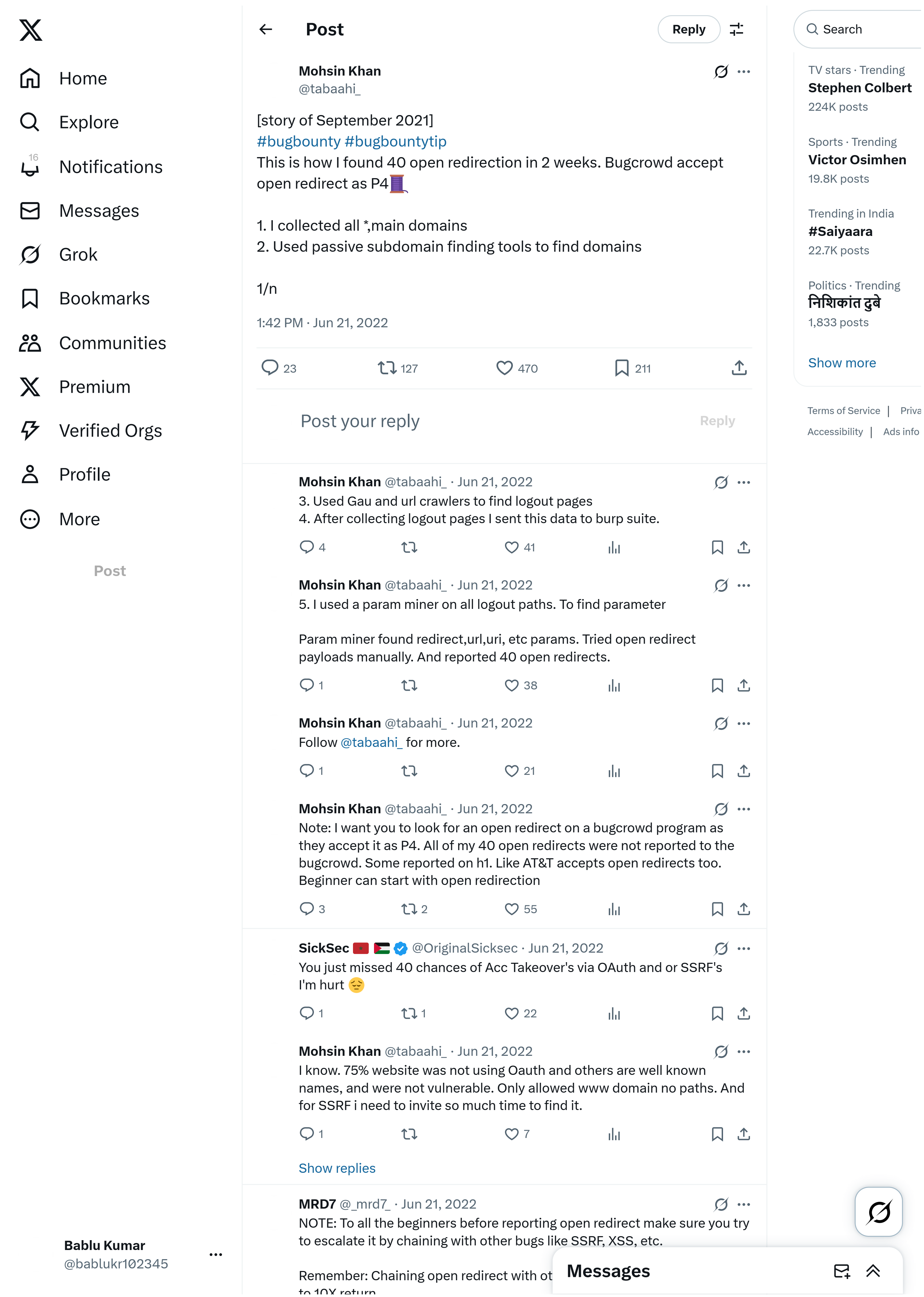

Mohsin Khan
@tabaahi_

[story of September 2021]
#bugbounty #bugbountytip
This is how I found 40 open redirection in 2 weeks. Bugcrowd accept open redirect as P4🧵

1. I collected all *,main domains
2. Used passive subdomain finding tools to find domains

1/n

1:42 PM · Jun 21, 2022

23 127 470 211

Post your reply Reply

Mohsin Khan @tabaahi_ · Jun 21, 2022
3. Used Gau and url crawlers to find logout pages
4. After collecting logout pages I sent this data to burp suite.

4 41

Mohsin Khan @tabaahi_ · Jun 21, 2022
5. I used a param miner on all logout paths. To find parameter

Param miner found redirect,url,uri, etc params. Tried open redirect payloads manually. And reported 40 open redirects.

1 38

Mohsin Khan @tabaahi_ · Jun 21, 2022
Follow @tabaahi_ for more.

1 21

Mohsin Khan @tabaahi_ · Jun 21, 2022
Note: I want you to look for an open redirect on a bugcrowd program as they accept it as P4. All of my 40 open redirects were not reported to the bugcrowd. Some reported on h1. Like AT&T accepts open redirects too. Beginner can start with open redirection

3 2 55

SickSec 🇲🇦 🇵🇸 @OriginalSicksec · Jun 21, 2022
You just missed 40 chances of Acc Takeover's via OAuth and or SSRF's
I'm hurt 😔

1 1 22

Mohsin Khan @tabaahi_ · Jun 21, 2022
I know. 75% website was not using Oauth and others are well known names, and were not vulnerable. Only allowed www domain no paths. And for SSRF i need to invite so much time to find it.

1 7

Show replies

MRD7 @_mrd7_ · Jun 21, 2022
NOTE: To all the beginners before reporting open redirect make sure you try to escalate it by chaining with other bugs like SSRF, XSS, etc.

Remember: Chaining open redirect with ot
to 10X return

Home
Explore
16
Notifications
Messages
Grok
Bookmarks
Communities
Premium
Verified Orgs
Profile
More
Post

to 10x return.

1 18

Mohsin Khan @tabaahi_ · Jun 21, 2022
agree

4

Siddharth @jeetbhdr · Jun 21, 2022
Bhai Paraminer only tests parameters which is used in that in the tools wordlist right?

1 2

Mohsin Khan @tabaahi_ · Jun 21, 2022
Yes you can also use X8 I guess. To find a param with a wordlist

2 8

Utsav Singh @cluelessguyyy · Jun 21, 2022
What is X8 ?

1 1

Mohsin Khan @tabaahi_ · Jun 21, 2022
Burp extension used to find parameters. Search on GitHub

6

khan mamun @mamunwhh · Jun 21, 2022
Step 3
Can you share this command?

1 2

Fahad Khan @fahadkhan__101 · Jun 22, 2022
@SaveToNotion #thread

1

Love Yadav @love_yadav_ · Jun 21, 2022
Bro what methods you use for open redirect

1 1

Darkry @Darkry741 · Jun 21, 2022
Thank you for awsome tip and story sir

Ibrahim AH @HouranyIbrahim · Jun 22, 2022
Good job bro👏👏

Mahmoud Hamed @7odamoo · Jun 22, 2022
Nice tip 👌

Bablu Kumar
@bablukr102345

Messages