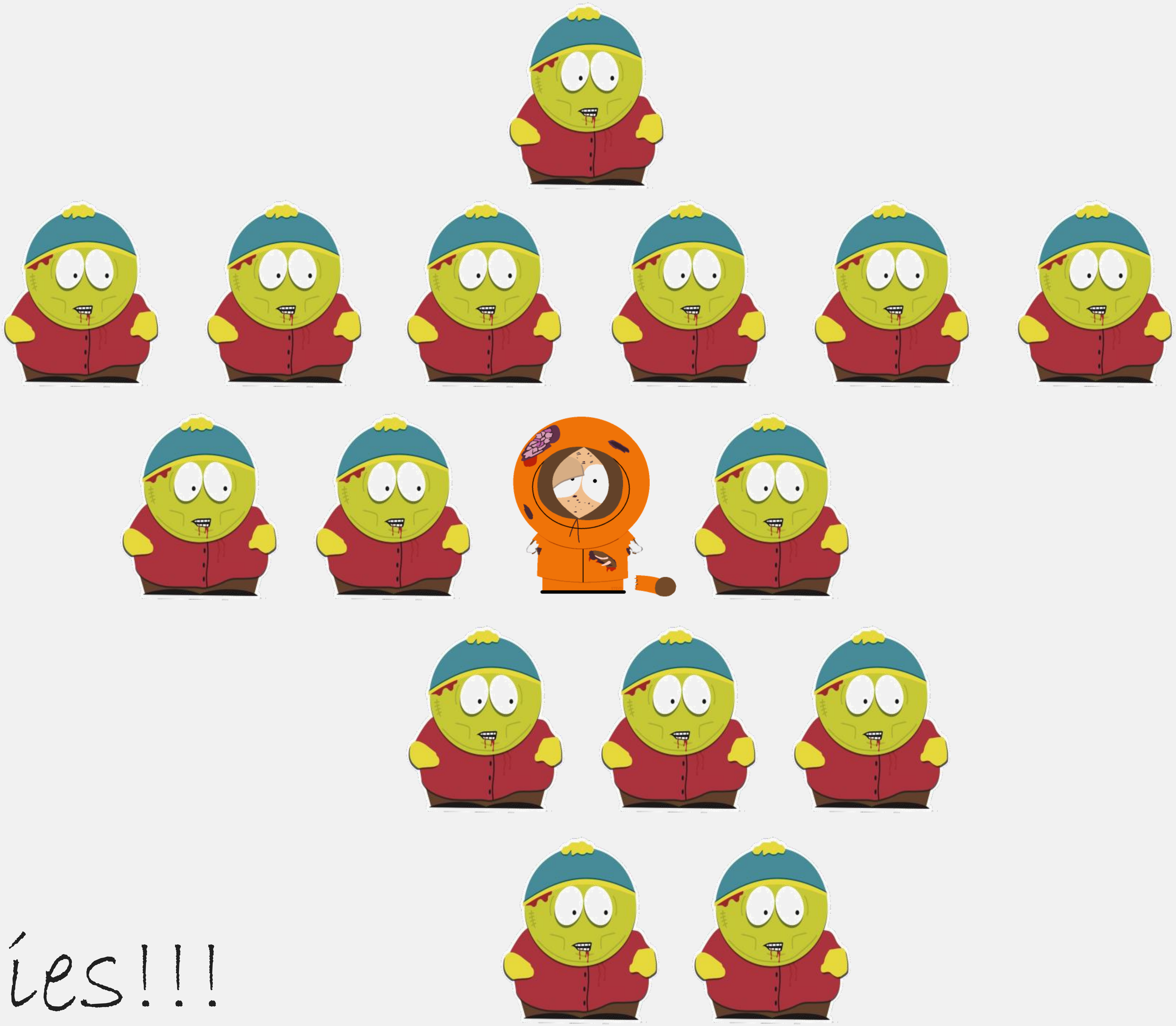
Bug Bounty Programs Evolution

Nir Valtman, CISSP
Blog: www.valtman.org
Twitter: @ValtmaNir

NCR



Zombies!!!

Defacement

AntiDef

Secure TDD

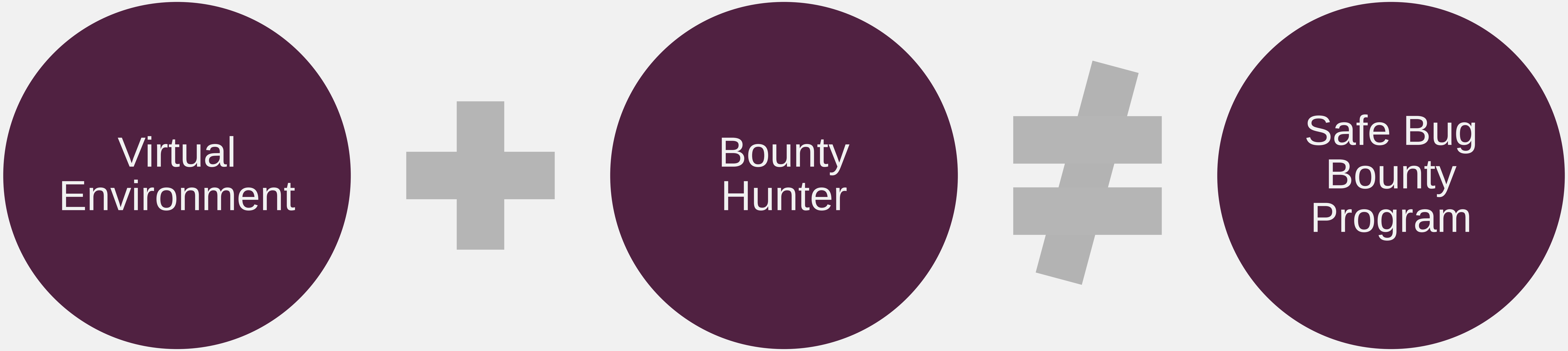
Memory Scraper

Research Bug Bounty Programs Since 2011

Academy
Final Project

If you can’t beat them, join them!

Not cost-effective



Virtual Environment + Bounty Hunter ≠ Safe Bug Bounty Program

Shay Fainberg

crowdome

safe crowd security testing

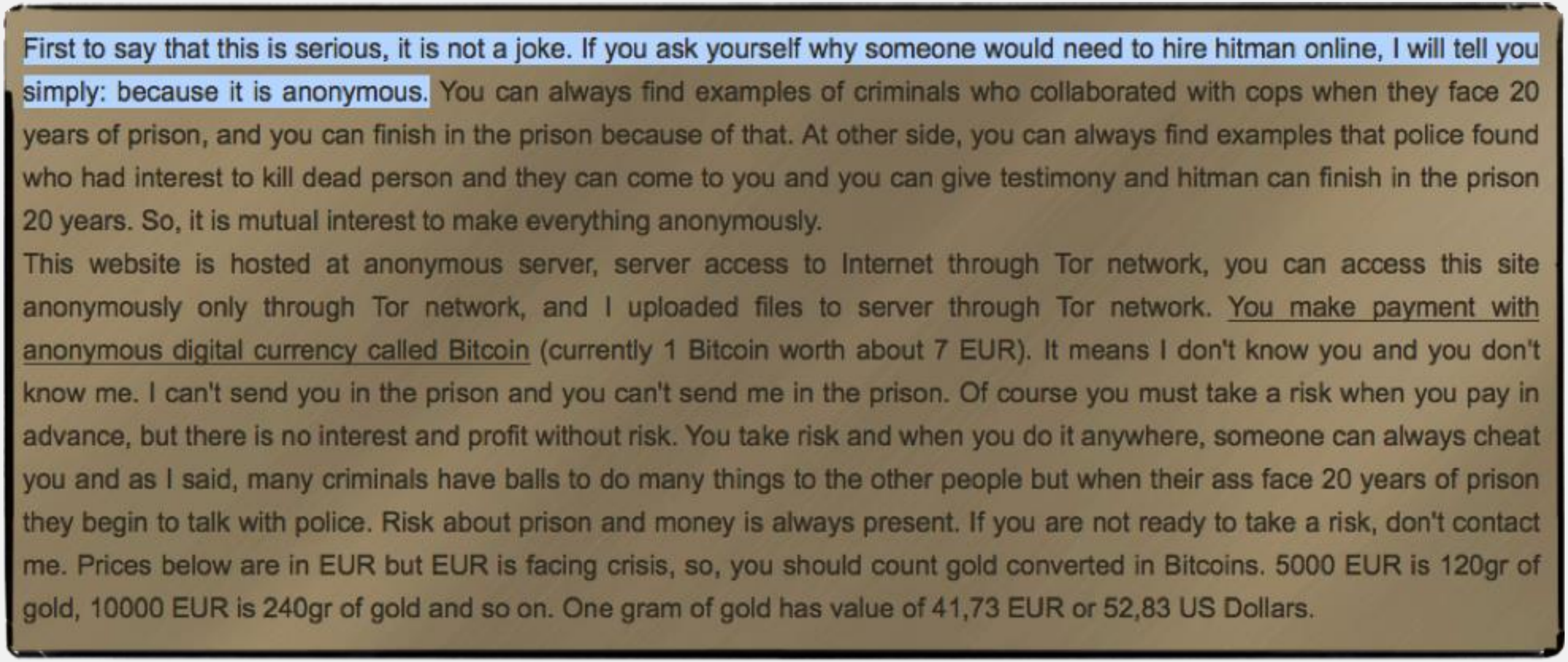
CLOSED

Ideas worth spreading

The Evolution

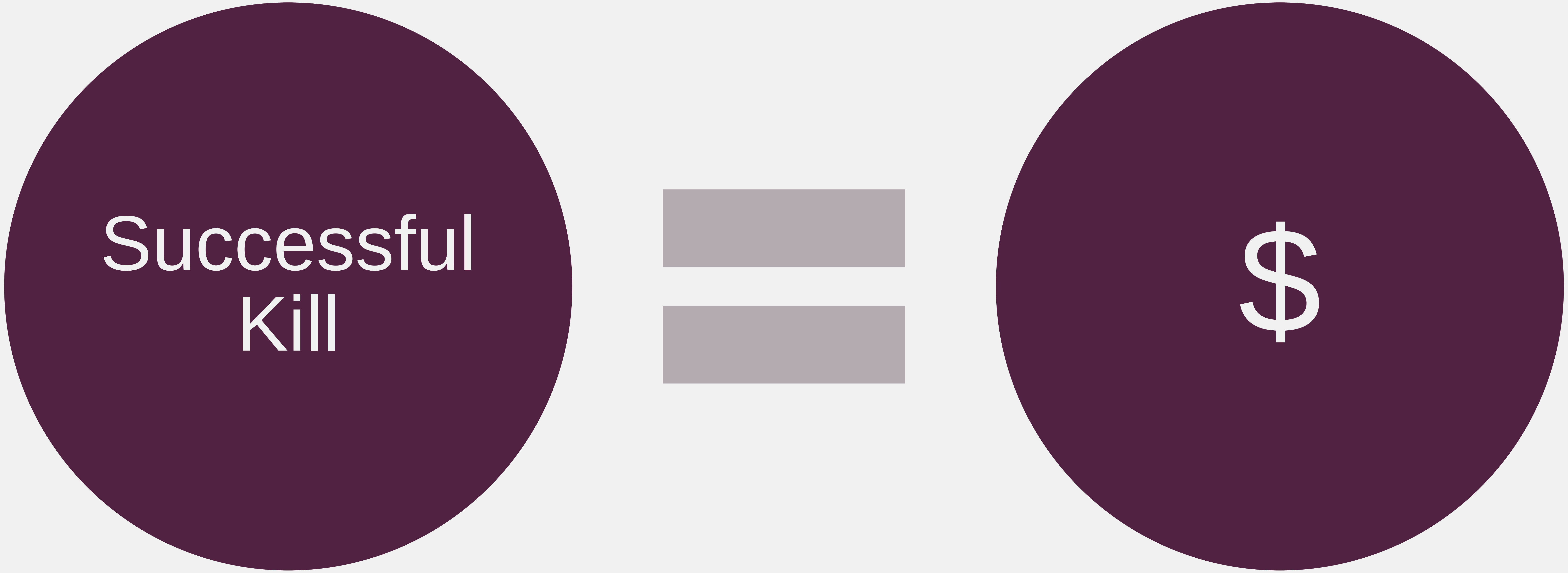
Bounty Hunters in Real Life

Terms & Conditions



First to say that this is serious, it is not a joke. If you ask yourself why someone would need to hire hitman online, I will tell you simply: because it is anonymous. You can always find examples of criminals who collaborated with cops when they face 20 years of prison, and you can finish in the prison because of that. At other side, you can always find examples that police found who had interest to kill dead person and they can come to you and you can give testimony and hitman can finish in the prison 20 years. So, it is mutual interest to make everything anonymously.

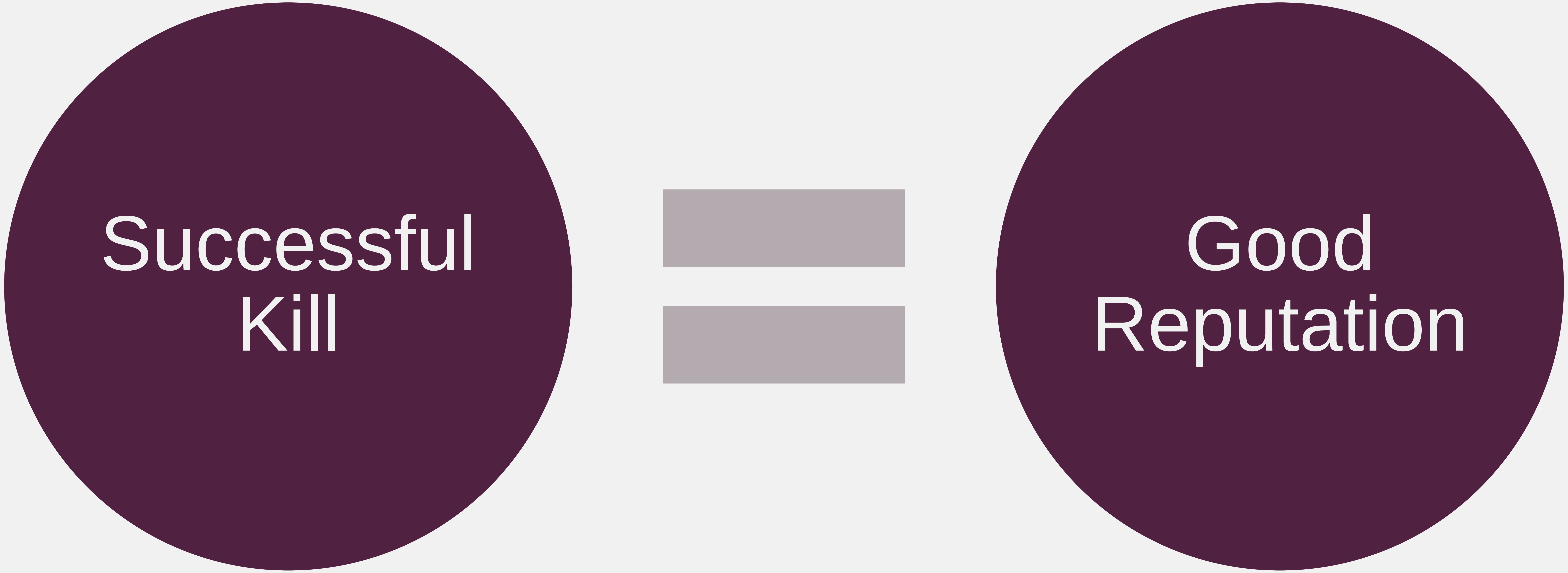
This website is hosted at anonymous server, server access to Internet through Tor network, you can access this site anonymously only through Tor network, and I uploaded files to server through Tor network. You make payment with anonymous digital currency called Bitcoin (currently 1 Bitcoin worth about 7 EUR). It means I don't know you and you don't know me. I can't send you in the prison and you can't send me in the prison. Of course you must take a risk when you pay in advance, but there is no interest and profit without risk. You take risk and when you do it anywhere, someone can always cheat you and as I said, many criminals have balls to do many things to the other people but when their ass face 20 years of prison they begin to talk with police. Risk about prison and money is always present. If you are not ready to take a risk, don't contact me. Prices below are in EUR but EUR is facing crisis, so, you should count gold converted in Bitcoins. 5000 EUR is 120gr of gold, 10000 EUR is 240gr of gold and so on. One gram of gold has value of 41,73 EUR or 52,83 US Dollars.



Successful Kill

=

$



Successful Kill

=

Good Reputation

Targets

Animals

VIP

Women

Politicians

Men

Kids

Hit men

1995

N
Netscape®
TM

1st Bug Bounty Program

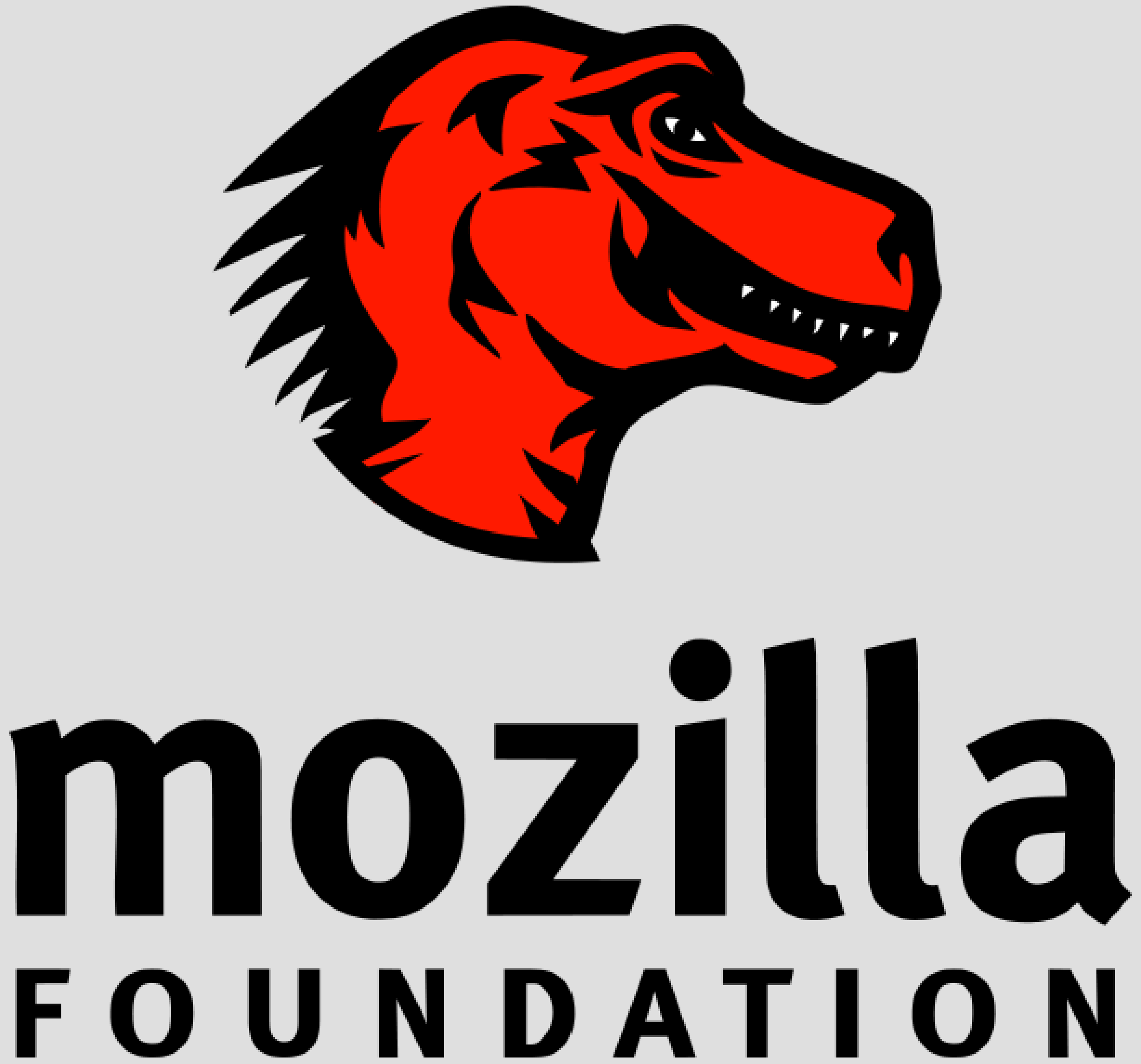
“…REFINE BETA VERSIONS AND ENSURE HIGHEST QUALITY SOFTWARE”

How did it work?

Winners Awards

Success || Failure Story?

2004



APR
24
2014

$10,000 Security Bug Bounty for Certificate Verification

Daniel Veditz

2

Firefox developer builds ("Nightly") are now using a new certificate verification library we've been working on for some time, and this code is on track to be released as part of Firefox 31 in July. As we've all been painfully reminded recently (Heartbleed, #gotofail) correct code in TLS libraries is crucial in today's Internet and we want to make sure this code is rock solid before it ships to millions of Firefox users. To that end we're excited to launch a special Security Bug Bounty program that will pay $10,000 for critical security flaws found and reported in this new code before the end of June.

Perspectives on Bug Bounty Programs

Business

Bounty Hunter

Start Your Own Online Program

- Technology
- Operations
- Legal

Start Your Own Online Program

Technology

Handle heavy traffic

Start Your Own Online Program

Technology

Stronger IPS

Start Your Own Online Program

Technology

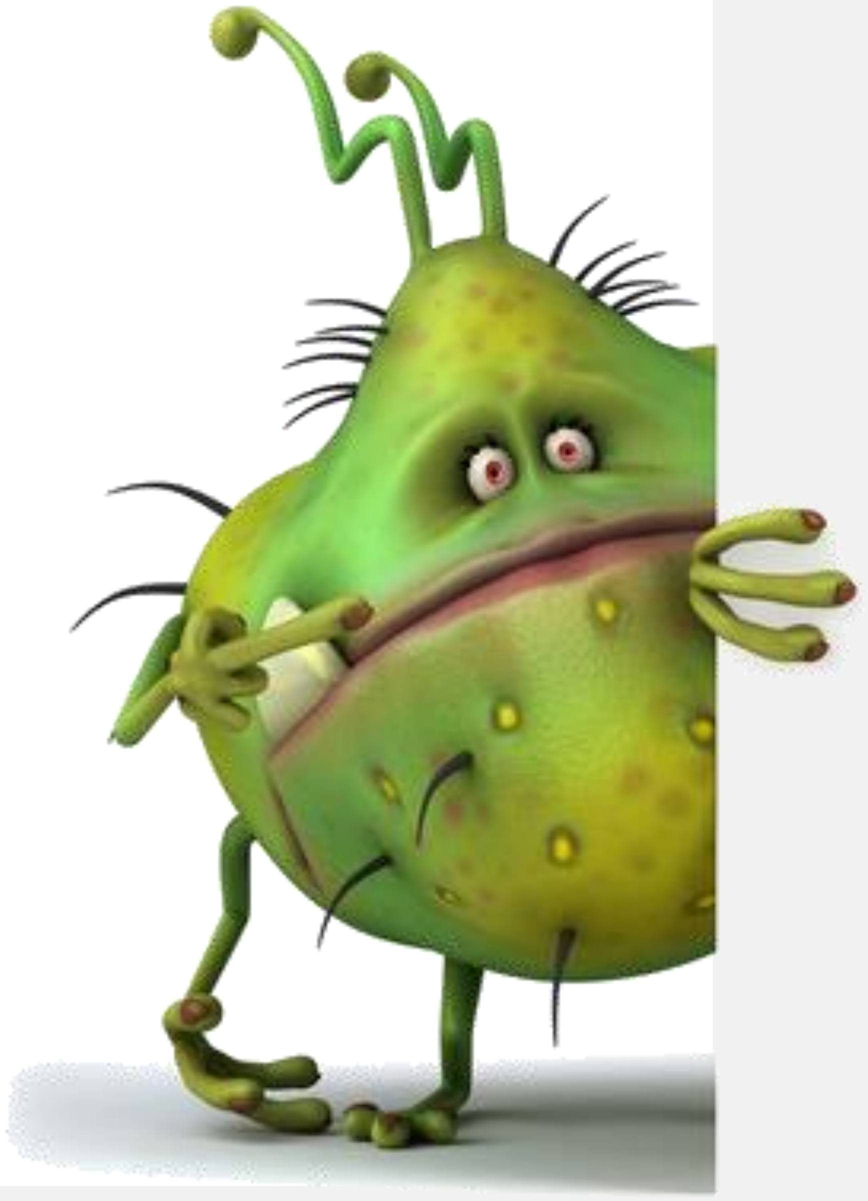
Stronger WAF

Start Your Own Online Program

Incident Response

Operations

Bugs Management



Start Your Own Online Program

Liability

Legal

AT&T Bug Bounty Program

Magento™
Open Source eCommerce

ebay

Google™

BarracudaLabs

f

GitHub

Self-Owned

Microsoft

Dropbox

in

avast!®
be free

redhat

Synack

Bugs4Bounty

HackaServer

HatForce

External

Bugwolf

h1

uTest®

bugcrowd™

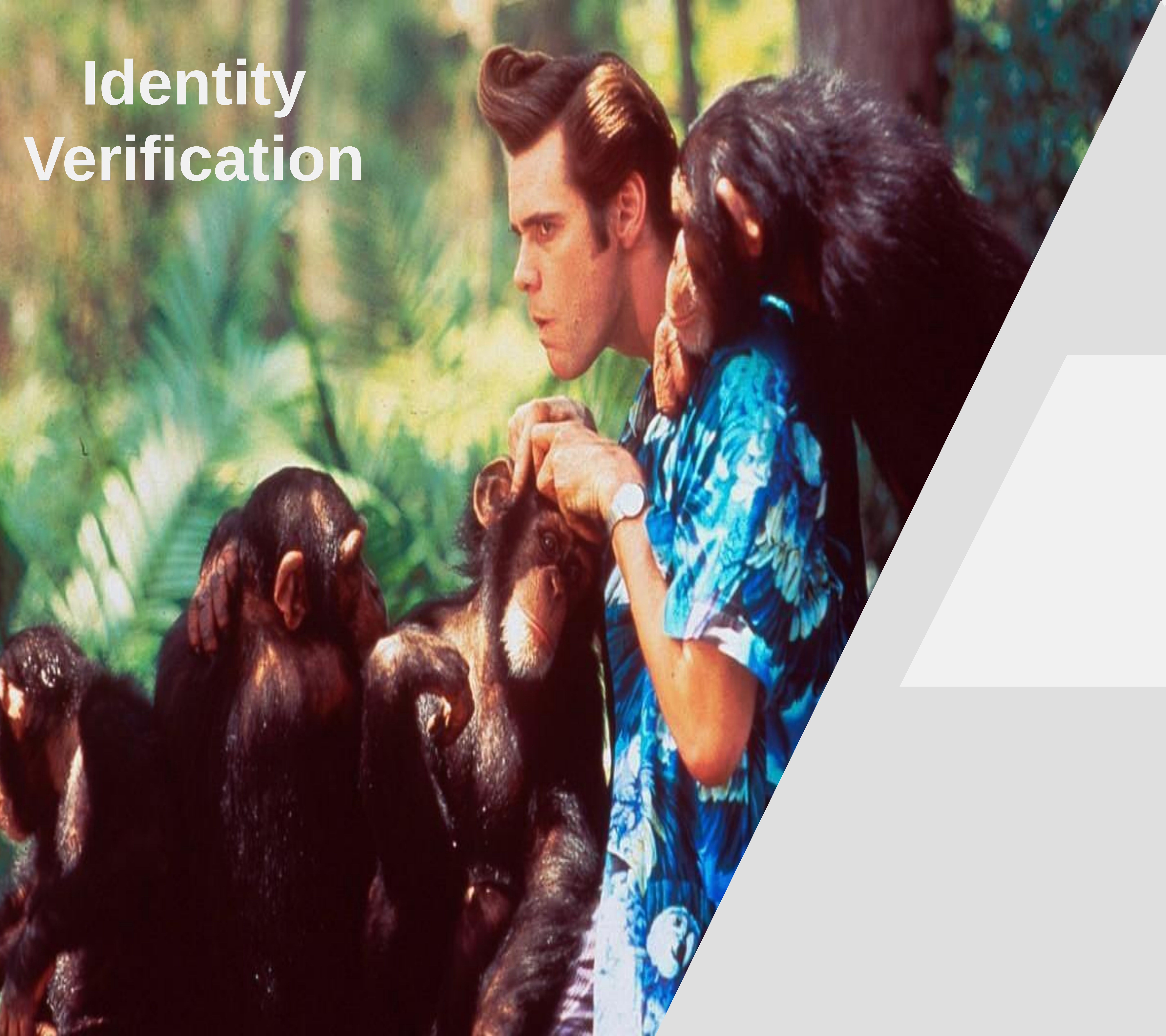
CrowdCurity
www.crowdcurity.com

CrowdSecurify
Private Bug Bounty Programs

A-TEAM

External

Identity Verification



External

External

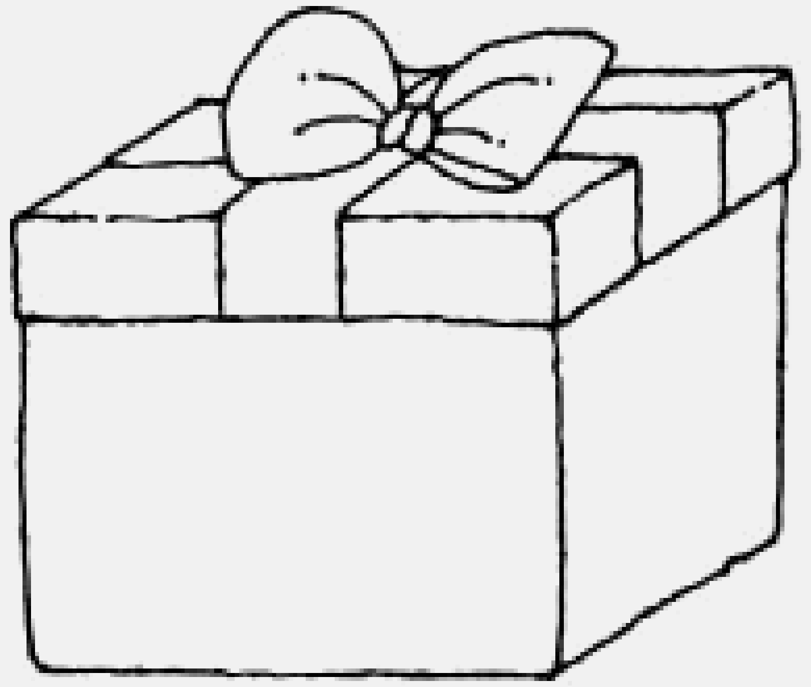
Traffic Shaping

External

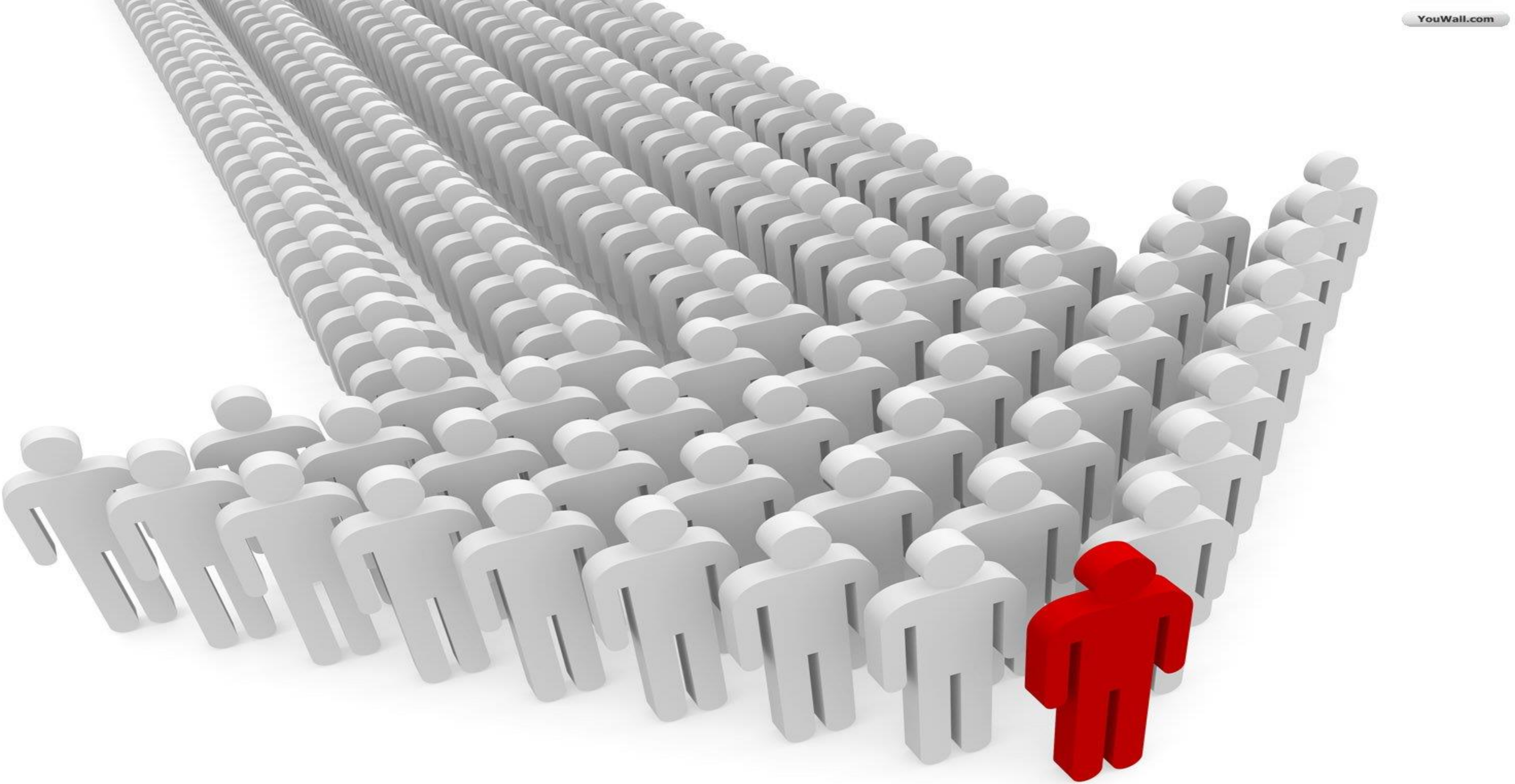
Benefits

Concerns

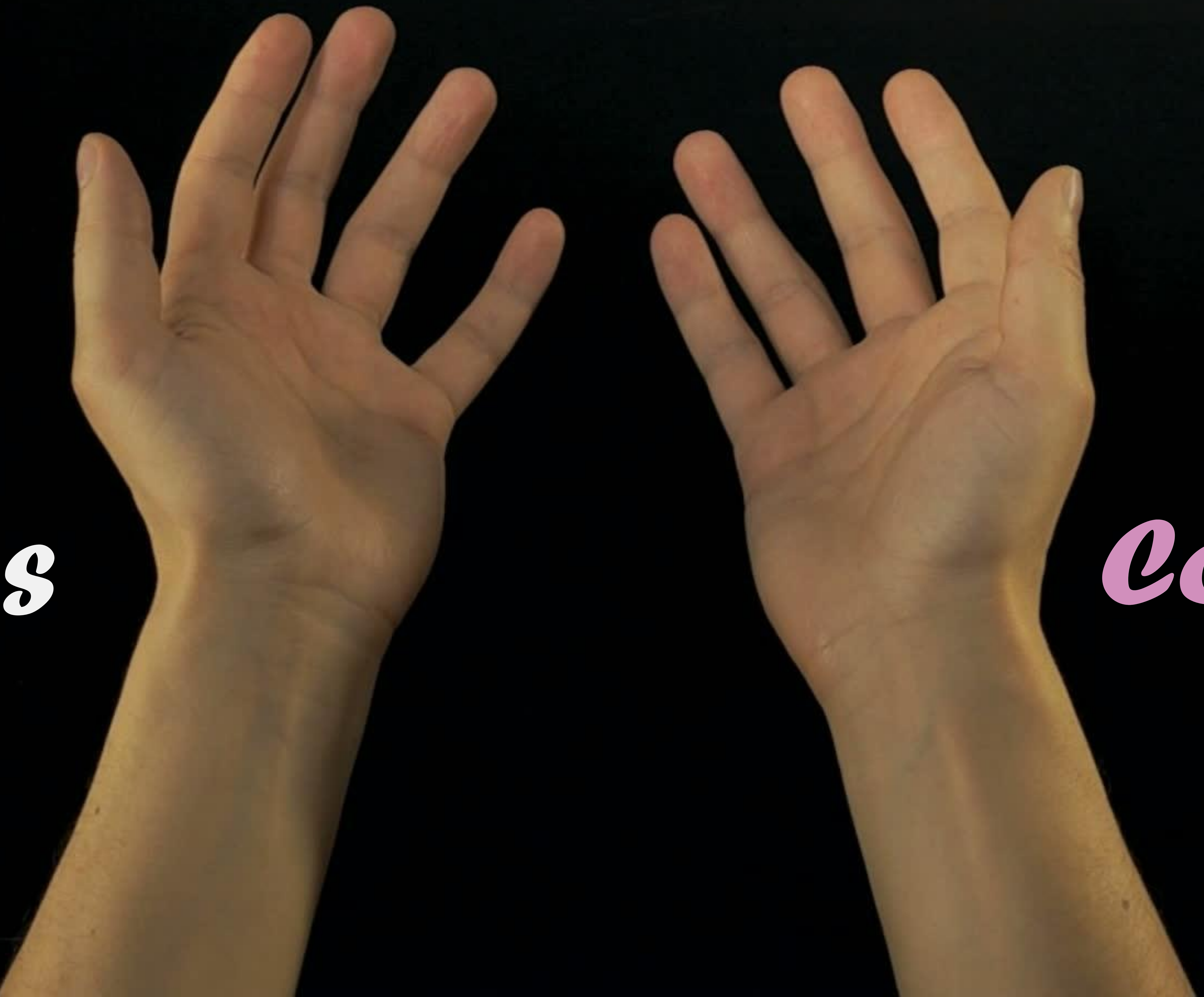
Payment Models



Real-World Hacking Scenario



Security Leader Positioning



Benefits

Concerns

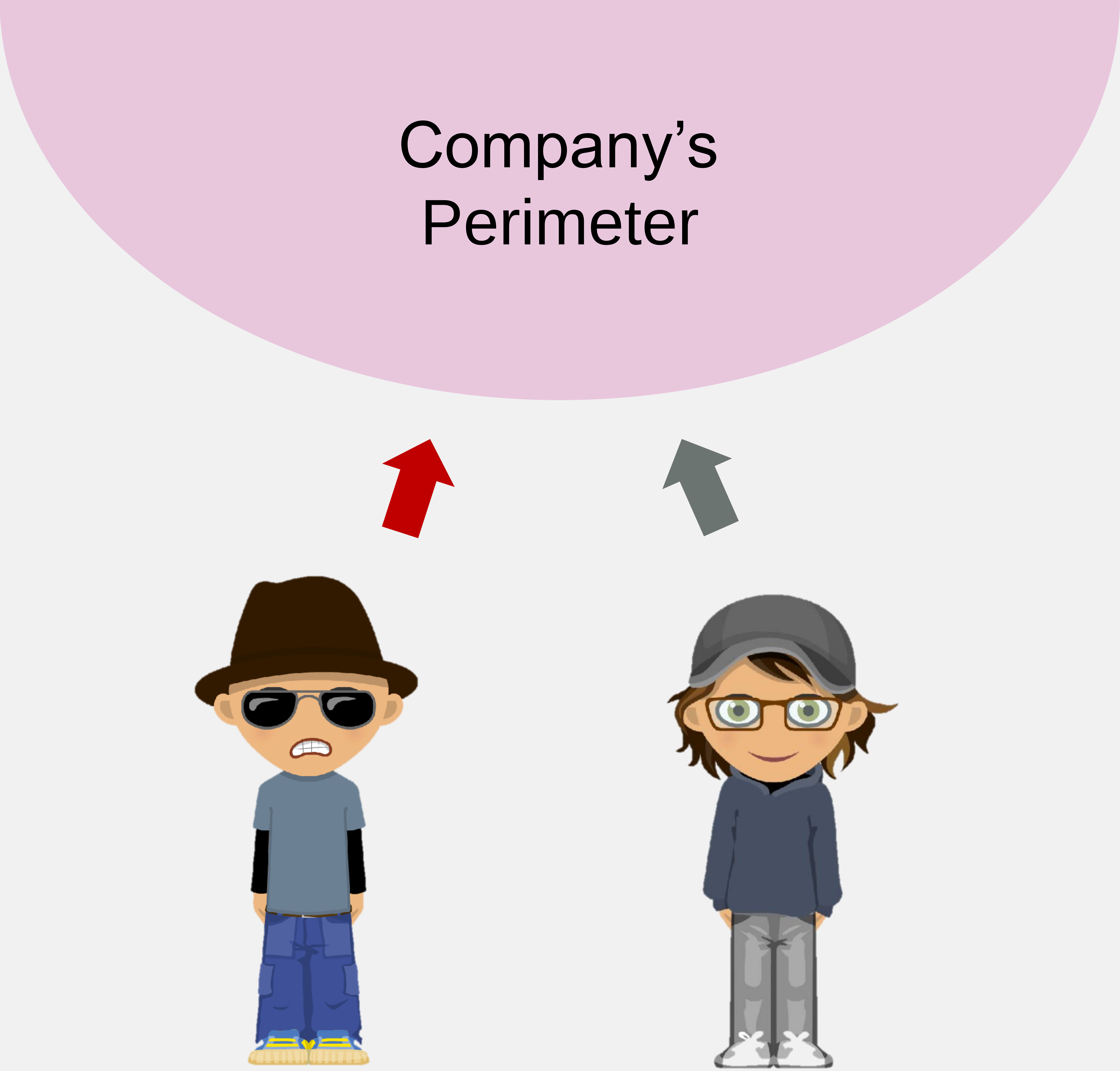
Test

Production

Sensitive Data Leakage

Denial of Service

Black Hats Detection



Company’s Perimeter

Facebook - Delete The Admin Of Any Page Exploit

1337day-2013-21699

[Important Info]

Verified	✓ Verified
Warnings	✓ 0
Rating	👎 ✓ 2 👍

[Price]

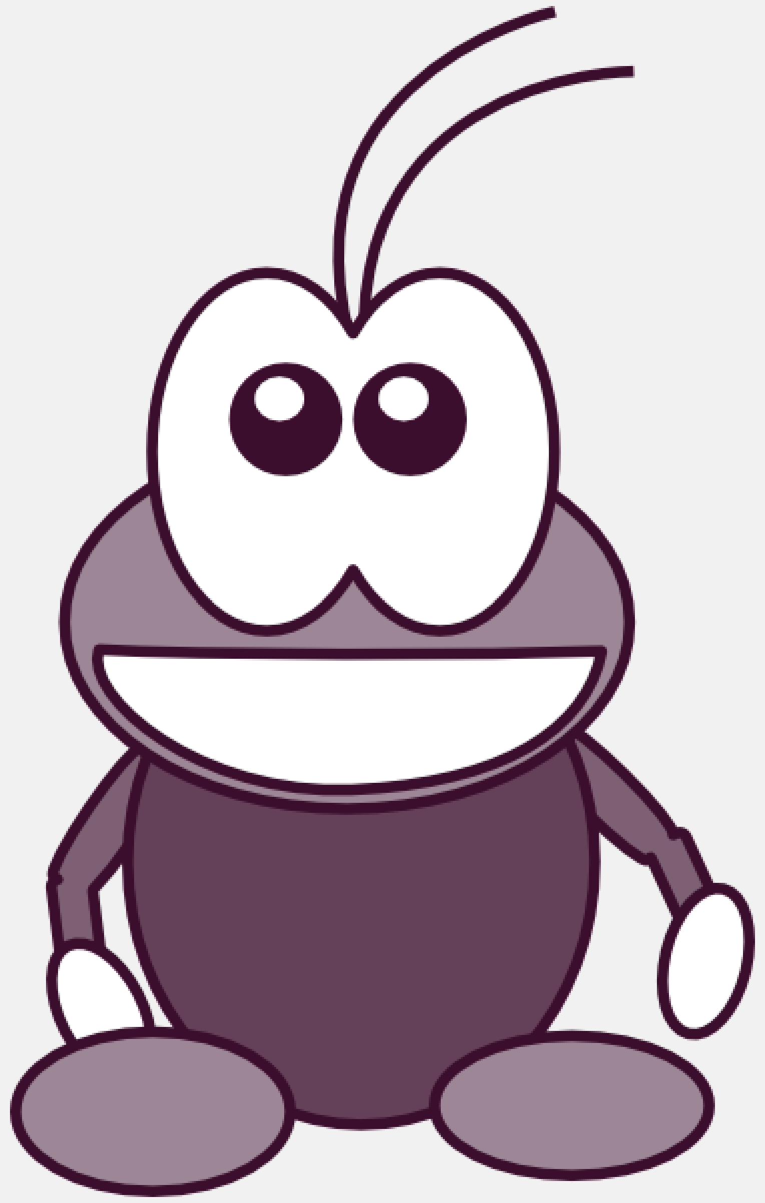
5000 Gold

[F.A.Q.]

- How to open Exploit?
- How to buy Exploit?
- How to get Gold?
- How to get more purchasers?
- How to know that it is works?

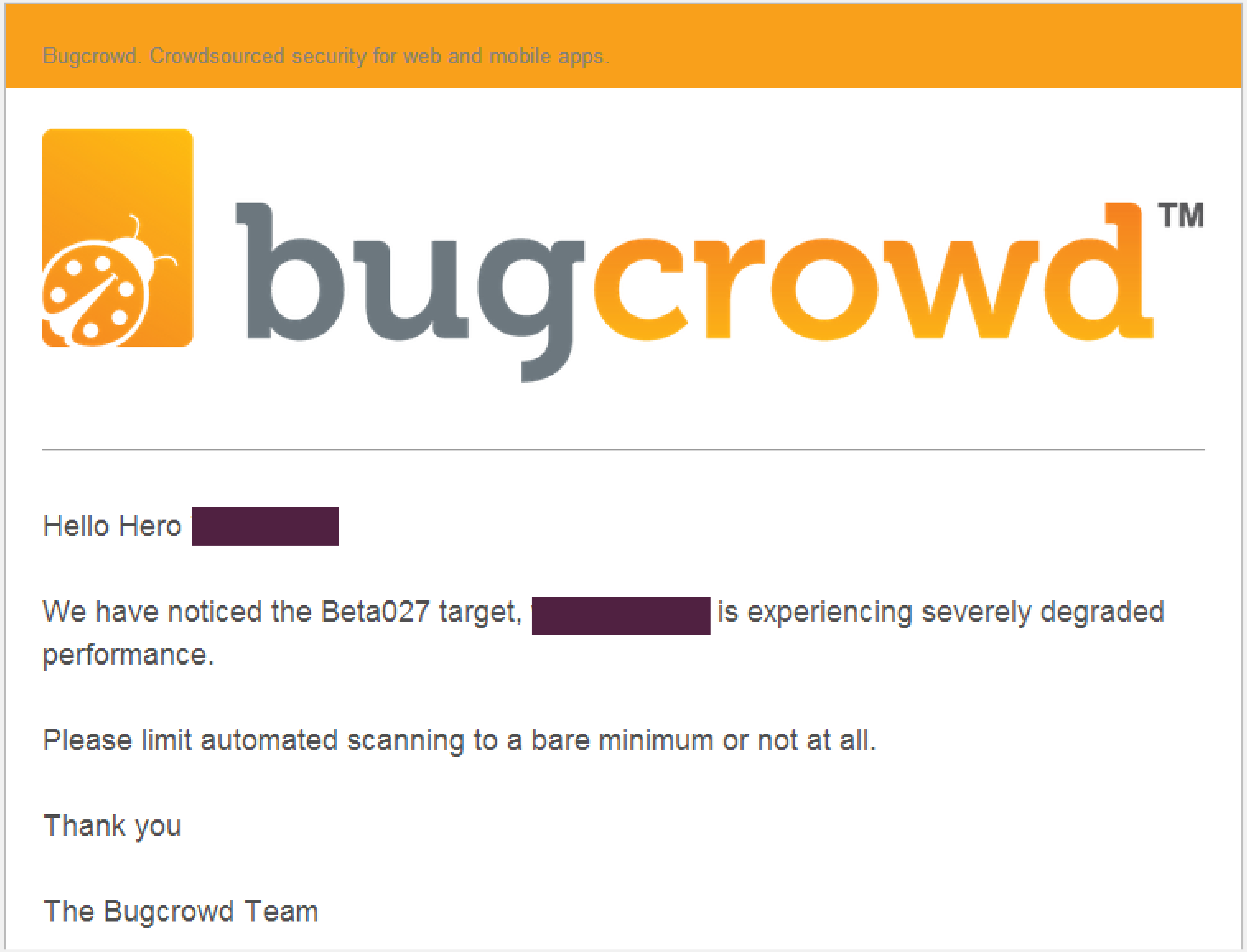
[Detailed Information]

Full title	Facebook - Delete The Admin Of Any Page Exploit
Date add	2013-12-23
Category	web applications
Platform	tricks
Risk	🟩🟩🟨🟧🟥
Description	It is possible to delete the admin of any page just with a single click.This can also be converted into a bot or a worm leading to the deletion of admin of thousands of pages. It is also possible to fully automate this worm.It is very effective when we aim for wide sp attack.Targeted attacks are also possible.This bug is not available public.This bug is tested against hundred's for pages and is found working 100%.
Usage info	I have automated all the process.Buy it and i will send it.very simple to use.
Tested on	Main Website Of Facebook
Solution	Not Yet Fixed By The Facebook Security Team
Tags	Facebook zero Dec 2013 Deletion of admin of any page UNPATCHED.
Comments	17
Views	37958



Non-security Bugs Handling

Side Effects



Bugcrowd. Crowdsourced security for web and mobile apps.

Hello Hero [redacted]

We have noticed the Beta027 target, [redacted] is experiencing severely degraded performance.

Please limit automated scanning to a bare minimum or not at all.

Thank you

The Bugcrowd Team

Minimize Exposure Time

Perspectives on Bug Bounty Programs

Business

Bounty Hunter

Experienced Researchers

Motivation

DEPTH
GAUGE
90 ft
CARL BARKS
© WALT DISNEY PRODUCTIONS

Frustration

Publications x
Sent Messages x
to me

Denial of service [redacted]

Nir Valtman 9/24/13

Hello, We would like to report about a denial of service exploit on mobile ap...

product-security@[redacted].com 9/26/13

Please include the line below in follow-up emails for this request. Follow-up...

Nir Valtman 10/7/13

Follow-up: [redacted] Hello, Have you managed to fix this exploit? Thanks, Nir

product-security@[redacted].com <product-security@[redacted].com> 10/9/13

Please include the line below in follow-up emails for this request.

Follow-up: [redacted]

Hello Nir,

In order to help us reproduce and investigate this issue, we will need some additional details. Can you please send us a the [redacted].

Best regards,
Brandon
[redacted] Product Security

Security Researchers for PayPal's Bug Bounty Program - PayPal - Mozilla Firefox
File Edit View History Bookmarks Tools Help
PayPal, Inc. (US)
https://www.paypal.com/us/webapps/mpp/security-tools/reporting-security-issues
Google
Most Visited
Getting Started
Latest Headlines
Security Researchers for PayPal's Bu...

Changes to Program Terms

The Bug Bounty Program is subject to change or cancellation by PayPal at any time, without notice. As such, PayPal may amend these Program Terms at any time by posting a revised version on our website. By continuing to participate in the Bug Bounty Program after PayPal posts any such changes, you accept the Program Terms, as modified.

Changes to Program Terms

The Bug Bounty Program is subject to change or cancellation by PayPal at any time, without notice.
posting a revised version on our website. By continuing to participate in the Bug Bounty Program af
as modified.

- What types of bugs are commonly rejected?
- What should I be aware of when testing?

eBay Inc. Terms and Conditions

Magento Bug Bounty Scope Information

Submit a Bug to PayPal or Magento

Case Study

Name: Oren Hafif

Source: www.orenh.com

Actual Risk

Exposing all hosted email addresses in Google

1st Response	DENIED!
2nd Response	$500 Reward

YAHOO! NEWS

FASHION TIMES

WIRED

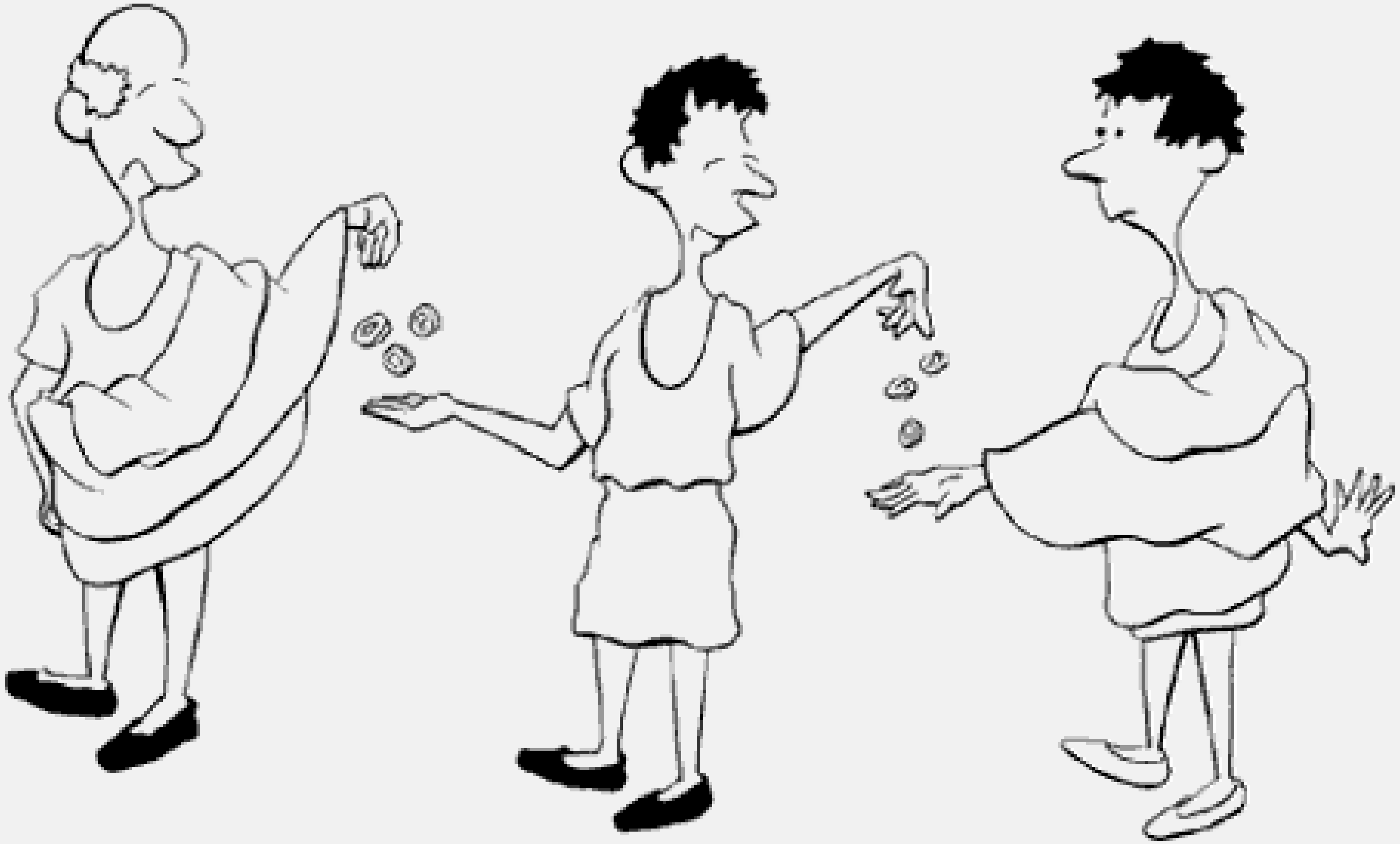
reddit

PogoWasRight.org
Privacy News from Around the World

INTERNATIONAL BUSINESS TIMES

Next Generation Bug Bounty Programs

Minimize Production Risks

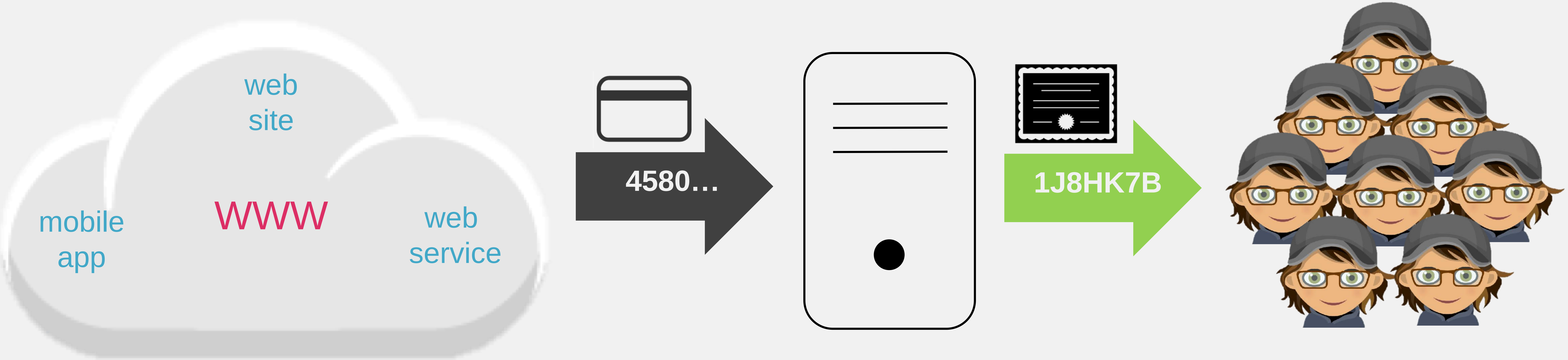


Minimize Production Risks

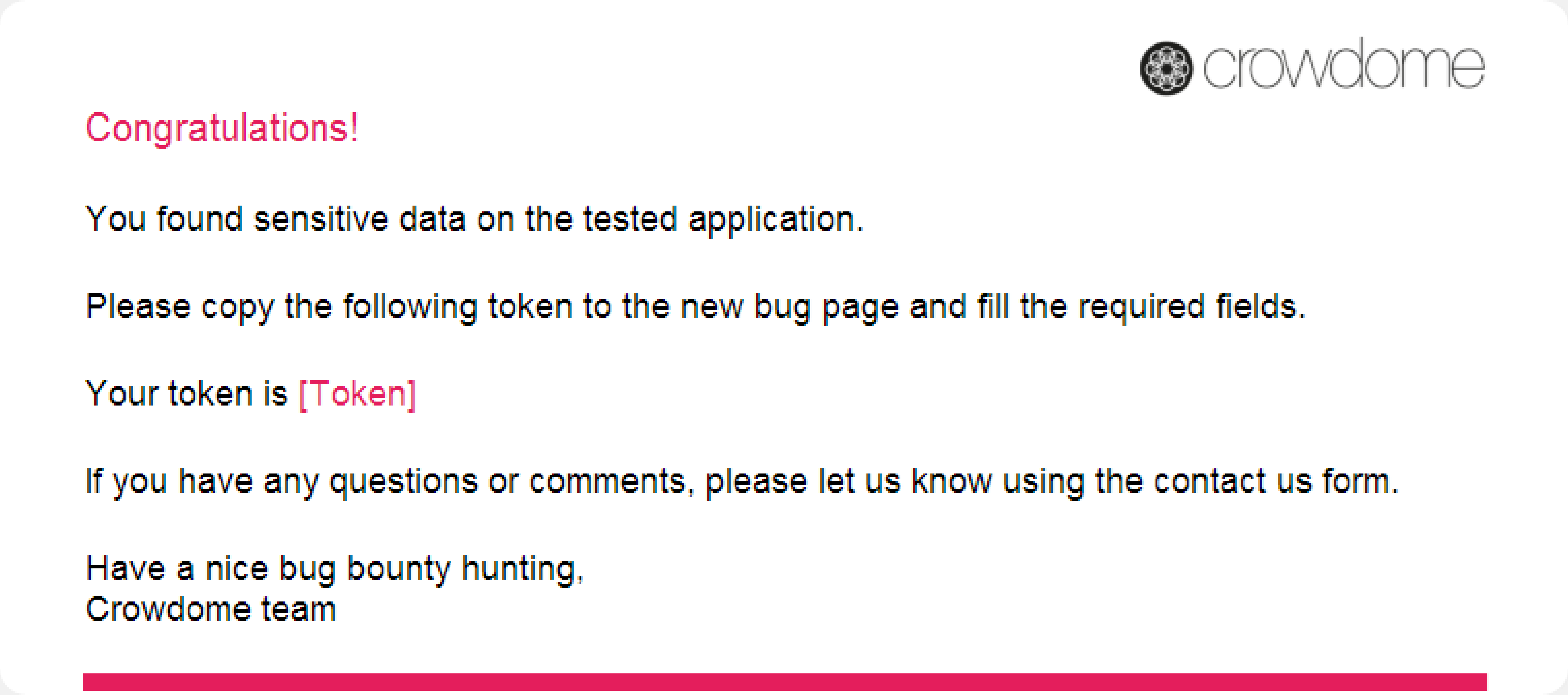
Allow Penetration Tests

Prevent Malicious Exploitation

Minimize Production Risks



Minimize Production Risks



crowdome

Congratulations!

You found sensitive data on the tested application.

Please copy the following token to the new bug page and fill the required fields.

Your token is [Token]

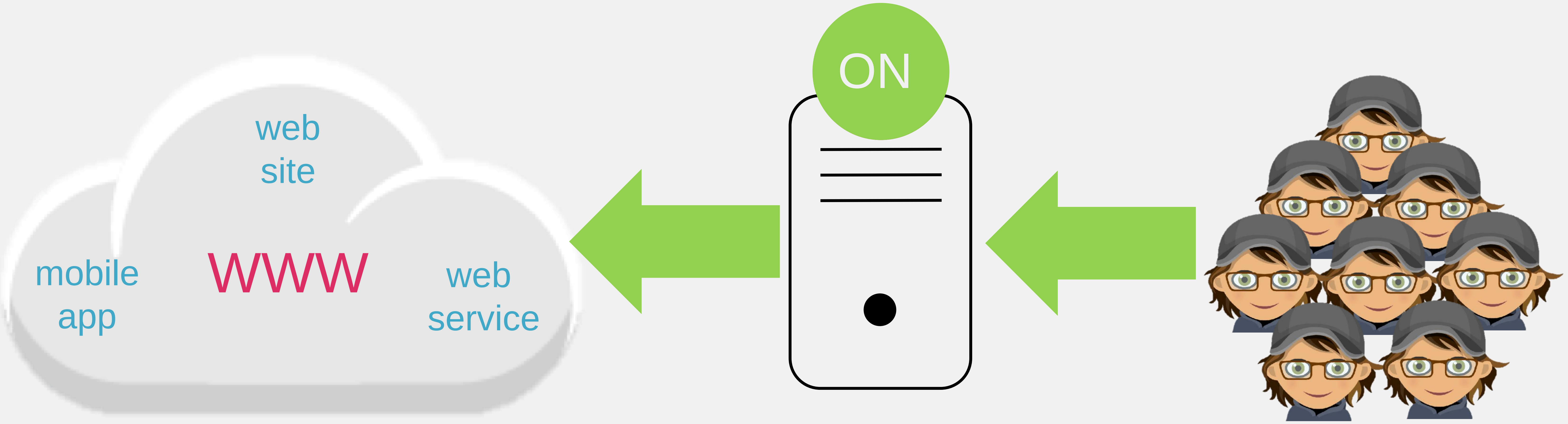
If you have any questions or comments, please let us know using the contact us form.

Have a nice bug bounty hunting,
Crowdome team

Minimize Production Risks

Minimize Production Risks

Minimize Production Risks



Minimize Production Risks

HOW TO IDENTIFY BLACK HAT HACKERS?

LEGITIMATE SQL INJECTION

```
‘ or ‘a’<‘b’;#
SELECT 0x457578
```

MALICIOUS SQL INJECTION

```
DROP myTable;#
DR/**/OP/*bypassing filter*/myTable;#
SELECT LOAD_FILE(0x633A5C626F6F742E696E69)
```

HOW TO BAN THEM?

BIFURCATION
ISLAND
CORE
THE DELTA
IS WHERE
RIDGES
RIDG

Business Analysts

Attorneys

ATTRACT NEW TESTER TYPES

SME

Quality Assurance

Developers

A LONG JOURNEY IN FRONT OF US

Thank You

Nir Valtman, CISSP
Blog: www.valtman.org
Twitter: @ValtmaNir