3

CORS (Cross-Origin Resource Sharing)

Share:

State	○ Resolved (Closed)
Disclosed	**October 5, 2016 7:19pm +0200**
Reported To	Legal Robot
Weakness	Improper Authentication - Generic
Bounty	$20
Severity	No Rating (---)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

burpman07 submitted a report to **Legal Robot**. Aug 26th (3 years ago)

Title: CORS (Cross-Origin Resource Sharing)

Category: Others

Affected URL: https://app.legalrobot.com/sockjs/info?cb=pcgb37npst

Description: The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request which allows access from any domain. Allowing access from all domains means that any domain can perform two-way interaction with the application via this request. Unless the response consists only of unprotected public content, this policy is likely to present a security risk.
Production Steps: Just look at the header. You found Access-Control-Allow-Origin: * .
The HTML5 cross-origin resource sharing policy controls whether and how content running on other domains can perform two-way interaction with the domain which 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. If another domain is allowed by the policy, then that domain can potentially attack users of the application.
If a user is logged in to the application, and visits a domain allowed by the policy, then any malicious content running on that domain can potentially retrieve content from the application, and sometimes carry out actions within the security context of the logged in user. Even if an allowed domain is not overtly malicious in itself, security vulnerabilities within that domain could potentially be leveraged by a third-party attacker to exploit the trust relationship and attack the application which allows access.

HTTP Header or Code:

```
GET /sockjs/info?cb=pcgb37npst HTTP/1.1
Host: app.legalrobot.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:50.0) Gecko/20100101 Firefox/50.0
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, br
Referer: https://app.legalrobot.com/profile
Cookie: __cfduid=d07034ecc66ad8b762187ba56471053821472189223; __asc=9d8907e8156c551ef42d543d803;
__auc=9d8907e8156c551ef42d543d803; _ga=GA1.2.1063111763.1472189297; galaxy-sticky=!fqm5S7o42sAL2eD8T-pcd7;
ajs_anonymous_id=%22200f23d8-2cc8-4d1d-9d52-7699609e8c77%22;
meteor_login_token=AP4RUAwKw32XsaKZMv6jKZWuLP5kw7QL17l2ezpplai; _gat=1
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Date: Fri, 26 Aug 2016 05:40:43 GMT
Content-Type: application/json; charset=UTF-8
Connection: keep-alive
Access-Control-Allow-Origin: *
Cache-Control: no-store, no-cache, no-transform, must-revalidate, max-age=0
Vary: Origin
Strict-Transport-Security: max-age=15552000; includeSubDomains
X-Content-Type-Options: nosniff
Server: cloudflare-nginx
CF-RAY: 2d84f357b9b030cc-SIN
Content-Length: 79
```

{"websocket":true,"origins":[":"],"cookie_needed":false,"entropy":1959258093}

Additional Info: Cross-site HTTP requests are HTTP requests for resources from a different domain than the domain of the resource making the request. For instance, a resource loaded from Domain A (http://domaina.example) such as an HTML web page, makes a request for a resource on Domain B (http://domainb.foo), such as an image, using the img element (http://domainb.foo/image.jpg). This occurs very commonly on the web today — pages load a number of resources in a cross-site manner, including CSS stylesheets, images and scripts, and other resources.

Thank You

danrubins closed the report and changed the status to **Resolved**. Aug 26th (3 years ago)

Thanks for the report, we have developed a fix and will deploy it during our next release.

Legal Robot rewarded burpman07 with a **$20** bounty. Aug 26th (3 years ago)

burpman08 filed a duplicate (#164123) and was invited to participate in this report. Aug 31st (3 years ago)

danrubins requested to disclose this report. Sep 5th (3 years ago)

snoopysecurity filed a duplicate (#164527) and was invited to participate in this report. Sep 5th (3 years ago)

This report has been disclosed. Oct 5th (3 years ago)