

# Getting started in Bug Bounty



Sahil Ahamad

Follow

Nov 8, 2018 · 12 min read

...

Hi Guys!

This embedded content is from a site that does not comply with the Do Not Track (DNT) setting now enabled on your browser.

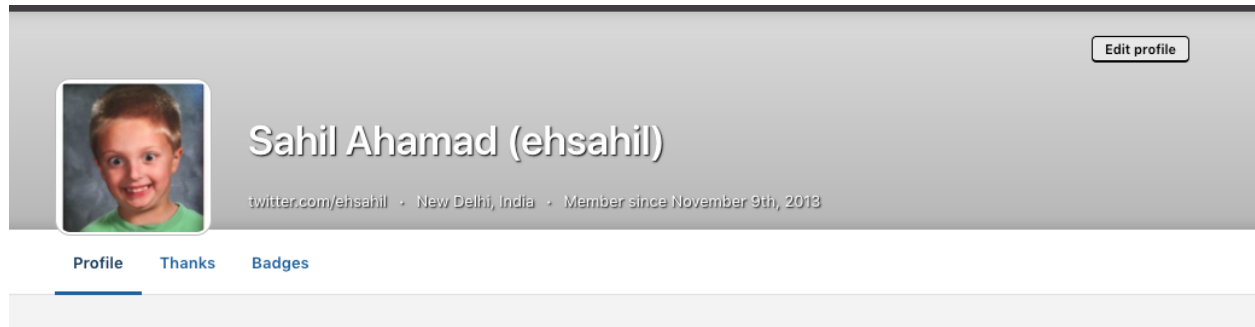
Please note, if you click through and view it anyway, you may be tracked by the website hosting the embed.

**[Learn More about Medium's DNT policy](#)**

**SHOW EMBED**



While I write this up, it's already **09–Nov–2018**, Here in India, Today I've completed 5 good years on **HackerOne** ♥



<https://hackerone.com/ehsahil> — A proud member since November 9th 2013

I will always be thankful to the whole information security community ♥



This embedded content is from a site that does not comply with the Do Not Track (DNT) setting now enabled on your browser.

Please note, if you click through and view it anyway, you may be tracked by the website hosting the embed.

**Learn More about Medium's DNT policy**

**SHOW EMBED**

love you all ♥

How to get started in Bug Bounties is a common question nowadays and I keep on getting messages on a day to day basis. It's not possible for me to respond to each and every message, so I thought I'd rather do a blog post and would direct all those beginners to this blog post.

I've been in bug bounty field for 5 years now. still, there is so much to learn each and every day, I'm yet not an expert and this post is NOT an expert advice. I am just sharing, what I've achieved in the past 5 years and doing continuously to improve my skills.



# Index

1. Introduction
2. Basic Technical things to get started.
3. Choosing your initial path
4. Books — I regularly take references from
5. Youtube channels & playlists
6. Practice! Practice! practice
7. Tools you should master (\*tool)
8. Bug bounties and Mental Health
9. Blogs you should follow
10. Follow cool guys on Github
11. Follow Active bug bounty guys on twitter
12. Credits and Closing meme.

. . .

## 1. Introduction

I've seen a lot of folks in Bug Hunting Community saying *"I am not from the technical field that's why I am not successful in bug bounty"*.

This is the misconception that someone needs to be from the



computer science background to be good in bug bounties. Being from the computer science background helps but it is not compulsory but you have to learn the computer science fundamentals yourself. So, If you are from the non-technical background you should get started only if you're more interested in learning about the information security not **ONLY** interested in \$\$\$\$.

This embedded content is from a site that does not comply with the Do Not Track (DNT) setting now enabled on your browser.

Please note, if you click through and view it anyway, you may be tracked by the website hosting the embed.

**Learn More about Medium's DNT policy**

**SHOW EMBED**

I am too from a **Mechanical Engineering** background but I am very much interested in the information security field from school time but joined mechanical field with the advice of family members but my main focus always been to Information security.

I can tell you many stories where people from the non-technical field are successful in the bug bounty or infosec field.



But, All of them have one thing in common that is “**INTEREST**” and willing to do the “**hard-work**”.

If you think you will become successful *overnight or over the week or over a month*, this is not a field you should join. Doing bug bounties are very competitive, it might take a year at least to do good in bug bounty. you have to continue your learning, sharing & more and more practice. You must-have curiousness to learn about new things and explore the field on your own. There is huge education content out there for free.

Do not pay **individuals** telling you to make you successful in bug bounties overnight. Most of them are scammers.

The following are the things you should know before starting in infosec.

No one will be able to tell you everything about this field, It's a long path but you have to travel it alone with help from others.

*“Do not expect someone will spoon feed you everything.”*

**How to ask a question?**

You should behave responsibly when asking a technical question to someone.



You shouldn't ask like **“Here is the endpoint, can you please bypass the XSS filter for me?”**

You should be on point when you ask a problem — that's it.

You should not expect people will respond to you within minutes. They will respond as soon as they get free times or they might not respond at all because of their busy schedule or whatever reason. You should also respect that — do not ping someone unnecessary.

**How to find Answer to every question?**

This is what I did previously, Doing now and will definitely do in future. Using **“Google”** for everything. (you can use other search engines too :P )



This embedded content is from a site that does not comply with the Do Not Track (DNT) setting now enabled on your browser.

Please note, if you click through and view it anyway, you may be tracked by the website hosting the embed.

**Learn More about Medium's DNT policy**

**SHOW EMBED**

. . .

## **2. Basic Technical things to get started.**

I am assuming you have a basic understanding of how things work on the internet. There are many things you have to learn but I cannot list of all of them here. I'm listing a few important topics and you should learn more by yourself.

**HTTP — TCP/IP Model**

**Linux — *Command line***

**Web Application technologies.**



## Networking basics

**Learning Basics of HTML, PHP, Javascript.** — These are only to get started, the list never ends, it totally depends upon the interest. You have to build your interest according to your need.

It's also very important to have a better understanding about different types of vulnerabilities, as soon as you can, I've added Web Application Security Basics section below.

. . .

### 3. Choosing your initial Path

Choosing a path in the bug bounty field is very important, it totally depends upon the person's interest but many of the guys choose the web application path first because according to me it's the easiest one.

1. Web application Security testing
2. Mobile Application Security Testing

But not limited to these two. it totally depends upon the type of interest you have.

### Web Application Security Basics.



## **OWASP Top 10 for 2010 OWASP top 10 for 2013 OWASP top 10 for 2017**

Start from the 2010 list, so you can understand the types of vulnerabilities were in the top in 2010, what happened to them in 2017. you will understand it by learning about them and practice them

## **OWASP Testing Guide V4**

You don't have to finish the testing guide and then start working, you should start working on the live (legal) targets, that's the only way you can improve your skills.

## **Mobile Application Security Testing.**

As you get more experience you are free to switch between anything you like :)

## **OWASP Mobile Top 10.**

**One stop for all mobile application security need,**

Mobile Security Wiki by **Aditya Agrawal**



**Mobile Security Wiki**

AppMon - AppMon is a runtime security testing & profiling framework for macOS, iOS and android apps. It is useful for...

[mobilesecuritywiki.com](http://mobilesecuritywiki.com)

**Application security Wiki also by Aditya Agrawal****Application Security Wiki**

Application Security Wiki is an initiative to provide all Application security related resources to Security...

[appsecwiki.com](http://appsecwiki.com)

. . .

**4. Books — I regularly take references from**

1. Web Application Hacker's Handbook
2. Mastering Modern Web Penetration Testing
3. The Hacker Playbook 1, 2 and 3
4. The Mobile Application Hacker's Handbook
5. Breaking into Information Security
6. Web Hacking 101



• • •

## 5. Youtube Channels And Playlist.

### **IppSec**

You probably know about my channel. Here's a bunch of other content I enjoy. Patreon Pages of Cool People...

[www.youtube.com](http://www.youtube.com)

### **LiveOverflow**

just a wannabe hacker...

[www.youtube.com](http://www.youtube.com)

### **Web Development Tutorials**

Hi, I'm Pete. I develop video tutorials about the various things I'm learning related to web development and

[www.youtube.com](http://www.youtube.com)



## Security Conference talks you should watch

**Akhil George** — Created a playlist for bug bounty talks on Youtube.

This embedded content is from a site that does not comply with the Do Not Track (DNT) setting now enabled on your browser.

Please note, if you click through and view it anyway, you may be tracked by the website hosting the embed.

**[Learn More about Medium's DNT policy](#)**

**SHOW EMBED**

How to Shot Web by **Jason Haddix**



This embedded content is from a site that does not comply with the Do Not Track (DNT) setting now enabled on your browser.

Please note, if you click through and view it anyway, you may be tracked by the website hosting the embed.

**Learn More about Medium's DNT policy**

**SHOW EMBED**

This embedded content is from a site that does not comply with the Do Not Track (DNT) setting now enabled on your browser.

Please note, if you click through and view it anyway, you may be tracked by the website hosting the embed.

**Learn More about Medium's DNT policy**

**SHOW EMBED**



This embedded content is from a site that does not comply with the Do Not Track (DNT) setting now enabled on your browser.

Please note, if you click through and view it anyway, you may be tracked by the website hosting the embed.

**Learn More about Medium's DNT policy**

**SHOW EMBED**

This embedded content is from a site that does not comply with the Do Not Track (DNT) setting now enabled on your browser.

Please note, if you click through and view it anyway, you may be tracked by the website hosting the embed.

**Learn More about Medium's DNT policy**

**SHOW EMBED**

. . .



## 6. Practice! Practice! Practice

It's pretty important to keep yourself updated with the trends and new vulnerabilities. While playing around with the server information disclosures, keep a close eye on publicly available exploits to escalate the attack.

You can start working on vulnerable applications.

1. Hacker101
2. Bug Bounty Notes
3. Pentesterlab
4. Hackthebox
5. *Damn Vulnerable Web application*
6. XSS Game by Google.
7. Vulnhub
8. hack me

Setting up Security testing labs — I've written detailed blog posts. you can be find them below:



### **Basic Android Security Testing lab — 1**

Hi Everyone,

medium.com

### **Basic iOS Apps Security Testing lab — 1**

Hi Everyone,

medium.com

### **Basic Penetration testing lab — 1**

I am setting up a new lab for me and thought to document the process, so anyone wants to do same can take

medium.com

**Bug Bounty Platforms** — These are the great places to test your skill. Do not get discouraged if you haven't found anything — you still have learned the reward of Experience, that is more important.



1. Hackerone
2. Bugcrowd
3. Synack
4. HackenProof
5. Intigriti
6. bountyfactory
7. Bugbounty Japan
8. Antihack

### **Twitter # tag you should follow**

#bugbounty

#bugbountytips

#infosec

#togetherwehitharder

. . .

## **7. Tools you should master (\*tool)**

**Burp Suite —**



You should start practice using the Burp Suite free version or the community edition and start working on bug bounty programs and as soon as you got sufficient bounty, purchase the Burp Suite Professional edition. You will not regret it.

Note: Do not use the pirated version of the Burp Suite professional, You should respect the great work **Portswigger** team is doing.

There are too many free resources out there to learn more about Burp Suite pro but If you are willing to invest some money. I can recommend the following things.

1. An online course by Pranav Hivarekar — Burp Suite Mastery
2. Burp Suite Essentials by Akash Mahajan

For information gathering or reconnaissance — I've Written a detailed blog post on the same topic. you can find it below:

**Recon — my way.**

A detailed blog post on my reconnaissance processes for web applications security testing. I always wanted to

[medium.com](#)



. . .

## 8. Bug bounties and Mental health.

Bug bounty field is a very competitive and you should also take care about your physical and mental health, that's very important. nothing else matters. My good friend Nathan wrote a great post on this topic.

You should definitely read it.

### **Bug Bounties and Mental Health**

In this post I want to discuss hunting for bugs, the effect on a hacker's mental health, burn out, and productivity.

[medium.com](#)

. . .

## 9. Blogs you should follow —

### **Detectify Labs**

How I made LastPass give me all your passwords " Hacking Slack using postMessage and WebSocket-reconnect to

[labs.detectify.com](https://labs.detectify.com)



### **InfoSec Write-ups**

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to

[medium.com](https://medium.com)

### **Appsecco**

Making sense of application security for everyone. Follow us to get a pragmatic view of the landscape including

[blog.appsecco.com](https://blog.appsecco.com)

### **These aren't the access\_tokens you're looking for - 🤖**

Edit description

[philippeharewood.com](https://philippeharewood.com)

### **Geekboy | Security Researcher**

Edit description

[geekboy.ninja](https://geekboy.ninja)



### **Learn | Think | Hack**

Describe this nonsense.

somdev.me

### **BUG BOUNTY HUNTING (METHODOLOGY , TOOLKIT , TIPS & TRICKS , Blogs)**

A bug bounty program is a deal offered by many websites and software developers by which individuals can receive...

medium.com

There are other great blogs out there, I can't list them all, you need to find them according to your need.

. . .

## **10. Follow cool guys on Github.**



**• GitHub**

Security engineer, internet sleuth and builder of tools. -  
michenriksen

[github.com](#)

**• GitHub**

Penetration tester from Australia. Current maintainer of  
NoSQLMap, VHostScan, Reconnoitre. Co-contributor to

[github.com](#)

**• GitHub**

Doing security stuff! Automating things because of my  
laziness to the fullest. - Ice3man543

[github.com](#)



**• GitHub**

nahamsec has 11 repositories available. Follow their code on GitHub.

[github.com](https://github.com)

**• GitHub**

Fixaholic, problem solver, coder, Go lover, car modifier, hedonist, AV nerd, knife enthusiast, foodie, not really a...

[github.com](https://github.com)

**• GitHub**

about3la has 2 repositories available. Follow their code on GitHub.

[github.com](https://github.com)



**• GitHub**

maurosoria has 2 repositories available. Follow their code on GitHub.

[github.com](https://github.com)

**• GitHub**

guelfoweb has 12 repositories available. Follow their code on GitHub.

[github.com](https://github.com)

**• GitHub**

Security Researcher, Red Team Manager, Gopher, Founder and Project Lead of OWASP Amass - [caffix](#)

[github.com](https://github.com)



**• GitHub**

Web developer reconverted to security researcher, playing bug bounty sometimes :) - gwen001

[github.com](https://github.com)

Consider donating small part of your bounties to them to support their open source contribution or you can contribute in other ways too. Only If they accept donation.

. . .

## 11. Follow Active Bug Bounty Hunters on Twitter (But not limited to this list)

**Frans Rosén (@fransrosen) | Twitter**

The latest Tweets from Frans Rosén (@fransrosen).  
Dev/Security/Founder at @centrahq/@detectify

[twitter.com](https://twitter.com)



### **Mathias Karlsson (@avlidienbrunn) | Twitter**

The latest Tweets from Mathias Karlsson (@avlidienbrunn).  
Web security fiddler. Bug bounty bastard. CTF with...

[twitter.com](https://twitter.com)

### **dawgyg@Home (@thedawgyg) | Twitter**

The latest Tweets from dawgyg@Home (@thedawgyg).  
Wall of Fame: Yahoo, Mail.Ru, Mapbox, Imgur, GM, Adobe,

[twitter.com](https://twitter.com)

### **Olivier Beg (@smiegles) | Twitter**

The latest Tweets from Olivier Beg (@smiegles). Head of  
researchers at @zerocopter, Co-founder

[twitter.com](https://twitter.com)



### **Jobert Abma (@jobertabma) | Twitter**

The latest Tweets from Jobert Abma (@jobertabma). I tweet about security and my experience as a hacker. Co-

[twitter.com](https://twitter.com)

### **STÖK (@stokfredrik) | Twitter**

The latest Tweets from STÖK (@stokfredrik). Hacker - Creative - Red Team Lead - Advisor - Conscious Fashion

[twitter.com](https://twitter.com)

### **Gerben Javado (@gerben\_javado) | Twitter**

The latest Tweets from Gerben Javado (@gerben\_javado). Security Engineer @Facebook. Into bug bounties.

[twitter.com](https://twitter.com)



### **Tanner (@itscachemoney) | Twitter**

The latest Tweets from Tanner (@itscachemoney).  
Somewhere between a builder and a breaker. San

[twitter.com](https://twitter.com)

### **Ben Sadeghipour (@NahamSec) | Twitter**

The latest Tweets from Ben Sadeghipour (@NahamSec).  
Hacker | Co-founder @bugbountyforum | Hacker

[twitter.com](https://twitter.com)

### **Yassine Aboukir (@Yassineaboukir) | Twitter**

The latest Tweets from Yassine Aboukir (@Yassineaboukir).  
Wearing my security analyst hat @Hacker0x01 by day and

[twitter.com](https://twitter.com)



### Geekboy (@emgeekboy) | Twitter

The latest Tweets from Geekboy (@emgeekboy). Full time bug bounty hunter 🌟🌟. India

[twitter.com](https://twitter.com)

### Patrik Fehrenbach 🧑🏻💻 (@ITSecurityguard) | Twitter

The latest Tweets from Patrik Fehrenbach 🧑🏻💻 (@ITSecurityguard): "I recently scored a 4000\$ bounty by

[twitter.com](https://twitter.com)

### Ed (@EdOverflow) | Twitter

The latest Tweets from Ed (@EdOverflow). Web developer & security researcher. | FA98 07A5 F836 9C61 A8C2 AC3B

[twitter.com](https://twitter.com)



### **x1m (@x1m\_martijn) | Twitter**

The latest Tweets from x1m (@x1m\_martijn). Ethical Hacker

[twitter.com](https://twitter.com)

### **Nathan (@NathOnSecurity) | Twitter**

The latest Tweets from Nathan (@NathOnSecurity). Infosec and such. "Confront the culture of power with the

[twitter.com](https://twitter.com)

### **Th3G3nt3lman (@Th3G3nt3lman) | Twitter**

The latest Tweets from Th3G3nt3lman (@Th3G3nt3lman). Security Researcher / Bug Bounty Hunter / Red Devil.

[twitter.com](https://twitter.com)



### **Uranium238 (@uraniumhacker) | Twitter**

The latest Tweets from Uranium238 (@uraniumhacker).

Tweets does not mean endorsement and does not

[twitter.com](https://twitter.com)

### **Santiago Lopez (@santi\_lopezz99) | Twitter**

The latest Tweets from Santiago Lopez (@santi\_lopezz99).

1# researcher on @Hacker0x01 #bugbounty. Insta...

[twitter.com](https://twitter.com)

### **Rahul Maini (@iamnoooob) | Twitter**

The latest Tweets from Rahul Maini (@iamnoooob).

<https://t.co/F8Xu6Nh4Wb> | <https://t.co/ZCLtc0QXbx> |...

[twitter.com](https://twitter.com)



### **Brett Buerhaus (@bbuerhaus) | Twitter**

The latest Tweets from Brett Buerhaus (@bbuerhaus).  
Blizzard Entertainment. Digital bounty hunter. Co9.io.

[twitter.com](https://twitter.com)

### **Harsh Jaiswal (@rootxharsh) | Twitter**

The latest Tweets from Harsh Jaiswal (@rootxharsh). You  
know. Indore, India

[twitter.com](https://twitter.com)

### **Paresh (@Paresh\_parmar1) | Twitter**

The latest Tweets from Paresh (@Paresh\_parmar1).  
bugbounty hunter/ gamer /. Ahmedabad

[twitter.com](https://twitter.com)



### Joel Margolis (@0xteknogeek) | Twitter

The latest Tweets from Joel Margolis (@0xteknogeek).  
Mobile security researcher, bug bounty hunter. RIT dropout.

[twitter.com](https://twitter.com)

### Abdullah Hussam (@Abdulahhusam) | Twitter

The latest Tweets from Abdullah Hussam  
(@Abdulahhusam). I don't trust bio. Iraq

[twitter.com](https://twitter.com)

### zseano🌟 (@zseano) | Twitter

The latest Tweets from zseano🌟 (@zseano). WebApp  
Security Researcher with a focus on bugbounties which

[twitter.com](https://twitter.com)



### **Ron Chan (@ngalongc) | Twitter**

The latest Tweets from Ron Chan (@ngalongc)

[twitter.com](https://twitter.com)

### **Parth Malhotra (@Parth\_Malhotra) | Twitter**

The latest Tweets from Parth Malhotra (@Parth\_Malhotra):

"Yay, I was awarded \$18,000 in bounties on @Hacker0x01

[twitter.com](https://twitter.com)

### **Prateek Tiwari (@prateek\_0490) | Twitter**

The latest Tweets from Prateek Tiwari (@prateek\_0490).

Security @Zomato | Security Nerd | I do nothing but eat,

[twitter.com](https://twitter.com)



### **Pranav Hivarekar (@HivarekarPranav) | Twitter**

The latest Tweets from Pranav Hivarekar

(@HivarekarPranav). REST-API Lover | Loves #bugbounty |

[twitter.com](https://twitter.com)

### **Jigar Thakkar (@jigarthakkar39) | Twitter**

The latest Tweets from Jigar Thakkar (@jigarthakkar39).

Security Researcher | Pentester | Logical Thinker |

[twitter.com](https://twitter.com)

### **nikhil (@niksthehacker) | Twitter**

The latest Tweets from nikhil (@niksthehacker). SRT member at @SynackRedTeam , Bug Bounty Hunter at

[twitter.com](https://twitter.com)



### **Rishiraj Sharma (@ehrishiraj) | Twitter**

The latest Tweets from Rishiraj Sharma (@ehrishiraj).  
Application Security Engineer at SecurityEscape. India

[twitter.com](https://twitter.com)

### **pwnmachine 🧑🏻‍💻 (@princechaddha) | Twitter**

The latest Tweets from pwnmachine 🧑🏻‍💻 (@princechaddha). OSCP | Synack Red Team  
| Eat Sleep Pwn Repeat...

[twitter.com](https://twitter.com)

### **Bull (@v0sx9b) | Twitter**

The latest Tweets from Bull (@v0sx9b). Because i had to.....|  
<https://t.co/bkoGpbvpqP> | <https://t.co/jBwjU1nqnv> | ...

[twitter.com](https://twitter.com)



**naffy (@nnwakelam) | Twitter**

The latest Tweets from naffy (@nnwakelam). CEO of Hackers Helping Hackers. My tweets are my own. STC is the

[twitter.com](https://twitter.com)

**shubs (@infosec\_au) | Twitter**

The latest Tweets from shubs (@infosec\_au). continuous security, @assetnote hack the planet, @hackershelling.

[twitter.com](https://twitter.com)

**Inti De Ceukelaire (@securinti) | Twitter**

The latest Tweets from Inti De Ceukelaire (@securinti). Ethical hacker and bug bounty hunter. Founder of...

[twitter.com](https://twitter.com)



### **Artem (@mskwsy) | Twitter**

The latest Tweets from Artem (@mskwsy): "That feeling when you do not want to leave Kiev. Thank you

[twitter.com](https://twitter.com)

### **Bhavuk Jain (@bhavukjain1) | Twitter**

The latest Tweets from Bhavuk Jain (@bhavukjain1). Programmer <https://t.co/St09FSu3Dw>. Delhi, India

[twitter.com](https://twitter.com)

### **Avinash Jain (@logicbomb\_1) | Twitter**

The latest Tweets from Avinash Jain (@logicbomb\_1). Lead Infrastructure Security Engineer @groferseng | DevSecops

[twitter.com](https://twitter.com)



### **Emad Shanab (@Alra3ees) | Twitter**

The latest Tweets from Emad Shanab (@Alra3ees). Lawyer & Ethical Hacker & Every Law has its own Bugs...

[twitter.com](https://twitter.com)

### **Ebrahim Hegazy (@Zigoo0) | Twitter**

The latest Tweets from Ebrahim Hegazy (@Zigoo0). #H1\_Triage team member & Vulnerabilities Hunter since

[twitter.com](https://twitter.com)

### **Yasser Ali (@garagosy) | Twitter**

The latest Tweets from Yasser Ali (@garagosy). Someone who adores Information Security!. Dubai, United Arab

[twitter.com](https://twitter.com)



### **Akhil Reni (@akhilreni\_hs) | Twitter**

The latest Tweets from Akhil Reni (@akhilreni\_hs). I TWEET  
AS AKHIL RENI !

[twitter.com](https://twitter.com)

### **ak1t4 🌊 (@akita\_zen) | Twitter**

The latest Tweets from ak1t4 🌊 (@akita\_zen). [ Bug  
Bounty Hunter - Zen Monk] "Beautiful things don't ask

[twitter.com](https://twitter.com)

### **mongo (@mongobug) | Twitter**

The latest Tweets from mongo (@mongobug). I like bug  
bounty programs and breaking things other people built. ::1

[twitter.com](https://twitter.com)



**Arbaz Hussain 🐸 (@ArbazKiraak) | Twitter**

The latest Tweets from Arbaz Hussain 🐸 (@ArbazKiraak).  
cat /etc/arbaz | grep Machine Learning && Bug Hunter 🤖

twitter.com

and others ❤️ can't add everyone here.

. . .

## 12. Credits

Thanks to these awesome guys **Prateek Tiwari Rishiraj Sharma & Geekboy** for proof reading this post :)

Feedbacks are always welcome.

until next time.



This embedded content is from a site that does not comply with the Do Not Track (DNT) setting now enabled on your browser.

Please note, if you click through and view it anyway, you may be tracked by the website hosting the embed.

**[Learn More about Medium's DNT policy](#)**

**SHOW EMBED**