visited site and they are usually identified by the site's domain name.

Then there are the **third-party cookies**, which come from those with an interest in the site such as advertisers and ad servers. They are difficult for the average user to identify because they can be connected to any banner ad on a site.

These third-party cookies allow advertisers and ad servers to alternate the ads sent to a specific computer and to track how often an ad has been viewed and by whom.

Associated Risks

7. Cookie hijacking and risks

“Cookie hijacking” is the term mostly used for unauthorized access to cookies.

If the hacker somehow gets their hands on the session or permanent cookies, that’s dangerous because this cookie hijacking creates a possible threat of unauthorized access to websites you’ve previously logged in to. The stolen cookies allow the hacker to get access to the user’s account without entering login details.

Cookie security is a major problem in the internet world. Security holes keep being found in different browsers which inadvertently can leak personal information to malicious users.

This can lead to all sorts of issues including credit card information theft, unauthorized access to personal email or other accounts and more.

8. Cookies and the law

European Union : In the EU the “cookie law” has been enforced across all countries for a few years now. This law requires businesses having an online presence to take consent from visitors and consumers before using cookies.

USA : In the USA the Behavioral Advertising Principles require website operators to disclose their use of cookies to the consumers when collecting sensitive information and they should take explicit consent.

Similarly, laws regarding disclosure and use of cookies exist throughout the world.

9. Final words

Despite all the privacy and security concerns, cookies are very useful and handy as they make it possible for the websites to remember us ensuring a comfortable and hassle-free browsing experience.

They certainly can pose security issues and privacy concerns if they’re being used without users’ consent and knowledge. This nuisance can be easily controlled though as modern browsers feature various settings to change the default cookie behavior.

Basic Demo

Code available at :
https://github.com/sethishivani/flask_cookie_example

Dependencies :
Flask, Python 3

Thank you !

References

- https://www.hotspotshield.com/resources/what-are-internet-cookies/
- https://www.websitepolicies.com/blog/cookies-guide
- https://www.webopedia.com/DidYouKnow/Internet/all_about_cookies.asp
- https://www.allaboutcookies.org/

Further Reading

- What are Super/Zombie Cookies ?
- Cross-domain cookie theft.

Dive Deep

- https://cookiecontroller.com/what-are-cookies