Cookies

Let's discuss another key concept of computer networking, cookies!

WE'LL COVER THE FOLLOWING

Introduction

You might have heard of the term ‘cookie’ used a lot in the context of computer networks and privacy. Let’s have a closer look at what they are.

HTTP is a stateless protocol, but we often see websites where session state is needed. For instance, imagine you are browsing for products on an e-commerce website. How does the server know if you are logged in or not, or if the protocol is stateless? How does the server know what’s in your shopping cart when checking out if the protocol is stateless? Cookies allow the server to keep track of this sort of information.

How Cookies Work

- Cookies are **unique string identifiers** that can be stored on the client’s browser.

- These identifiers are **set by the server through HTTP headers** when the

client first navigates to the website.

- After the cookie is set, it's sent along with subsequent HTTP requests to the same server. This **allows the server to know who is contacting it** and hence serve content accordingly.

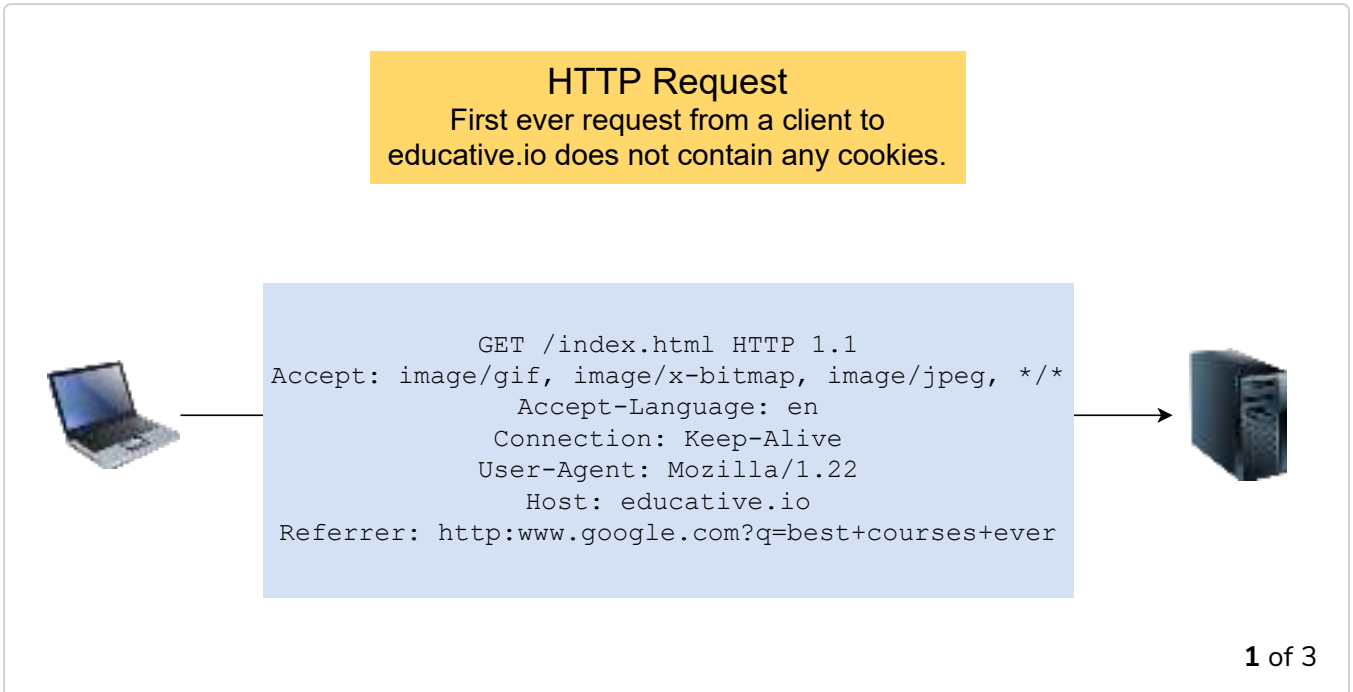
So the HTTP request, the HTTP response, the cookie file on the client's browser, and a database of cookie-user values on the server's end are all involved in the process of setting and using cookies.

`Set-cookie` Header

Let's look at how cookies work in a bit more detail. When a server wants to set a cookie on the client-side, it includes the header `Set-cookie: value` in the HTTP response. This value is then **appended to a special cookie file stored on your browser**. The cookie file contains:

- The website's domain
- The string value of the cookie
- The date that the cookie expires (yes, much like actual cookies, they do expire)

Have a look at the following slides to see how cookies work in practice.



HTTP Response

can include a session identifier, i.e., a cookie via the `set-cookie` header that tracks a user once they have authenticated

```
HTTP/1.1 200 OK
Date: Sat, 19 Feb 2011 02:32:58 GMT
Server: Apache/2.2.3 (CentOS)
Connection: Keep-alive
Last-Modified: Tue, 18 Aug 2015 15:11:03 GMT
Set-cookie: session=44ecb091; path=/servlets
Content-Length: 6821

<HTML> website content ... </HTML>
```

2 of 3

Follow-up HTTP Request

Cookies sent along with requests

```
GET /login.html/user=postman&pass=secret HTTP 1.1
Accept: image/gif, image/x-bitmap, image/jpeg, */*
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/1.22
Host: educative.io
Cookie: session=44ecb091; path=/servlets
```

3 of 3

The Dangers of Cookies ☠

cookie monster; image attribution:

While cookies seem like a great idea to make HTTP persistent when needed, cookies have been **severely abused in the past**.

If a website has stored a cookie on your browser, **it knows exactly when you visit it, what pages you visit and in what order**. This itself makes s

people uncomfortable.

https://www.flickr.com/photos/tomcrouse/23712101

Third-party Cookies

Also, websites may not necessarily know personally identifiable information about you such as your name (by the way, websites that require you to sign-up *do* know your name), and they may only know the value of your cookie. But what if **websites can track what you do on *other* websites**? Well, they can. Welcome to the concept of third-party cookies.

While we can't go into too much detail, it suffices to know that **third-party cookies are cookies set for domains that are not being visited**.

Example

1. A user visits amazon.com.
2. A cookie for **free-stats.com** is subsequently set on their browser because free-stats has placed an advertisement on Amazon. Notice that this is **a third-party cookie**!
3. Suppose, the user visits ebay.com, and **eBay also has placed an advertisement for free-stats.com**.
4. The **same cookie set on the Amazon site will be reused** and sent to free-stats along in an HTTP request with the name of the host that the user is on.
5. Free-stats **can in this way track every website the user visits** that they are advertising on and create more targeted ads in order to generate greater revenue.

Also, the public has largely considered third-party cookies to be a breach of privacy and so rejected them. Most modern browsers come with the in-built option to block third-party cookies.

Blocking Third-Party Cookies Is Not Enough!

However, firms have come up with several workarounds including but not

limited to:

- Respawning cookies
- Flash cookies
- Entity tags
- Canvas fingerprinting

Quick Quiz!

1 What is a cookie?

COMPLETED 0%

1 of 2

Now that we know the basics of cookies, let's look at them in practice with a quick exercise!