upGrad

#RahoAmbitious

Full Stack Software Development

upGrad

Course: JavaScript and Server-Side Communication

Lecture On: Security and Authorization using AJAX

Instructor: Siddhesh Prabhugaonkar

In the previous class, we covered…

- Introduction to JSON and how to parse JSON
- Introduction to AJAX
- Differences among GET, POST, PUT and DELETE requests
- Introduction to HTTP requests and responses
- HTTP headers
- Debugging the code

Poll 1 (15 Sec)

According to you, which of the following is NOT an idempotent request?

1. GET
2. POST
3. PUT
4. DELETE

Poll 1 (Answer)

According to you, which of the following is NOT an idempotent request?

1. GET
2. **POST**
3. PUT
4. DELETE

Poll 2 (15 Sec)

Which of the following is not an HTTP header?

1. Entity Header
2. Presentation Header
3. General Header
4. Request/Response Header

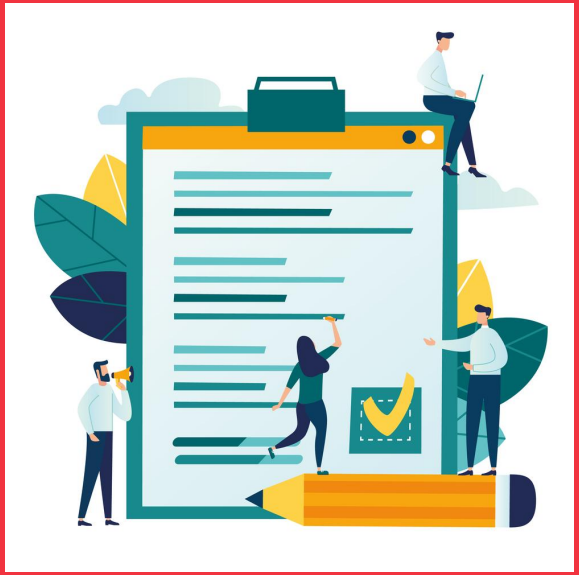
Poll 2 (Answer)

Which of the following is not an HTTP header?

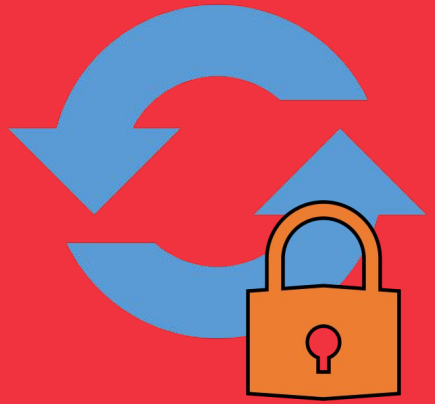
1. Entity Header
2. **Presentation Header**
3. General Header
4. Request/Response Header

Today's Agenda

- Secure AJAX calls
- Authorisation and access tokens



Secure AJAX Calls Using Authorisation



Secure AJAX Calls

upGrad

- Information such as passwords or credit card details should not be transferred over the server as simple plain text.
- Suppose you log in to your private email; your credentials, which is plain text, get intercepted by the hacker; and they misuse your data.
- To avoid such situations, you need to adopt a mechanism that ensures secure transmission of data over the server.
- You should encode your data using an encoding technique before sending it over the server.

Secure AJAX Calls

upGrad

- The **window.btoa()** method encodes a string in base64 encoded ASCII.
- The **window.atob()** method decodes a string encoded using base64 encoding scheme.

```
let str = "Hello World!";
let enc = window.btoa(str);
console.log(enc); // SGVsbG8gV29ybGQh
let dec = window.atob(enc);
console.log(dec); // Hello World!
```

- You can read more about *Base64 Encoding and Decoding* here.

Poll 3 (15 Sec)

What will be the output of the code given in the adjoining screenshot?
(**Hint:** Try to run the given code on your browser's DevTool, and answer the question.)

1. U2VjdXJl
2. Secure
3. SGVsbG8gV29ybGQh
4. None of the above

```
let str = "Secure";
let enc = window.btoa(str);
console.log(enc);
```

Poll 3 (15 Sec)

What will be the output of the code given in the adjoining screenshot?
(**Hint:** Try to run the given code on your browser's DevTool, and answer the question.)

1. **U2VjdXJl**
2. Secure
3. SGVsbG8gV29ybGQh
4. None of the above

```
let str = "Secure";
let enc = window.btoa(str);
console.log(enc);
```

Poll 4 (15 Sec)

What will be the output of the code given in the adjoining screenshot?

1. U2VjdXJl
2. Secure
3. SGVsbG8gV29ybGQh
4. None of the above

```
let str = "Secure";
let enc = window.btoa(str);
let dec = window.atob(enc);
console.log(dec);
```

Poll 4 (15 Sec)

What will be the output of the code given in the adjoining screenshot?

1. U2VjdXJl
2. **Secure**
3. SGVsbG8gV29ybGQh
4. None of the above

```
let str = "Secure";
let enc = window.btoa(str);
let dec = window.atob(enc);
console.log(dec);
```

upGrad

Authentication and Access Tokens

Authorisation and Access Tokens

upGrad

- OAuth 2.0 is an authorisation technique that allows users to share specific data with an application while keeping the usernames, passwords and other information secure.
- The OAuth 2.0 flow is called the implicit grant flow.
- To understand the entire authorisation process with OAuth 2.0, refer to this document: JavaScript Implicit Flow.

You can read more about the best practices for generating an access token here.

Poll 5 (15 Sec)

State whether the following statement is true or false.

The access token is unique for each user.

1. True
2. False

Poll 5 (Answer)

State whether the following statement is true or false.

The access token is unique for each user.

1. **True**
2. False

Poll 6 (15 Sec)

State whether the following statement is true or false.

An access token that is generated randomly is more secure than that generated using an algorithm.

1. True
2. False
3. Both the methods - generating access token randomly and using an algorithm have their own pros and cons.

Poll 6 (Answer)

State whether the following statement is true or false.

An access token that is generated randomly is more secure than that generated using an algorithm.

1. True
2. False
3. **Both the methods of generating access token randomly and using an algorithm have their own pros and cons.**

Poll 7 (15 Sec)

State whether the following statement is true or false.

An access token that is generated randomly is easy to retrieve compared with that generated using an algorithm.

1. True
2. False
3. Both the methods of generating access token randomly and using an algorithm have their own pros and cons.

Poll 7 (Answer)

State whether the following statement is true or false.

An access token that is generated randomly is easy to retrieve compared with that generated using an algorithm.

1. True
2. **False**

Retrieving data for an entirely random string takes much more time than that required for a string that has been generated by encoding the data sent by the user. This is because, the token generated randomly needs to be searched in the entire database and checked if it matches or not which obviously is cumbersome.

3. Both the methods of generating access token randomly and using an algorithm have their own pros and cons.

upGrad

Doubt Clearance (5 mins)

Hands-On Exercise (10 mins)

upGrad

Watch the adjoining video to understand the requirement.

The stub code is provided here.

The solution is provided here.

upGrad

Project Work

(Let's use the API you learnt about yesterday in our project, and make our complete project dynamic.)

You can refer to the solution here.

Key Takeaways

- OAuth 2.0 is an authorisation technique that allows users to share specific data with an application while keeping the usernames, passwords and other information secure.
- The **window.btoa()** method encodes a string in base64 encoded ASCII.
- The **window.atob()** method decodes a string encoded using base64 encoding scheme.

Tasks to Complete After Today's Session

MCQs
Coding Questions
Project - Checkpoint 5

upGrad

#RahoAmbitious

Thank you!