

2

Cross-origin resource sharing misconfig

Share:



State

○ Duplicate (Closed)

Disclosed

March 13, 2018 3:23pm +0100

Reported To

SEMrush




Weakness

Improper Authentication - Generic

Severity

Low (0.1 ~ 3.9)

Participants



Duplicate Of

#193559

Visibility

Disclosed (Full)

Collapse

TIMELINE · EXPORT



asad_anwar submitted a report to SEMrush.

Feb 2nd (about 1 year ago)

Description

An HTML5 cross-origin resource sharing (CORS) policy controls whether and how content running on other domains can perform two-way interaction with the domain that publishes the policy. The policy is fine-grained and can apply access controls per-request based on the URL and other features of the request.

Trusting arbitrary origins effectively disables the same-origin policy, allowing two-way interaction by third-party web sites. Unless the response consists only of unprotected public content, this policy is likely to present a security risk.

If the site specifies the header Access-Control-Allow-Credentials: true, third-party sites may be able to carry out privileged actions and retrieve sensitive information. Even if it does not, attackers may be able to bypass any IP-based access controls by proxying through users' browsers.

POC1

Request

```
GET /socket.io/?EIO=3&transport=polling&t=M5Ni0Fs HTTP/1.1
Host: mentions.semrush.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:58.0) Gecko/20100101 Firefox/58.0
Accept: /
Accept-Language: ru,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://www.semrush.com/projects/?1517589649
Origin: https://evil.com
Cookie: io=IAU18qXkXe-If7YJKWLc; ref_code=default; usertype=Free-User;
marketing=%7B%22user_cmp%22%3A%22%22%2C%22user_label%22%3A%22%22%7D; localization=%7B%22locale%22%3A%22en%22%7D;
db=us; ga=GA1.2.825109836.1509826800; userdata=%7B%22tz%22%3A%22GMT+5%22%2C%22ol%22%3A%22ru%22%7D;
wp13557=UWYYADDDDDHHKYHHMV-LYXV-XVCW-CMYX-CIXBZKAZVAUVDXVZLAJAB-BCHK-XJKX-CJVC-HVBXKVBXTXYTCDIltkNlo_Jht;
visit_first=1509826800000; referer_purchase=https%3A%2F%2Fmentions.semrush.com%2Fen%2F; __insp_uid=1996669760; exp_cid=0ef68d9d-
5e88-4ef5-bb86-b4f5a34fe13b; referer_url=http%3A%2F%2Fburp%2F; referer_register=https%3A%2F%2Fmentions.semrush.com%2Fen%2F;
__cfduid=d432a9bbe54424efa84dbb3f77c11c1d11515707368; _gid=GA1.2.22716635.1517579789; _bizo_bzid=f15471c2-3666-49b8-8404-
4ca3b049bb62; _bizo_cksm=1F4E1C8613F59F3C; _bizo_np_stats=155%3D3579%2C; [REDACTED]; n_userid=LuWkz1p0bgl3nWHOBFUPAg=;
_gat=1; _uetid=_uet49e7f290; __insp_wid=1632961932; __insp_slim=1517594581797; __insp_nv=false;
__insp_targlpu=aHR0cHM6Ly93d3cuc2VtcnVzaC5jb20vcHJvamVjdHMvPzEIMTc1ODk2NDkj; __insp_targlpt=U0VNcnVzaA%3D%3D;
__insp_norec_sess=true
DNT: 1
Connection: close

Response:
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 02 Feb 2018 19:25:11 GMT
Content-Type: application/octet-stream
Content-Length: 101
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://evil.com
Set-Cookie: io=iSEF-IpwSxyLwaTKW_-
[REDACTED], "upgrades":["websocket"], "pingInterval":25000, "pingTimeout":60000
```

Impact

Take note from request I inject a header Origin: <https://evil.com> then from response it returns Access-Control-Allow-Origin: <https://evil.com> , Which mean there is CORS misconfig here.

1 attachment:
F259746: [sem.JPG](#)



[alla](#) posted a comment.
Thanks for the report, we will investigate this.

Feb 6th (about 1 year ago)



[alla](#) closed the report and changed the status to **Duplicate (#193559)**.
This is a duplicate.

Feb 6th (about 1 year ago)



[asad_anwar](#) requested to disclose this report.

Feb 6th (about 1 year ago)



[sergin](#) agreed to disclose this report.

Mar 13th (about 1 year ago)



This report has been disclosed.

Mar 13th (about 1 year ago)