

???????CORS????????????

1. 浏览器 发起 CORS 请求 请求头 Web
Access-Control-Allow-Origin: *
Access-Control-Allow-Origin: https://trusted-domain.com

2. 浏览器 发起 CORS 请求 请求头
Access-Control-Allow-Origin: *
Access-Control-Allow-Origin: https://trusted-domain.com

Access-Control-Allow-Origin: https://trusted-domain.com

3. 浏览器 发起 CORS 请求 请求头

浏览器 发起 CORS 请求 请求头 cookies 请求头 HTTP 请求头
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://trusted-domain.com

Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://trusted-domain.com

4. 浏览器 发起 HTTP 请求 请求头

浏览器 发起 HTTP 请求 请求头
Access-Control-Allow-Methods: GET, POST

5. 浏览器 发起 CORS 请求 请求头

浏览器 发起 CORS 请求 请求头
Access-Control-Allow-Headers: Content-Type, Authorization

6. 浏览器 发起 CORS 请求 请求头

浏览器 发起 CORS 请求 请求头 Access-Control-Max-Age 请求头
Access-Control-Max-Age: 600

7. 浏览器 发起 CORS 请求 请求头

浏览器 发起 CORS 请求 请求头 CORS 请求头

Nginx 配置

[[[Nginx [[CORS [[[[

```
server {
    listen 80;
    server_name api.example.com;

    location /api/ {
        add_header 'Access-Control-Allow-Origin' 'https://trusted-domain.com';
        add_header 'Access-Control-Allow-Methods' 'GET, POST';
        add_header 'Access-Control-Allow-Headers' 'Content-Type, Authorization';
        add_header 'Access-Control-Allow-Credentials' 'true';
        add_header 'Access-Control-Max-Age' '600';

        if ($request_method = 'OPTIONS') {
            return 204;
        }

        proxy_pass http://backend-server;
    }
}
```

Apache [[[[

[[[Apache [[[CORS [[[[

```
<VirtualHost *:80>
    ServerName api.example.com

    Header set Access-Control-Allow-Origin "https://trusted-domain.com"
    Header set Access-Control-Allow-Methods "GET, POST"
    Header set Access-Control-Allow-Headers "Content-Type, Authorization"
    Header set Access-Control-Allow-Credentials "true"
    Header set Access-Control-Max-Age "600"

    <Location "/api/">
        # [ [ [ [ [ [ [ [ 204
        <If "%{REQUEST_METHOD} == 'OPTIONS'">
            Header always set Content-Length "0"
            Header always set Content-Type "text/plain"
            Require all granted
        </If>
    </Location>
</VirtualHost>
```

[[[CORS [[[[

```
from flask import Flask, request, jsonify

app = Flask(__name__)

ALLOWED_ORIGINS = ["https://trusted-domain.com"]

@app.after_request
def add_cors_headers(response):
    origin = request.headers.get('Origin')
    if origin in ALLOWED_ORIGINS:
        response.headers['Access-Control-Allow-Origin'] = origin
        response.headers['Access-Control-Allow-Methods'] = 'GET, POST'
        response.headers['Access-Control-Allow-Headers'] = 'Content-Type, Authorization'
        response.headers['Access-Control-Allow-Credentials'] = 'true'
    return response

@app.route('/api/data', methods=['GET', 'POST'])
def api_data():
    return jsonify({"message": "Hello, World!"})

if __name__ == "__main__":
    app.run()
```

XXX

XXXXX CORS XXXXXXXXXXXXXXXXXXXXXXX
XX HTTPSXXXXXXXXXXXXXXXXXXXX
XX CSRF XXXXXXXXXXXXXXXXXXXXXXX CSRF XXXXXX

XXXXXXXXXXXX CORS XXXXXXXXXXXXXXX