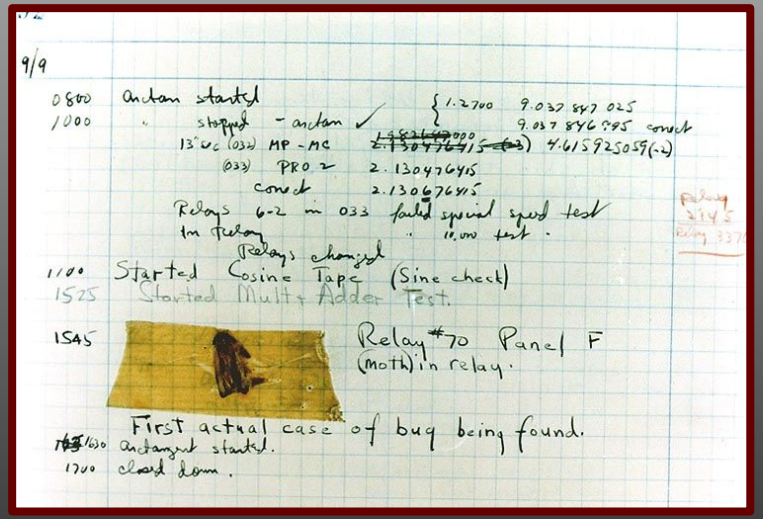
El milenario arte del...

Bug Bounty Jitsu

BUG

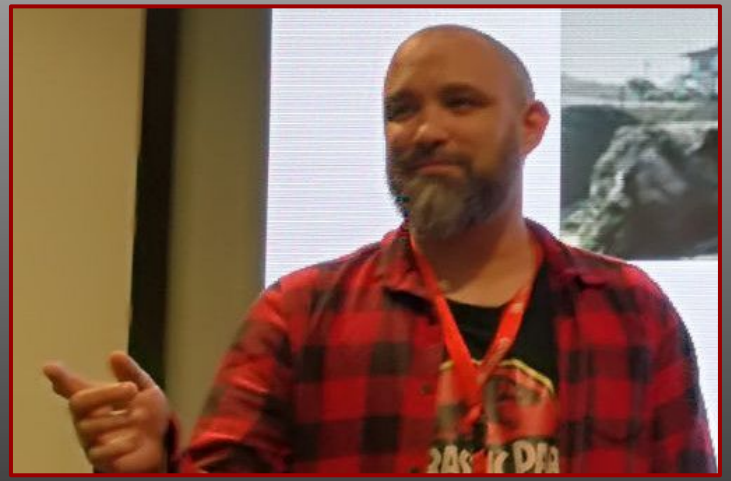


(a) Industry Average: "about 15 - 50 errors per 1000 lines of delivered code.
Steve McConnell, from the “Code Complete” book.

BOUNTY

Google - Since 2010 >10M USD
Verizon Media - Since 2014 >6M USD
Uber - Since 2014 >2M USD

Sensei



@afernandesvigo

- CISO by Day & BugHunter by Night
- Cyber & Innovation Advisor

Bug Bounty Reigi

ACTUALIDAD

Justicia denuncia al informático que destapó el fallo de Lexnet

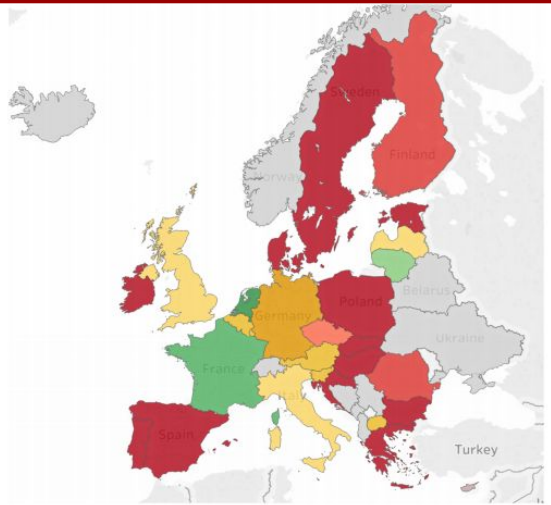
Por **Redaccion DJ** - 9 febrero, 2018

Síguenos

SOBRESEEN PROVISIONALMENTE LA DENUNCIA CONTRA FGV

El juez cita como investigado al denunciante del agujero de seguridad en la 'app' de Metrovalencia

Estefanía Pastor



Status
- No information available
- No activity
- Policy released by their CERT, although there are no ongoing discussions and legal framework.
- Discussions planned for 2018, although there is no legal framework.
- Discussions planned for 2018
- Ongoing discussions on this issue
- Ongoing discussions and pilot
- Ongoing discussions and preliminary work done
- CVD policy proposed but failed to be incorporated in the law
- Implemented CVD policy for a specific sector, ongoing discussions and national framework expected for summer 2018
- CVD policy established, but partial protection of the researcher
- CVD policy established, full protection of the researcher

Source: CEPS' own elaboration.

June 2018 -

1. Amending Directive 2013/40/EU on attacks against information systems (the EU cybercrime Directive) to support CVD.
2. **Protection of security researchers. "The legal liability and responsibilities of security researchers should be fully clarified to enable them to continue their work without fear of prosecution."**
3. Incentives for security researchers. Appropriate policies should be adopted with the aim of encouraging 'white-hat hackers' to actively participate in coordinated vulnerability disclosure programmes.
4. Directive on security of network information systems (NIS). In transposing the NIS Directive, particularly its Article 14, member states may explicitly consider including CVD as one of the technical and organisational measures.
5. **General Data Protection Regulation (GDPR). According to the GDPR, software owners and tech firms become data controllers when they exercise overall control over the purpose for which, and the manner in which personal data are processed. Assuming that irresponsible handling of vulnerabilities could lead to personal data breaches falling within the scope of GDPR, CVD should be viewed as one of the necessary tools to mitigate the relevant risks.**
6. Cybersecurity Act Amendments. State that ENISA can contribute to the harmonised development of CVD in the EU by having its mandate amended. A provision in Article 47 (1)j of the Cybersecurity Act provides the possibility to introduce CVD in a European Cybersecurity Certification Scheme, which in fact may encourage CVD as a standard practice.
7. Software vulnerabilities in durable goods such as cars and medical devices
8. Amending national legislation to support CVD
9. Framework Programmes for Research and Innovation (focus on EU research funding)
10. GDDP characteristics recommended to adopt (GDDP is the EU version of The United States' Vulnerabilities Equities Process) and survey of member states' GDDP is also suggested.

CVD/VDP/RDP

Coordinated Vulnerability Disclosure (Policy)
Vulnerability Disclosure Policy
Responsible Disclosure Policy

- ¿Son lo mismo?
- ISO 29147

Bug Bounty

- Swag / Hall of Fame
- Bounty

Introducción: Se da el mensaje a clientes, socios y hackers, sobre el por que de la política y la importancia de los datos.

Protección: Debe especificarse la protección a los hackers si se siguen las reglas de la política.

Scope: Hay que explicar a los hackers que entendemos por vulnerabilidad, que activos, productos y/o servicios forman son sujetos a sufrir una investigación por su parte y cuáles no...

Canal de comunicación: En esta parte hay que definir un canal seguro para reportar al equipo o software responsable los descubrimientos.

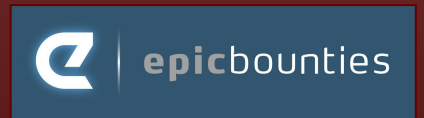
Reglas del Juego: En esencial explicar las particularidades que queramos, es decir, uso de alguna cabecera específica, uso o no de herramientas automáticas, etc... Así como cualquier detalle sobre hacer públicos o no los descubrimientos en nuestro programa.

Bounty: ¿Pagamos? ¿No Pagamos? ¿Hay Hall of Fame?

Dojos


bugcrowd


YES WE HACK


epicbounties


hackerone


INTIGRITI
ETHICAL HACKING PLATFORM


zerocopter

Generalitat de Catalunya

govern.cat

CONTACTA EN

El Govern | Cohesió social | Prosperitat econòmica | Enfortiment democràtic | Pla de Govern | Premsa | President.cat

/ Enfortiment democràtic / L'Agència de Ciberseguretat de Catalunya, en col·laboració amb el Departa...

2 febrer 2021 12:44 Nota de premsa

L'Agència de Ciberseguretat de Catalunya, en col·laboració amb el Departament de la Vicepresidència, endega una prova pionera per detectar vulnerabilitats a l'Administració Pública

Economia i Hisenda Comunicació

- Durant 2 setmanes i amb la participació exclusiva d'un conjunt de reputats experts en ciberseguretat, s'han identificat 5 *bugs* en els actius inclosos en l'abast de la prova pilot
- El Catalonia-CERT de l'Agència de Ciberseguretat ha supervisat el desenvolupament programa pilot amb la validació de les vulnerabilitats identificades i la gestió de la seva corresponent solució
- La Generalitat utilitzarà programes *bug bounty* per aconseguir uns sistemes d'informació més segurs, promoure la participació i aproximar l'Administració Pública a la ciutadania

¿ Figura del Gestor ?

Bug Bounty Kumite

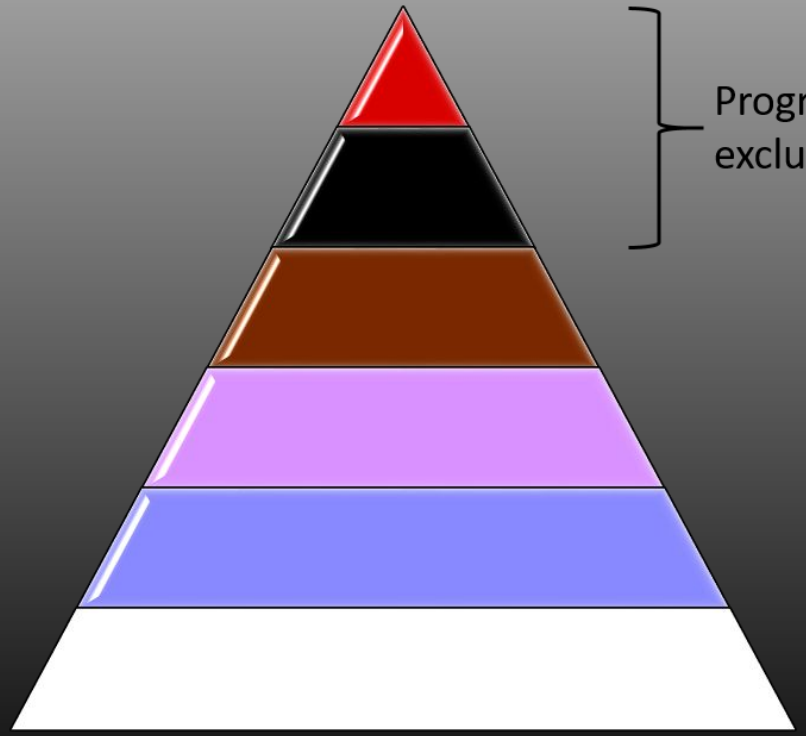
Realidad de las Empresas

- ¿S-SDLC?
- ¿Activos?
- ¿Actualizar?
- ¿Pentests?

Realidad en el mundo del Bug Bounty

- Se integra en Jira, Jenkins...
- El Recon es un arte en si mismo
- Lo desactualizado es siempre un mejor objetivo
- Constante a lo largo del tiempo

Cintos



Programas exclusivos

Programas privados

Programas públicos y VDP

BugBountokas Destacados

try_to_hack

Bug Bounty
Millionaire

Stok

Bug Bounty
Creator

0xd0m7

Bug Bounty
top 50

Bug Bounty ES

Bug Bounty ES 1394 members

Antonio Fernandes
Normas: * ISO 29147 * Se habla en Español/Castellano como prefiera cada uno denominarlo. * No se habl...

cacheDub❤️ joined group via invite link

Thursday, November 14, 2019

Jaime Restrepo admin 8:29:33 AM
> **Dokkillo**
> Por fin!!! 11 meses después me han cerrado un rce que detec...

Que bien, yo pensé que el que me pagaron hoy de 3 meses era mucho 😂

Darko admin 1:26:02 PM
Entonces me tocará esperar bastante para cobrar un RCE...

Antonio Fernandes admin 1:26:27 PM
Eso temo compañero :D

Write a message...

Bug Bounty Gourmet

Bug Bounty Gourmet 13 members

安龙
https://www.seebug.org/vuldb/ssvid-98060 -> Webmin https://www.seebug.org/vuldb/ssvid-98062 -> Puls...

? 1:08:03 PM

0xd0m7 admin 1:09:24 PM
pues despues de tirar 03294810293 payloads, la solucion era mas simple de lo que me pennsaba

Samu 1:11:19 PM
Buenísima

0xd0m7 admin edited 1:11:21 PM
cuando este resuelto, os paso como lo hize , entended que pase el host

Samu 1:11:32 PM
Crack 👏

Write a message...

OSS!!

¿Preguntas?