# Leaking API keys in Bing Maps Portal

Sai Krishna Kothapalli
Dec 31, 2015 · 4 min read

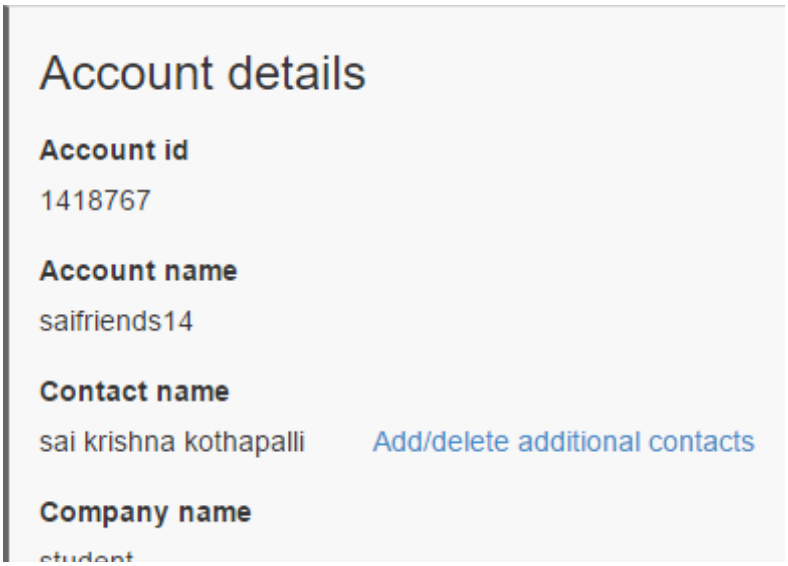
Since I promised to write about how I got listed in Microsoft Hall Of Fame. Here it is at last.

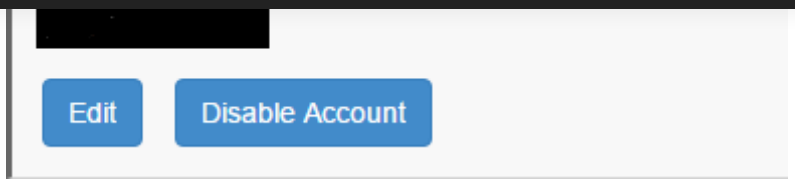
Some background info

- This is my first time reporting a Security Vulnerability to a Major Company .
- Yes, I had a little prior knowledge on Web Security.

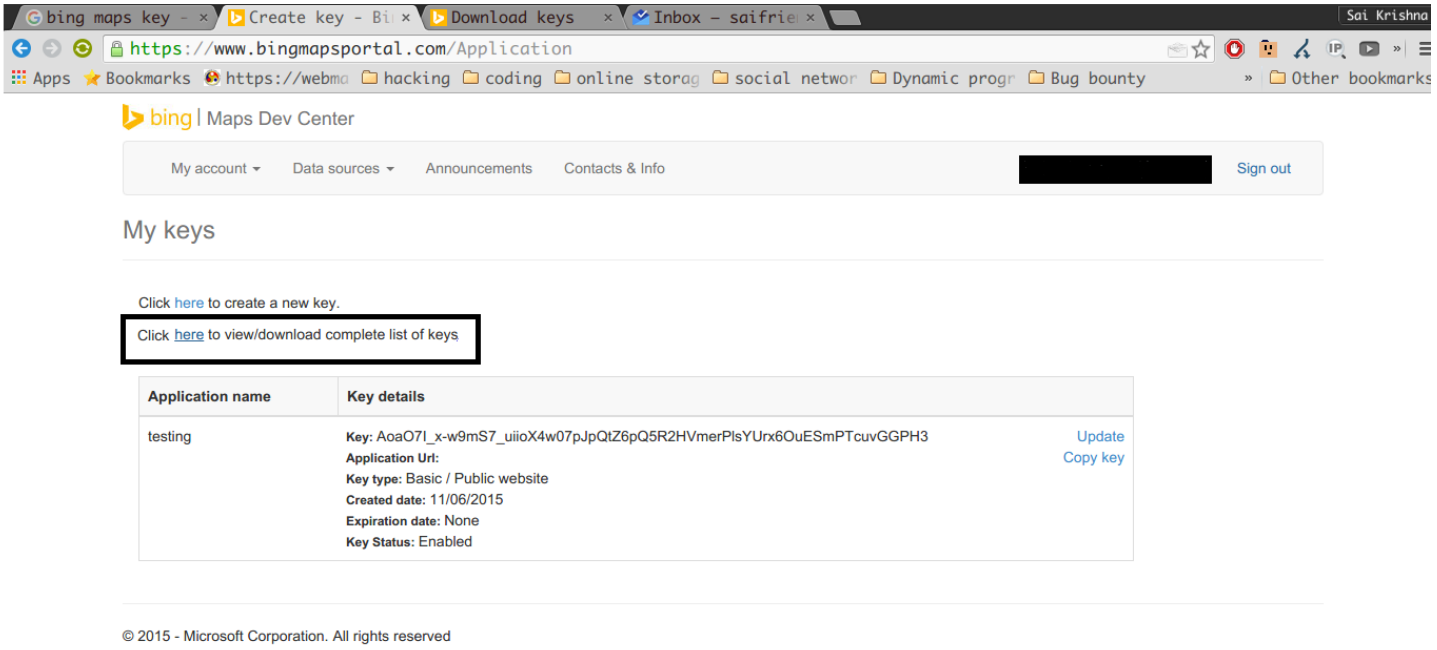
Every year Microsoft conducts a Hackathon named code.fun.do in some IIT's .The theme for the Hackathon was to build a web or mobile application using one of the Microsoft technologies.

We decided to participate and our Idea involved Bing maps. In order to use any API you need an API key.So does Bing maps . You can manage your applications and their keys for Bing maps at https://www.bingmapsportal.com/ . So I also registered






I was making myself familiar with the website and trying to create new API keys and use them.




(Don't worry I deleted that Application and key :P)

Then there was this page where you could see the usage details of all the API keys

Well there were no statistics because I hadn’t used the key yet but have you noticed

Look at the URL. While making the get request it is sending the Account ID as a parameter. So what I did next was to change the Account ID to 1418766 (Mine is 1418765) and pressed enter and then BOOM !! I got the API keys of that user.

Just Imagine !! I can get the API keys , Application Names, Usage details and Every damn statistics you can possibly imagine of every User ever registered.

There were even enterprise level API keys.

If I hadn't reported this bug, may be someday you would have seen that some hackers hacked Microsoft and posted API keys and some other details on pastebin or something 😀

Was that complicated ? Nope right. Anyone can change that Account ID . But in this case I was the one 😀 . In case you are wondering why I did that the answer is I am used to it although I never participated in any Bug bounties I practice a lot on our Institute websites and servers and so many other sites online.

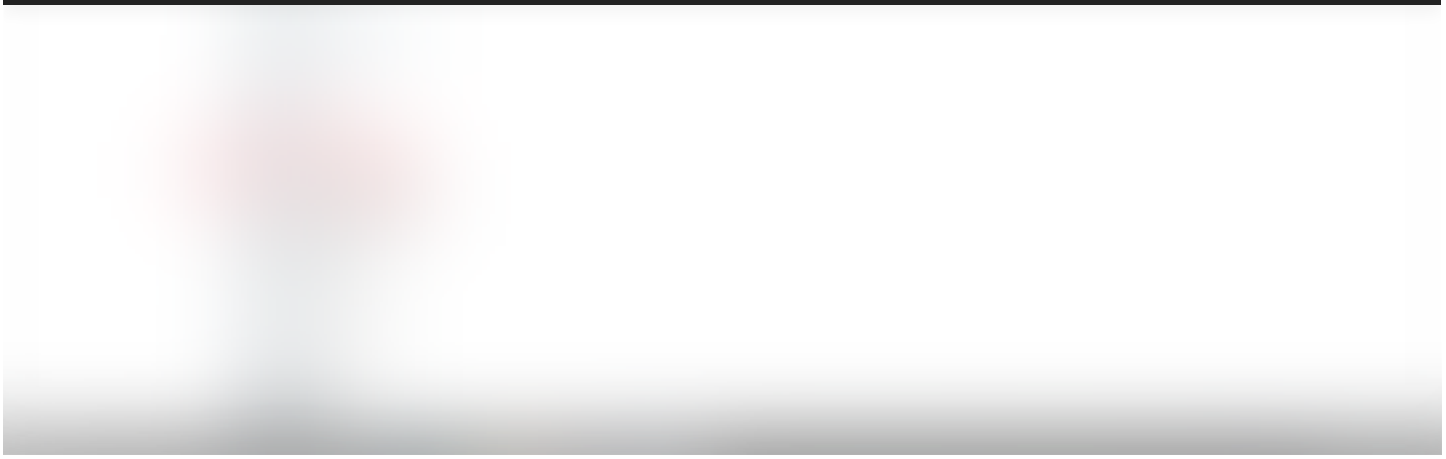
My knowledge grew in this area because I practice in a lot of CTF's (Capture The Flag contests) and once you do so many contests you get that instinct to check everything and you know where to look for finding bugs.

It's not a special talent though and anyone with some dedication can master this art.

The guys at Microsoft fixed the bug, and the URL now look like this

and the vulnerability has been patched.

And that's how I got into Microsoft Hall Of Fame for the month of November.



That's it for now.

## Timeline:-

10/11/2015 — Sent bug Report.

11/11/2015 — Got a mail saying that they are analysing the bug.

12/11/2015- They fixed it (I checked).

17/11/2015 — Got an official mail asking for my details.

Finally I got started with Bug Bounties while I was not looking for bugs.

We didn't win the Hackathon but it's still a win.

Thank you for reading.

Peace. :D

I reported another Vulnerability in the same website in the same month

. . .

*Originally published at kmskrishna.wordpress.com on December 31, 2015.*

WRITTEN BY

## Sai Krishna Kothapalli

Founder/CEO Hackrew | Security Researcher | Indian | Student @ IIT Guwahati

Follow

## InfoSec Write-ups

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. In a nutshell, we are the largest InfoSec publication on Medium. Maintained by Hackrew

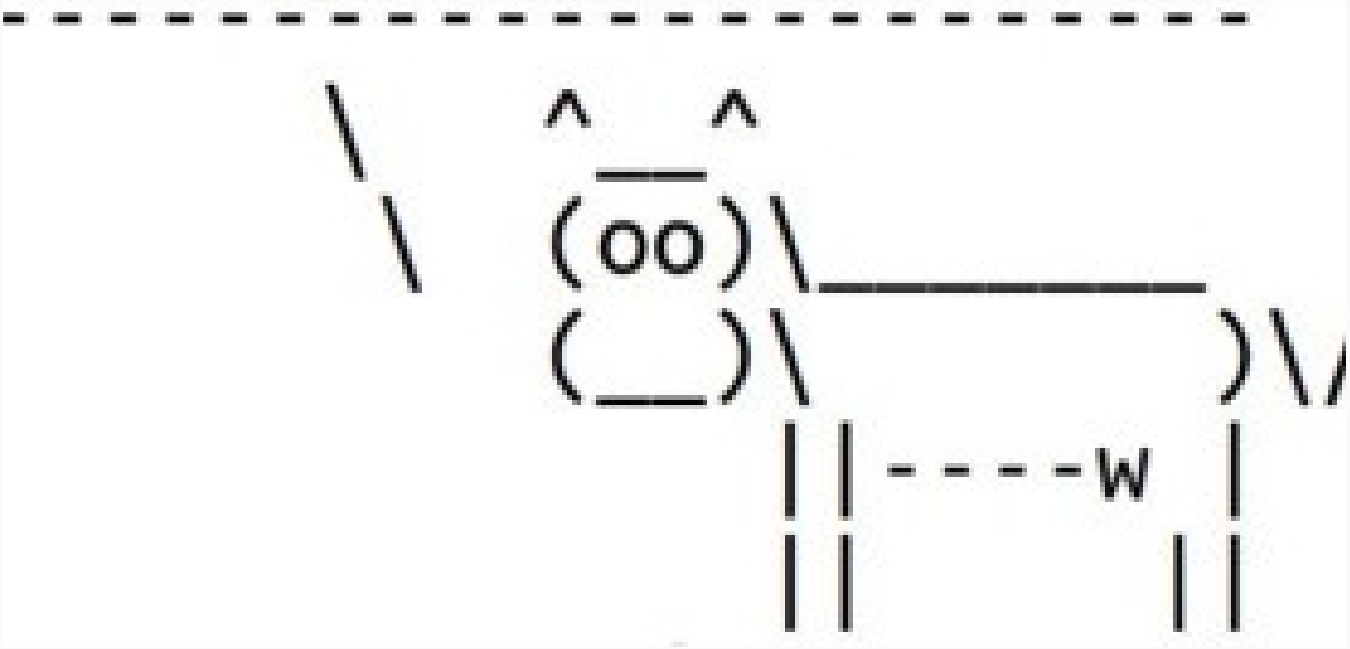
Follow

See responses (1)

## More From Medium

More from InfoSec Write-ups

INFOSEC WRITE-UPS

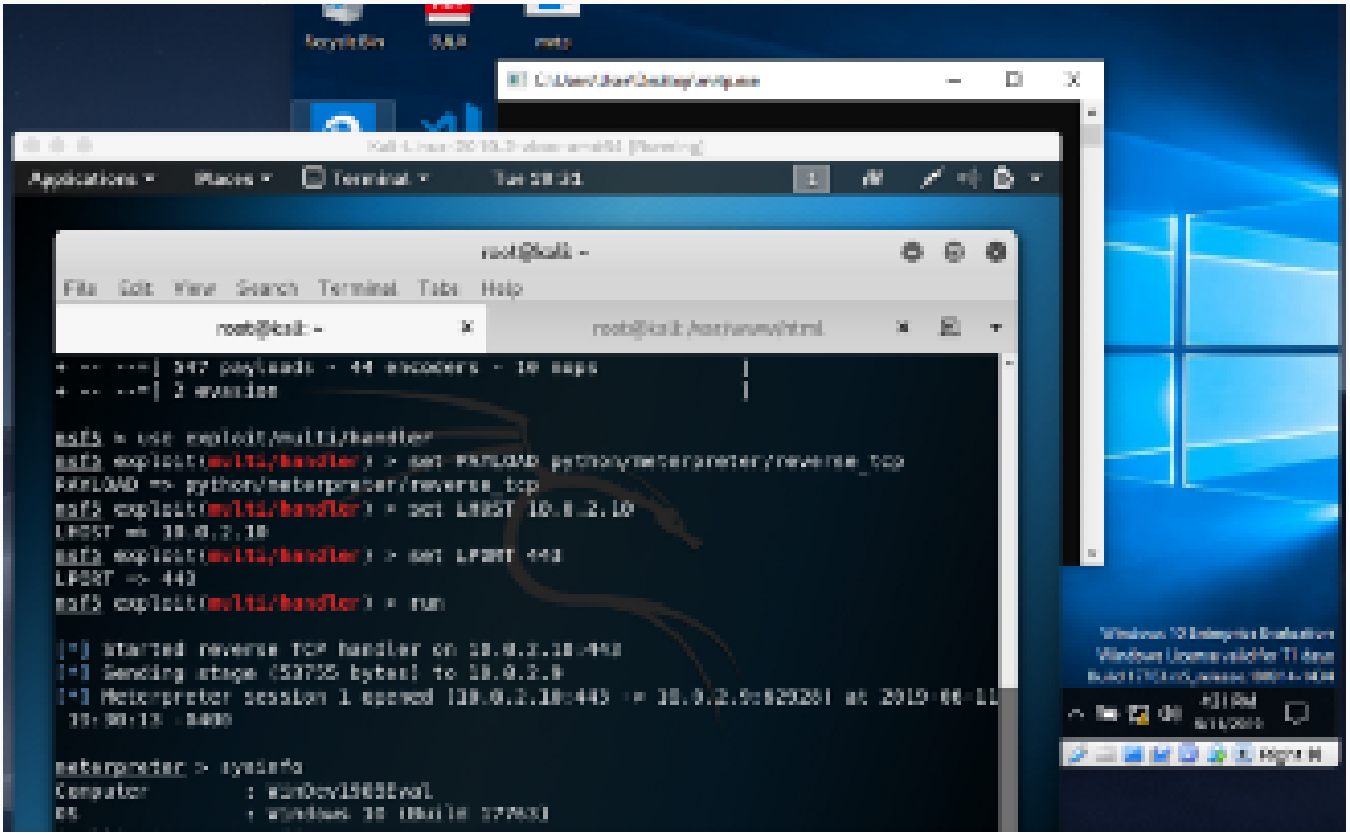



# Safer deserialization in Spring Security OAuth2

Artem Smotrakov in InfoSec Write-ups
Nov 16 · 5 min read ★



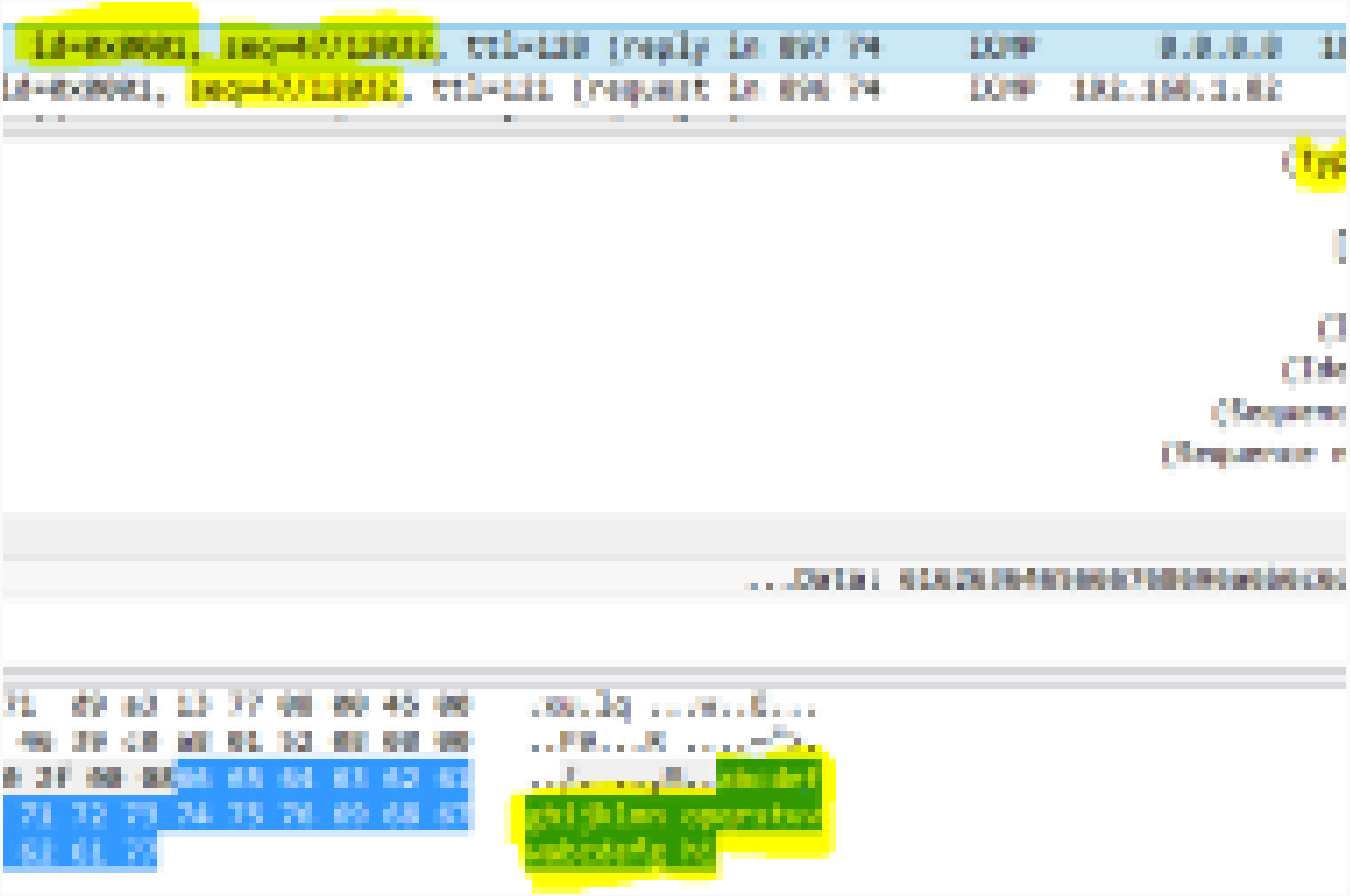
More from InfoSec Write-ups



Marcelo Sacchetin in InfoSec Write-ups
Jun 11 · 6 min read ★



More from InfoSec Write-ups



# Ping Power — ICMP Tunnel

Nir Chako in InfoSec Write-ups
Dec 17, 2018 · 8 min read