BUG BOUNTY HUNTING

BB001

sachin

BB001-1

Bug bounty is to:

Learn how internet works
Secure online things
Respect others
And earn money

Not to:

Hack insecure websites/apps
Take revenge/Harm others

sachin

BB001-2

Key to success:

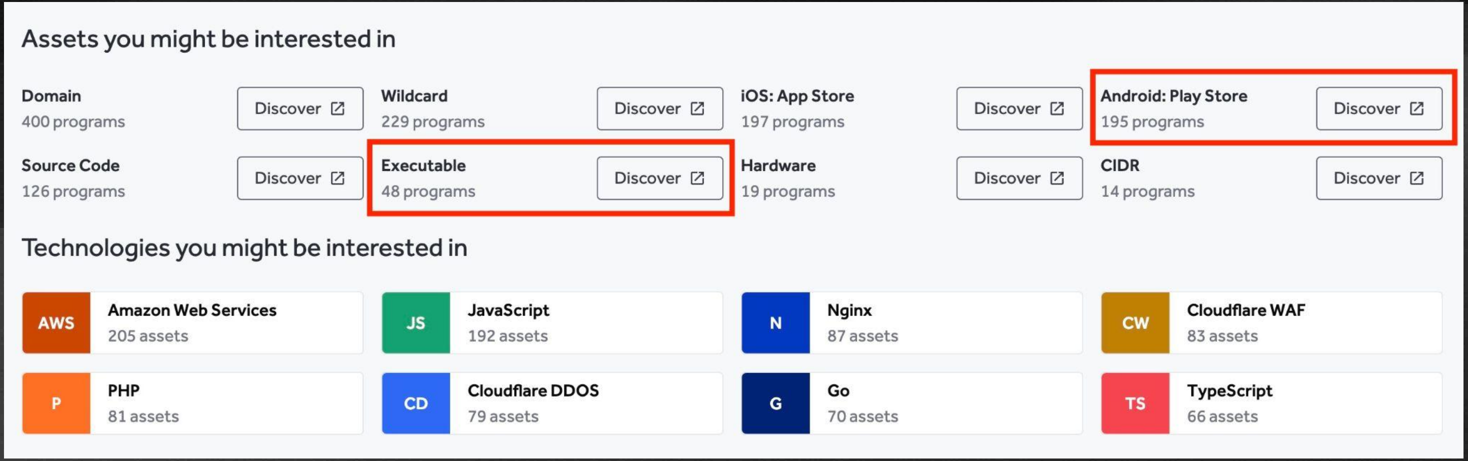
Read less, understand more
No need to learn every topic, understand your learning deeply.

Be uniq
If you do what other people do you will get nothing. So create your own perspective to hack.

sachin

BB001-3

Choose less crowded targets



Assets you might be interested in

Domain 400 programs	Wildcard 229 programs	iOS: App Store 197 programs	Android: Play Store 195 programs
Source Code 126 programs	Executable 48 programs	Hardware 19 programs	CIDR 14 programs

Technologies you might be interested in

AWS Amazon Web Services 205 assets	JS JavaScript 192 assets	N Nginx 87 assets	CW Cloudflare WAF 83 assets
P PHP 81 assets	CD Cloudflare DDOS 79 assets	G Go 70 assets	TS TypeScript 66 assets

sachin

BB001-3

Choose less crowded targets

In my journey, I found that android apps are more vulnerable than webapps.

I will show an example with one of by finding

SSTI [Server Side Template Injection] leads to RCE (Remote code execution)

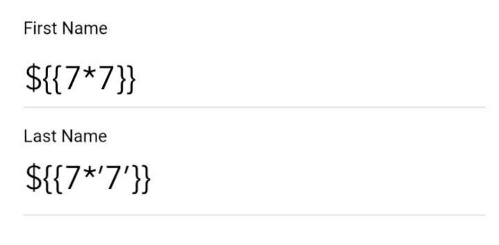
sachin

BB001-3

Story-001 : SSTI [Server Side Template Injection]

I put SSTI payload in name fields and some days later i receive a mail that starts with

Dear $49

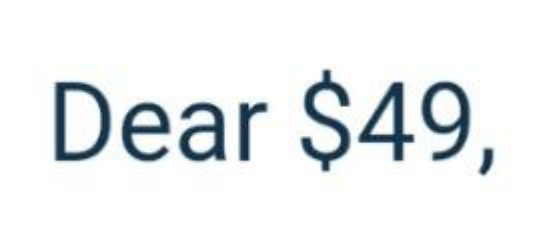


First Name

${{7*7}}

Last Name

${{7*'7'}}



Dear $49,

BB001-3

Story-001 : SSTI [Server Side Template Injection]

Backend code

```
email_template =
Dear {{NAME}},
Our terms and conditions are changed…
```

```
email_template =
Dear {{${{7*7}}}},                    —> Dear $49
Our terms and conditions are changed…
```

sachin

BB001-3

Story-002 : WaF Bypass

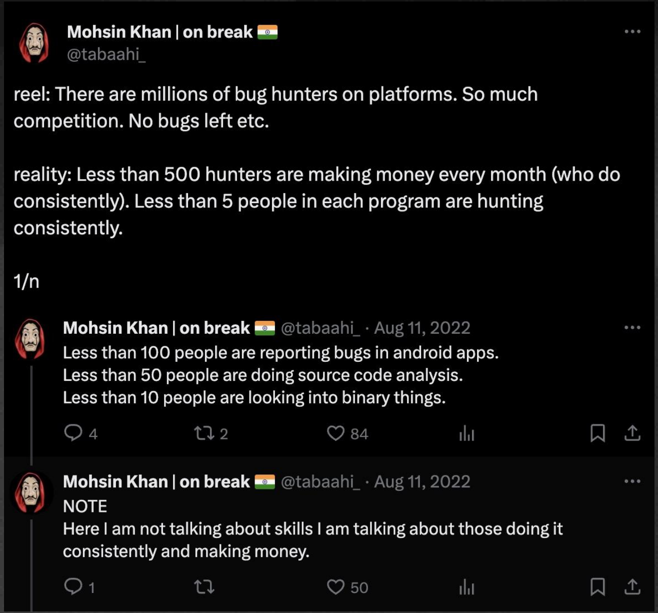
```
Web app
        Address : “><svg/onload=alert(1)>          → 403

Android app
        Address : “><svg/onload=alert(1)>          → 200
```

sachin

BB001-4

If you are doing it consistently there is no competitor.



Mohsin Khan | on break 🇮🇳
@tabaahi_

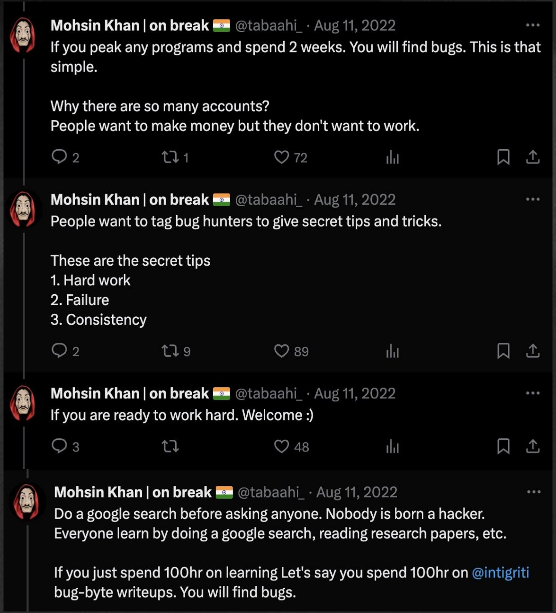
reel: There are millions of bug hunters on platforms. So much competition. No bugs left etc.

reality: Less than 500 hunters are making money every month (who do consistently). Less than 5 people in each program are hunting consistently.

1/n

Mohsin Khan | on break 🇮🇳 @tabaahi_ · Aug 11, 2022
Less than 100 people are reporting bugs in android apps.
Less than 50 people are doing source code analysis.
Less than 10 people are looking into binary things.

Mohsin Khan | on break 🇮🇳 @tabaahi_ · Aug 11, 2022
NOTE
Here I am not talking about skills I am talking about those doing it consistently and making money.



Mohsin Khan | on break 🇮🇳 @tabaahi_ · Aug 11, 2022
If you peak any programs and spend 2 weeks. You will find bugs. This is that simple.

Why there are so many accounts?
People want to make money but they don't want to work.

Mohsin Khan | on break 🇮🇳 @tabaahi_ · Aug 11, 2022
People want to tag bug hunters to give secret tips and tricks.

These are the secret tips
1. Hard work
2. Failure
3. Consistency

Mohsin Khan | on break 🇮🇳 @tabaahi_ · Aug 11, 2022
If you are ready to work hard. Welcome :)

Mohsin Khan | on break 🇮🇳 @tabaahi_ · Aug 11, 2022
Do a google search before asking anyone. Nobody is born a hacker.
Everyone learn by doing a google search, reading research papers, etc.

If you just spend 100hr on learning Let's say you spend 100hr on @intigriti bug-byte writeups. You will find bugs.

sachin

BB001-EOF

Be Uniq
Be Creative
Thanks for watching

Contact : https://shinchina.in

sachin