

87

## Subdomain takeover of resources.hackerone.com

Share:

State Resolved (Closed)Disclosed **May 15, 2020 11:46pm +0530**Reported To **HackerOne**Asset <https://www.hackerone.com>  
(Domain)

Weakness None

Bounty \$500

Severity Low (3.6)

Participants

Visibility Disclosed (Full)

[Collapse](#)

## TIMELINE · EXPORT

**amans** submitted a report to **HackerOne**.

May 1st (about 1 month ago)

Hello,

I just went to <https://resources.hackerone.com/> and it shows an error "Non-hub domain, The URL you've accessed does not provide a hub. Please check the URL and try again." also i've checked the CNAME is pointing to read.uberflip.com which means if it is not added it can be added to any account, as [Uberflip documentation](#) suggests that after your subdomain is pointing to their CNAME which is read.uberflip.com, your subdomain should be added to your account so it shows the URL you chose for your hub. As i couldn't sign up on their website to test due to sign up problems, i just wanted your confirmation whether this subdomain is added in uberflip account or not. If not then claim it otherwise any one can add or claim this to their Uberflip account

**Impact**

Subdomain takeover.

**lasagna** HackerOne triage posted a comment.

May 1st (30 days ago)

Hi **@amans**,

Thank you 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,

**@lasagna****amans** posted a comment.

Updated May 15th (16 days ago)

I just contacted Uberflip personally through their helpdesk, looks like resources.hackerone.com is not setup and maybe added to any account. I'd request your review.

**bencode** HackerOne staff posted a comment.

May 9th (22 days ago)

Hey **@amans**,

Sorry, I don't fully understand how Uberflip works, so I'm also unsure if there is a validation step when someone attempts to register a subdomain. I'm reaching out to a few folks to get some answers. Thanks for your patience!

**amans** posted a comment.

May 9th (22 days ago)

**@bencode** - Alright!**bencode** HackerOne staff changed the status to Triaged.

May 11th (20 days ago)


Response from Uberflip:

The only protection is the customer's proper management of their subdomains.

For this reason we do not recommend customers point wildcards to us, and that they follow DNS management best practices by periodically reviewing all their hostnames and subdomains.


Looks like a subdomain takeover was possible for this.

 **bencode** HackerOne staff changed the status to Retesting. Updated May 11th (20 days ago)

 **amans** posted a comment. Updated May 11th (20 days ago)  
Hello **@bencode** - Oops, i apologies i got retest part wrong. I can still see in dig response that resources.hackerone.com is still pointing to CNAME read.uberflip.com, it is not removed. Can you confirm sir?


Thanks

 **amans** completed a retest. May 11th (20 days ago)


 **amans** posted a comment. Updated May 11th (20 days ago)  
As such i can't see the uberflip page anymore when I go to resources.hackerone.com and I know that DNS changes takes sometime to reflect changes, also you have not mentioned that CNAME was removed or not but due to precaution I chose that it's still reproducible. Just looking for your confirmation.

Thanks!!


 **bencode** HackerOne staff updated the severity to Low (3.4). May 12th (20 days ago)


 **HackerOne** rejected the retest from the retester. Updated May 20th (11 days ago)  
Fair point and sorry for the lack of communication on what we changed. From our side, we still needed the subdomain, so instead we claimed the subdomain in Uberflip, so I think you shouldn't be able to see the "Non-hub domain" error message any longer. Can you confirm that?

 **bencode** HackerOne staff changed the status to Triaged. May 12th (20 days ago)  
Revert report state from retesting to previous state


 **amans** posted a comment. May 12th (20 days ago)  
**@bencode** - I can confirm that i don't see "Non-hub domain..." message anymore, but may I know why the severity is low? whereas this is subdomain takeover?


 **bencode** HackerOne staff changed the scope from <https://hackerone.com> to <https://www.hackerone.com>. May 12th (20 days ago)

 **bencode** HackerOne staff posted a comment. May 12th (20 days ago)  
There are a couple factors, but I think primarily the privileges and confidential data were the primary factors in the lower score. The privileges was high as you need to sign up via uberflip and buy some version of their product. Additionally, the [www.hackerone.com](https://www.hackerone.com) domain has less confidential data as compared to our platform data and was lowered.

 **bencode** HackerOne staff posted a comment. May 12th (20 days ago)  
**@bencode** - I can confirm that i don't see "Non-hub domain..." message anymore  
Thanks for confirming, I'll award a \$50 bonus for the retest effort when we award the bounty.

 **bencode** HackerOne staff changed the status to Retesting. Updated May 12th (20 days ago)

 **amans** posted a comment. Updated May 12th (20 days ago)  
**@bencode** - Unfortunately sir, Signing up was not an issue, as this is a security issue we just need to prove it, if you had asked me to provide a PoC, it would have never been a issue, secondly uberflip is a public product not a private, anyone can signup and do whatever they want to but requires little extra steps which can be done but will take some time. I would have managed to sign up and buy the product too if you had asked me to. If its a matter of just signing-up and buying product then sir i'd say it is not justifiable for severity. Its a subdomain takeover and I'd have hosted and shown whatever i wanted to representing hackerone, subdomain takeover is same for all, I don't know how are you reviewing this but unfortunately i'd request a little more justification because I am not satisfied. I have seen many takeover where info.hacker.one which was not even near to hackerone was handled with good severity and still mine is a main domain subdomain. Looking for your review kindly. An attacker could've used someone's or theirs uberflip account if they had one to takeover. if not then creating one was not a big issue. Subdomain takeover is different, 95% of companies who strictly doesn't allow \*.domain.com testing, only specific domain testing, accepts subdomain takeovers with a good severity and handle them with priority. As this was hackerone and trustworthy enough so i thought proving vulnerability would be fine but i didn't know signing up would cause issue here, if it was then you could've asked me to provide clear PoC after you have confirmed that it can be taken over. [www.hackerone.com](https://www.hackerone.com) is a marketing site and you shouldn't consider my vulnerability with it, mine is subdomain takeover,

i've not found something in resources.hackerone.com i have found an issue to takeover it completely. It is a subdomain which is not Out-of-scope by hackerone, also hackerone states that anything found in our systems we'll fix it, you should consider this as a subdomain takeover sir kindly and shouldn't compare it with [www.hackerone.com](http://www.hackerone.com) .

Thanks



amans completed a retest.

May 12th (20 days ago)



amans posted a comment.

May 12th (20 days ago)

I'd have to research how uberflip works and what could we have achieved after taking over subdomain. Give me sometime kindly.

Would be thankful.



amans posted a comment.

Updated May 15th (16 days ago)

@bencode Sir, i asked them about if it'd be possible to show our content, this was their reply, this is what i can most do without having access to the hub itself because if i had access to the hub i could myself check what could be achieved. Anyways this was their reply to show content of our choice from other web. If we are able to even little content of our choice then i believe the subscription charges are worth it which i know are expensive but we can gather much data because of that and due to hackerone.com subdomain. Still, i'd request a review on severity. I have given my points. Rest decision is yours.

Thanks

██████████



amans posted a comment.

Updated May 12th (19 days ago)

Ability to add as little content of our choice changes the impact alot, we can gather data aswell as exploit.

Thanks



HackerOne awarded \$50 to the retester for completing the retest.

Updated May 20th (11 days ago)

Thanks for verifying!



bencode HackerOne staff closed the report and changed the status to Resolved.

May 12th (19 days ago)



bencode HackerOne staff posted a comment.

May 12th (19 days ago)

@amans, let me review the information you provided with my team and I'll get back to you.



amans posted a comment.


May 12th (19 days ago)

@bencode - Sure sir!



amans posted a comment.

Updated May 15th (16 days ago)

@bencode Sir - Some more options to show content of our choice, i have attached it below and sir i have noticed that in CVSS you have chosen privileges requirement `high` i'd request you to set it to `low` because Uberflip is a public product not private, if they were totally private i would have agreed with your decision, they must be costly but i have mentioned before that we can show content of our choice and not stuck to only [www.hackerone.com](http://www.hackerone.com)  due to this benefit attacker can use someone's, their company uberflip because they are in benefit in this takeover, using uberflip is not a issue, main thing is taking over subdomain, also i don't think if convinced Uberflip would mind providing us a trial, because there's no user interaction required in taking over subdomain, but once a subdomain is registered, it's of uberflip we can ask them to display content of our choice and there are various ways to display our content aswell i have mentioned before some and attaching now too.

██████████



amans posted a comment.

May 15th (16 days ago)

As mentioned above one of the option to show pages of our choice is iFraming website pages of our choice would display those pages in our subdomain which is registered for uberflip hub.



HackerOne rewarded amans with a \$500 bounty.

May 15th (16 days ago)

Hi @amans - thanks again for your report! We've reviewed this internally and are sticking with our initial assessment that this was a low severity vulnerability for us. You are correct that an attacker could've used this to deface a HackerOne.com domain, but it didn't affect the confidentiality of anything. Thanks!



amans requested to disclose this report.

Updated May 15th (16 days ago)

Well, that'd be a first subdomain takeover being treated with a low severity and of hackerone aswell. I don't know what more we look forward to achieve after taking over subdomain. Just wondering what subdomain takeover are meant then? in CVSS you set privilege escalation `high`

whereas it should be `low` uberflip is a public product not private the one more reason of setting it up `high` was this vulnerability don't reach `medium` severity, i have shown a way where we can deface H1 subdomain and at first you thought that subdomain would only serve as [www.hackerone.com](https://www.hackerone.com) once taken over and that is why it was being treated as `low` vulnerability, if not `low` cause this is a subdomain takeover must be treated as a `medium` vulnerability, I am not happy with your severity and reward decision and the justification about this vulnerability, wasn't expecting this from HackerOne, this didn't affect confidentiality but could have used in a way to affect it badly you know that aswell, also how other companies treat subdomain takeovers you know that too. Anyways, i would recommend removing this line from your policy we'll gladly work with you to resolve that issue and ensure you are fairly compensated for your discovery. I have seen info.hackerone.com takeover disclosure too and it was treated above than my vulnerability. Kindly accept the disclosure request and make sure to remove [REDACTED] and [REDACTED] because it discloses uberflip support representative's names.

Thanks



amans posted a comment.

May 15th (16 days ago)

Here is a hackerone blog <https://www.hackerone.com/blog/Guide-Subdomain-Takeovers> showing subdomain takeovers and its impacts, and here @jobert telling this wouldn't hurt confidentially. Right. H1 just looks forward to teach researchers so they can find good issues in other companies but not in H1 itself. Thanks



jobert HackerOne staff posted a comment.

May 15th (16 days ago)

Hi @amans - we're happy to agree to the disclosure! Before we do though, you're saying that you disagree with my take on the impact on confidentiality here but aren't telling us why you think so. We don't have any good reason to low-ball you on a bounty award, but do expect you to help us understand the impact better if we (apparently) fail to do so correctly. Thanks!



amans posted a comment.

Updated May 15th (16 days ago)

@jobert Okay sir, how this #202767 affected confidentially directly? whereas it was info.hacker.one and mine is hackerone.com subdomain, it was rewarded with \$1000 independently twice for two takeovers saying that " While this is a vulnerability in a third-party service (Unbounce), we had started using for a few marketing landing pages as a test, so we greatly appreciate the report to make sure that any services and systems we use are protected. " and not even a hackerone.com subdomain, it is 3 years old report whereas now companies are more concerned about security and rewards etc everything improved as of now than 3 years before, i have a question why did you treated that report well when it was a hacker.one subdomain and reporter didn't even show impact anywhere and now i have to? Hacker.one was no where in scope back then if seen with fact but it was still treated nicely? do we or hackerone customers go to hacker.one to submit vulnerabilities or view reports? i don't go there. I go to hackerone.com but why? due to the trust, and if attacker has defaced hackerone.com subdomain, victim would surely go there due to hackerone.com subdomain and trust! It can be used for phishing, data entry, surveys, xss and many more things I believe defacing means that right? you chose `High` option in severity for `Privilege Escalation` i mentioned before it should be `low` if not `none` because uberflip is a public product, but you chose it `high` so this vulnerability doesn't go above `low` severity because changing it to `low` would make this vulnerability `medium` severe. I am quite surprised I have to explain the impact of that vulnerability which is quite straight forward and not complex. The main thing is a domain, which is hackerone.com domain, which people trusts and due to hackerone.com subdomain we could have done much more actions. People wont trust a phishing page with pleaselogin.tk domain but would trust resources.hackerone.com.

At first you said it would serve as [www.hackerone.com](https://www.hackerone.com) only after taking over subdomain that's why it is being treated low, I shown the way of defacing it, then still its a low severe vulnerability. Totally fine. As i couldn't takeover myself and see what could happen. Here are some points i am mentioning below what could be achieved after defacing and how it'd hurt confidentially.

I have a recommendation, why don't you put any type of survey in resources.hackerone.com and mention that winner would get \$500 as a reward, and once done just tell me, I'd send that link to victims and let's see if they'd respond or not, I think that'd affect confidentiality of hackerone customers and researchers, and also think that if that survey was served in other domain which is not known and random to people, would people still fill that survey for that website then? and now you'd say this is social engineering i believe, well what are subdomain takeovers then? I am hoping that i'd just get more questions so the severity don't get increased, This was a `high` severity issue if was treated fairly, but unfortunately, it was never. I can't argue more, you can disclose the report after review and don't forget to remove the attachments I mentioned previously before disclosure if possible, thanks.



jobert HackerOne staff updated the severity from Low (3.4) to Low (3.6).

May 15th (16 days ago)



jobert HackerOne staff posted a comment.

May 15th (16 days ago)

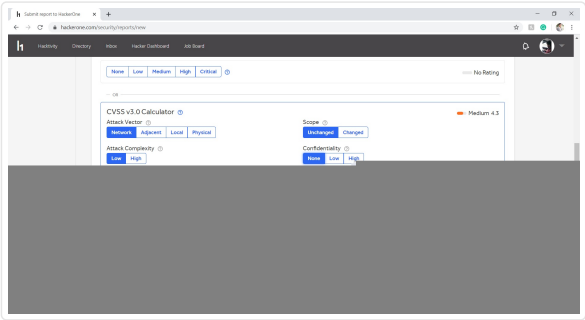
Hi @amans - our threat model looks very different from 3 years ago. What could've achieved with a subdomain takeover in the past is not a guarantee for the future. We currently are not using resources.hackerone.com (e.g. we don't pull data from it and don't link to it). You're right that you could've set it up to host a rogue survey to ask people questions that could impact confidentiality, but that's a potential side effect of social engineering and phishing and not of the vulnerability itself. I've updated the CVSS based on your feedback, but it still ended up being a low severity vulnerability. Our marketing sites have their Environmental Score set to `C:M, I:L, A:L`, which brings down the severity of a medium to a low.



amans posted a comment.

May 15th (16 days ago)

@jobert - I am unsure sir, how your CVSS calculator works and how mine works.



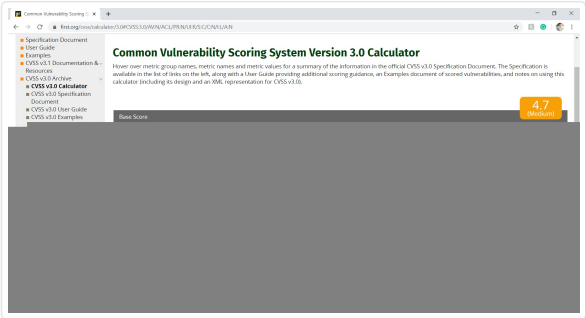
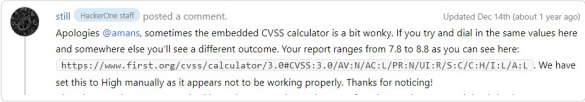
1 attachment:  
F829805: [Hackerone\\_CVSS.jpg](#)



jobert HackerOne staff posted a comment. May 15th (16 days ago)  
@amans Can you select [www.hackerone.com](#) as asset? That should reduce it to a 3.6. Here is another CVSS calculator that shows the same: <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>. The vector string for this vulnerability is:  
AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/CR:M/IR:L/AR:L/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X.



amans posted a comment. Updated May 15th (16 days ago)  
After using first.org CVSS its medium 4.3 <https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N> Also in one of my report H1 staff mentioned that CVSS of H1 is sometime is bit wonky i can link to the report if want and you changed user interaction = required but without confidentially being hurt? Obviously if user interacts they'll provide with some information? so confidentially would hurt so confidentially would = low too.



2 attachments:  
F829814: [first\\_CVSS\\_calculator.jpg](#)  
F829813: [H1\\_Staff.jpg](#)



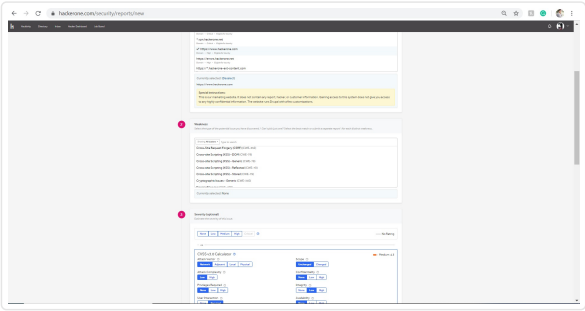
jobert HackerOne staff posted a comment. Updated May 15th (16 days ago)  
Can you set the Environmental Score to:  

- Confidentiality: Medium
- Integrity: Low
- Availability: Low

The scope is also set to Unchanged for this report, not Changed. The score should come out to 3.6, which is the same as our platform.



amans posted a comment. May 15th (16 days ago)  
After selecting www asset same is result, and after modifying and defacing resources.hackerone.com, i don't find out if there is any meaning of [www.hackerone.com](#) anymore. Still, here are results.



1 attachment:

F829816: [www\\_asset.jpg](#)



amans posted a comment.

Updated May 15th (16 days ago)

@jobert I am still unsure how integrity requirement (IR) is **Low** when victim would be filling up survey or anything of resources.hackerone.com and not a random domain? also we are not bound to surveys can do much more actions too. It should be changed to **medium** which would turn vulnerability severity to **medium**, that'd be a first hackerone report where CVSS is being look after so closely, i have seen a report where H1 staff mistakenly leaked their session and it was treated with critical severity and here using hackerone.com real subdomain can't we even trap a single customer or hacker and still this is being treated as low, anyways sir you can go ahead and disclose this report? Thanks!

- our threat model looks very different from 3 years ago.

Well, i think threats are increased in years than years ago because hackerone has grown in years and has more customers, researchers than years ago + it was hacker.one subdomain not hackerone.com subdomain.



jobert HackerOne staff posted a comment.

Updated May 15th (16 days ago)

@amans It looks like you may have stumbled upon a functional bug, because I get the correct results (see screenshot). When I calculate the CVSS on NIST or MITRE, I also end up with a CVSS of 3.6 - so I trust that it's calculating it correctly. I'll escalate this to the team to look into it. It won't change the outcome of this report though.

○

1 attachment:

F829824: [Screen\\_Shot\\_2020-05-15\\_at\\_11.12.24\\_AM.png](#)



jobert HackerOne staff changed the report title from **Possible subdomain takeover [Uberflip]** to **Subdomain takeover of resources.hackerone.com**.

May 15th (16 days ago)



jobert HackerOne staff agreed to disclose this report.

May 15th (16 days ago)

Thanks again, @amans!



This report has been disclosed.

May 15th (16 days ago)



amans posted a comment.

Updated May 15th (16 days ago)

Thanks for disclosing :-)