“Domain Takeover In Google”

- (‘/Abhishek S’/)

DEF CON DC 0471 TRIVANDRUM

29th September, 2018

$Who am i

#Abhishek S

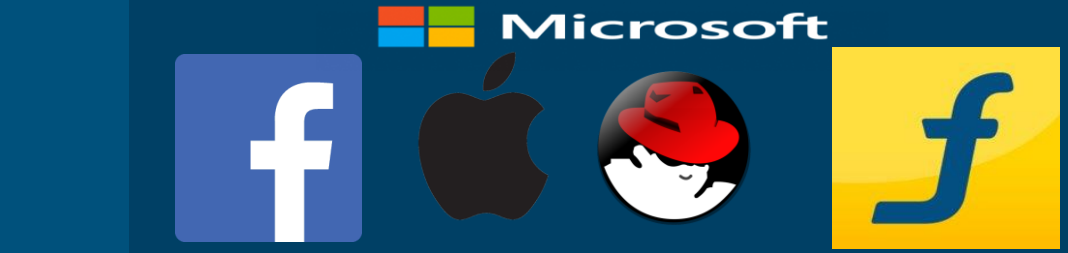
⟶ Pursuing CS @ Amrita School Of Engineering

→ Member Of Team Bi0S (Academic CTF Team Of Amrita University)

→ Listed In Google Hall Of Fame Page 1 [One Of TOP VRP Researchers Of Google all over the world and Ranked #3 in India]

Acknowledged By 40+ International Companies For Reporting Security Vulnerabilities.

Acknowledged By



Let’s Begin, Topic Time!

The presentation is all about a ‘**domain takeover**’ vulnerability i’ve found in a google acquisition, in the post-triage state, Google classified the vulnerability as a **P1 S2** one, and it was rectified within some hours.

Pssh, you might have heard about subdomain takeover,

But you might be wondering ‘why its a domain takeover here’?

We’ll see!!

Concepts First!

What is a domain takeover?

A domain takeover is considered a high severity threat and boils down to the registration of a domain by somebody else (with bad intentions) in order to gain control over the domain. This presents an interesting attack vector, which can even lead to several high severity risks, like

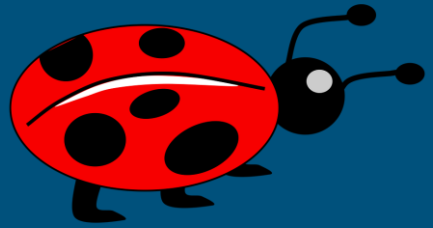
- **CSP Bypass in other domains, where the vulnerable domain is defined as allowed**
- **You can host anything you want in the domain, an ideal example would be some malicious content.**

How did the journey start? (Recon Mode 0x01)

I was bored one day, and I thought to hunt for some bugs in Google,

At first, I thought to look for XSS in google, but it is so hard to find XSS in the main google products, then i got the idea to hunt for XSS in acquisitions (the companies which were bought by Google is in scope of their VRP program if they have passed 6 months since the date of buying, I wanted some new targets as most famous acquisitions and main products were hunted by a lot of other hunters! I've got an idea……...

The !dea, in brief!!!



I was wondering how many domains did Google own, and since all applications owned by Google are in scope, i was looking for some webapplication of google which was not known by many, and my search landed me up in a blog which gave me details of a conference called "**Google India Search Masters Conference**"

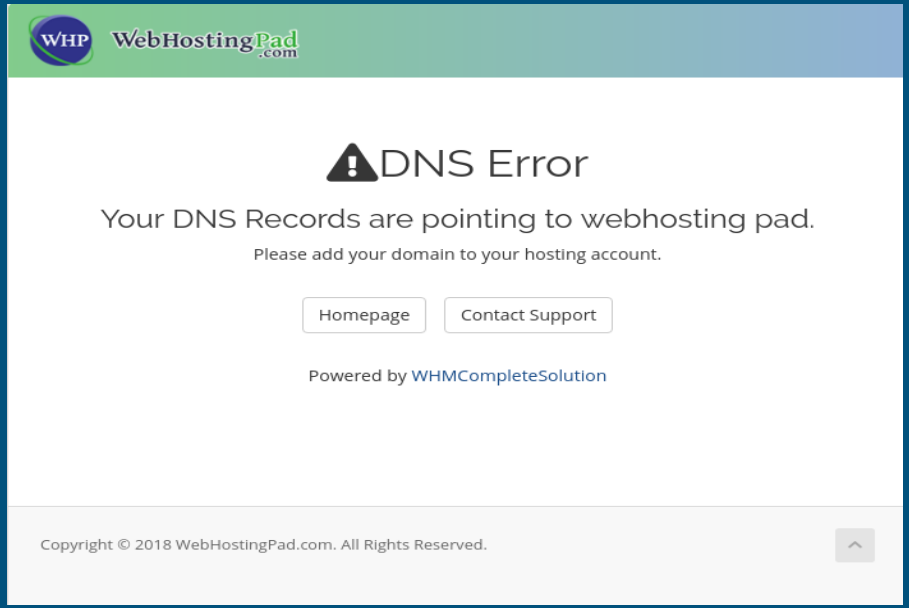
Reference: http://www.seolion.com/google-india-search-masters-2009/

And there was a domain for the same owned by Google, it was called

http://www.indiasearchmasters.com/

Then what!

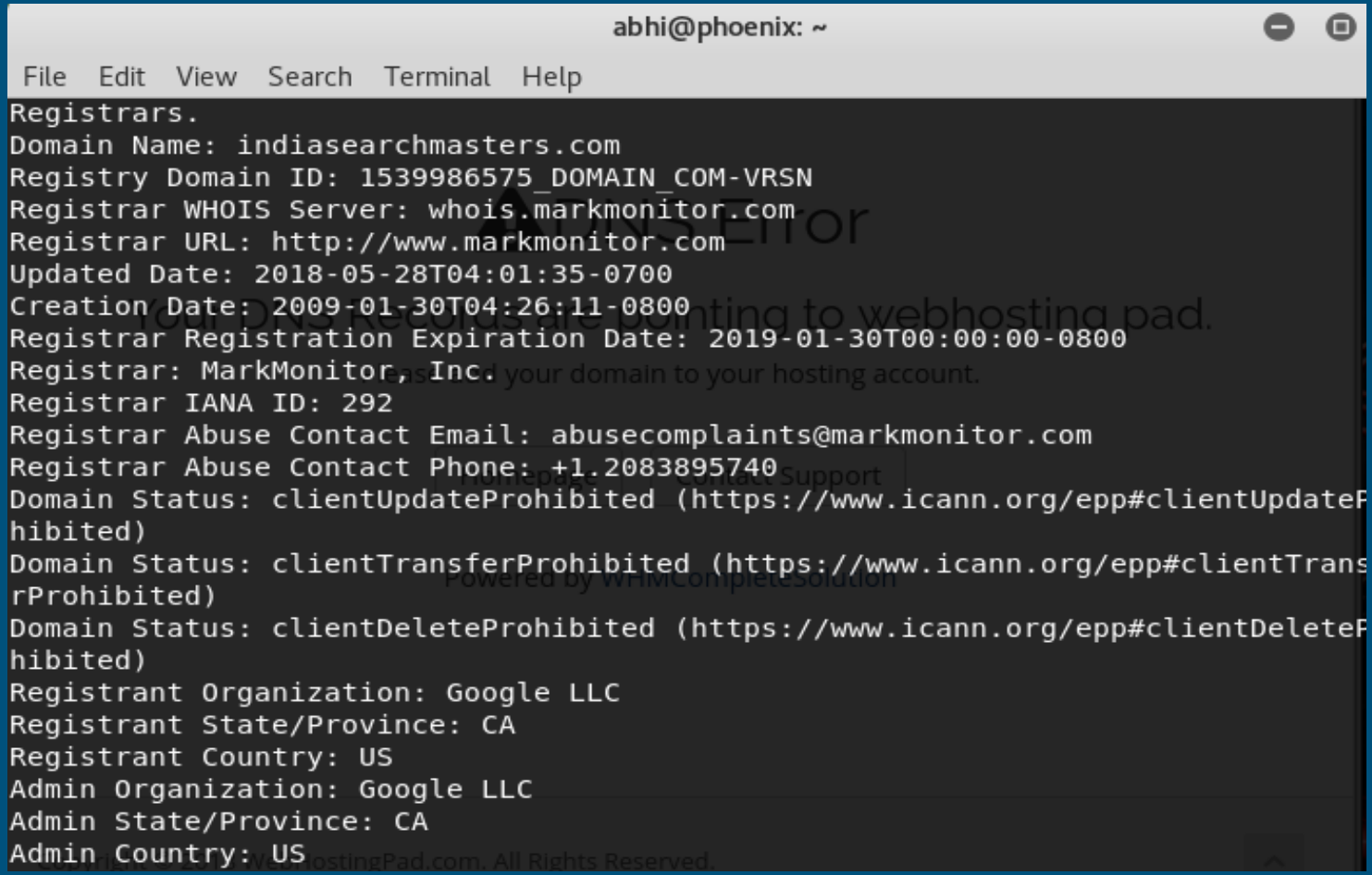
Since my idea was to test for XSS, i just visited the website and i was like WTH!!!
When i saw this page



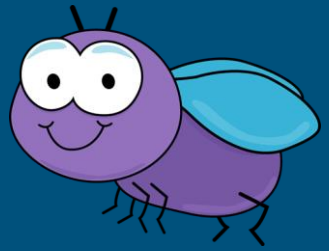
What’s with the error page?

From the page, I understood that there was some misconfiguration in DNS records, or just the nameserver/A address was pointing to the host but there was no hosting account linked to the domain, I wanted to confirm whether this domain was owned by google, and wanted to see the DNS records of the domain, i did this by using the basic linux command (whois)

$whois indiasearchmasters.com


abhi@phoenix: ~
File Edit View Search Terminal Help
Registrars.
Domain Name: indiasearchmasters.com
Registry Domain ID: 1539986575_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2018-05-28T04:01:35-0700
Creation Date: 2009-01-30T04:26:11-0800
Registrar Registration Expiration Date: 2019-01-30T00:00:00-0800
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateP
hibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTrans
rProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteP
hibited)
Registrant Organization: Google LLC
Registrant State/Province: CA
Registrant Country: US
Admin Organization: Google LLC
Admin State/Province: CA
Admin Country: US

Confirmed!



The DNS entry was showing

Registrant Name: Google LLC
Admin Organisation: Google LLC

And the import thing, the DNS records (nameservers in this case, since A address was not given) were pointing to

Ns1.webhostingpad.com
Ns2.webhostingpad.com

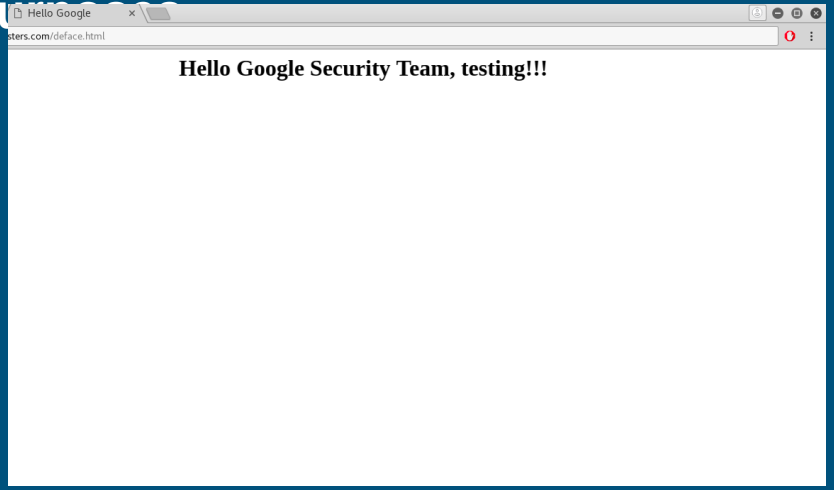
Then what!

Since it was confirmed that it was owned by Google and the DNS records were pointing to webhostingpad, i decided to create a linux hosting account in webhostingpad, but unfortunately it costed $2 to get one, aand I was lucky enough to notice that they were providing 30 day trial with just credit card verification, I've did that and successfully made a hosting account….

Now, i wanted to see whether it was possible to add the domain, i went to DNS management and added the domain 'indiasearchmasters.com' under my domains, and it asked me to wait 24 hours for DNS propagation….

After 3-4 hours!

The error page was replaced by a blank white page, I understood that the DNS propagation was over, and the domain was linked to my hosting account, i added a webpage to the website called deface.html, for POC purposes



Report Timeline

I reported this to Google VRP with all these info through g.co/vulnz

Report Date: March 31 2018

Report Triaged on : April 4 2018

Fixed On : April 4 2018

VRP Reward/Decision on : April 24 2018.

And, that’s all, I’m done, Thank you!

Abhishek S

Ab2op4u

+919048900600