# Synthetic identities

An appsec point of view

Timur Yunusov

OWASP®

PAYMENT VILLAGE

To a man with a hammer, everything looks like a nail (Abraham Maslow)

- Appsec since 2008
- Payment security research since 2015
- Hacking ATMs, POSes, Apple/Google Pay, Visa, MC


Live Streaming OWASP London Chapter Meetup at Revolut
Recorded live
OWASP London Chapter
WASP
Revolut.
Radically Better

# My results in seven years

- Angry vendors
- Customers don’t patch/fix their bugs
- Money issues are not in the “Top 3 priorities” list
- Need to talk the same language

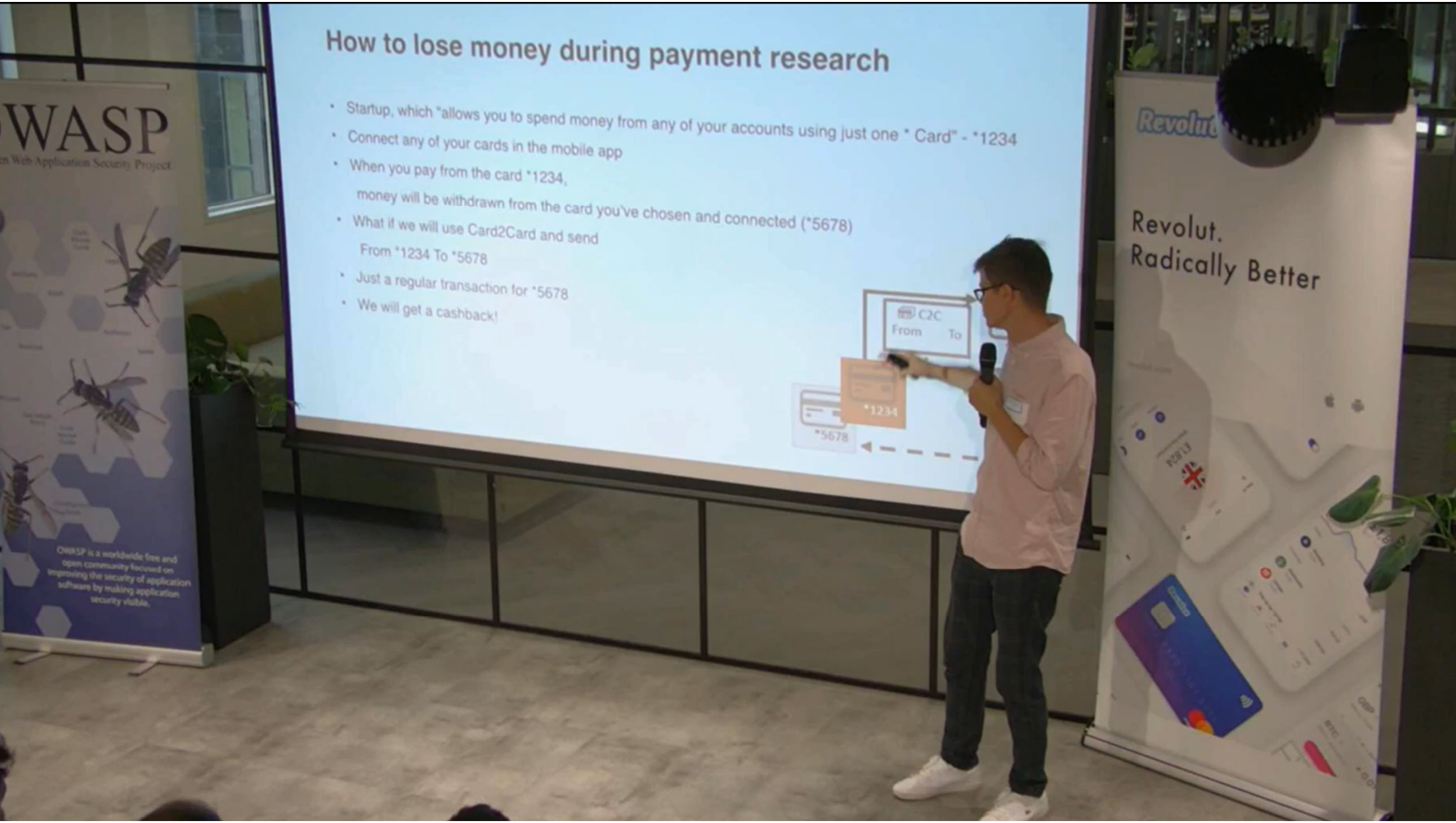
# Talking the same language

- Vulnerabilities are everywhere
- Bugs, Exploits and Attacks
- Fraud, Risks and Threats
- “Bug bounty in payments”

# Disclaimer

- Opinions are my own
- Good, bad and ugly
- Do not violate the law

# The Good, The Bad and The Ugly


How to lose money during payment research
Startup, which "allows you to spend money from any of your accounts using just one * Card" - *1234
Connect any of your cards in the mobile app
When you pay from the card *1234,
money will be withdrawn from the card you've chosen and connected (*5678)
What if we will use Card2Card and send
From *1234 To *5678
Just a regular transaction for *5678
We will get a cashback!
C2C
From
To
*1234
*5678
WASP
Revolut.
Radically Better

# Example 1. Curve

- Brilliant startup
- Bug bounty

# Example 1. Curve

- Brilliant startup
- Bug bounty… for six months

# Example 1. Curve

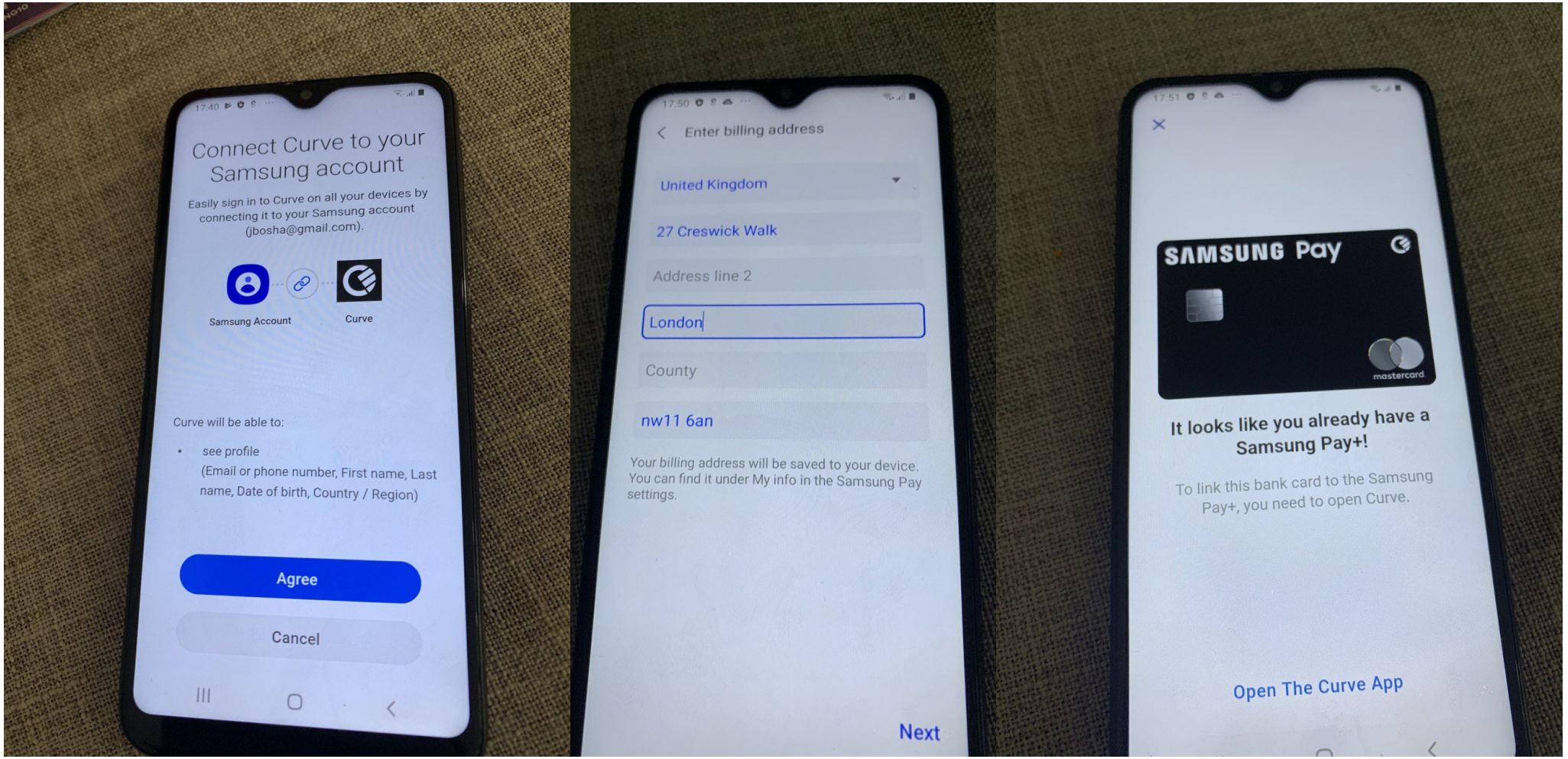
- Constant rotation of the security staff

# Example 1. Curve

- Shady ethics

  *Leaked numbers show $200 million fintech startup Curve has far fewer active users than the number of 'customers' it has claimed (c) 2019 Business Insider*

# Samsung Pay+


Connect Curve to your Samsung account
Easily sign in to Curve on all your devices by connecting it to your Samsung account (jbosha@gmail.com).
Samsung Account
Curve
Curve will be able to:
see profile
(Email or phone number, First name, Last name, Date of birth, Country / Region)
Agree
Cancel
Enter billing address
United Kingdom
27 Creswick Walk
Address line 2
London
County
nw11 6an
Your billing address will be saved to your device. You can find it under My info in the Samsung Pay settings.
Next
SAMSUNG Pay
mastercard
It looks like you already have a Samsung Pay+!
To link this bank card to the Samsung Pay+, you need to open Curve.
Open The Curve App

# Antifraud Red Team

- Red Team vs Pentest vs Product Security
- Vulnerabilities vs Risks and Threats
- Remediation steps are vital

# Example 2.

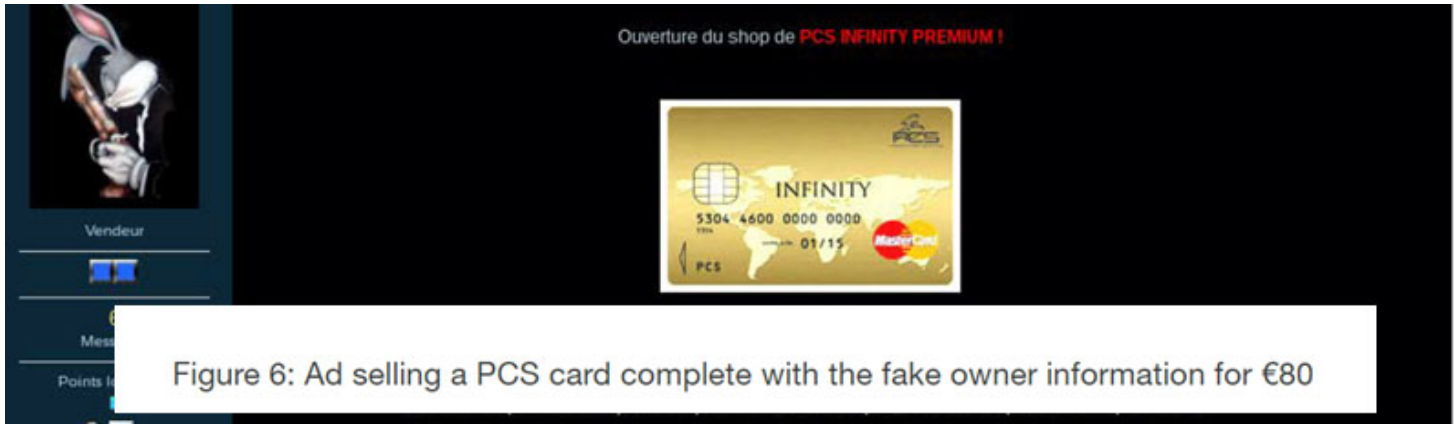



Figure 6: Ad selling a PCS card complete with the fake owner information for €80

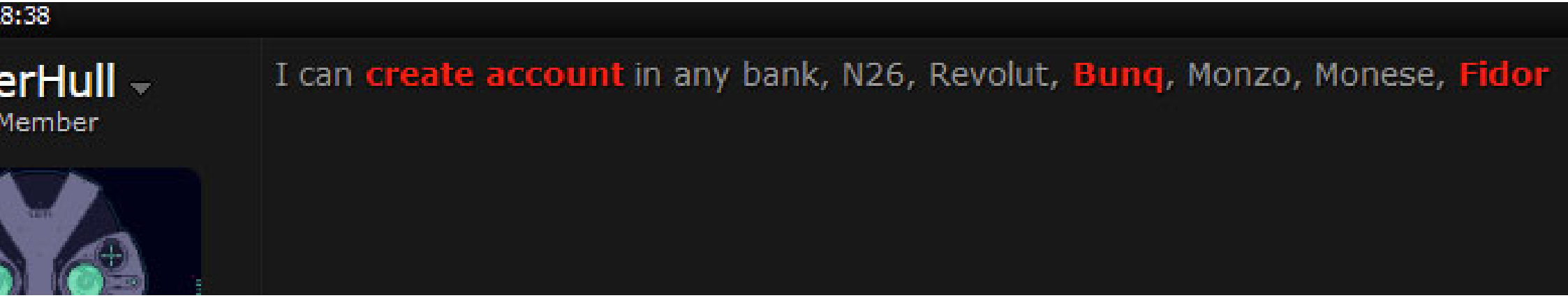
**Looking for UK HSBC phisical card! / Off Topic / DreamMarket Forum**

*http://tmskhzavkxyf6avd.onion.st/viewtopic.php?pid=206557*

Looking for UK HSBC phisical card!

* Topics: Active [] | Unanswered [] * Index [] * » Off Topic [] * » Looking for UK HSBC phisical

#1 2017-12-15 06:26:03 [] Madoxman [] Member Registered: 2017-10-20 Posts: 37 Looking for




myPOS Go
BLACK MASS
9.07.2019г
myPOS
BUSINESS
5392 6023 2392 8018
06/22
MasterCard
myPOS
F1
F2
F

Graham Barrow

# Chris Elliot ZUCKERBERG

Filter appointments

☐ Current appointments

Total number of appointments 2

Date of birth
**November 2002**

## INSTERGRAM LIMITED (NI691871)

Company status
**Active**

Correspondence address
**20 Galgorm Industrial Estate, Fenaghy Ro**
**Ireland, BT42 1PY**

Role ACTIVE
**Director**

Appointed on
**14 October 2022**

Nationality
**British**

Country of residence
**United Kingdom**

Oc
Dir

## META PLATFORMS, INC LIMITED (NI691870)

# Example 2.


BUNDESREPUBLIK DEUTSCHLAND
L18M97NFR
PERSONALAUSWEIS
KAUFMANN
MARAT
19.06.1986 DEUTSCH
KÖLN
362204
14.03.2021
DRIVING LICENCE
1. COSTER
2. MEGAN DAWN
3. 30.04.1988 UNITED KINGDOM
4a. 07.11.2015 4c. DVLA
4b. 06.11.2025
5. COSTE8043085MD9KV 40
8. 63 ELMWOOD, SAWBRIDGEWORTH, HERTFORDSHIRE, CM21 9NN
9. AM/B/f/k/q
ČESKÁ REPUBLIKA
OBČANSKÝ PRŮKAZ
CZECH REPUBLIC IDENTIFICATION CARD
998000398
SPECIMEN
VZOR
08.10.1981
RICANY
okr. PRAHA-VÝCHOD
ČESKÁ REPUBLIKA
11.02.2013
11.02.2023
California
DRIVER LICENSE
FEDERAL LIMITS APPLY
I1234562
CLASS C
08/31/2014
END NONE
SAMPLE
ALEXANDER JOSEPH
2570 24TH STREET
ANYTOWN, CA 95818
08/31/1977
RSTR NONE
08311977
SEX M
HGT 5'-08"
HAIR BLK
WGT 150 lb
EYES BRN
08/31/2009


UA
УКРАЇНА ПОСВІДЧЕННЯ ВОДІЯ
УКРАИНА ВОДИТЕЛЬСКОЕ УДОСТОВЕРЕНИЕ
UKRAINE DRIVING LICENCE
UKRAINE PERMIS DE CONDUIRE
1 ДЕПАРДЬЄ КСАВЬЄ
DEPARDYE KSAVYE
2. ЖЕРАР МАРСЕЛЕВИЧ
JERAR
3. 27.12.1948 СУМСЬКА
SUMSKA
27.12.2018
4b. 27.12.2050
4c. ТСЦ 5154
TSC 5154
5. KBI 654231
7.
9. B1 B C1
MIA UKRAINE


ESPAÑA
PASAPORTE
PASSPORT
Tipo/Type/Type Código/Code/Code PASAPORTE Nº/PASSPORT NO/PASSPORT Nº
P ESP
BB109068
(1) Apellidos/Surname/Nom
MATROSKIN
(2) Nombre/Given Name/Prénom
KOT
(3) Nacionalidad/Nationality/Nationalité
ESPAÑOLA
(4) Fecha de nacimiento/Date of Birth/Date de naissance
02-09-1964
(6) Lugar de nacimiento/Place of Birth/Lieu de naissance
CORDOBA
(7) Fecha de expedición/Date of issue/
Date de délivrance
28-02-2008
(8) Firma del titular/Holder's signature/Signature du titulaire
(9) Autoridad/Authority/Autorité
(5) Fecha de caducidad/Date of expiry/
Date d'expiration
27-02-2028
ESP
M
P<ESPMATROSKIN<<KOT<<<<<<<<<<<<<<<<<<<<<<<
BB109068<4ESP6409029M2802275A2006018900<<<40

# Example 2.

Need:

- Photoshop
- Imagination
- Access to a KYC platform

# Report

**Success**

Completed 16 Feb 2022, 11:31 AM

## Document analysis

- Validity and authenticity
  - Not expired
  - Face detected
  - Face matched with ID
  - OCR
  - Valid MRZ
  - Comparison Front and Back
  - Comparison data sources
  - Cryptographically checked
  - Not visual tampering detection
  - Valid template
  - NFC
  - NFC genuine check
  - NFC revokation check
- Other
  - Not in compromised list
  - Fields checked against issuer
  - Dedup check
- Data capture
  - Country *
  - Given name
  - Document photo
  - Full name *
  - Document id *
  - Date of issue
  - Family name
  - Class
  - Document type *
  - Frontside *
  - Address
  - Gender
  - Date of expire
  - Date of birth
  - Age

** The field is required for request*

- Conditions
  - Date of expire is later than 16 [illegible] 2022



```
POST /api/v2/capture/documents HTTP/1.1
Host: api
Content-Type: multipart/form-data; boundary=alamofire.boundary.253979255aebd578
Connection: keep-alive
X-Token: NzA5MTc2N2ZlNzM3M2NhZDI1NDBhMDM5MTY5Mzg4MzVR66gvJDE0NThlNTFhL
X-Device: 1458e51a-4ba0-4bf5-8b6d-9b33c677d687
Accept: */*
User-Agent:                (environment: Production; build:20; iPhone SE 1st Gen; iOS 13.3) Fo
Accept-Language: en-GB
Accept-Encoding: gzip;q=1.0, compress;q=0.5
Content-Length: 259662

--alamofire.boundary.253979255aebd578
Content-Type: application/json
Content-Disposition: form-data; name="data"; filename="data"
```




# Re: Application for verification status - Ticket #15589

Inbox ×

**Customer Support** <help@ .com>

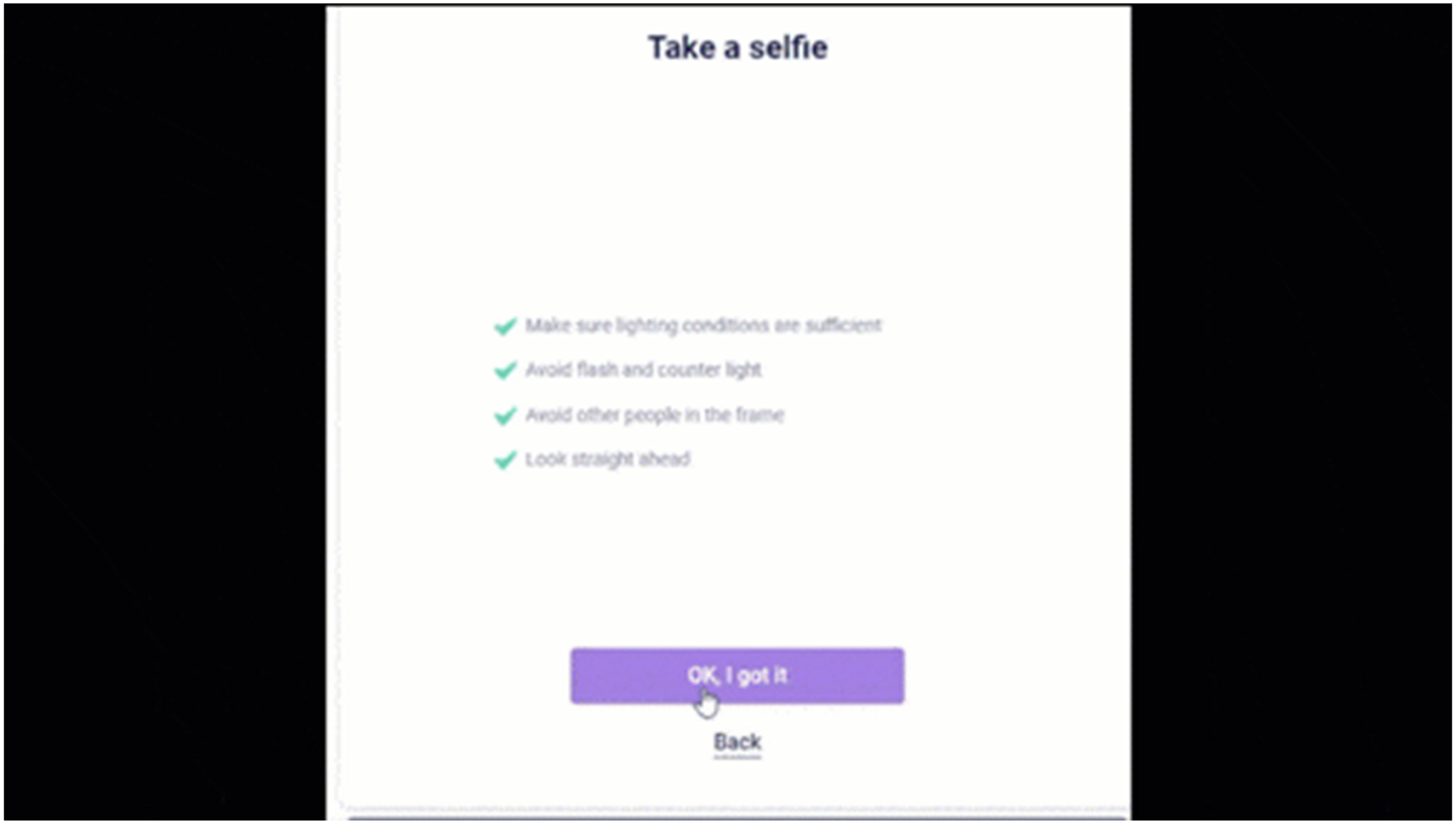
Hi Timu

Thank you for contacting us.

We would like to inform you that your account has been blocked by our Compliance department based on our internal policies and rules.
Should we have new information concerning your case, we will let you know by email.

We apologise for any inconvenience caused.

# Deepfake Offensive Toolkit



# Deepfake Offensive Toolkit

# Example 3.

# Video/audio deepfakes

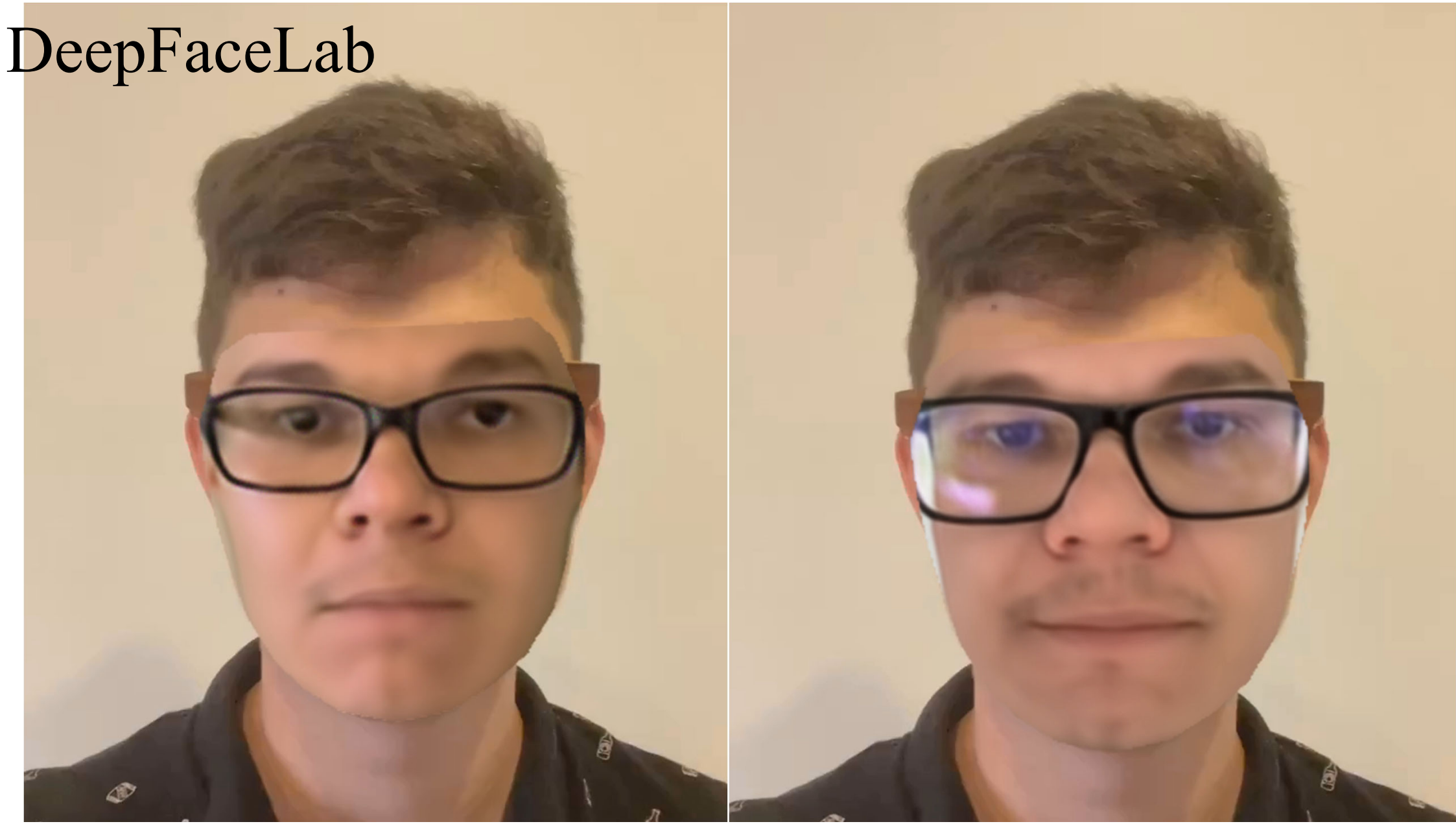
Need

- Use a mix of opensource and commercial products
- Find the right “victim” (@i_bo0om)
- Find a way to sending hundreds requests (humans) or thousands/hundreds of thousands (AI)

# Deepfake Offensive Toolkit

+

=


DeepFaceLab

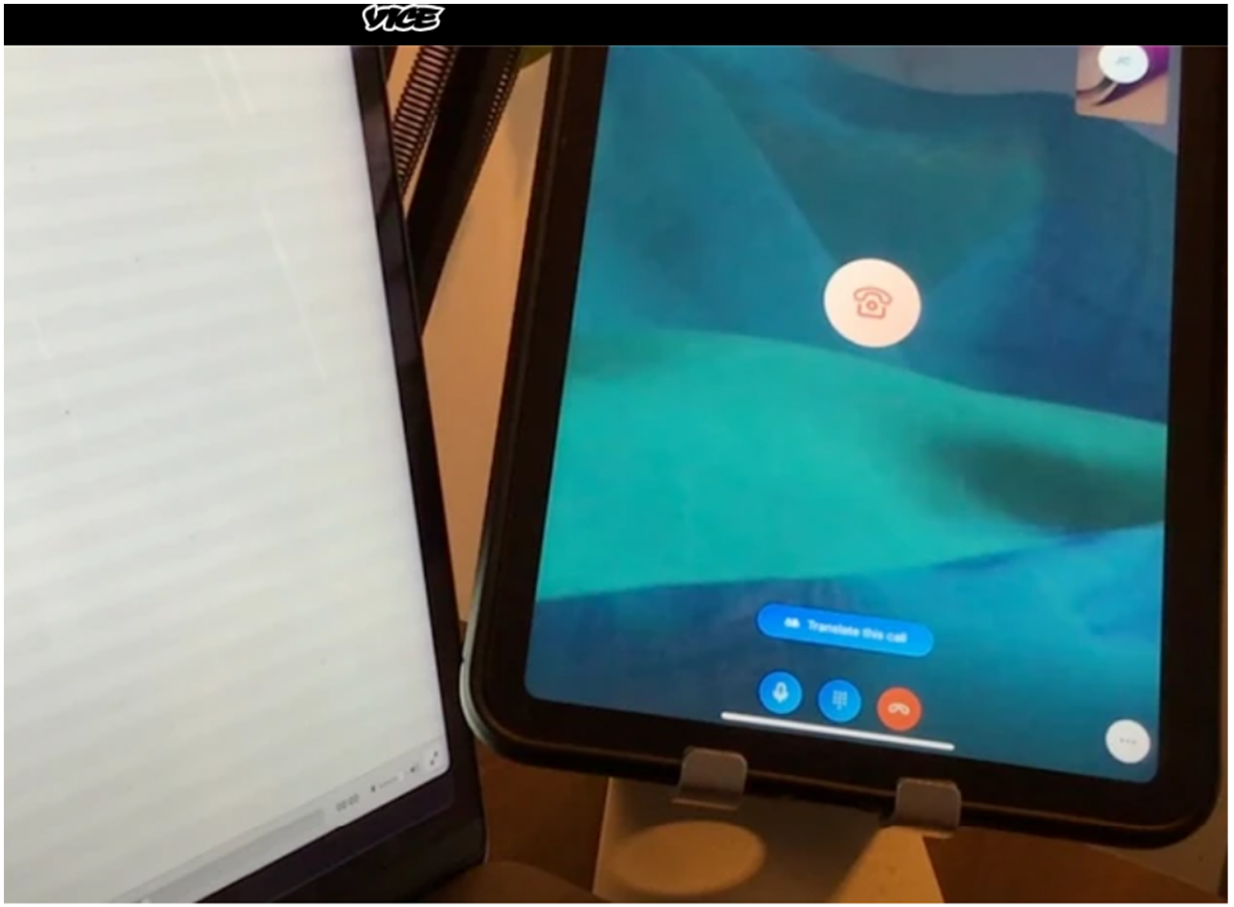



IMAGE: MOTHERBOARD

MOTHERBOARD
TECH BY VICE

# How I Broke Into a Bank Account With an AI-Generated Voice

PAYMENT VILLAGE

What has it to do with appsec?

# What has it to do with appsec?

It is possible that attackers can gather information on an application by monitoring the time it takes to complete a task or give a respond.

In cryptography, a timing attack is a side-channel attack in which the attacker attempts to compromise a cryptosystem by analyzing the time taken to execute cryptographic algorithms.

# What has it to do with appsec?

- Device attestation failures
- Trial and error aka bruteforce
- Information leakage via demo access
- Lack of replay protection

# What has it to do with appsec?

- A01:2021-Broken Access Control
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A07:2021-Identification and Authentication Failures
- A09:2021-Security Logging and Monitoring Failures

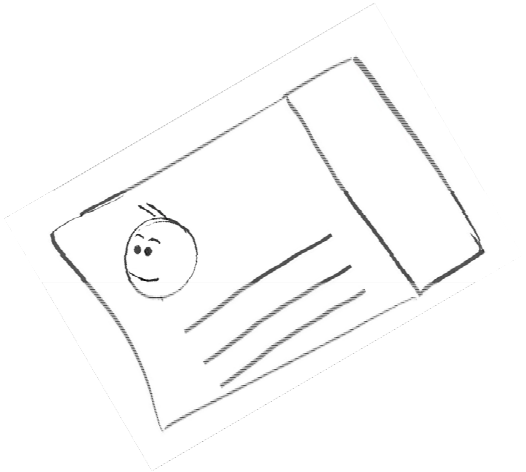
# We can do better

Companies

- Try Red Team exercises
- Do not launch bug bounty if you're not ready
- Application Security is vital

Hackers

- Change the way of delivering the findings



# QUESTIONS?

Paymentvillage.org

OWASP®

PAYMENT VILLAGE