Crowdsourced Security

Get hacked before you get hacked

DPI Privacy Café - 27/06/2018

By @intidc

Whoami

- Inti De Ceukelaire
- Uit het wondermooie Aalst
- 23 y/o
- Creative Developer @stubru
- Ethical hacker & bug bounty hunter

@intidc

Hoe we ons voelen vs hoe we er uit zien

@intidc

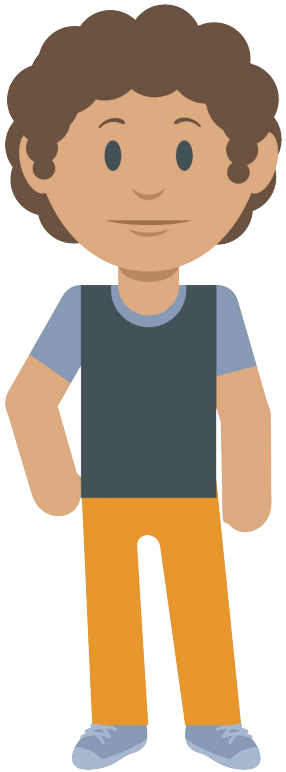
“Security is hard”

@intidc

“Je kan niet voorkomen dat je gehackt wordt. Maar je kan het de hackers wel minder makkelijk maken.”

- Mezelf

Een security expert



- Skilled
- Creatief
- Up-to-date
- Flexibel
- Duur

@intidc

1000 security experts

- Skilled x 1000 👍
- Creatief x 1000 👍
- Up-to-date x 1000 👍
- Flexibel x 1000 👍
- Duur x 1000 👎

@intidc

De oplossing:

Crowdsourced Security & Bug Bounties

Bug bounty basics

Hey Facebook, ik kan jou hacken!

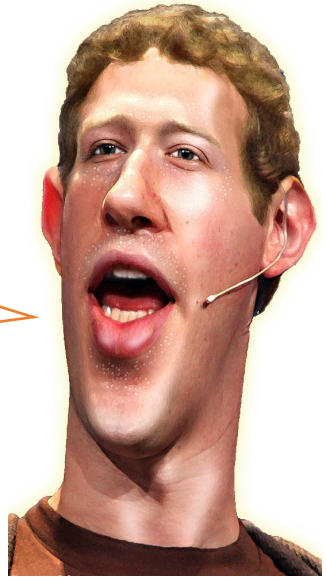
Cool! Hoe?
Nog aan niemand vertellen he!

@intidc

Bug bounty basics

{technische praat}

Dat meen je niet!
We fixen dat en hier is
$2000

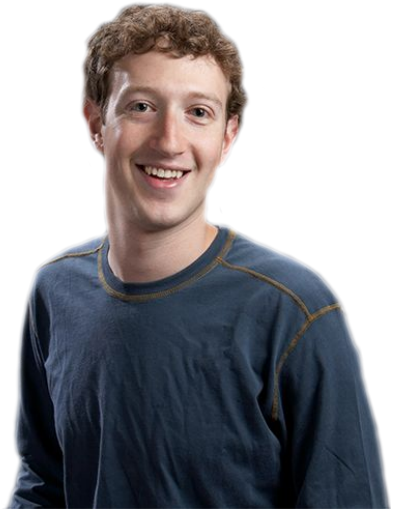


@intidc

Bug bounty basics

✓

win!



✓

win!

@intidc

voordelen

- **Prijs**: no cure, no pay
- **Frequentie**: 24/7, nieuwe features
- **Hoeveelheid**: elke dag nieuwe, verse ogen
- **Diversiteit**: nieuwe perspectieven

Excuses

excuus #1

“wij hebben daar de tijd en infrastructuur niet voor”

bug bounty platforms

@intidc

bug bounty platforms

- Bug bounty as a service (BBaaS)
- Betrouwbare hackers
- Vlotte betalingen
- Veilige ontmoetingsplaats

excuus #2

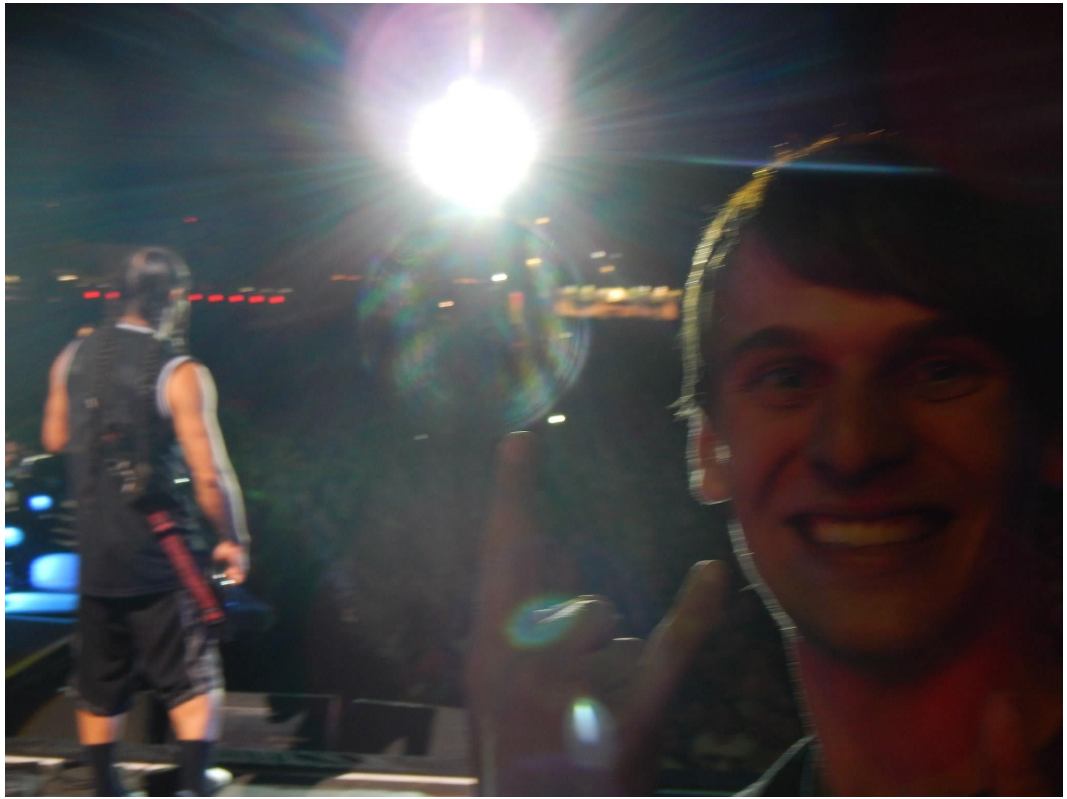
“wij hebben daar het budget niet voor”

It’s not all about the $$$

- Reputatie punten
- Hall of Fame
- T-Shirts
- Airmiles, Beltegoed, Kadobonnen...

Metallica

Metallica



@intidc

controle over je budget

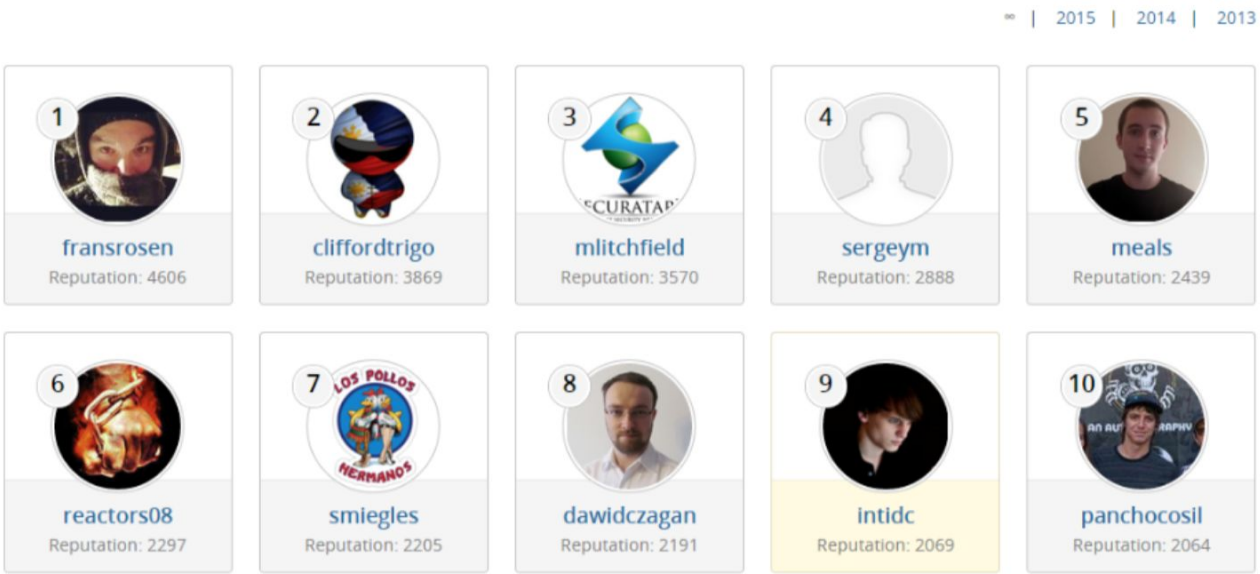
- Bepaal zélf je minimum en maximum
- Werk met een gelimiteerd budget
- Werk met een bounty pool

excuus #3

“we kunnen niet zomaar hackers vertrouwen”

@intidc

gekend & betrouwbaar



@intidc

excuus #4

“We zijn daar
niet klaar voor.”

schaalbaarheid

- Kies een scope
  - bvb: enkel staging.bedrijf.be
- Zoek naar specifieke kwetsbaarheden
  - bvb: enkel customer data leaks
  - bvb: geen phishing
- Limiteer aantal hackers

excuus #5

“Dat is slecht voor onze PR en team legal gaat flippen.”

Als zij het kunnen...

Google

Microsoft

Dropbox

SnapChat

YAHOO!

facebook

UBER

Pornhub

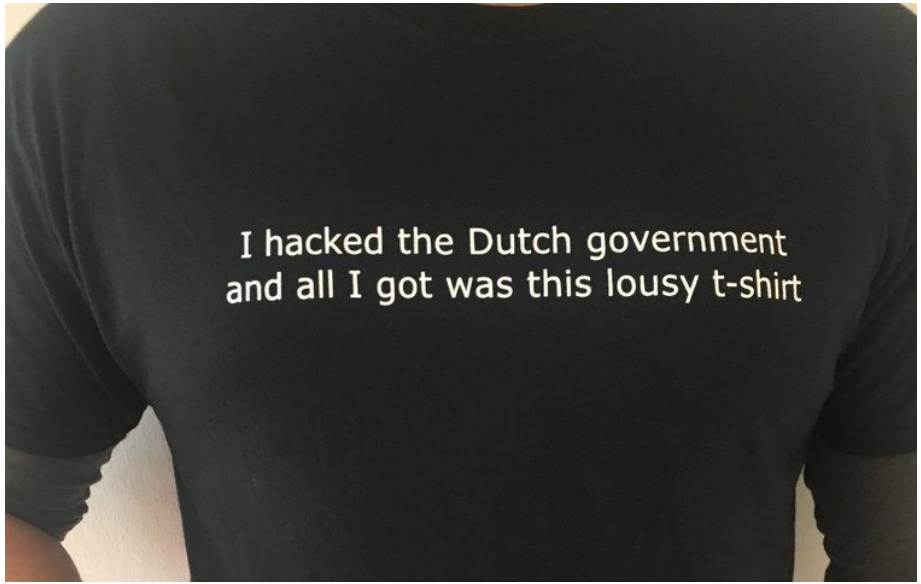
@intidc

The GitHub Blog

Four years of the GitHub Security Bug Bounty

Mar 14, 2018 gregose Engineering

Last month GitHub celebrated the fourth year of our Security Bug Bounty program. As we've done in the past, we're sharing some details and highlights from 2017 and looking ahead to where we see the program going in 2018.



Patrick
@pathetiq

Follow

Best #BugBounty t-shirt! Thanks @Pornhub!

@intidc

Ja, maar in België...

Euh:

@intidc

Ja, maar in België...

En zelfs...

GAMMA

@intidc

Nog excuses?

Dan ontkracht ik ze nu graag!

tijd voor

TIPS

@intidc

tip #1

“communicatie
is alles.”

communicatie

- Wees transparant
- Wees duidelijk
- Ga in dialoog
- Neem elk rapport serieus

https://www.facebook.com/zuck
Mark Zuckerberg
Mark Zuckerberg
Timeline
About

tip #2

“heb vertrouwen.”

vertrouwen

- Bouw zakelijke relaties op
- Help je hackers
- Bescherm je researchers

DRONE WRECK —

Man gets threats—not bug bounty—after finding DJI customer data in public view

A bug bounty hunter shared evidence; DJI called him a hacker and threatened with CFAA.

SEAN GALLAGHER - 11/17/2017, 7:30 PM

Enlarge / A security researcher says he was trying to play fair with DJI's bug bounty program. DJI calls him a hacker who exposed

http://www.digitalmunition.com/WhyIWalkedFrom3k.pdf

@intidc

safe harbor policy

slecht:

Rules

We want to close all security issues, but we urge researchers and testers to stick to the scope and rules as defined here. There are many reasons for this. The primary reason is the safety of our customers. Second, we want to make you, as a researcher, aware that there are laws you must not break. Finally, it's required to be eligible for our hall or fame or any reward.

Before attempting anything please be aware that, testing our environment can be designated as a criminal act by the relevant authorities, if you are violating German law or any other law. Our rules do not supersede any applicable laws.

@intidc

safe harbor policy

goed:

Consequences of Complying with This Policy

We will not pursue civil action or initiate a complaint to law enforcement for accidental, good faith violations of this policy. We consider activities conducted consistent with this policy to constitute "authorized" conduct under the Computer Fraud and Abuse Act. To the extent your activities are inconsistent with certain restrictions in our Acceptable Use Policy, we waive those restrictions for the limited purpose of permitting security research under this policy. We will not bring a DMCA claim against you for circumventing the technological measures we have used to protect the applications in scope.

If legal action is initiated by a third party against you and you have complied with Dropbox's bug bounty policy, Dropbox will take steps to make it known that your actions were conducted in compliance with this policy.

Please submit a HackerOne report to us before engaging in conduct that may be inconsistent with or unaddressed by this policy.

@intidc

tip #3

“groei mee.”

groei

- Start met een privéprogramma
- Kies voor een kleine maar interessante scope
- Evalueer
- Vraag om hulp indien nodig

dat wast.

nog vragen?