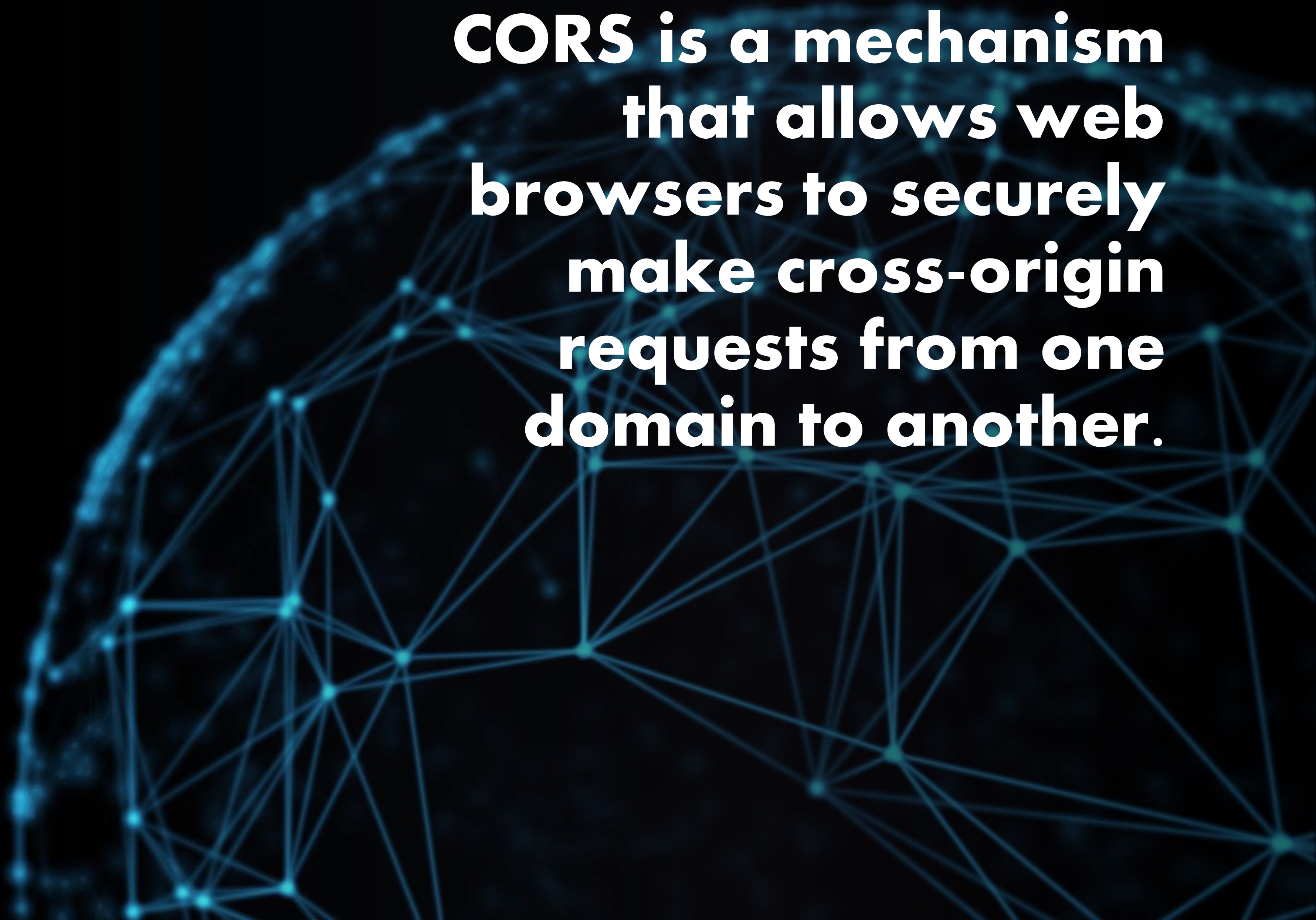
Understanding CORS: Cross-Origin Resource Sharing

Andrii Sukhoi



CORS is a mechanism that allows web browsers to securely make cross-origin requests from one domain to another.

origin

- Protocol: The protocol used for the web request, such as HTTP or HTTPS.
- Domain: The domain name of the web page that initiated the request.
- Port: The port number used for the request (if specified).

Same-Origin Policy

- By default, web browsers enforce the Same-Origin Policy, which restricts web pages from making requests to a different origin. This policy is in place for security reasons, as it helps prevent unauthorized access to sensitive information or actions on behalf of the user.

Reasons why cross-origin requests are made

- Accessing APIs:
- Single-Page Applications (SPAs)
- Microservices Architecture
- Cross-Domain Authentication
- Embedding External Content
- Cross-Domain Messaging
- Resource Sharing

CORS Headers

Access-Control-Allow-Origin

- This response header is sent by the server.
- Specifies the allowed origins that can access the server's resources.
- The value can be either an exact match of the requesting origin or a wildcard (*) to allow any origin.
- Example: **`Access-Control-Allow-Origin:`** [`http://example.com`](http://example.com)

Access-Control-Allow-Methods

- This response header is sent by the server.
- Specifies the HTTP methods (verbs) that are allowed for cross-origin requests.
- Example: **`Access-Control-Allow-Methods: GET, POST, PUT`**

Access-Control-Allow-Headers

- This response header is sent by the server.
- Specifies the allowed request headers for cross-origin requests.
- Example: **`Access-Control-Allow-Headers: Content-Type, Authorization`**

01

Access-Control-Allow-Credential

02

Access-Control-Expose-Headers

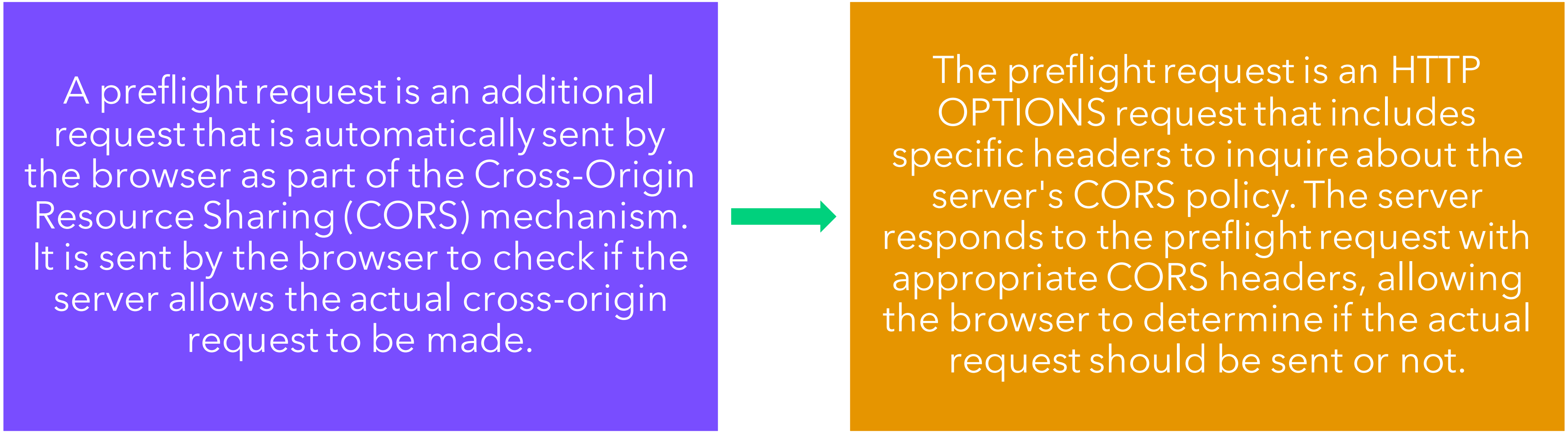
03

Access-Control-Request-Method

04

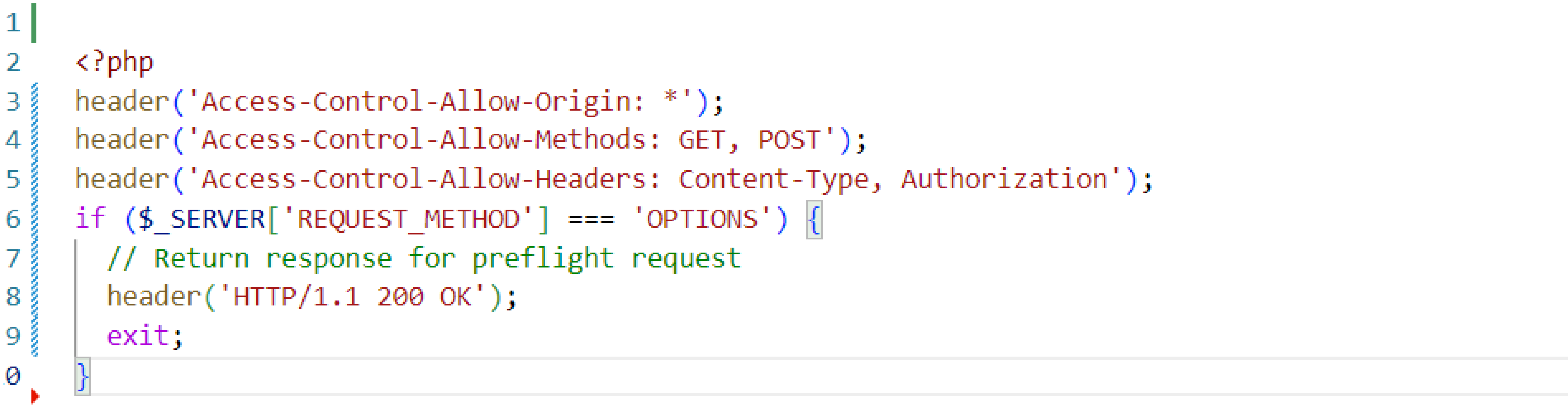
Access-Control-Request-Headers

Preflight request



A preflight request is an additional request that is automatically sent by the browser as part of the Cross-Origin Resource Sharing (CORS) mechanism. It is sent by the browser to check if the server allows the actual cross-origin request to be made.

The preflight request is an HTTP OPTIONS request that includes specific headers to inquire about the server's CORS policy. The server responds to the preflight request with appropriate CORS headers, allowing the browser to determine if the actual request should be sent or not.



```php

<?php
header('Access-Control-Allow-Origin: *');
header('Access-Control-Allow-Methods: GET, POST');
header('Access-Control-Allow-Headers: Content-Type, Authorization');
if ($_SERVER['REQUEST_METHOD'] === 'OPTIONS') {
  // Return response for preflight request
  header('HTTP/1.1 200 OK');
  exit;
}
```