

Forum:[Hack Forums](#)

Thread: [CORS and Basic Auth](#)

Is CSG - April 13, 2020, 2:57 pm

So I'm performing a penetration test and I'm 99% I found a FP, but want to bounce it off someone else who might be able to reaffirm what I'm seeing. All API endpoints authenticate using Basic Auth. Credentials are not cached from visiting the API directly(no prompt). I don't see how anyone could exploit this since essentially if you attempt to cross origins, you get a API key missing due to no cookie being used.

Request Mockup

```
GET /v0/somethingcool HTTP/1.1
Host: api.myapp.com
Origin: [maliciousurl]
Authorization: Basic BASICAUTHINFO
```

Response Mockup

```
HTTP/1.1 202 Accepted
access-control-allow-credentials: true
access-control-allow-headers: *, Content-Type, Accept, AUTHORIZATION, Cache-Control
access-control-allow-methods: POST, GET, OPTIONS
access-control-allow-origin: [maliciousurl]
access-control-expose-headers: Cache-Control, Content-Language, Content-Type, Expires,
Last-Modified, Pragma
access-control-max-age: 1728000
content-type: application/json
```

{API DATA}

?? - April 13, 2020, 3:59 pm

Did you try XMRHTTP request? CORS can not be exploited directly, in most cases you need to chain it with something like Reflected or STORED XSS.

Is CSG - April 13, 2020, 5:42 pm

I did attempt a XMRHTTP and utilized burp to see if the request was being sent with data in the get parameter like below. I think the problem is it's a standalone API not used by other things. So basically if I do a request, there is nothing cached to utilize because a user doesn't have a cookie or anything saving credentials.

Thoughts?

[pastebin.com/bRtmzLWV](#)