Hacking the 0day Market

CROWDFENSE

VULNERABILITY RESEARCH HUB

#WhoAmI -- Andrea Zapparoli Manzoni

- Director of Crowdfense Limited
- Most recently, Head of Cyber Security for KPMG
- Working in the ICT security field since the XX century ☺
- Member of the National Security Observatory (Italy) --> contributed to write Italy's "National Cyber Strategy"
- Author of many cyber-security guidelines and best practices:
  - Italy's "Cybersecurity Framework"
  - ENISA's "Cybersecurity and Resilience for Smart Hospitals"
  - ….

The 0day Market Today

Historically, it’s unsafe, chaotic and inefficient from a business pov.

This hampers the (now strategic) ability of law enforcement and intelligence agencies to fight crime / terrorism / hostile geopolitical actors in the cyber domain.

Researchers are often underpaid for their exponentially complicated efforts.

There is a talent vacuum as underpaid researchers seek more lucrative fields / do research as a second job.

The 0day Market Today

To combat the inefficiencies in the current market, we need to “normalize” and streamline this business:

- Protect and pay researchers more
- Reduce unnecessary middle men
- Dedicate more economic resources
- Develop and adopt best practices

Come on… It’s not 2003 anymore.

Hacking the 0day Market

Step #1: Launched the largest Public Bug Bounty Program in History

Seeking single exploits and full / partial exploit chains to support our customers in their targeted information gathering activities (LE and Intel).

Highest payouts in our industry.

Step #2: Launched the Vulnerability Research Hub

An innovative web-based collaboration platform that allows vulnerability researchers to safely submit, discuss and quickly sell single 0day exploits and chains of exploits.

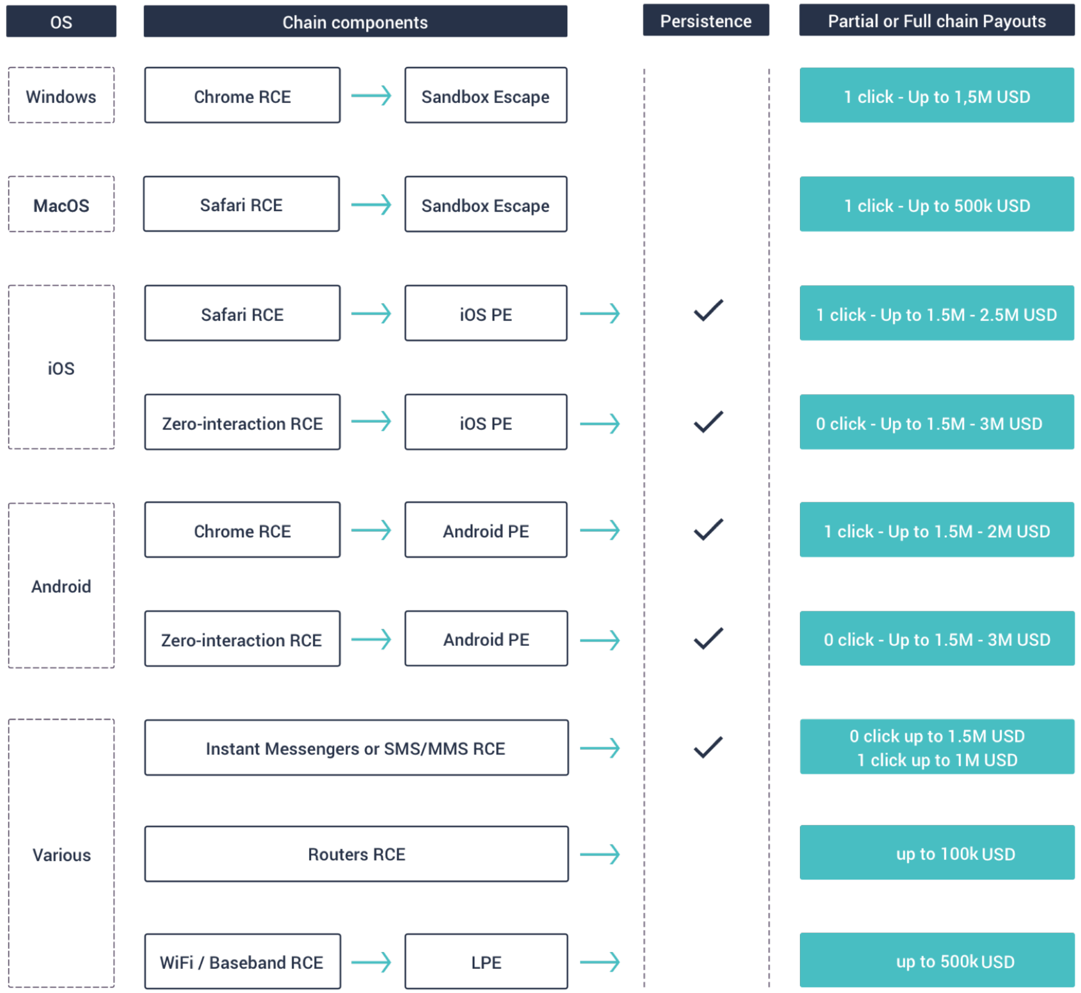
Legal, safe and easy to use.

The Public Bug Bounty Program

In April 2018 we launched our 10M USD Public Bug Bounty program, which offers the highest bounties ever paid for these classes of exploits.

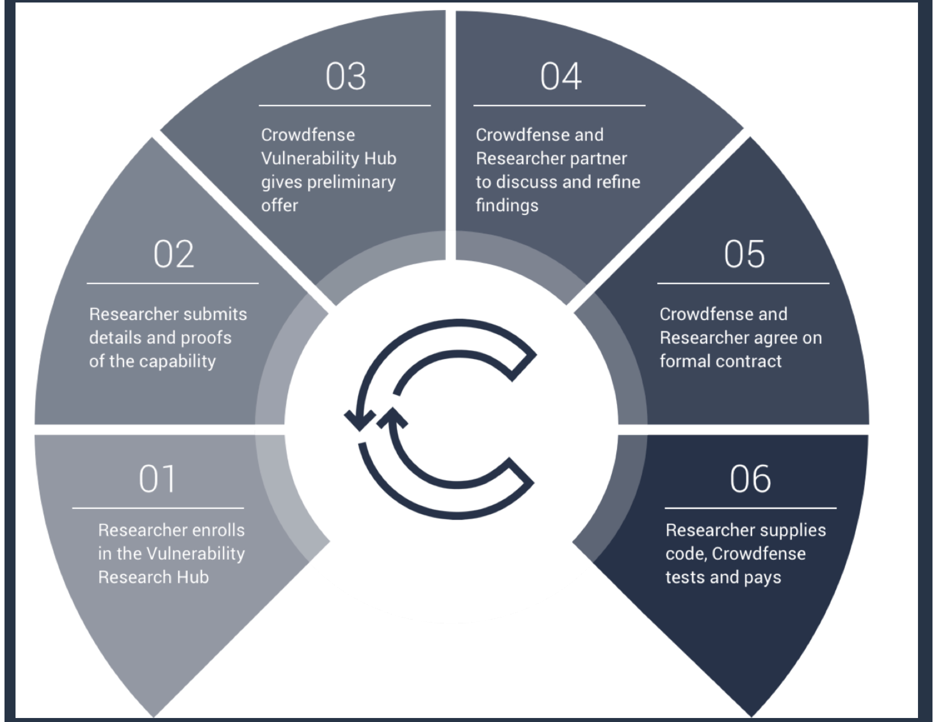
Thanks to this program, we were able to purchase top quality capabilities, and are in the process of buying more.

In 2019 we added more bounties (15M USD) and include more classes of exploits in our program.



OS	Chain components	Persistence	Partial or Full chain Payouts
Windows	Chrome RCE → Sandbox Escape		1 click - Up to 1,5M USD
MacOS	Safari RCE → Sandbox Escape		1 click - Up to 500k USD
iOS	Safari RCE → iOS PE →	✓	1 click - Up to 1.5M - 2.5M USD
	Zero-interaction RCE → iOS PE →	✓	0 click - Up to 1.5M - 3M USD
Android	Chrome RCE → Android PE →	✓	1 click - Up to 1.5M - 2M USD
	Zero-interaction RCE → Android PE →	✓	0 click - Up to 1.5M - 3M USD
Various	Instant Messengers or SMS/MMS RCE →	✓	0 click up to 1.5M USD 1 click up to 1M USD
	Routers RCE →		up to 100k USD
	WiFi / Baseband RCE → LPE →		up to 500k USD

The Vulnerability Research Hub (VRH)



01 Researcher enrolls in the Vulnerability Research Hub

02 Researcher submits details and proofs of the capability

03 Crowdfense Vulnerability Hub gives preliminary offer

04 Crowdfense and Researcher partner to discuss and refine findings

05 Crowdfense and Researcher agree on formal contract

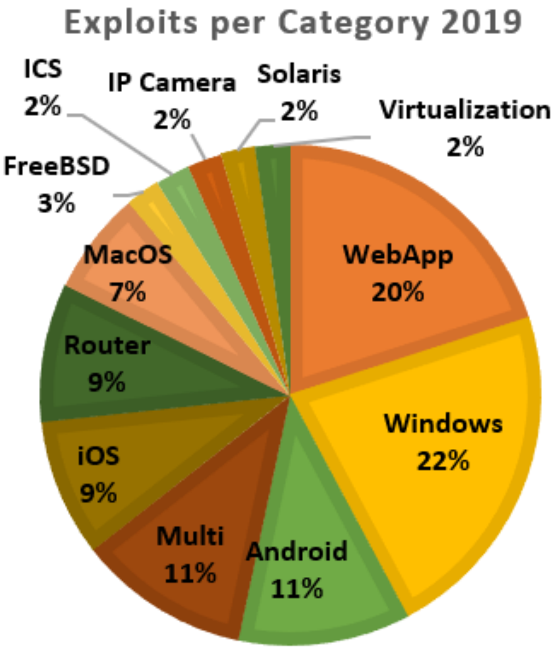
06 Researcher supplies code, Crowdfense tests and pays

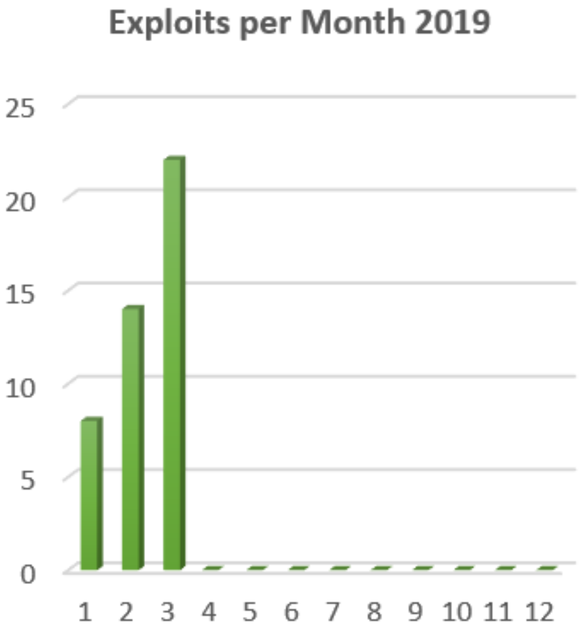
Step by step, user friendly workflows manage submission, discussion, testing, evaluation, contracting and payment.

Findings can be both within the scope of the Bug Bounty Program or freely proposed by researchers (within our Code of Conduct).

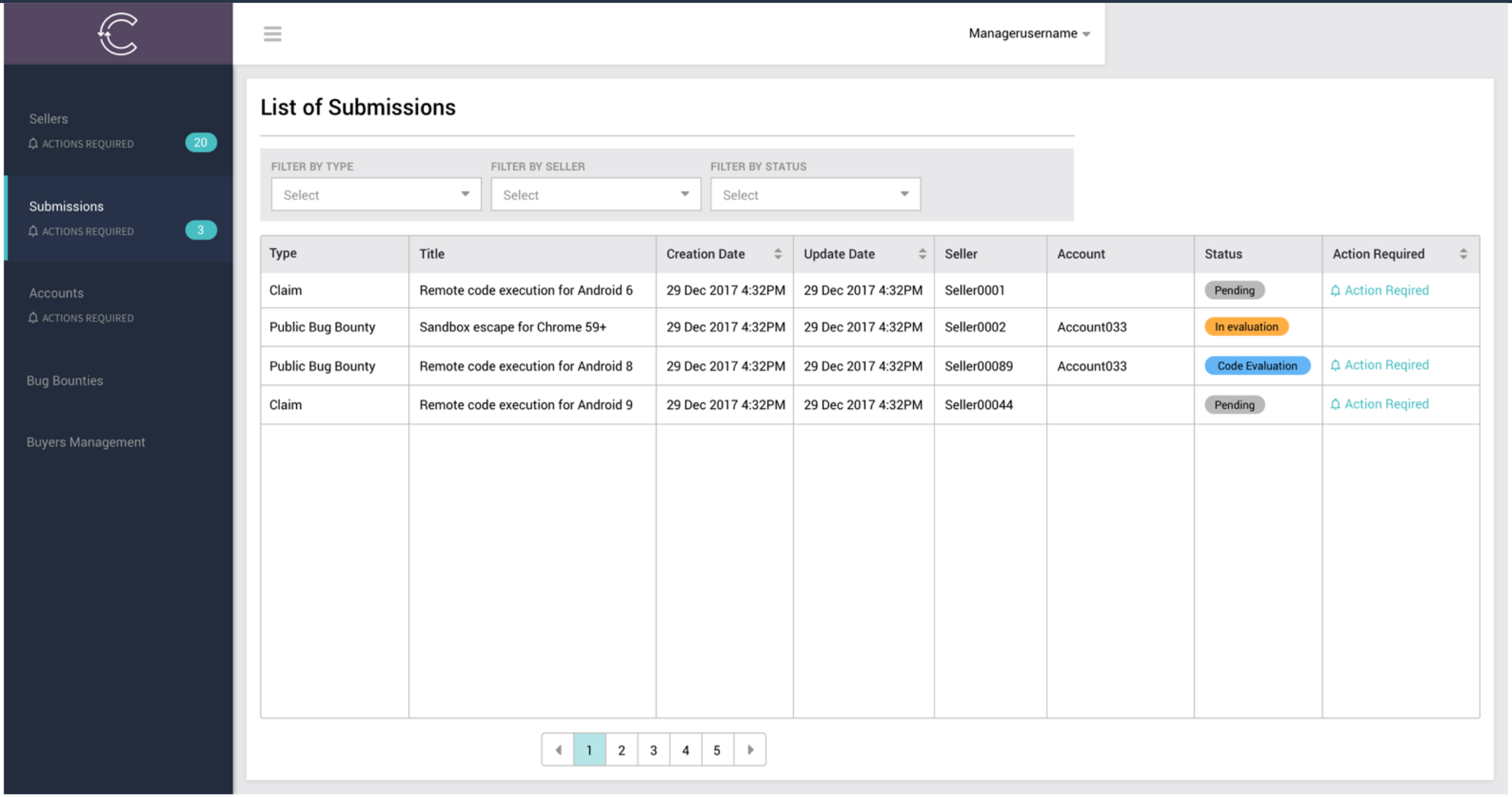
Based on a zero-trust model with maximum OpSec for all participants.

Some VRH stats from Q1 2019





The VRH



List of Submissions

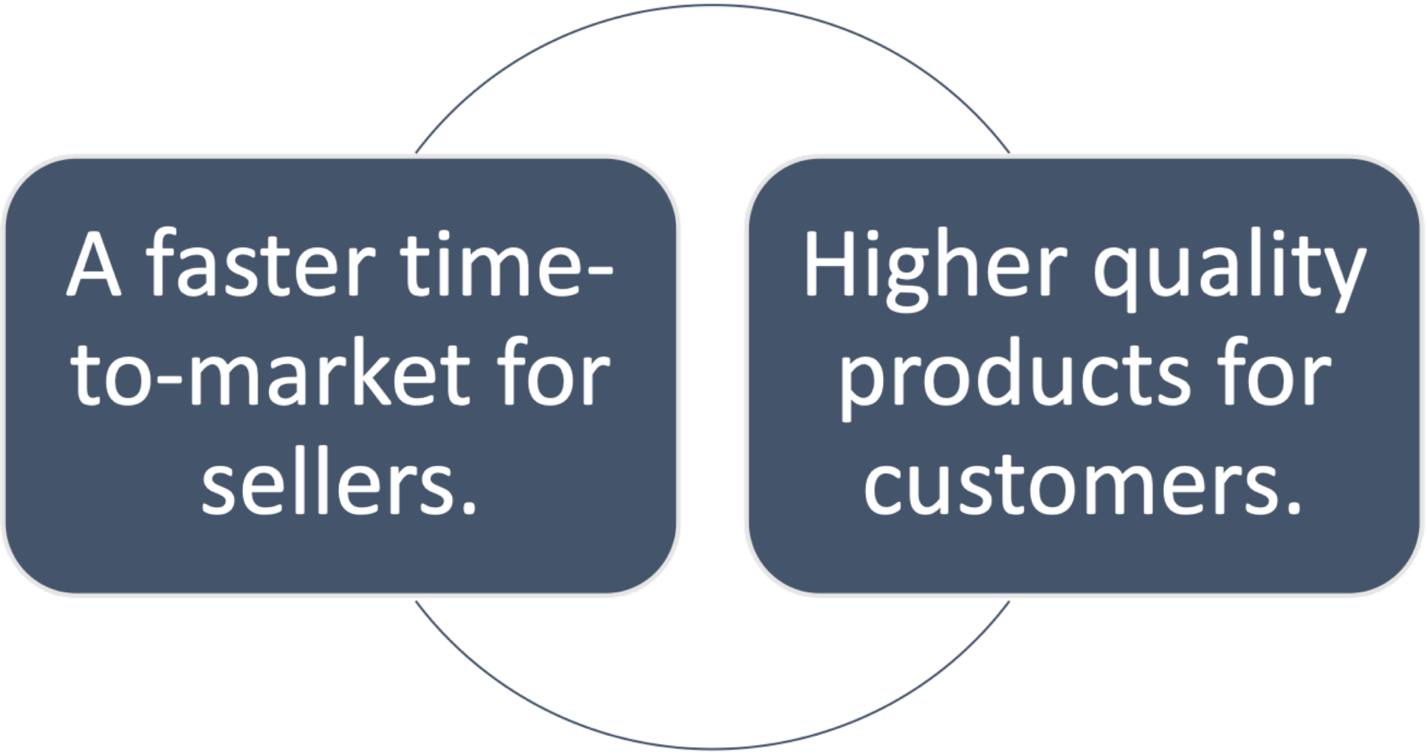
FILTER BY TYPE: Select

FILTER BY SELLER: Select

FILTER BY STATUS: Select

Type	Title	Creation Date	Update Date	Seller	Account	Status	Action Required
Claim	Remote code execution for Android 6	29 Dec 2017 4:32PM	29 Dec 2017 4:32PM	Seller0001		Pending	Action Reqired
Public Bug Bounty	Sandbox escape for Chrome 59+	29 Dec 2017 4:32PM	29 Dec 2017 4:32PM	Seller0002	Account033	In evaluation	
Public Bug Bounty	Remote code execution for Android 8	29 Dec 2017 4:32PM	29 Dec 2017 4:32PM	Seller00089	Account033	Code Evaluation	Action Reqired
Claim	Remote code execution for Android 9	29 Dec 2017 4:32PM	29 Dec 2017 4:32PM	Seller00044		Pending	Action Reqired

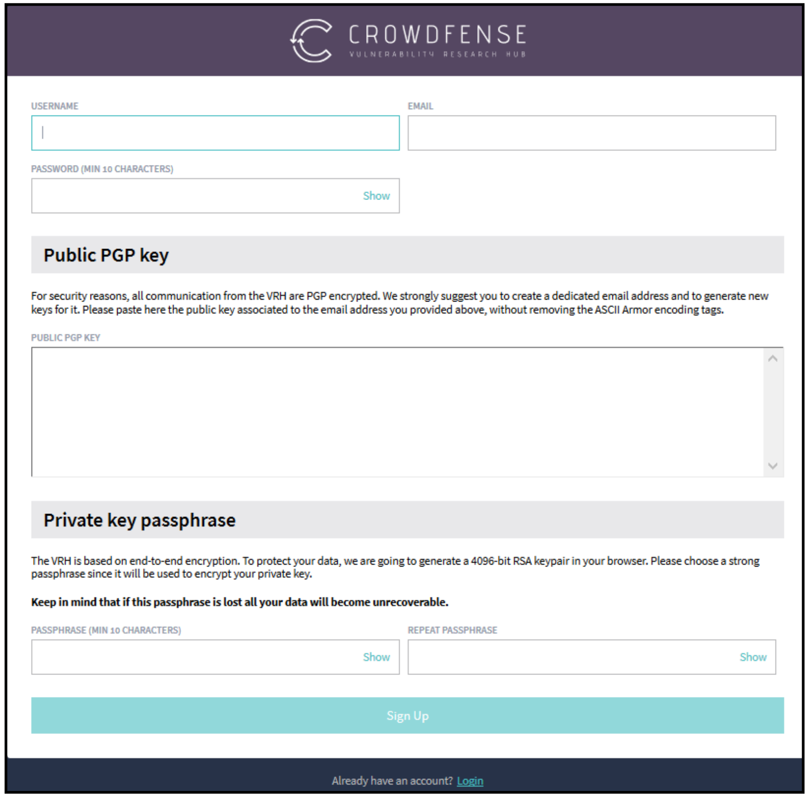
VRH Goals



A faster time-to-market for sellers.

Higher quality products for customers.

How to join the VRH



USERNAME

EMAIL

PASSWORD (MIN 10 CHARACTERS)

Public PGP key

For security reasons, all communication from the VRH are PGP encrypted. We strongly suggest you to create a dedicated email address and to generate new keys for it. Please paste here the public key associated to the email address you provided above, without removing the ASCII Armor encoding tags.

PUBLIC PGP KEY

Private key passphrase

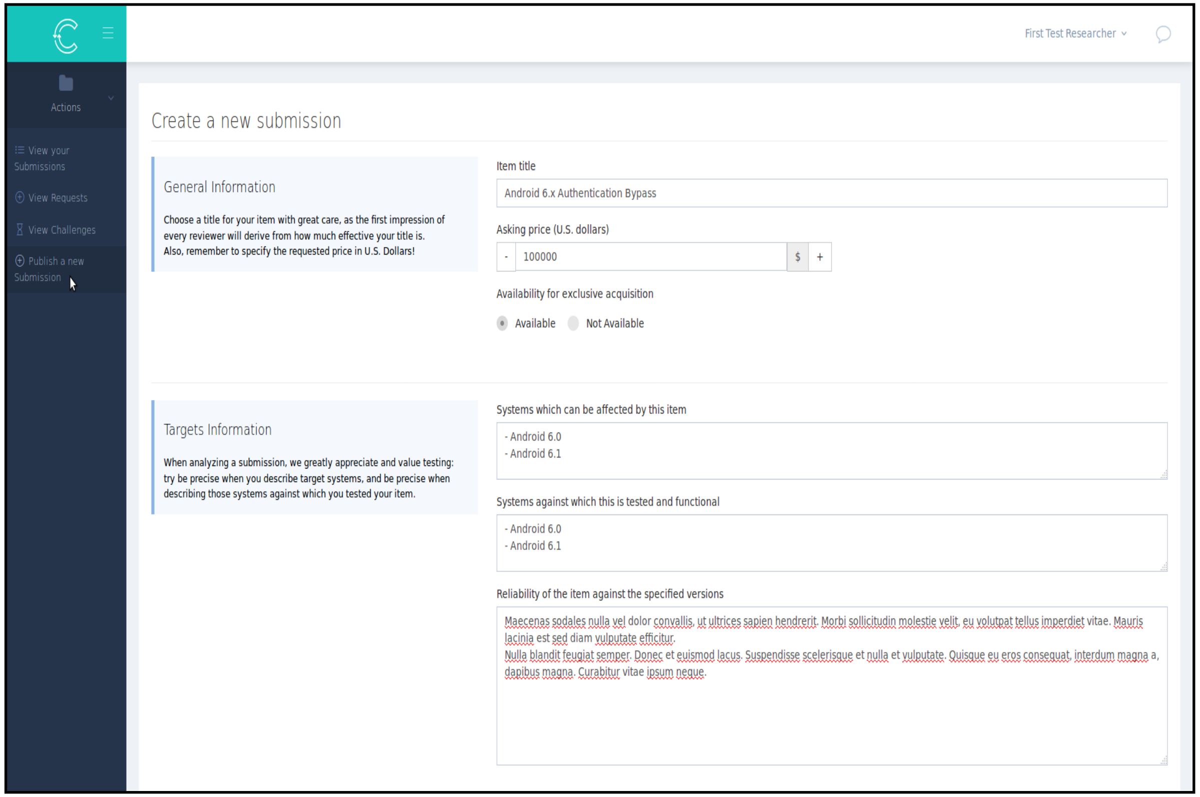
The VRH is based on end-to-end encryption. To protect your data, we are going to generate a 4096-bit RSA keypair in your browser. Please choose a strong passphrase since it will be used to encrypt your private key.

Keep in mind that if this passphrase is lost all your data will become unrecoverable.

PASSPHRASE (MIN 10 CHARACTERS)

REPEAT PASSPHRASE

Already have an account? Login



Create a new submission

General Information

Choose a title for your item with great care, as the first impression of every reviewer will derive from how much effective your title is.
Also, remember to specify the requested price in U.S. Dollars!

Item title: Android 6.x Authentication Bypass

Asking price (U.S. dollars): 100000 $

Availability for exclusive acquisition

● Available ○ Not Available

Targets Information

When analyzing a submission, we greatly appreciate and value testing: try be precise when you describe target systems, and be precise when describing those systems against which you tested your item.

Systems which can be affected by this item

- Android 6.0
- Android 6.1

Systems against which this is tested and functional

- Android 6.0
- Android 6.1

Reliability of the item against the specified versions

Maecenas sodales nulla vel dolor convallis, ut ultrices sapien hendrerit. Morbi sollicitudin molestie velit, eu volutpat tellus imperdiet vitae. Mauris lacinia est sed diam vulputate efficitur.
Nulla blandit feugiat semper. Donec et euismod lacus. Suspendisse scelerisque et nulla et vulputate. Quisque eu eros consequat, interdum magna a, dapibus magna. Curabitur vitae ipsum neque.

Thank you !

To learn more about or to discuss ways to partner with Crowdfense come speak to us after this presentation or visit our website: crowdfense.com

To join the VRH: vrh.crowdfense.com

For inquiries:
Researchers and customer: info@crowdfense.com
Media: press@crowdfense.com