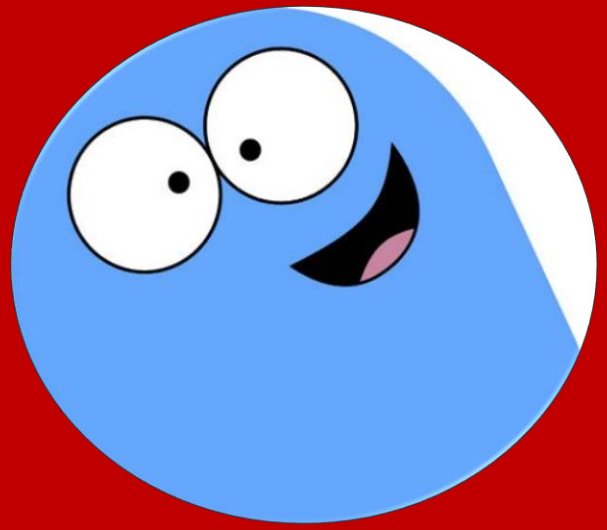
Discovery To Disclosure

Journey from Discovering Vulnerabilities Towards Disclosure

BeeFaauBee, Security Researcher
hello@beefaaubee.com
Twitter : @BeeFaauBee09

WHOAMI



- Head of Cyber Security in Financial Institution Pakistan
- Security Researcher, Developer
- Mobile Apps, IoT

Focus Of Talk

- Android Application Security
- Why Android?
- API Security

Mobile App Security Breaches

Data Breach Warn

BBC Sign in

CNBC SIGN IN

Over 4000 Android Apps Expose Users' Data via Misconfigured Firebase Databases

May 12, 2020 Ravie Lakshmanan

Popular This Week

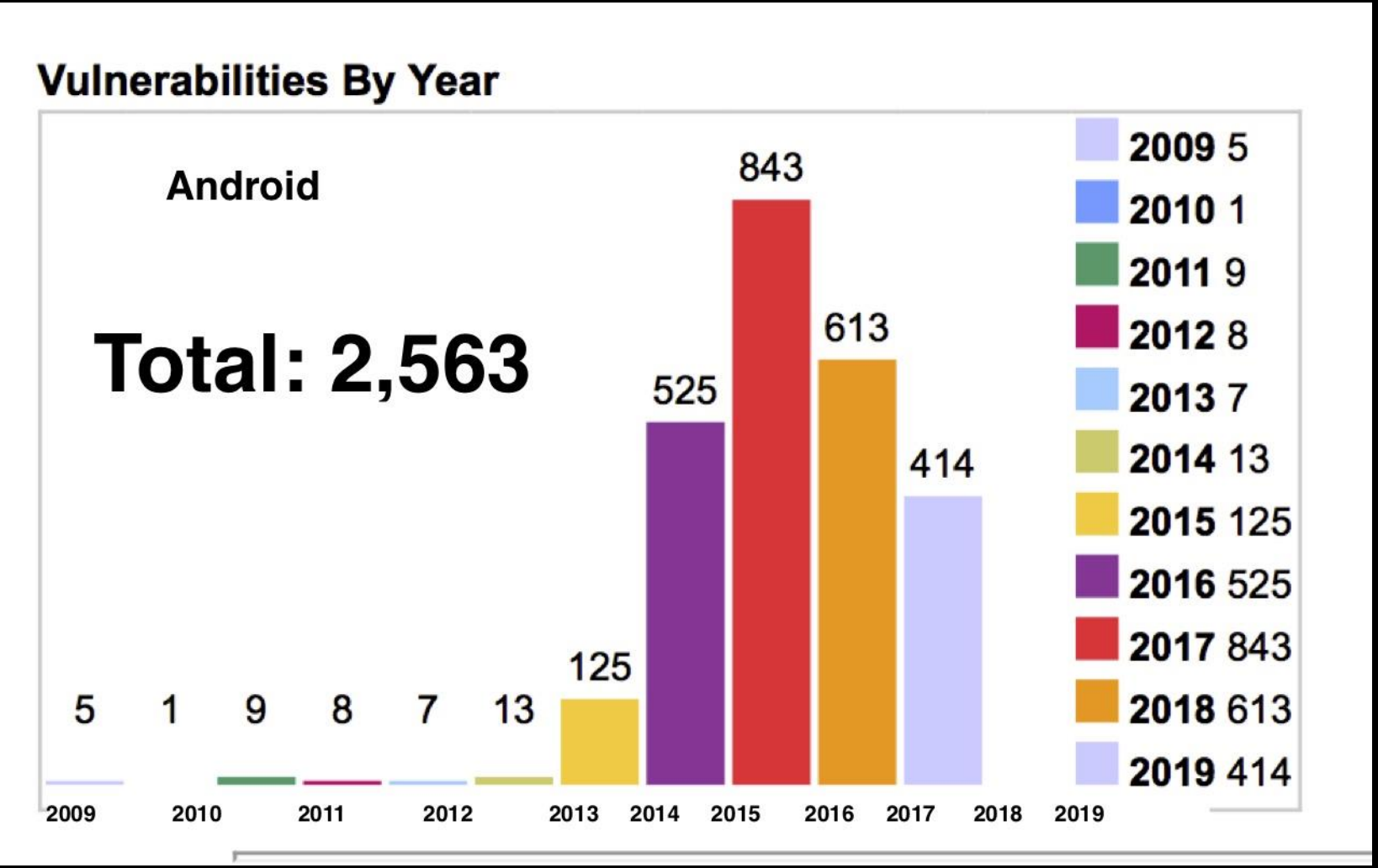
17-Year-Old 'Mastermind', 2 Others Behind the Biggest Twitter Hack Arrested

US Government Warns of a New Strain of Chinese 'Taidoor' Virus

Researcher Demonstrates 4 New Variants of HTTP Request Smuggling Attack

EU sanctions hackers from

Mobile App Security Breaches



Sources : Now Secure


How I Discovered ?

CorpApp.apk

Recon

- 1.5 Million Downloads of App Store
- Premium Services
- Great Reputation

CorpApp.apk

Recon

- Firebase For Data Storage
- Google Cloud Platform
- Google Identity Toolkit (Relyingparty)

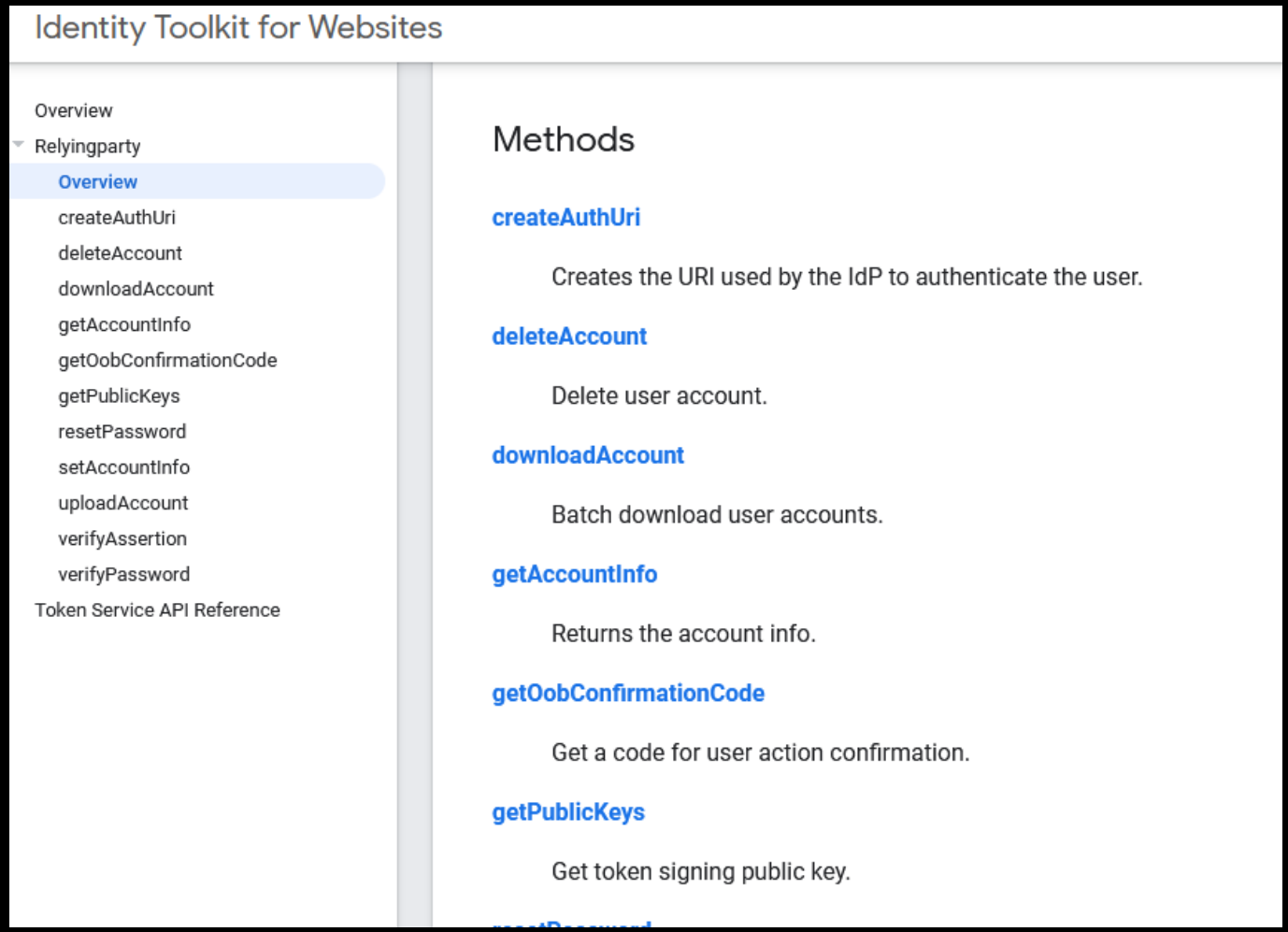
CorpApp.apk

Recon

- Firebase For Data Storage
- Google Cloud Platform
- Google Identity Toolkit (Relyingparty)

CorpApp.apk

Recon



CorpApp.apk

Recon

Relyingparty: getAccountInfo

Returns the account info.

Request

HTTP request

```
POST https://www.googleapis.com/identitytoolkit/v3/relyingparty/getAccountInfo
```

CorpApp.apk

Attack Scenario 1

- Search for Organization Emails
- no-reply@corpapp.com available for Sign Up
- Logged in As CorpApp user with same privileges

CorpApp.apk

Attack Scenario 2

- LocalId in API parameters along UserName 1
- Replaced LocalId-1 with LocalId-2 and Username 1 with UserName 2
- Request submitted as LocalId-1

CorpApp.apk

Attack Scenario 3

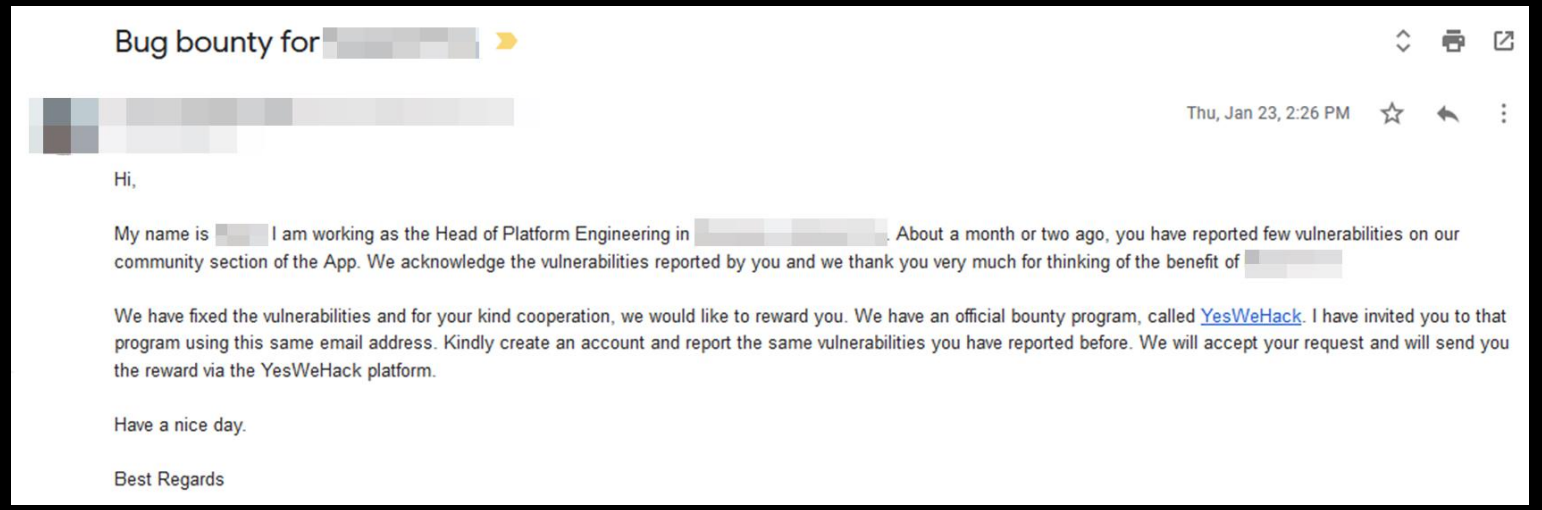
- Marketing API inside APK
- Discovered other domains
- Access to Internal Portals


Found Everything? Disclose It !

CorpApp.apk Hypothesis

- Reached out on their support platform
- Submitted all bugs through email
- Received response from Engineering Team

CorpApp.apk Hypothesis



Bug bounty for [redacted]

[redacted] Thu, Jan 23, 2:26 PM

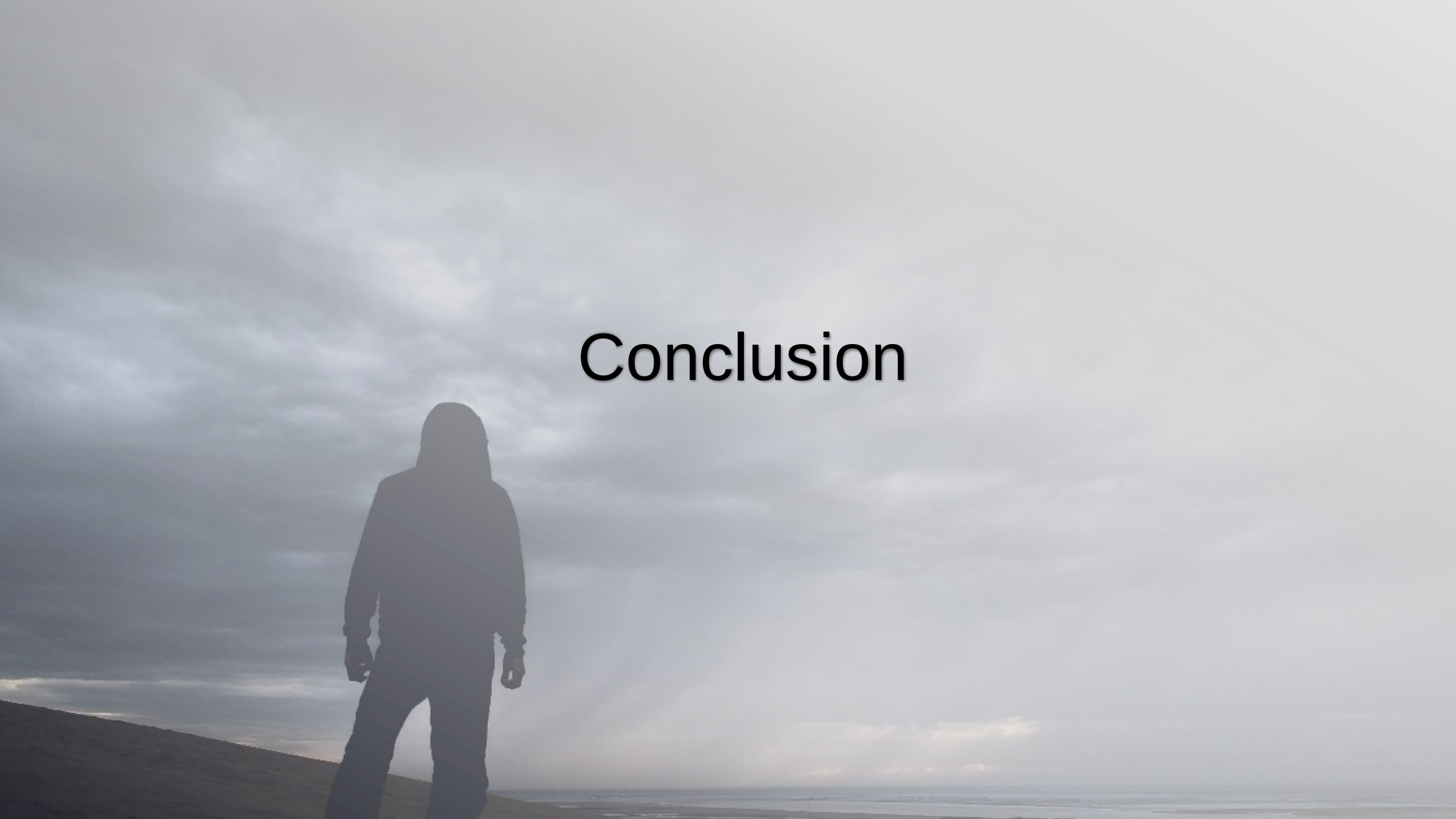
Hi,

My name is [redacted] I am working as the Head of Platform Engineering in [redacted]. About a month or two ago, you have reported few vulnerabilities on our community section of the App. We acknowledge the vulnerabilities reported by you and we thank you very much for thinking of the benefit of [redacted]

We have fixed the vulnerabilities and for your kind cooperation, we would like to reward you. We have an official bounty program, called YesWeHack. I have invited you to that program using this same email address. Kindly create an account and report the same vulnerabilities you have reported before. We will accept your request and will send you the reward via the YesWeHack platform.

Have a nice day.

Best Regards



Conclusion

CorpApp.apk Conclusion

- Act Responsibly
- Respect Privacy
- Play within Boundaries
- Patience !

CorpApp.apk Conclusion

- YesWeHack VPD Finder
- Bug Bounty Platforms.
- Development/Engineering Department

Thank You

Stay Safe & Hack The Planet (Responsibly)