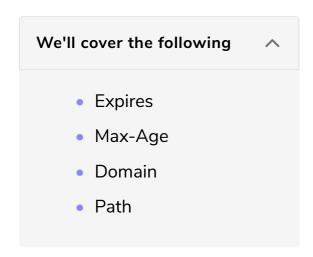
What's Behind a Cookie?

In this lesson, we'll study how cookies are set, requested, and what directives they can have.



A server can send a cookie using the Set-Cookie header.

```
HTTP/1.1 200 Ok
Set-Cookie: access_token=1234
...
```

A client will then store this data and send it in subsequent requests through the Cookie header.

```
GET / HTTP/1.1
Host: example.com
Cookie: access_token=1234
...
```

Note that servers can send multiple cookies at once,

```
HTTP/1.1 200 Ok
Set-Cookie: access_token=1234
Set-Cookie: user_id=10
...
```

and clients can do the same in their request.

```
GET / HTTP/1.1
Host: example.com
Cookie: access_token=1234; user_id=10
```

. . .

In addition to the plain *key* and *value*, cookies can carry additional directives that limit their time-to-live and scope.

Expires

Specifies when a cookie should expire, so that browsers do not store and transmit it indefinitely. A clear example is a session ID, which usually expires after some time. This directive is expressed as a date in the form of Date: <day-name>, <day>
<month> <year> <hour>:<minute>:<second> GMT, like Date: Fri, 24 Aug 2018 04:33:00
GMT. Here's a full example of a cookie that expires on the first of January, 2018:
access_token=1234;Expires=Fri, 24 Aug 2018 04:33:00 GMT

Max-Age

Similar to the Expires directive, Max-Age specifies the number of seconds until the cookie should expire. A cookie that should last one hour would look like the following: access_token=1234;Max-Age=3600

Domain

This directive defines which hosts the cookie should be sent to. Remember, cookies generally contain sensitive data, so it's important for browsers not to leak them to untrusted hosts. A cookie with the directive <code>Domain=trusted.example.com</code> will not be sent along with requests to any domain other than <code>trusted.example.com</code>, not even the root domain, <code>example.com</code>. Here's a valid example of a cookie limited to a particular subdomain: <code>access_token=1234;Domain=trusted.example.com</code>

Path

Path is similar to the <code>Domain</code> directive but applies to the URL path (<code>/some/path</code>). This directive prevents a cookie from being shared with untrusted paths, such as in the following example: <code>access_token=1234;Path=/trusted/path</code>.

In the next lesson, we'll study session and persistent cookies.