

Bug Bounty POC

All Bug Bounty POC write ups by Security Researchers.



GUEST WRITEUP

9



Bugcrowd's Domain & Subdomain Takeover!


BY [MUHAMMADKHIZERJAVED](#) · AUGUST 18, 2017

Hello [BugBountyPoc](#) viewers, this is Khizer again, I decided to Write about this Issue because I have seen some people are still confused about "Fastly error: unknown domain" Many Subdomains of BugBounty programs have This error on their Subdomains and People Report is Without Claiming or Try to claim That..

But If you try to claim such Subdoamin it will ask U to add Main domain instead of subdomain... So back to the main story, last Sunday i decided to test Bugcrowd itself as it's one of most secure BugBounty programs!

While i was checking Reverse IP Lookup For bugcrowd.com I got these 2 results

Reverse IP Lookup Results — 2 domains hosted on IP address 104.20.60.51		
Domain	View Whois Record	Screenshots
1. bugcrowd.com		
2. bugcrowdtrafficcontrol.com		


DOMAINTOOLS

[PROFILE](#)
[CONNECT](#)
[MONITOR](#)
[ACQUIRE](#)
[SUPPORT](#)





Enter an IP address and our patented Reverse IP Lookup tool will show you all of the domains currently hosted there. Results include all gTLD domains and any known ccTLD domains.

Lookup Connected Domains

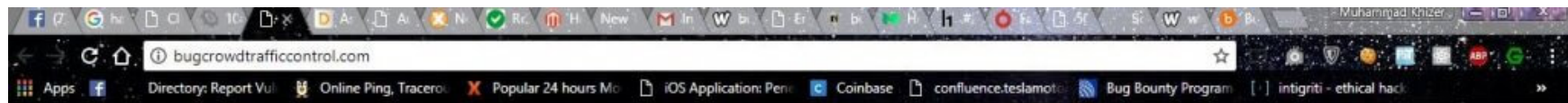
LOOKUP

Example: 65.55.53.233 or 64.233.161.%

Reverse IP Lookup Results — 2 domains hosted on IP address 104.20.60.51

Domain	View Whois Record	Screenshots
1. bugcrowd.com		
2. bugcrowdtrafficcontrol.com		

As I Frequently Visit bugcrowd.com The other domain bugcrowdtrafficcontrol.com was New for Me as I haven't seen this domain I decided to Pay a Visit 😊 and I saw an error on the domain!



Fastly error: unknown domain: bugcrowdtrafficcontrol.com. Please check that this domain has been added to a service.

When I saw the error It suddenly clicks to my mind That I have seen such errors on subdomains of some websites but when I tried to takeover them via Fastly services They ask to add the main domain But in this case It was the main domain. So I checked the WHOis info for this domain and it was!

Whois	Website Info	History	DNS Records	Diagnostics
DNS Records for bugcrowdtrafficcontrol.com				
Hostname	Type	TTL	Priority	Content
bugcrowdtrafficcontrol.com	SOA	3599		edna.ns.cloudflare.com dns.cloudflare.com 2025379154 10000 2400 604800 3600
bugcrowdtrafficcontrol.com	NS	86399		edna.ns.cloudflare.com
bugcrowdtrafficcontrol.com	NS	86399		lee.ns.cloudflare.com
bugcrowdtrafficcontrol.com	A	299		104.20.4.239
bugcrowdtrafficcontrol.com	A	299		104.20.5.239
bugcrowdtrafficcontrol.com	MX	299	5	alt2.aspmx.l.google.com
bugcrowdtrafficcontrol.com	MX	299	5	alt1.aspmx.l.google.com
bugcrowdtrafficcontrol.com	MX	299	1	aspmx.l.google.com
bugcrowdtrafficcontrol.com	MX	299	10	alt4.aspmx.l.google.com
bugcrowdtrafficcontrol.com	MX	299	10	alt3.aspmx.l.google.com
www.bugcrowdtrafficcontrol.com	A	299		104.20.61.51
www.bugcrowdtrafficcontrol.com	A	299		104.20.60.51
www.bugcrowdtrafficcontrol.com	AAAA	299		2400:cb00:2048:1::6814:3c33
www.bugcrowdtrafficcontrol.com	AAAA	299		2400:cb00:2048:1::6814:3d33
www.bugcrowdtrafficcontrol.com	CNAME	299		www.bugcrowd.com

Diagnostics

DNS Records for bugcrowdtrafficcontrol.com

Hostname	Type	TTL	Priority	Content
----------	------	-----	----------	---------

bugcrowdtrafficcontrol.com	SOA	1551		edna.ns.cloudflare.com dns.cloudflare.com 2025379154 10000 2400 604800 3600
----------------------------	-----	------	--	---

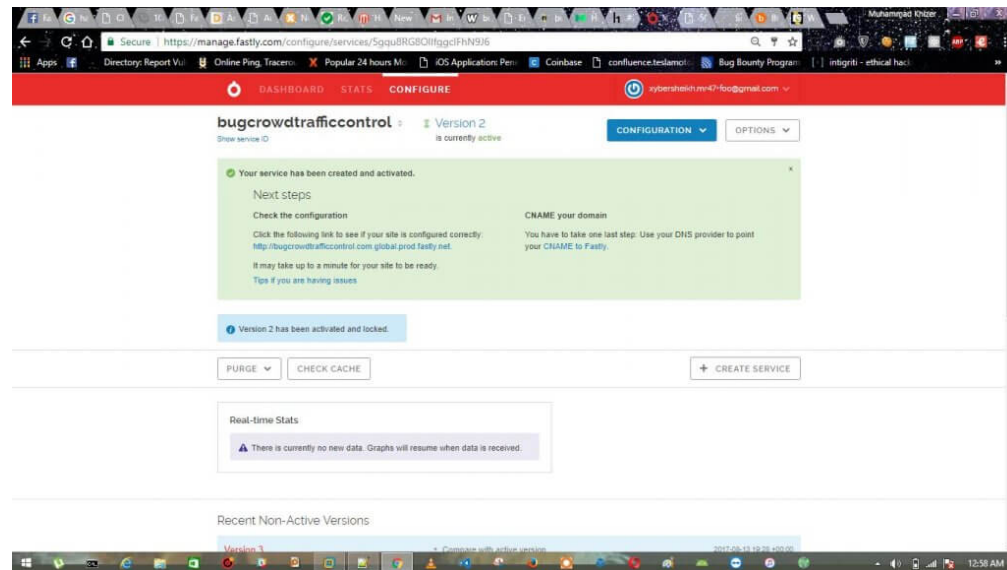
bugcrowdtrafficcontrol.com	NS	86399		edna.ns.cloudflare.com
----------------------------	----	-------	--	------------------------

bugcrowdtrafficcontrol.com	NS	86399	lee.ns.cloudflare.com
bugcrowdtrafficcontrol.com	A	299	104.20.5.239
bugcrowdtrafficcontrol.com	A	299	104.20.4.239
bugcrowdtrafficcontrol.com	MX	299 5	alt2.aspmx.l.google.com
bugcrowdtrafficcontrol.com	MX	299 5	alt1.aspmx.l.google.com
bugcrowdtrafficcontrol.com	MX	299 1	aspmx.l.google.com
bugcrowdtrafficcontrol.com	MX	299 10	alt4.aspmx.l.google.com
bugcrowdtrafficcontrol.com	MX	299 10	alt3.aspmx.l.google.com
www.bugcrowdtrafficcontrol.com	A	299	104.20.60.51
www.bugcrowdtrafficcontrol.com	A	299	104.20.61.51
www.bugcrowdtrafficcontrol.com	AAAA	299	2400:cb00:2048:1::6814:3c33
www.bugcrowdtrafficcontrol.com	AAAA	299	2400:cb00:2048:1::6814:3d33
www.bugcrowdtrafficcontrol.com	CNAME	299	www.bugcrowd.com

and this Information is Enough for Me to Confirm that the domain was indeed owned by Bugcrowd!

TAKEOVER:

Well I opened My Fastly account and tried to make a Service named bugcrowdtrafficcontrol.com & With teh IP of the domain....., And Boom... It says!



Your service has been created and activated.

Domain 'bugcrowdtrafficcontrol.com' was created

2017-08-13 19:15 +00:00

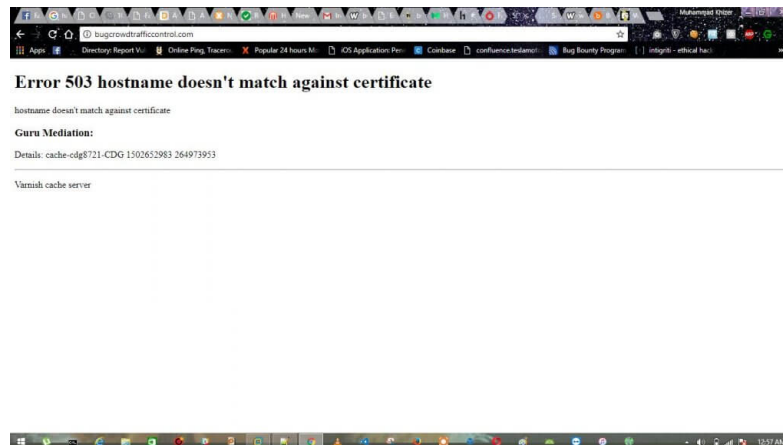
by khizer

Click the following link to see if your site is configured correctly:

<http://bugcrowdtrafficcontrol.com.global.prod.fastly.net>.

It may take up to a minute for your site to be ready.

So Now as The domain is added to my account i visit the domain again an This time the error was changed to



Error 503 hostname doesn't match against certificate

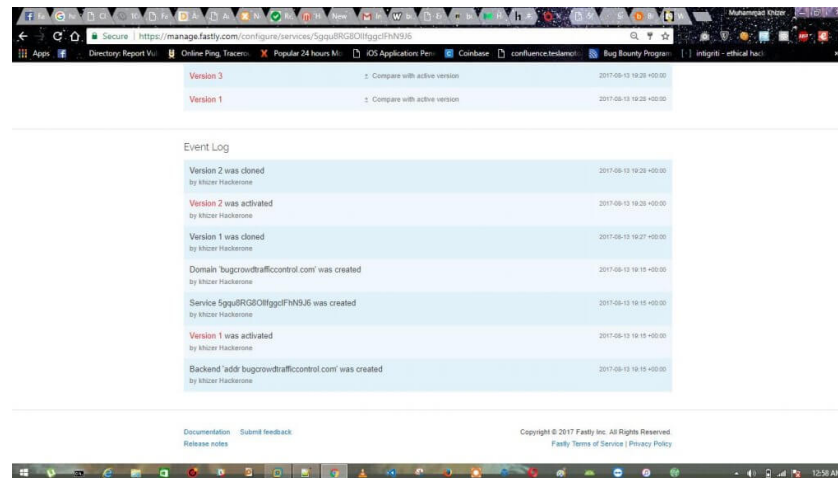
hostname doesn't match against certificate

Guru Mediation:

Details: cache-cdg8721-CDG 1502652983 264973953

Varnish cache server

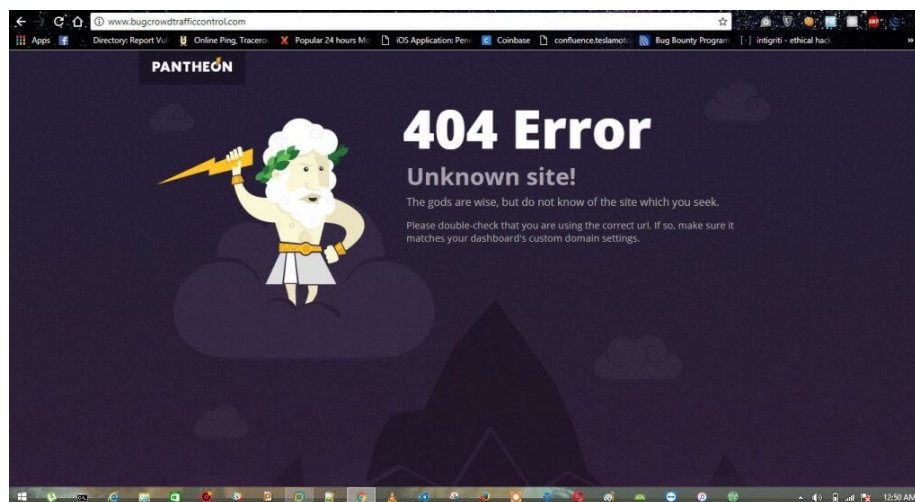
the Error was same to My Fastly service URL <http://bugcrowdtrafficcontrol.com.global.prod.fastly.net>, The Error was generate due to My mistake... I'm unaware of how to use these services so a little messed Up! But i quickly figured out that if i add the same service to my cloudfront account and change the Plan to Business (it cost upto 200\$) You can gain Complete Access of the domain 😊



Now if You remember the WHOis information showed me another thing The Subdomain

www.bugcrowdtrafficcontrol.com

When i visited that subdomain and It showed Me an error!



Well as soon as i saw this error I remember that some days a go a guys published a Blog about taking over DonaldJTrump's Website subdomain by same service and i tried to follow his steps But Unfortunately My card was declined while buying the services to Takeover the subdomain That's Why I was Unable to takeover The Subdomain Completely!

How to takeover:

1. Signed up as client in Pantheon service.
2. Created a Sandboxed domain as WordPress or Drupal.
3. Added a credit card, then subscribed as 'Professional' to setup the sandboxed domain.
4. Used a feature called "custom domains" to add the vulnerable subdomain to my account.
5. Waited for the verification and building process to be finish.
6. Boom You will be the admin of the subdomain

So At the end I reported this To Bugcrowd! 🙄 Because potentially the domain & Subdomain both was owned by Bugcrowd...

Their Reply:



Comment 2017-08-15 21:14:37 UTC

paul_bugcrowd added a comment

Hi MuhammadKhizerJaved,
Apologies for the delay and thank you for your report. We have confirmed that the DNS configuration `bugcrowdtrafficcontrol.com` domain was previously vulnerable to takeover via the Pantheon third-party service.
Bugcrowd owns this domain, however, we have never used it to host content or promoted it in any way, and consider it to be of minimal business value. It is also not listed as an in-scope target per our program brief. As such, this submission would generally be ineligible for a reward. However, because we made a DNS change in light of the submission, we are happy to pay you a small bonus as a token of our appreciation.
We encourage you to explore more of the targets listed as in-scope on our program brief. Thanks again and happy hunting!



Submission updated 2017-08-15 21:14:54 UTC

paul_bugcrowd changed the VRT from **Other** to **Server Security Misconfiguration > Misconfigured DNS**



State changed 2017-08-15 21:15:10 UTC

paul_bugcrowd changed state to **not applicable**

This submission was marked not applicable. It is not a rewardable submission at this time.



Reward added 2017-08-15 21:15:16 UTC

paul_bugcrowd added a reward of **\$600**

The Report was Closed as N/A 😬 lol I was Hoping it to Be closed as Resolved 😬 But I still got 600\$ 😊

Thanks 😊

Hope it will solve the problem for some about Fastly error 😊

Tags: [subdomain takeover](#)

👍 YOU MAY ALSO LIKE...



Stored XSS(cross site scripting) in
Picturepush.com

APRIL 1, 2016



Badoo Account Takeover

MARCH 27, 2016



Open URL Redirection and Xss In
Dato Capital

JUNE 6, 2016

9 RESPONSES

[🗨️ Comments](#) **8** [🔗 Pingbacks](#) **1**



Mike Kawasaki 🕒 August 19, 2017 at 5:55 am

Nice! i really love it. next time RCE? haha 😊

Reply



MuhammadKhizerJaved 🕒 August 19, 2017 at 6:55 am

Sure I'll Try 😊

Reply



MuhammadKhizerJaved 🕒 August 28, 2017 at 3:44 pm

Just going to publish SQLi POC in an Hour 😊

Reply



Tej 🕒 August 19, 2017 at 3:56 pm

Which tool you are using for CANME scanning?

Reply



MuhammadKhizerJaved 🕒 August 28, 2017 at 3:43 pm

It was domain tools online website

Reply



Nouman 🕒 October 6, 2017 at 2:33 pm

Nice one mate

Reply



Tauheedkhan 🕒 September 23, 2018 at 5:18 am

i am getting error while configuring domain in fastly it says that domain is already registered to another customer.

host command out put

```
$ host dev.example.com
dev.examplecom is an alias for dev.example.com.tw.map.fastly.net

Dig Command

$ dig dev.example.com

;; ANSWER SECTION:
dev.example.com. 106 IN CNAME dev.example.com.tw.map.fastly.net.
```

Also getting the Fastly unkown domain error when i visit the website

Reply



Pushkal 🕒 October 12, 2018 at 6:21 am

Awesome Leet

Reply

LEAVE A REPLY

Comment

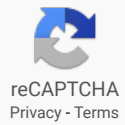
Name *

Email *

Website




I'm not a robot



Post Comment



Bug Bounty POC © 2020. All Rights Reserved.

Powered by  - Designed with the Hueman theme