Two vulnerabilities makes an Exploit!! (XSS and CSRF in Bing)

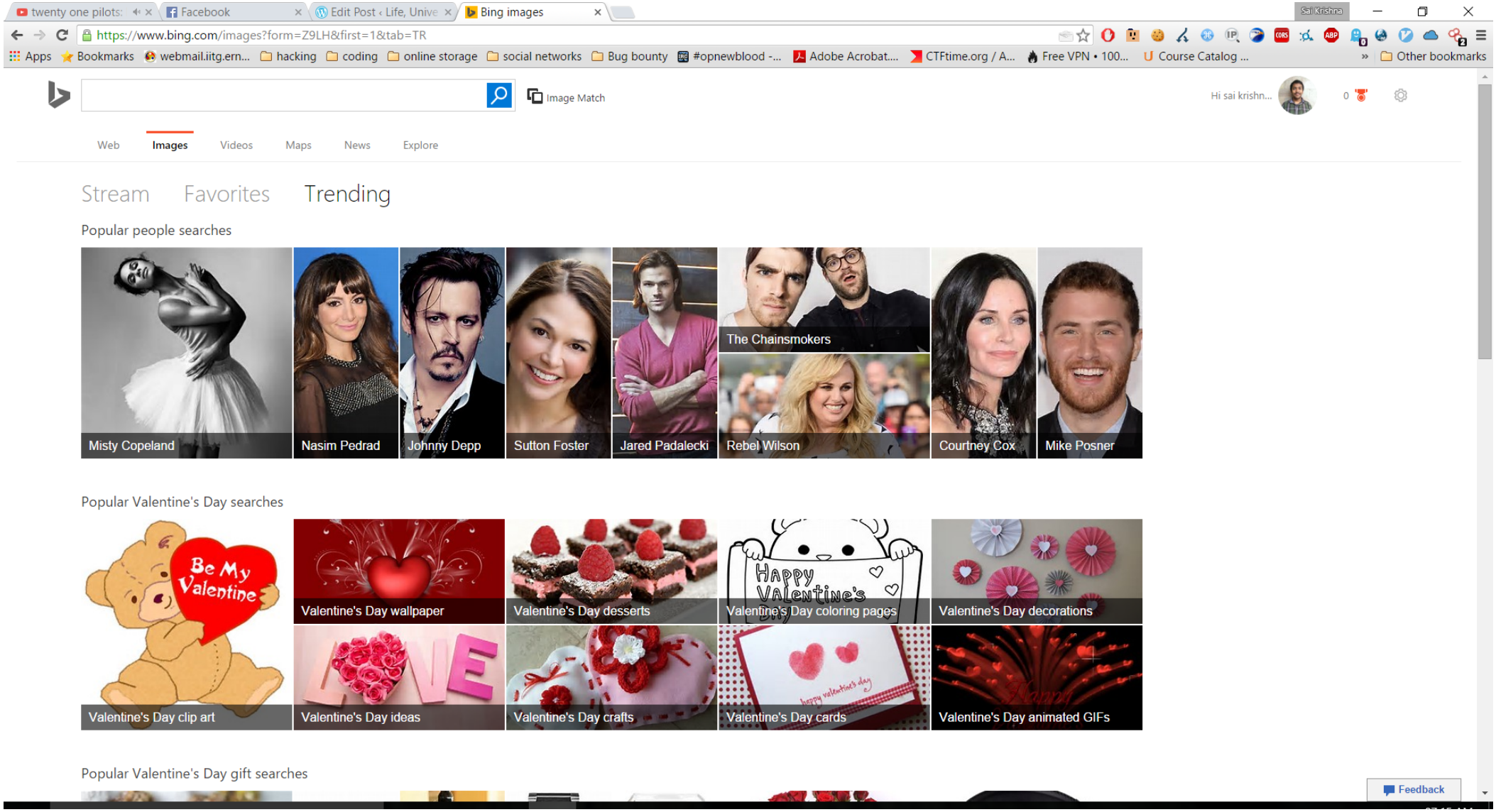
Sai Krishna Kothapalli Follow
Jun 10, 2016 · 3 min read

Hello !!

This post will be about my 4th and 5th valid bug reports I submitted to Microsoft. Open the Images in a new tab if you find them difficult to view. I took the screenshots in a 1080p screen.

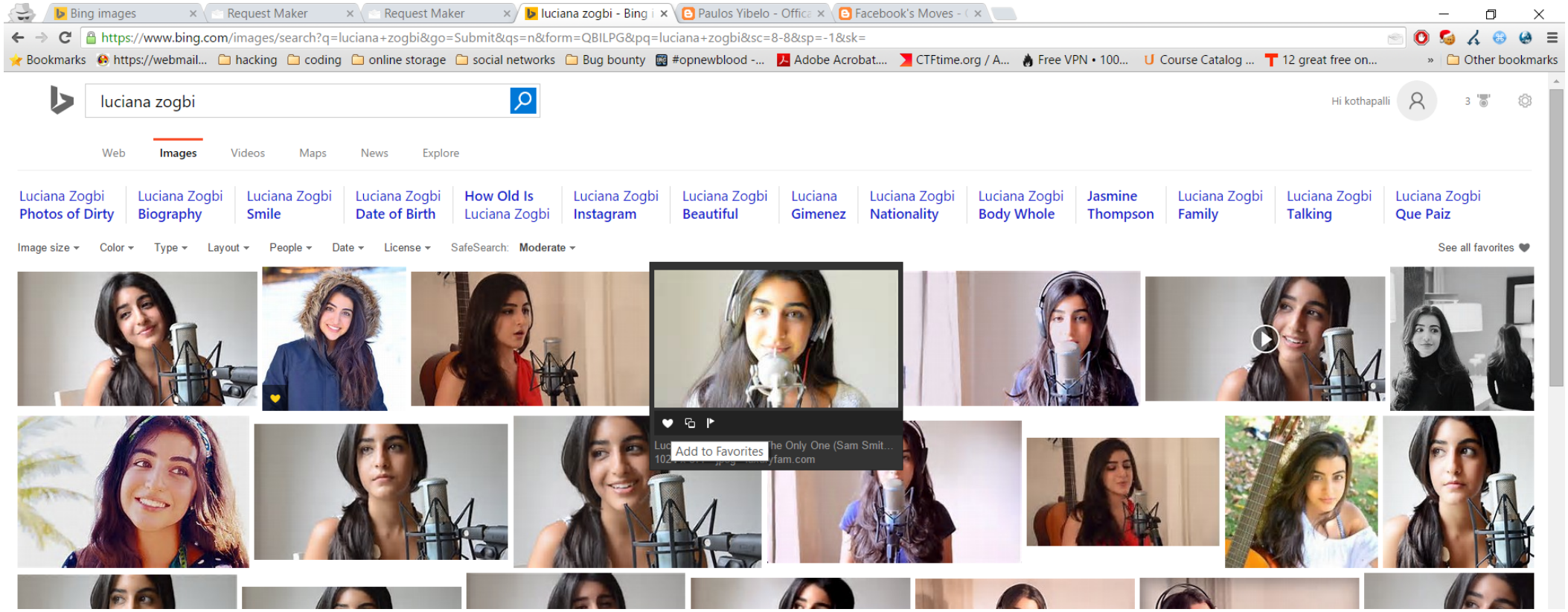
This time I have found a **XSS** and **CSRF** vulnerabilities in `Bing`.

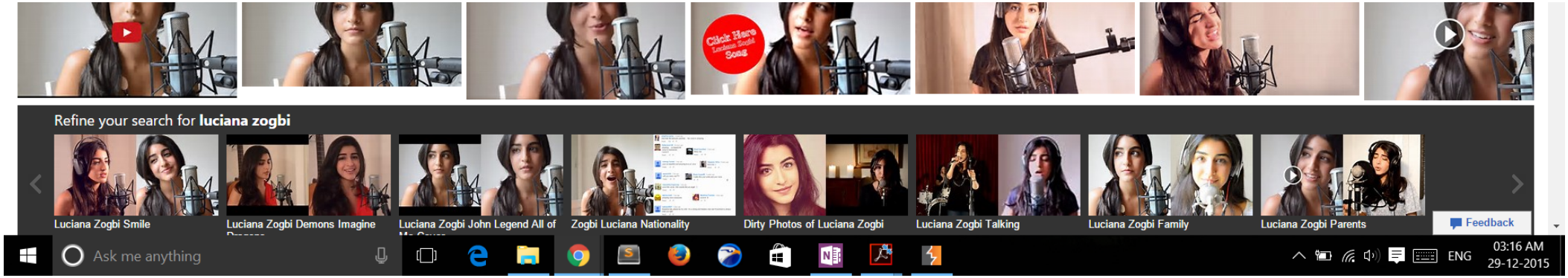
Bing images is testing 3 new features called **Stream** , **Favorites** , **Trending** which are still in beta.



So I was going through this and there is this option where you can search and directly add images to your favourites.

It was cool, So I wanted to take a look at how it is implemented.





When you click on the heart symbol after the image search, the image is added to your favourites.

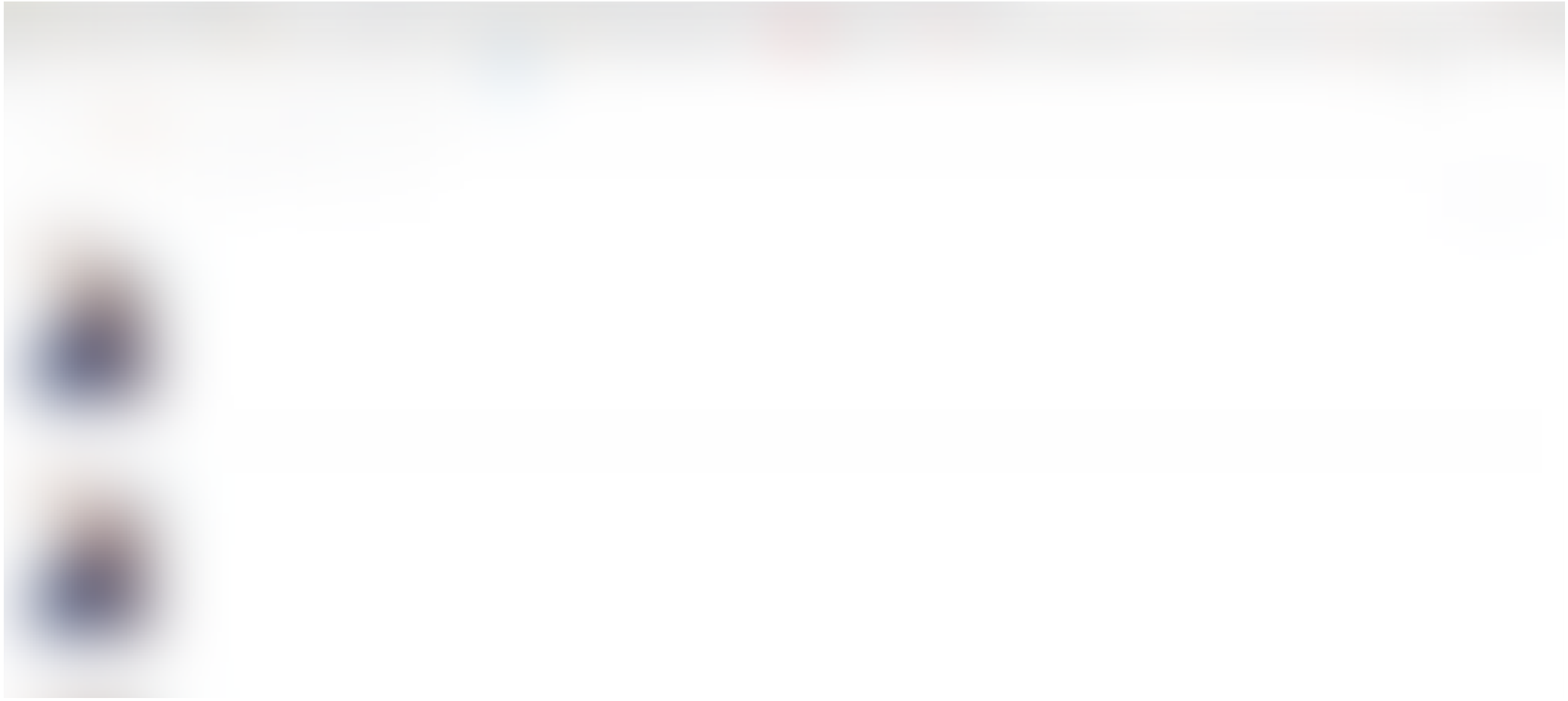
and the request looks like this

It’s URL-Encoded. Once decoded it looks like this

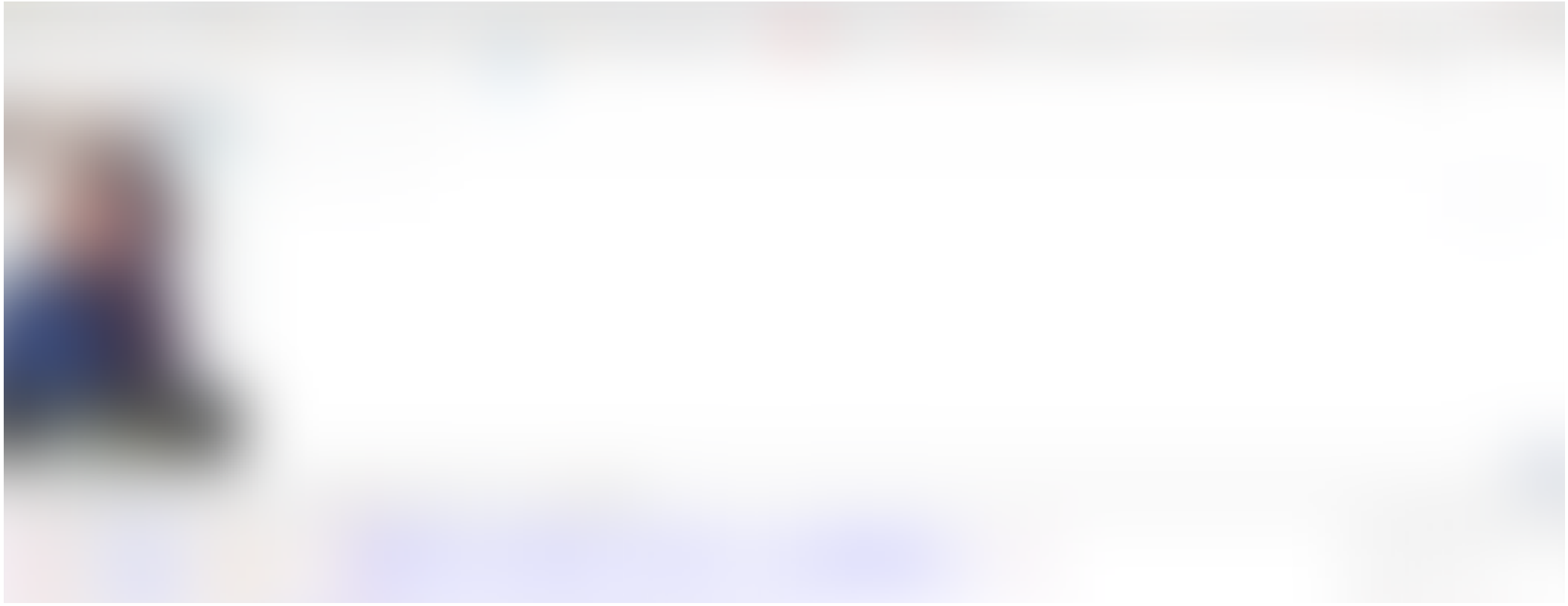

```
{“WriteNewCollection”:true,”query”:”lucianazogbi”,”mid”:”5689B0BFCDB0
E64E595A3B6C2B7A0865A4DC236C”,”description”:”lucianazogbi”,”MediaUrl”
:”https://beautifulgeniuses.files.wordpress.com/2015/01/lucianazogbi.
jpg&#8221;,”SourceUrl”:”http://beautifulgeniuses.com/2015/01/14/lucia
nazogbi/&#8221;,”ThWidth”:300,”ThHeight”:300,”MediaWidth”:640,”MediaH
eight”:640,”MD5":”md5_5c6aa5d2768f0d2255dab627015da340",”MediaFormat”
:””,”ThumbnailId”:“OIP.M5c6aa5d2768f0d2255dab627015da340o2",”Collecti
onType”:0,”ContentId”:”XGql0naP”}
```

Interesting there is no **CSRF token** and there is no `X-Requested-With : XMLHttpRequest` header.

Which means it is vulnerable to **CSRF** attacks. Another interesting thing is the webpage is displaying this data in the Favorites tab.



Then why not try to inject some **JavaScript** there. I tried all the fields but none of them worked. When I almost gave hope I saw this.



This link is vulnerable to **XSS** . It is accepting links `javascript:code` in the <a> href tag .

So when I click on it. BAMN

Our favourite popup.

So, by sending the user to a single malicious site it is possible to compromise his account.

If I have stopped after the CSRF I would have not found the XSS. So, by successfully combining 2 vulnerabilities we made an exploit to compromise Bing.

I reported this to Microsoft and now it is fixed.

Since, that feature is still in beta-testing they took more than 5 months to fix that in order to make it more secure.

My name will be in the March 2016 Hall Of Fame.

Thank you for reading.

Peace :D

Feel free to comment and give some suggestions.

. . .

Originally published at kmskrishna.wordpress.com on June 10, 2016.

Security Microsoft Bug Bounty Bing Hacking

126 claps

WRITTEN BY

Sai Krishna Kothapalli

Follow

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

InfoSec Write-ups

Follow

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. Powered by Hackrew

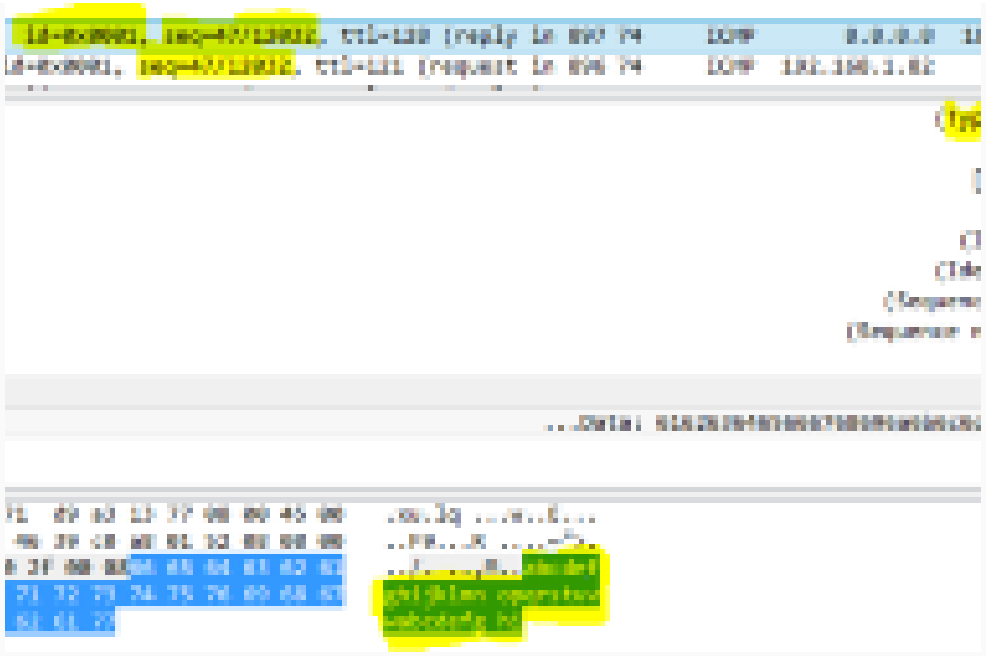
See responses (1)

More From Medium

More from InfoSec Write-ups

Ping Power — ICMP Tunnel

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



More from InfoSec Write-ups

Picture Yourself Becoming a Hacker Soon (Beginner's Guide)

Abanikanda in InfoSec Write-ups
Aug 16 · 16 min read ★

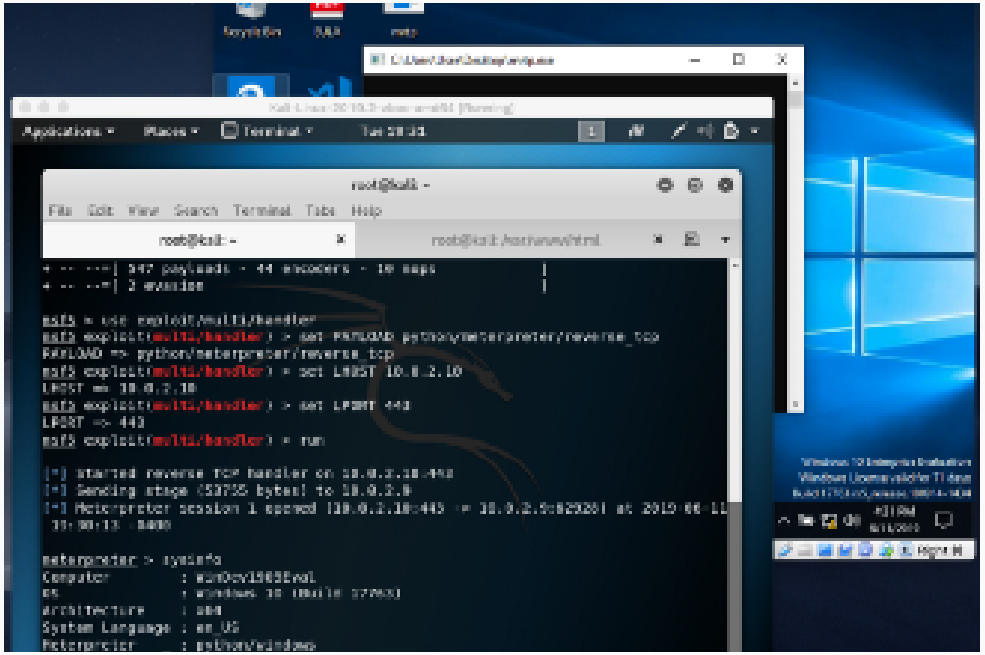
More from InfoSec Write-ups

Antivirus Evasion with Python

Marcelo Sacchetin in InfoSec Write-ups

Jun 11 · 6 min read ★

610



Discover Medium

Welcome to a place where words matter. On Medium, smart voices and original ideas take center stage - with no ads in sight. Watch

Make Medium yours

Follow all the topics you care about, and we'll deliver the best stories for you to your homepage and inbox. Explore

Become a member

Get unlimited access to the best stories on Medium — and support writers while you're at it. Just $5/month. Upgrade