La divulgation des vulnérabilités pour fédérer

Guillaume Vassault-Houlière

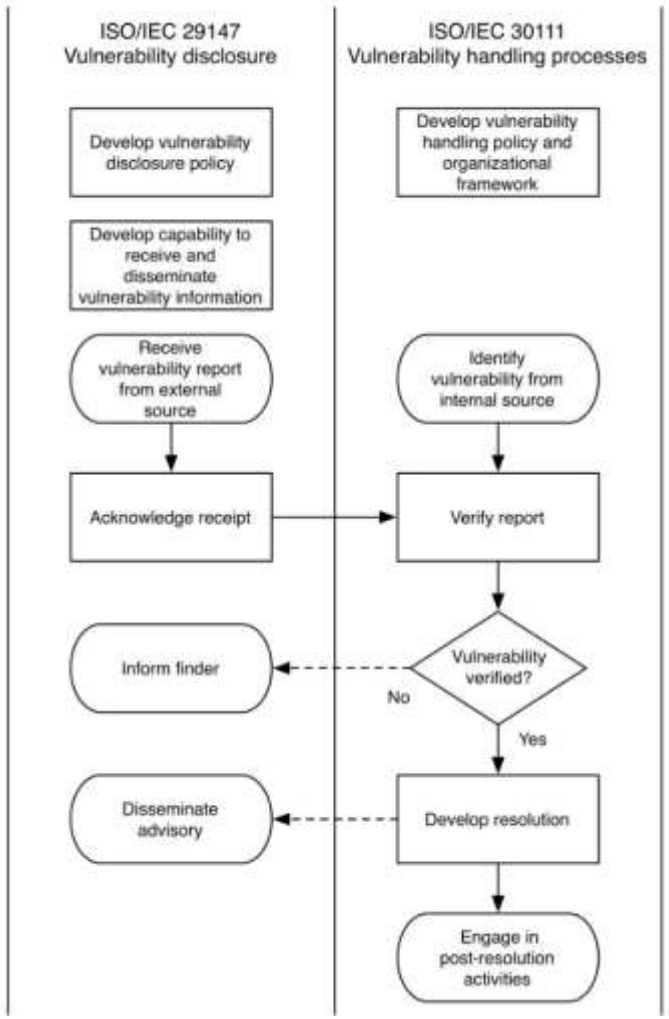
CEO

CLUSIF

« La divulgation des vulnérabilités est un processus par lequel les fournisseurs et les personnes qui découvrent des vulnérabilités peuvent travailler en collaboration pour trouver des solutions qui réduisent les risques associés à une vulnérabilité. »

Norme ISO/CEI 29147 définissant la Divulgation de Vulnérabilités

Interconnexion : ISO 29147 et 30111



Source 2013: Katie Moussouris

Remontée coordonnée de vulnérabilité
Coordinated Vulnerability Disclosure aka CVD

Principes

- Réduire les risques donc les dommages
- Croire aux bonnes actions donc aux bons samaritains
- Éviter le hasard
- Stimuler la coopération
- Suivre la déontologie
- Apprendre de la boucle OODA

Objectifs

- Veiller à ce que les vulnérabilités identifiées soient prises en compte
- Réduire au minimum le risque
- Fournir aux entreprises suffisamment d'informations pour évaluer les risques liés aux vulnérabilités de leurs systèmes

Acteurs

- **Chercheur en sécurité** – la personne ou l'organisation qui identifie la vulnérabilité.
- **Rapporteur** – la personne ou l'organisation qui avise le fournisseur de la vulnérabilité.
- **Fournisseur** – la personne ou l'organisation qui a créé ou entretient le produit vulnérable.
- **Administrateur système** – personne ou organisation qui doit déployer un correctif ou prendre d'autres mesures correctives.
- **Coordinateur** – personne ou organisation qui facilite le processus d'intervention coordonnée.

Canaux de confiance

- Responsible Disclosure Policy
- Security.txt
- Bug Bounty
- Article 47 – 2016 (loi pour une République numérique)
- Zerodisclo.com
- …

Responsible Disclosure Policy

CERT-EU Responsible Disclosure Policy

What to report to CERT-EU:

Security Incidents and Vulnerabilities, which occur in software components, protocols, or hardware of websites or systems of EU Institutions Agencies or Bodies, and may affect significant number of users and/or critical infrastructure.

Vulnerability reporting policy:

CERT-EU reserves the right to accept or reject any vulnerability disclosure report at its discretion, based on the following general criteria:

1. Pre-disclosure handling of the potentially sensitive vulnerability details:
   - The vulnerability should have not already been publicly disclosed.
   - It is important to report the vulnerability as quickly as possible after its discovery.
   - Even after reporting the vulnerability, no information on the security problem should be shared with others until the incident has been processed and resolved. Failure to comply with this requirement may result in the reported being removed from the CERT-EU Hall of Fame.
2. The vulnerability finding must be new and severe enough to be considered as eligible for a mention in the Hall of Fame of CERT-EU. The severity of a vulnerability finding is assessed by CERT-EU at its own discretion. CERT-EU reserves the right to reject reports of vulnerabilities, which have already been previously reported.

Vulnerability reporting instructions:

- E-mail your findings to reports (at) cert.europa.eu.
- Encrypt your email using the PGP key available on CERT-EU website
- Provide as much information as possible regarding the finding, in order for CERT-EU to handle the incident as efficiently as possible.

If more information is required, CERT-EU will contact the reporter, therefore any contact details (email address and telephone number) should be valid.
If the previously mentioned conditions are satisfied, CERT-EU will proceed with notification to the impacted party. Once the issue has been fixed or no later than 3 months since the initial report, the reporter may be mentioned (at his own discretion) in the Hall of Fame of CERT-EU (this page) with a short description of the type of vulnerability reported.

CERT-EU

Security.txt (DRAFT RFC)

Secure | https://www.google.com/.well-known/security.txt

```
Contact: https://g.co/vulnz
Contact: mailto:security@google.com
Encryption: https://services.google.com/corporate/publickey.txt
Acknowledgements: https://bughunter.withgoogle.com/
Policy: https://g.co/vrp
Hiring: https://g.co/SecurityPrivacyEngJobs
```

Secure | https://www.facebook.com/.well-known/security.txt

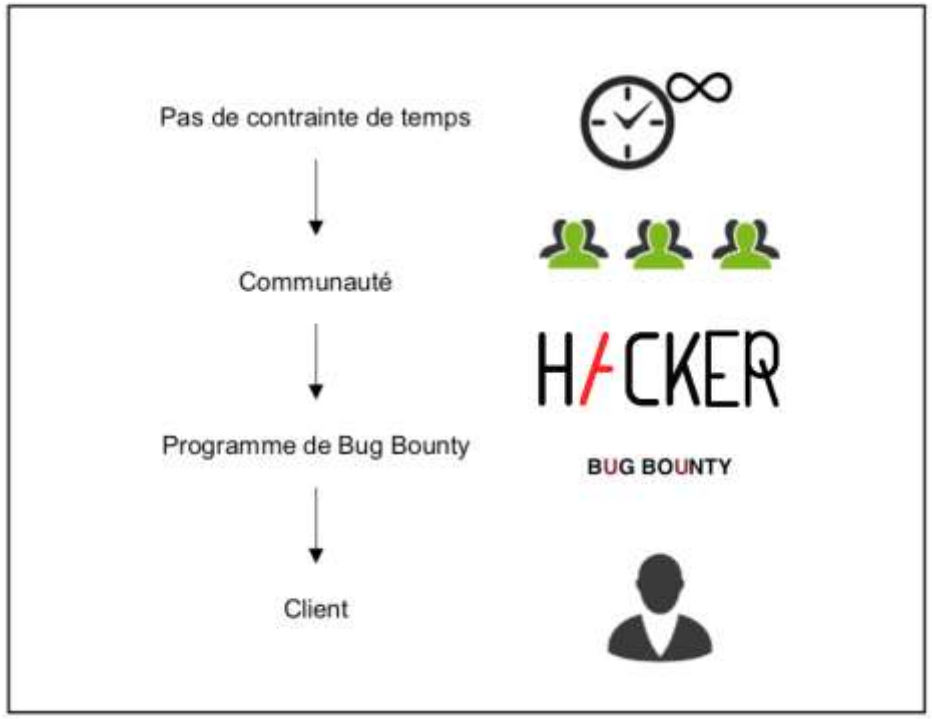
```
Contact: https://www.facebook.com/whitehat/report/
Acknowledgments: https://www.facebook.com/whitehat/thanks/
Policy: https://www.facebook.com/whitehat/info/
Hiring: https://www.facebook.com/careers/teams/security/
```

Secure | https://www.blablacar.fr/.well-known/security.txt

```
#
# SECURITY.TXT for BlaBlaCar
# https://securitytxt.org/
#
# If you would like to report a security issue
# you may report it to me on Bounty Factory
Contact: https://bountyfactory.io/blablacar/bug-bounty-program-blablacar
Acknowledgement: https://bountyfactory.io/ranking
Hiring: https://www.blablacar.com/dreamjobs
```

Bug Bounty

Méthode « Crowd Security »



Rules

While we are trying our best to keep OVH services as safe as possible, We know that some vulnerabilities have slip

If you believe you've found a security issue in the services listed in our scope, we will work with you to resolve it pro

English and French spoken !

Nous parlons anglais et français !

Scope

The scope of this program is limited to security vulnerabilities found in :

- https://api.ovh.com
- https://www.ovh.com/manager
- *.osp.ovh.com
- Private Cloud product (for more information: https://www.ovh.com/us/dedicated-cloud/)
- www.ovh.com (excluding : /managerv3/* and /soapi/* uri)

Note that BETA feature are also eligible.
A lot of API endpoint work with OVH purchased products.
OVH will refund a 30-day period to hunters having submitted a confirmed vulnerability on the product.

Vulnerabilities reported on **other services or applications** are currently not eligible for monetary reward and will be h
they will be added to this section.

Eligibility

We are happy to work with everyone who submits valid reports which help us improve the security of OVH.

However, only those that meet the following eligibility requirements may receive a monetary reward:

• You need to be the first person to responsibly disclose an unknown issue

Rewards

OVH may provide rewards to eligible reporters of qualifying vulnerabilities. Our minimum reward is €50 and our maximum rewards is €10,000. R

OVH reserves the right to decide if the minimum severity threshold is met and whether the scope of the reported vulnerability is actually already
the discretion of OVH. To qualify for a reward under this program, you should respect all the above-mentioned eligibility criterias.

Payments are made through bountyfactory.io only.

Article 47 (loi pour une République numérique)

VOUS SOUHAITEZ DÉCLARER UNE FAILLE DE SÉCURITÉ OU UNE VULNÉRABILITÉ ?

Vous avez découvert une faille de sécurité ou une vulnérabilité et vous souhaitez nous la déclarer ?

C'est désormais possible grâce à la loi pour une République numérique *.

Adressez-nous un message (cert-fr.cossi[at]ssi.gouv.fr) en transmettant tous les éléments techniques nous permettant de procéder aux opérations nécessaires.
Il est également possible d'opérer votre signalement par voie postale.

Merci d'adresser votre courrier et vos compléments d'information à :

Agence nationale de la sécurité des systèmes d'information
Secrétariat général de la défense et de la sécurité nationale
51, boulevard de La Tour-Maubourg
75700 Paris 07 SP

Retrouvez toutes les modalités pour nous contacter https://www.cert.ssi.gouv.fr/contact/

L'ANSSI préservera la confidentialité de votre identité ainsi que les éléments de votre déclaration **.

* Loi pour une République numérique n° 2016-1321 du 7 octobre 2016

Article 47

Le chapitre Ier du titre II du livre III de la deuxième partie du code de la défense est complété par un article L. 2321-4 ainsi rédigé :

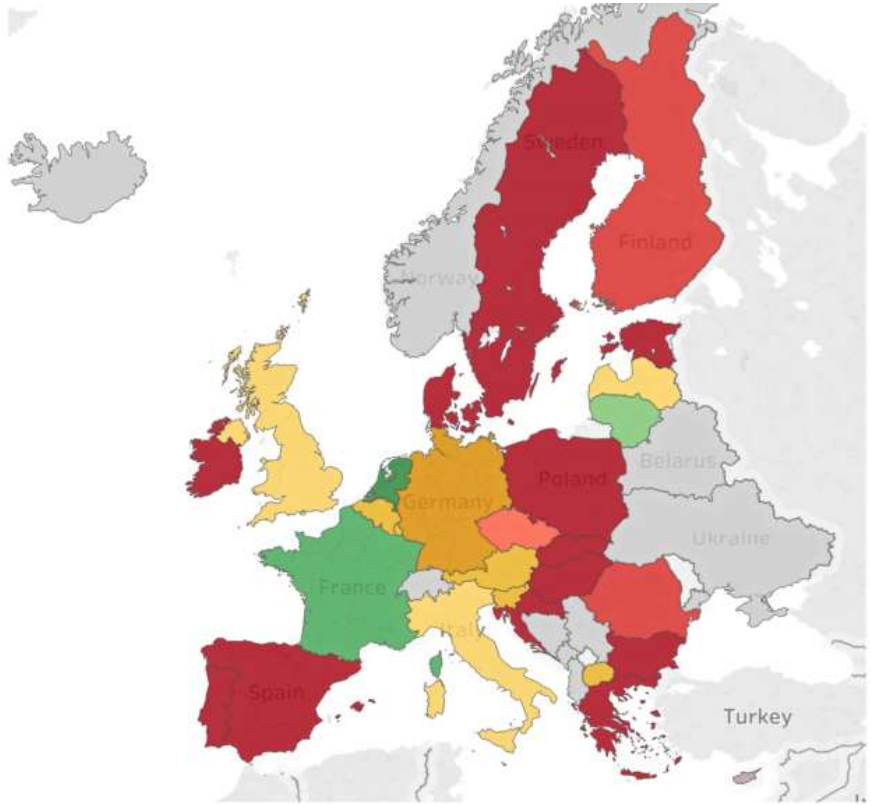
** *« Art. L. 2321-4. – Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données.*

« L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée.

« L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information. »

ELI: www.legifrance.gouv.fr/eli/loi/2016/10/7/ECFI1524250L/jo/article_47 | Alias: www.legifrance.gouv.fr/eli/loi/2016/10/7/2016-1321/jo/article_47

CVD en Europe

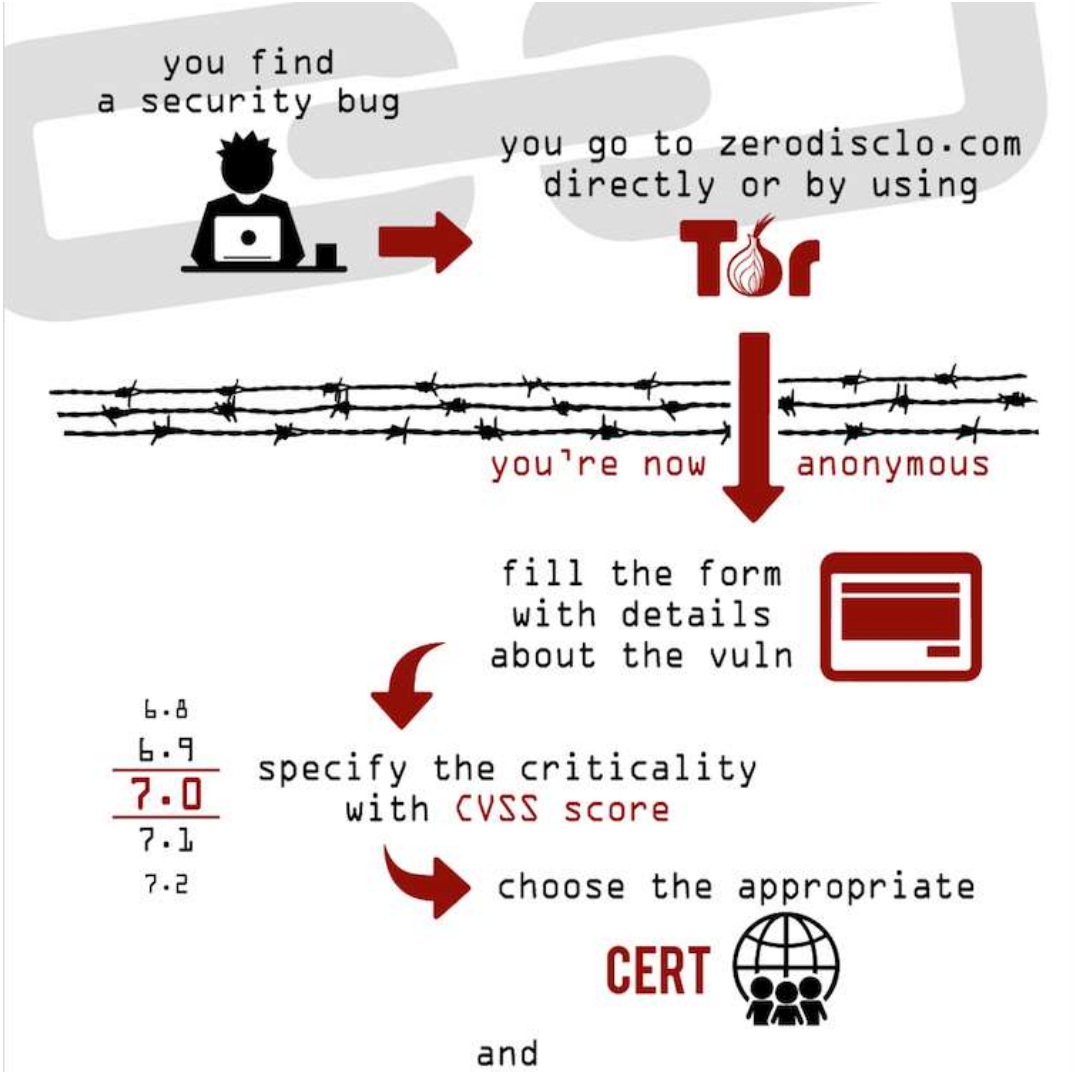


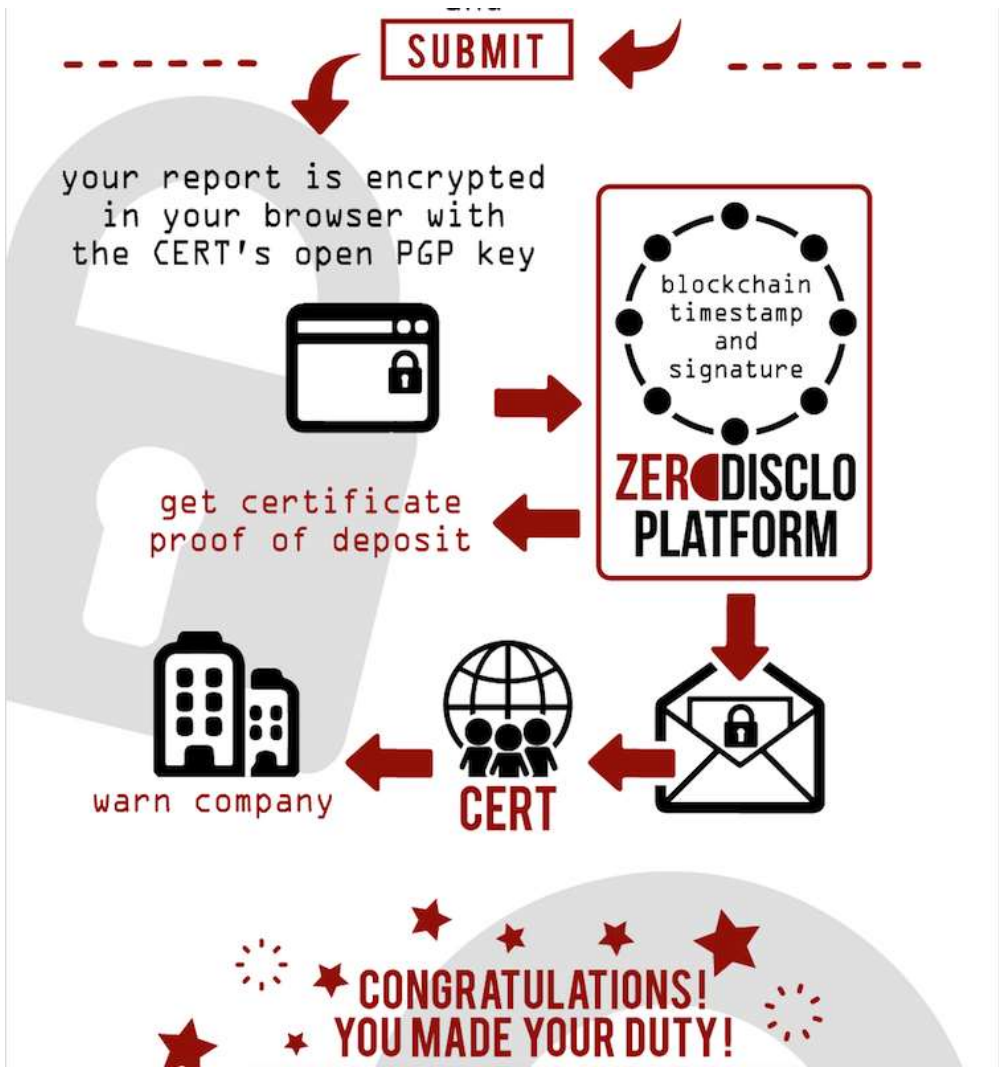
Source: CEPS' own elaboration.

CVD policy at national level	Status	Country
YES	CVD policy established, full protection of the researcher	Netherlands
	CVD policy established, but partial protection of the researcher	France
IN PROGRESS	Implemented CVD policy for a specific sector, ongoing discussions and national framework expected for summer 2018	Lithuania
	Ongoing discussions and preliminary work done	Italy
	See dedicated chapter	Latvia
	Ongoing discussions and pilot	United Kingdom
		Austria

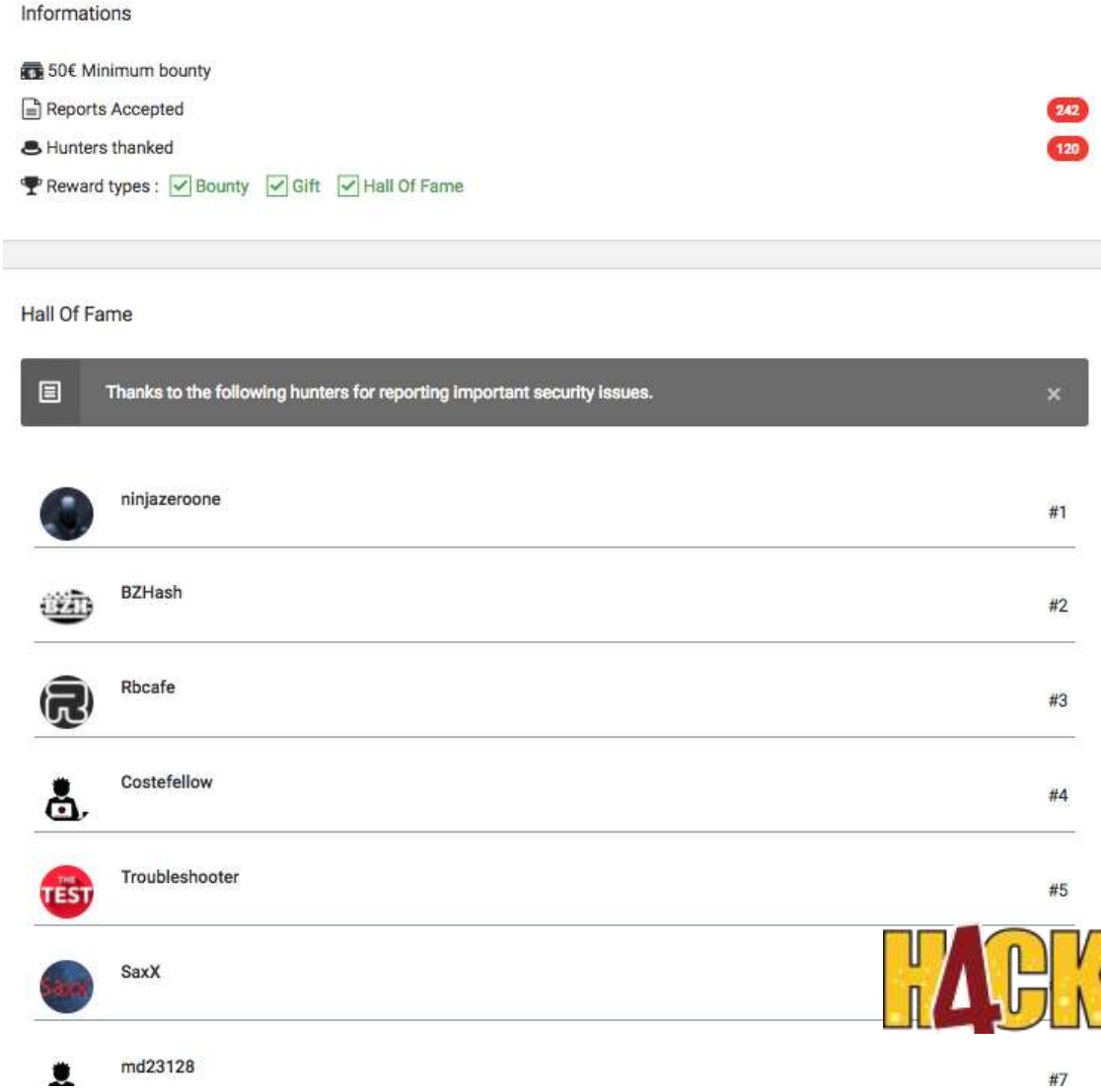
Source 2018 : www.ceps.eu

Zerodisclo.com





Fédérer



HACKPÉRO

IT SECURITY IS AN ILLUSION

Crowdsecurity is the new reality

CLUSIF

CLUSIF

Merci

YES WE HACK

@yeswehack

contact@yeswehack.com