SOP, CORS

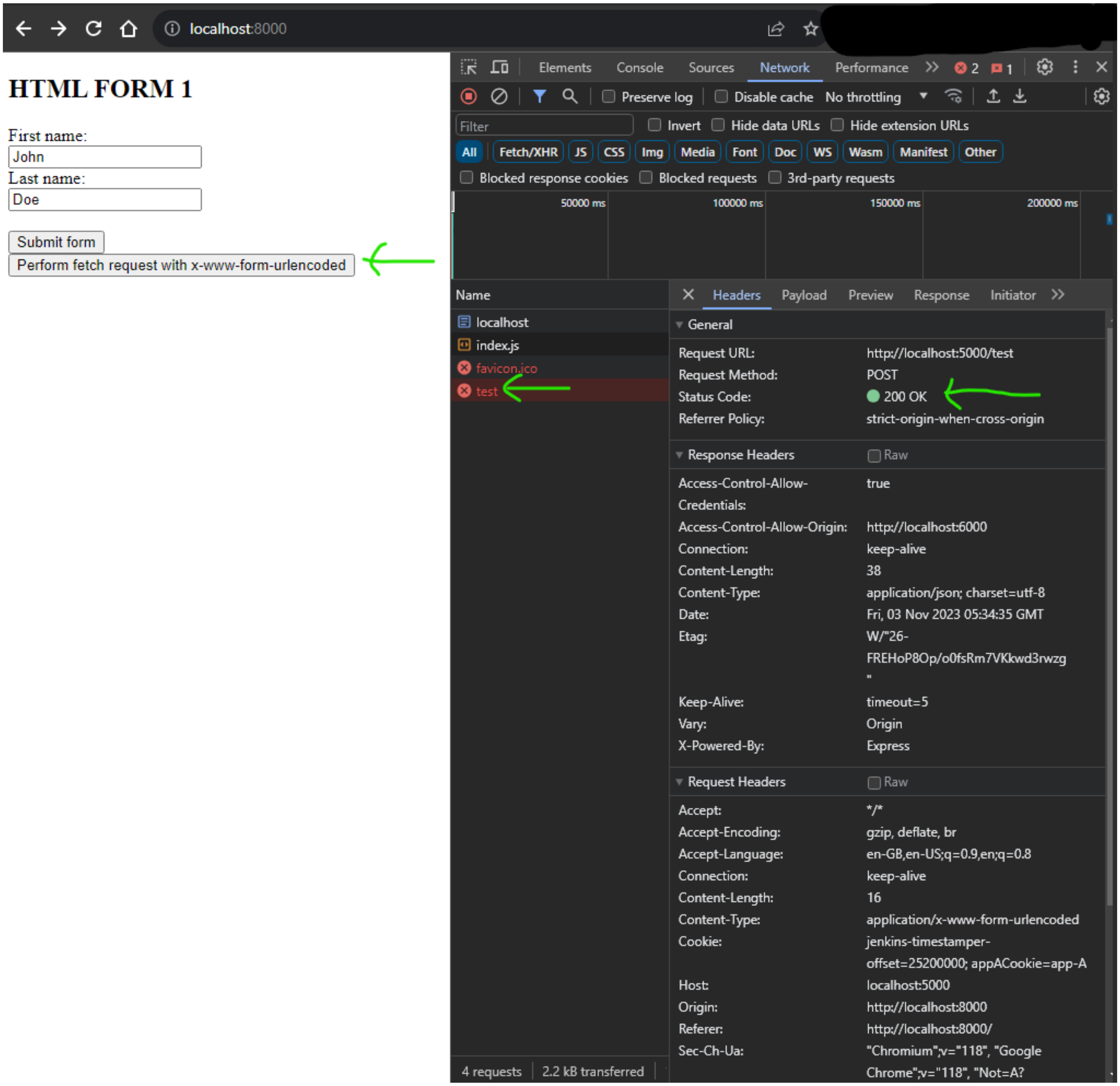
No preflight request when performing fetch with 'x-www-form-urlencoded':

```
//CLIENT
const submitButton = document.getElementById("submitReq");
submitButton.addEventListener("click",()=>{
    fetch("http://localhost:5000/test", {
        method: "POST",
         credentials: 'include',
        headers:{
            'Content-Type':'application/x-www-form-urlencoded'
        },
        body: JSON.stringify({"name":"ivory"})
    })
    .then(res =>{
        if(res.status==200){
            return res.json();
        }else{
           return;
        }
    })
    .then((data) =>{
        console.log("data from backend: ",data);
    })
    .catch(err =>{
        console.log("error occured: ",err);
        return;
    })
});

//SERVER
const express = require("express");
const app = express();
const cors = require('cors');
const port = 5000;
// parse requests of content-type - application/json
```

```
app.use(express.json());
// parse requests of content-type - application/x-www-form-urlencoded
app.use(express.urlencoded({ extended: true }));
  let corsOptions = {
    origin: 'http://localhost:6000',
    credentials: true, // ******* DO NOT set credentials attr to true for all the paths
  }
  app.use(cors(corsOptions));
  app.post('/test', (req, res) => {
    console.log("req is: ",req.body);
    console.log(JSON.stringify(req.headers))
   // res.cookie('appACookie','app-A',{httpOnly: true, secure: true });
    res.status(200).send({message:"Here! have your response"});
  })
app.listen(port, () =>{
    console.log(`listening on port: ${port}`);
});
```

Setting the credentials to be included in the request to make sure it triggers a preflight request.
As you can see in the server side code that the CORS is set to allow only origin "http://localhost:6000".
Client side Origin is "http://localhost:8000".
Backend running on "http://localhost:5000"
Request goes to the server and you can see that the server returns 200 response.
But we still see an error in the browser.



HTML FORM 1

First name:
John

Last name:
Doe

Submit form

Perform fetch request with x-www-form-urlencoded

General

Request URL:	http://localhost:5000/test
Request Method:	POST
Status Code:	● 200 OK
Referrer Policy:	strict-origin-when-cross-origin

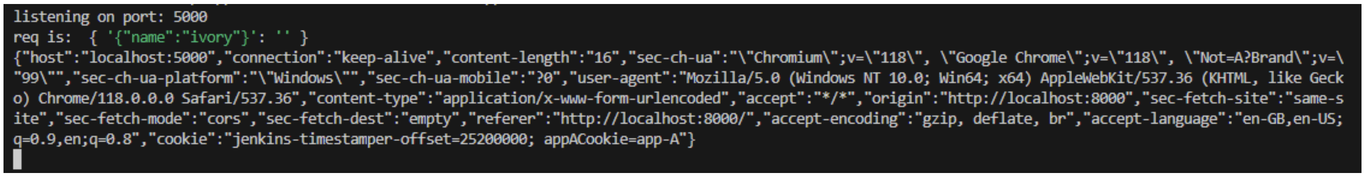
Response Headers ☐ Raw

Access-Control-Allow-Credentials:	true
Access-Control-Allow-Origin:	http://localhost:6000
Connection:	keep-alive
Content-Length:	38
Content-Type:	application/json; charset=utf-8
Date:	Fri, 03 Nov 2023 05:34:35 GMT
Etag:	W/"26-FREHoP8Op/o0fsRm7VKkwd3rwzg"
Keep-Alive:	timeout=5
Vary:	Origin
X-Powered-By:	Express

Request Headers ☐ Raw

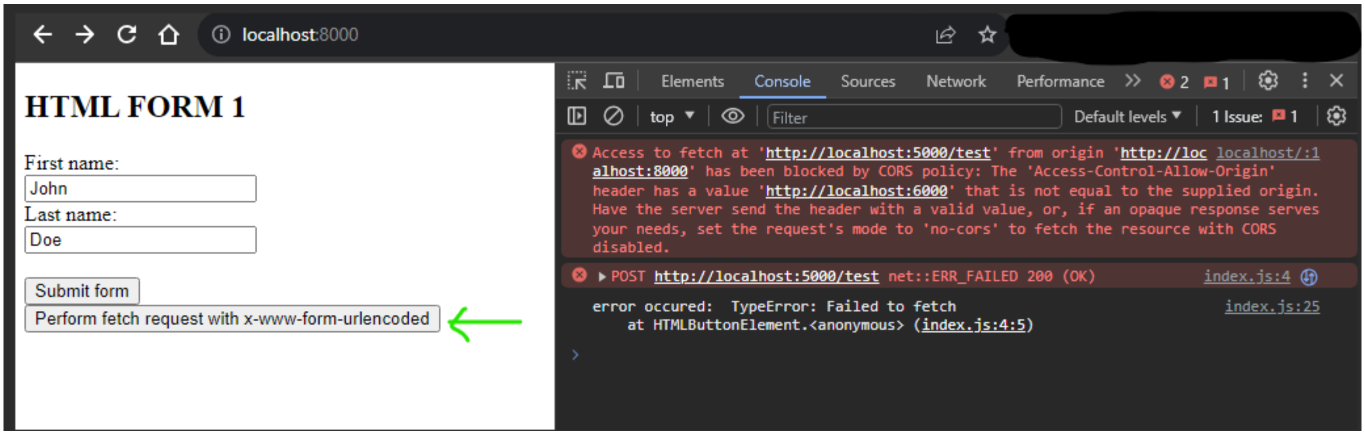
Accept:	*/*
Accept-Encoding:	gzip, deflate, br
Accept-Language:	en-GB,en-US;q=0.9,en;q=0.8
Connection:	keep-alive
Content-Length:	16
Content-Type:	application/x-www-form-urlencoded
Cookie:	jenkins-timestamper-offset=25200000; appACookie=app-A
Host:	localhost:5000
Origin:	http://localhost:8000
Referer:	http://localhost:8000/
Sec-Ch-Ua:	"Chromium";v="118", "Google Chrome";v="118", "Not=A?

Server received the request:



```
listening on port: 5000
req is:  { '{"name":"ivory"}': '' }
{"host":"localhost:5000","connection":"keep-alive","content-length":"16","sec-ch-ua":"\"Chromium\";v=\"118\", \"Google Chrome\";v=\"118\", \"Not=A?Brand\";v=\
"99\"","sec-ch-ua-platform":"\"Windows\"","sec-ch-ua-mobile":"?0","user-agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck
o) Chrome/118.0.0.0 Safari/537.36","content-type":"application/x-www-form-urlencoded","accept":"*/*","origin":"http://localhost:8000","sec-fetch-site":"same-s
ite","sec-fetch-mode":"cors","sec-fetch-dest":"empty","referer":"http://localhost:8000/","accept-encoding":"gzip, deflate, br","accept-language":"en-GB,en-US;
q=0.9,en;q=0.8","cookie":"jenkins-timestamper-offset=25200000; appACookie=app-A"}
```

Browser CORS error: it says the fetch failed. Request reached the server though. That should be enough for my CSRF attack.



[redacted]

HTML FORM 1

First name: John

Last name: Doe

Submit form

Perform fetch request with x-www-form-urlencoded

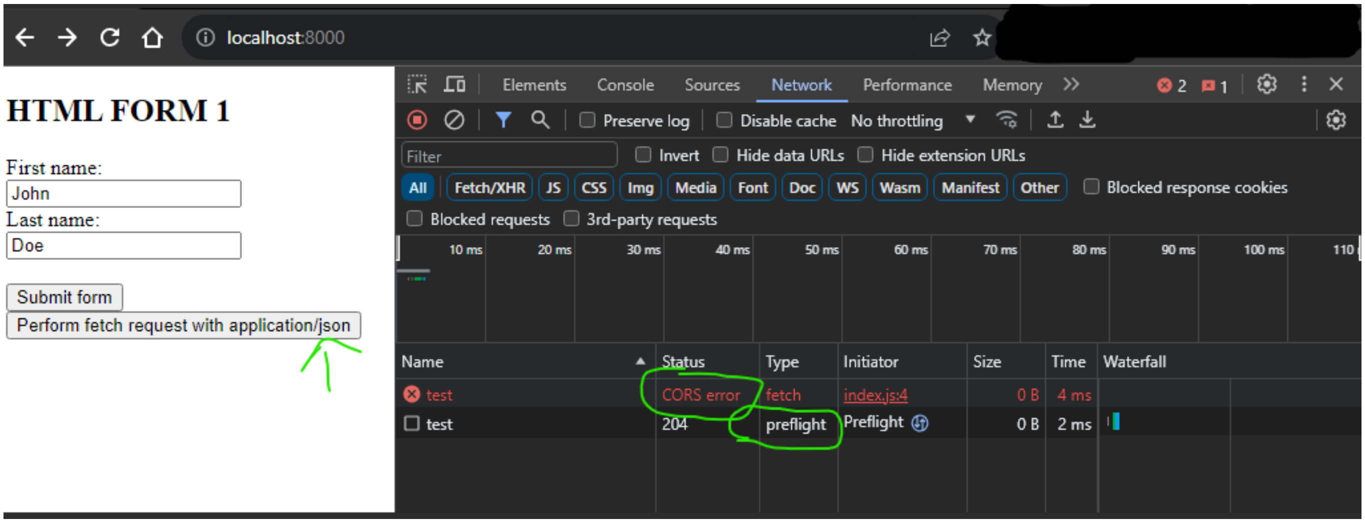
```
Access to fetch at 'http://localhost:5000/test' from origin 'http://localhost:8000' has been blocked by CORS policy: The 'Access-Control-Allow-Origin' header has a value 'http://localhost:6000' that is not equal to the supplied origin. Have the server send the header with a valid value, or, if an opaque response serves your needs, set the request's mode to 'no-cors' to fetch the resource with CORS disabled.          localhost/:1
▸ POST http://localhost:5000/test net::ERR_FAILED 200 (OK)          index.js:4
error occured:  TypeError: Failed to fetch          index.js:25
    at HTMLButtonElement.<anonymous> (index.js:4:5)
```

Content-Type 'application-json' in fetch request:

Change content type in the request to 'application/json':

```
headers:{
        'Content-Type':'application/json'
 },
```

You see that a pre flight request was sent to the server.



[redacted]

HTML FORM 1

First name: John

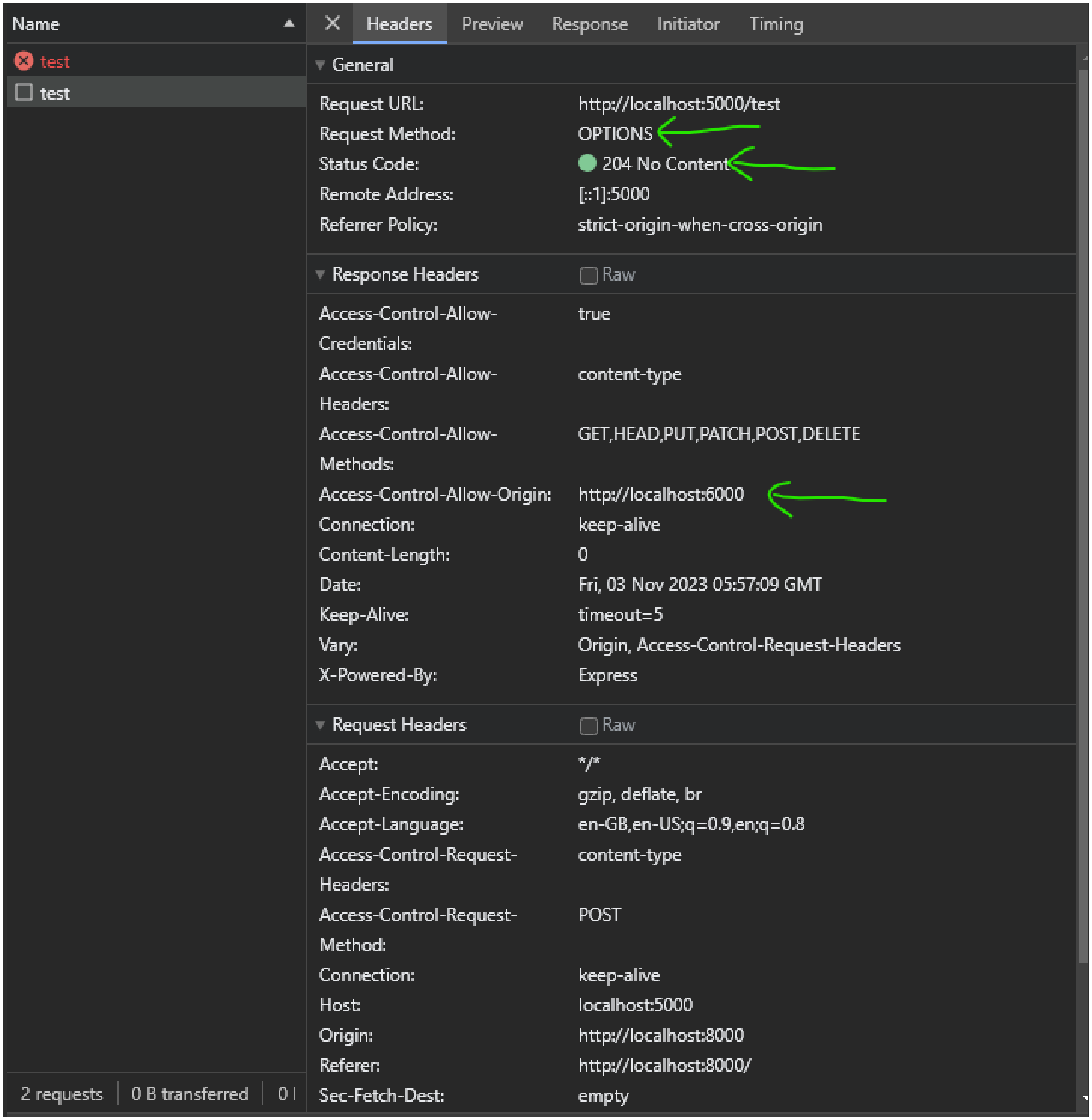
Last name: Doe

Submit form

Perform fetch request with application/json

Name	Status	Type	Initiator	Size	Time	Waterfall
test	CORS error	fetch	index.js:4	0 B	4 ms	
test	204	preflight	Preflight	0 B	2 ms	

Response from header shows that only origin allowed is 'http://localhost:6000'



☒ test
□ test

2 requests | 0 B transferred | 0 l

▼ General

Request URL:	http://localhost:5000/test
Request Method:	OPTIONS
Status Code:	● 204 No Content
Remote Address:	[::1]:5000
Referrer Policy:	strict-origin-when-cross-origin

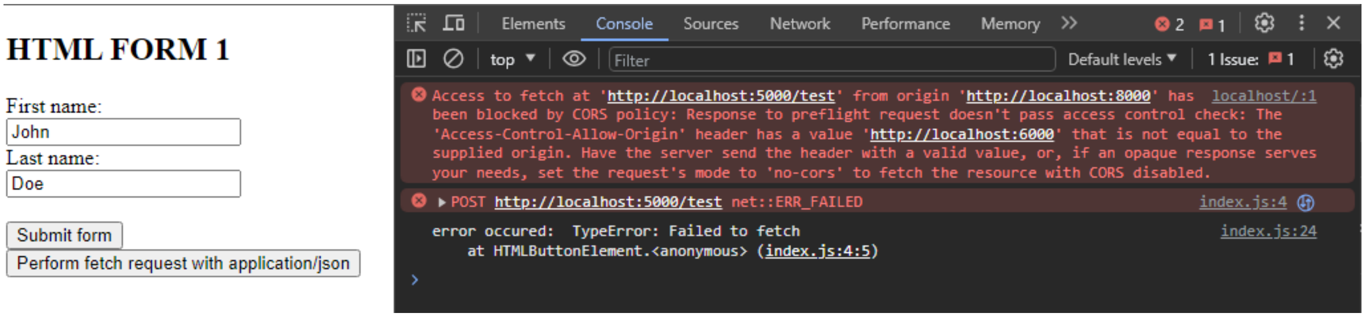
▼ Response Headers □ Raw

Access-Control-Allow-Credentials:	true
Access-Control-Allow-Headers:	content-type
Access-Control-Allow-Methods:	GET,HEAD,PUT,PATCH,POST,DELETE
Access-Control-Allow-Origin:	http://localhost:6000
Connection:	keep-alive
Content-Length:	0
Date:	Fri, 03 Nov 2023 05:57:09 GMT
Keep-Alive:	timeout=5
Vary:	Origin, Access-Control-Request-Headers
X-Powered-By:	Express

▼ Request Headers □ Raw

Accept:	*/*
Accept-Encoding:	gzip, deflate, br
Accept-Language:	en-GB,en-US;q=0.9,en;q=0.8
Access-Control-Request-Headers:	content-type
Access-Control-Request-Method:	POST
Connection:	keep-alive
Host:	localhost:5000
Origin:	http://localhost:8000
Referer:	http://localhost:8000/
Sec-Fetch-Dest:	empty

You will also see an error in the browser console:



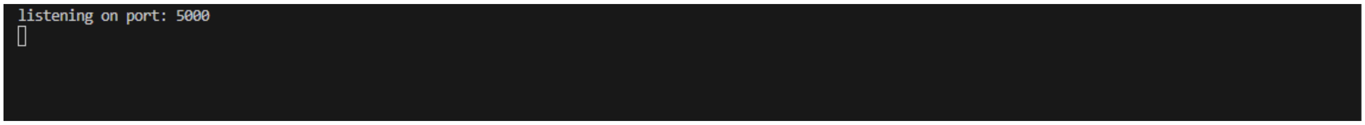
HTML FORM 1

First name:
John
Last name:
Doe

Submit form
Perform fetch request with application/json

```
Access to fetch at 'http://localhost:5000/test' from origin 'http://localhost:8000' has  localhost/:1
been blocked by CORS policy: Response to preflight request doesn't pass access control check: The
'Access-Control-Allow-Origin' header has a value 'http://localhost:6000' that is not equal to the
supplied origin. Have the server send the header with a valid value, or, if an opaque response serves
your needs, set the request's mode to 'no-cors' to fetch the resource with CORS disabled.
▶ POST http://localhost:5000/test net::ERR_FAILED                                       index.js:4
error occured:  TypeError: Failed to fetch                                                index.js:24
    at HTMLButtonElement.<anonymous> (index.js:4:5)
>
```

The server did not receive any request:



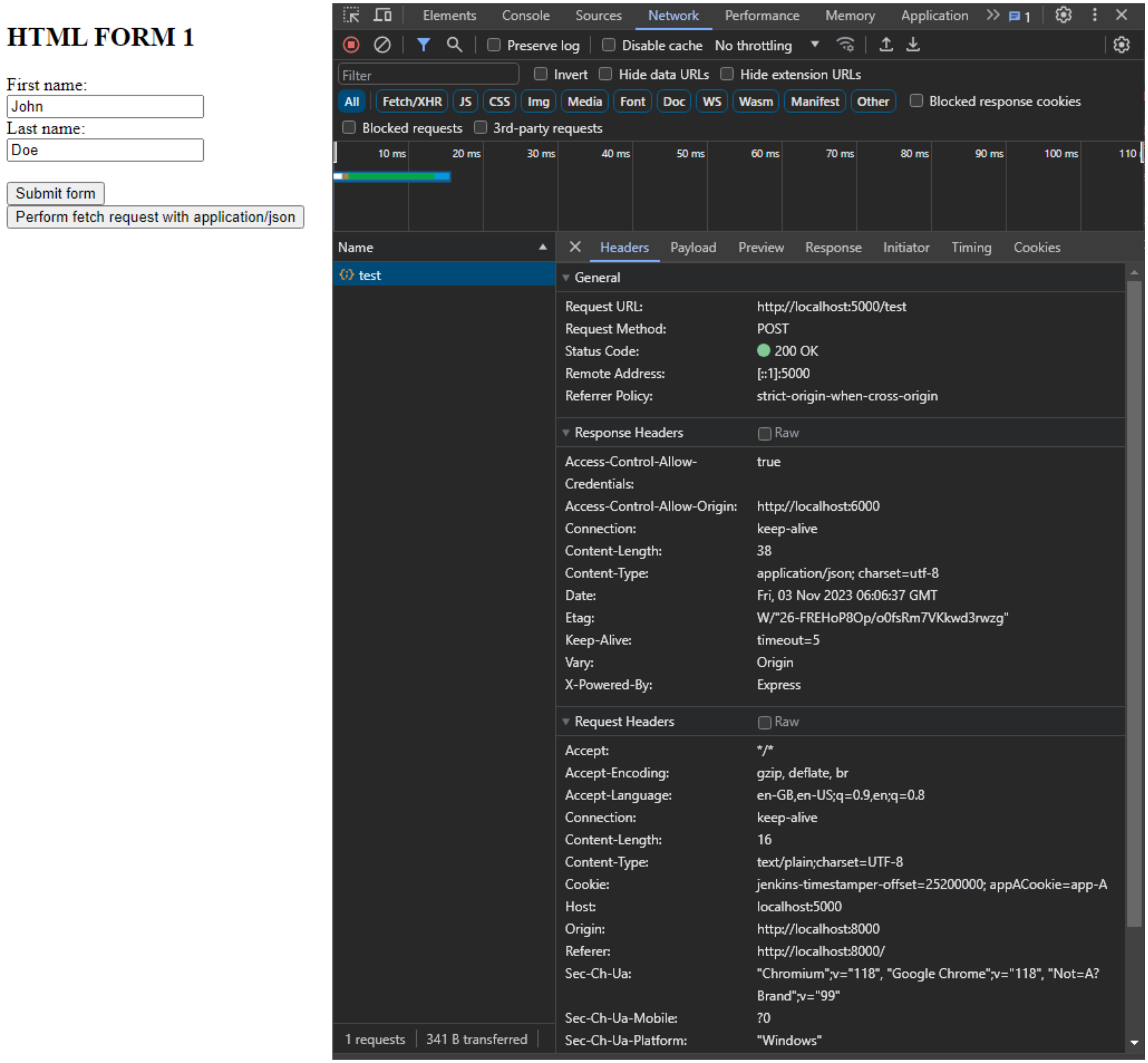
```
listening on port: 5000
```

Set 'mode' to 'no-cors' in request with 'application/json' content type:

```
mode: 'no-cors'
```

No preflight request is sent.

server returns 200 status code.



HTML FORM 1

First name: John

Last name: Doe

General

Request URL:	http://localhost:5000/test
Request Method:	POST
Status Code:	● 200 OK
Remote Address:	[::1]:5000
Referrer Policy:	strict-origin-when-cross-origin

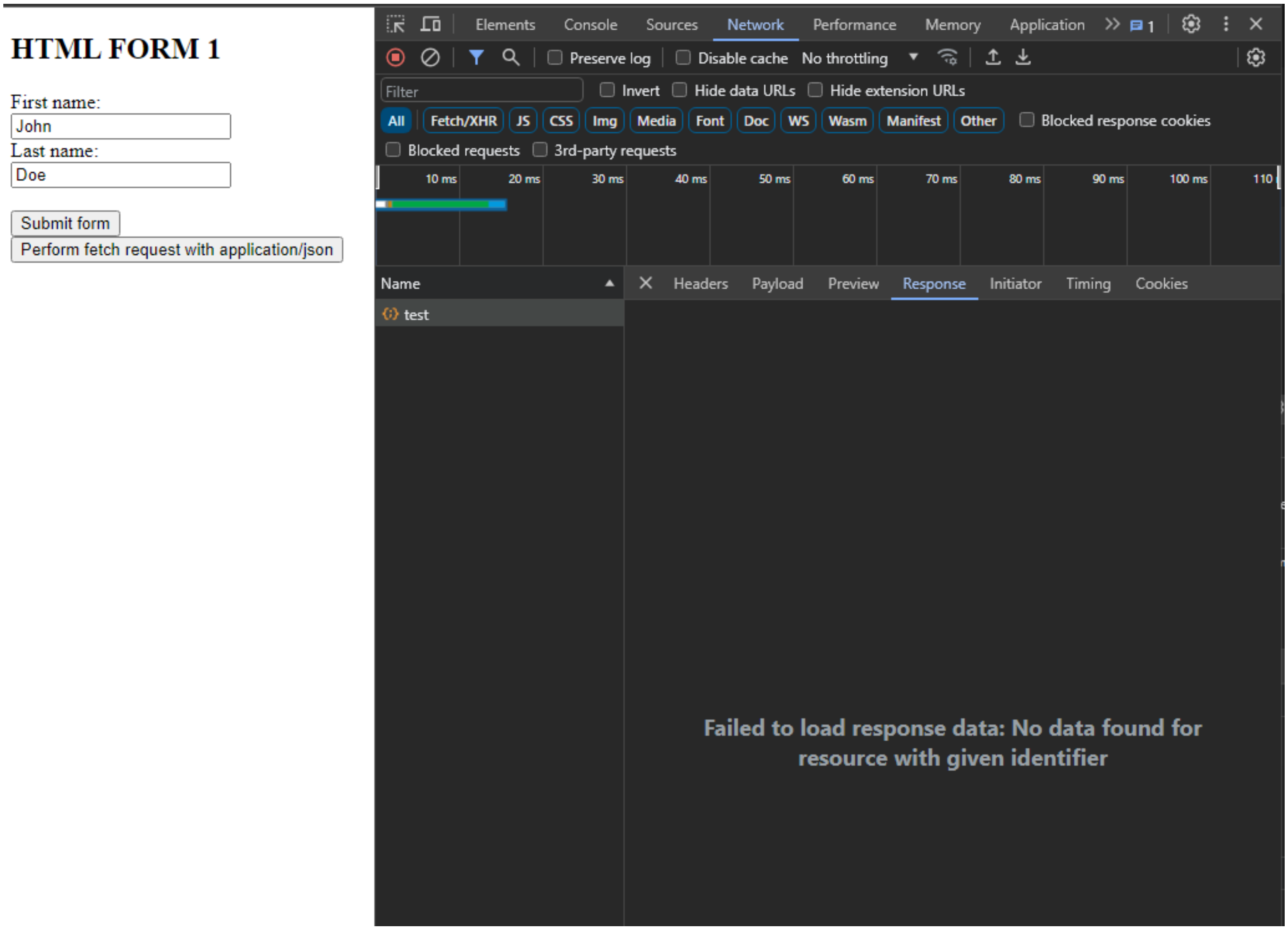
Response Headers □ Raw

Access-Control-Allow-Credentials:	true
Access-Control-Allow-Origin:	http://localhost:6000
Connection:	keep-alive
Content-Length:	38
Content-Type:	application/json; charset=utf-8
Date:	Fri, 03 Nov 2023 06:06:37 GMT
Etag:	W/"26-FREHoP8Op/o0fsRm7VKkwd3rwzg"
Keep-Alive:	timeout=5
Vary:	Origin
X-Powered-By:	Express

Request Headers □ Raw

Accept:	*/*
Accept-Encoding:	gzip, deflate, br
Accept-Language:	en-GB,en-US;q=0.9,en;q=0.8
Connection:	keep-alive
Content-Length:	16
Content-Type:	text/plain;charset=UTF-8
Cookie:	jenkins-timestamper-offset=25200000; appACookie=app-A
Host:	localhost:5000
Origin:	http://localhost:8000
Referer:	http://localhost:8000/
Sec-Ch-Ua:	"Chromium";v="118", "Google Chrome";v="118", "Not=A?Brand";v="99"
Sec-Ch-Ua-Mobile:	?0
Sec-Ch-Ua-Platform:	"Windows"

No data returned by the server though:



HTML FORM 1

First name: John

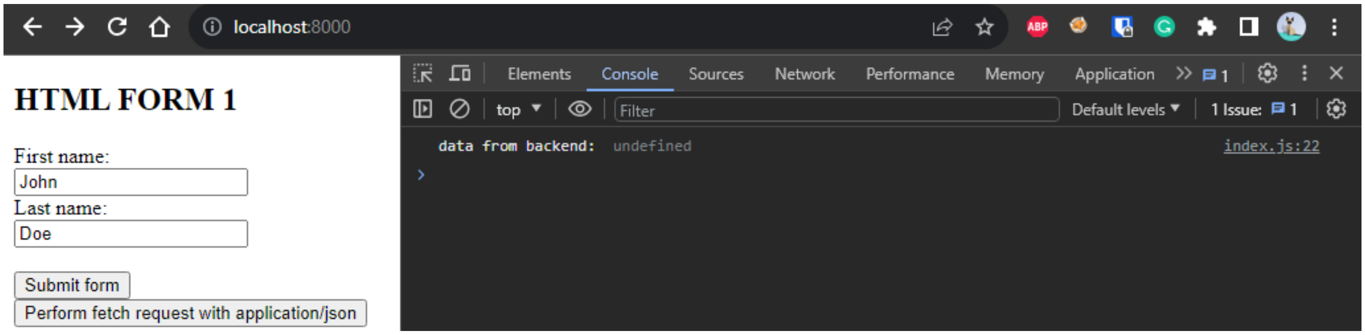
Last name: Doe

Submit form

Perform fetch request with application/json

Failed to load response data: No data found for resource with given identifier

Hence no data written to console from out javascript console.log statement:



HTML FORM 1

First name: John

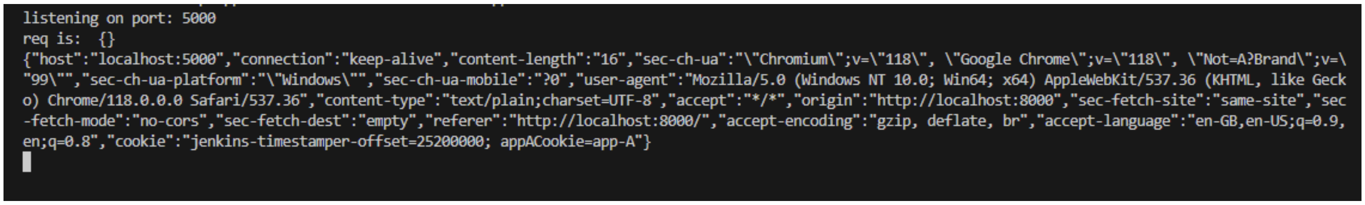
Last name: Doe

Submit form

Perform fetch request with application/json

```
data from backend:  undefined                                   index.js:22
```

In the server also there is no data that was received:



```
listening on port: 5000
req is:  {}
{"host":"localhost:5000","connection":"keep-alive","content-length":"16","sec-ch-ua":"\"Chromium\";v=\"118\", \"Google Chrome\";v=\"118\", \"Not=A?Brand\";v=\
"99\"","sec-ch-ua-platform":"\"Windows\"","sec-ch-ua-mobile":"?0","user-agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck
o) Chrome/118.0.0.0 Safari/537.36","content-type":"text/plain;charset=UTF-8","accept":"*/*","origin":"http://localhost:8000","sec-fetch-site":"same-site","sec
-fetch-mode":"no-cors","sec-fetch-dest":"empty","referer":"http://localhost:8000/","accept-encoding":"gzip, deflate, br","accept-language":"en-GB,en-US;q=0.9,
en;q=0.8","cookie":"jenkins-timestamper-offset=25200000; appACookie=app-A"}
```

What's going on????

TODO: build a cors proxy to bypass preflight requests and allow credentials to be sent.