@Code.Clash

Cookies

JavaScript

What are Cookies?

Have you ever noticed that when you visit a website, it remembers things about you? Like your username or the items in your shopping cart? That's because of cookies!

- Cookies are small pieces of data that websites store on your computer or mobile device.
- They are important in web development because they allow websites to remember information about the user, such as their preferences or login credentials.

How Cookies Works?

When a user sends a request to a server, the server treats each request as if it's from a new user.

- To recognize returning users, we add a cookie to the response from the server.
- The cookie is stored on the user's browser, and whenever they send a new request, the browser automatically adds the cookie to it.
- This allows the server to recognize the user and personalize their experience.

Setting Cookies

To create a cookie using JavaScript, you can use the document.cookie property.

Here is an example of setting a cookie:

```
document.cookie = "username=Code Clash";
```

You can also add an expiry date (in UTC time). and With a path parameter and you can also tell the browser what path the cookie belongs to.

```
document.cookie = "username=Code; expires=Thu, 30 Apr 2024 12:00:00 UTC; path=/";
```

Reading Cookies

To read the value of a cookie using JavaScript, you can use the document.cookie property again.

Here is an example of reading a cookie:

```
let allcookies = document.cookie;
console.log("All Cookies : " + allcookies);
```

Here you will get all cookies in one string much like: cookie1=value; cookie2=value; .

You can use strings split() function to break a string into key and values.

Deleting Cookies

To delete a cookie using JavaScript, you can set the expiration date to a past date, which will cause the browser to remove the cookie from the user's device.

Here is an example of deleting a cookie:

```
document.cookie = "username=; expires=Thu, 01 Jan 1970 00:00:00 UTC;";
```

Best Practices

When using cookies in web development, it is important to follow best practices to ensure that the user's privacy and security are protected.

Here are some tips:

- Avoid storing sensitive information in cookies, such as passwords or credit card numbers.
- Use secure and HTTP-only cookies to prevent cross-site scripting (XSS) attacks and other security vulnerabilities.
- Set reasonable expiration dates for cookies to ensure that they are not stored on the user's device indefinitely.
- Use cookies sparingly and only when necessary, to minimize the amount of data stored on the user's device.

Conclusion

- Cookies are a powerful tool in web development that can make websites more personalized and convenient to use.
- By learning how to set, read, and delete cookies in JavaScript, you can start creating websites that remember information about users and improve their experience.
- Remember to use cookies responsibly and follow best practices to protect users' privacy and security.
- As always, I hope you enjoyed the post and learned something new.
- If you have any queries then let me know in the comment box.

SAVE THIS FOR LATER

&

FOLLOW FOR MORE

@webuniverse02

Was this post helpful ?
Drop a comment
It gives me motivation

Link in bio