CICLO DE CHARLAS Y ENTREVISTAS
05.06.20

HACKERSPACE CÓRDOBA

Bug Bounty: utilidad para hackers y organizaciones

Eduardo Casanovas – Carlos Tapia

UNDEF Universidad de la Defensa Nacional IUA

Universidad de la Defensa Nacional

HACKERSPACE CÓRDOBA

Agenda de la charla

Qué es BB? Diferencias entre PT y BB

Qué es una plataforma de BB?

Visión del Bug Bounty para el hacker

Recomendaciones de inicio para el hacker

Beneficios y consideraciones para las empresas

Comentarios de cierre

UNDEF Universidad de la Defensa Nacional IUA
Universidad de la Defensa Nacional

HACKERSPACE CÓRDOBA

Diferencias entre pentesting y bug bounty…

	Pentesting	Bug Bounty
Informe	Todo tipo de vulnerabilidad	Sólo vulnerabilidades relevantes
Tiempo	Más extenso	Foco en la prueba
Planificación	Todas las fases	Sólo fase de ejecución
Recompensa	Pago por completamiento	Pago por hallazgo comprobado

UNDEF Universidad de la Defensa Nacional IUA

Universidad de la Defensa Nacional

HACKERSPACE CÓRDOBA

Plataformas de Bug Bounty…

- HackerOne (h1)
- Bugcrowd
- Synack
- Cobalt
- SafeHats
- Intigriti
- Yes We Hack
- Open Bug Bounty
- …

- Término “BBaaS”
- Fórmula Hackers VS. Organizaciones → Hackers + Organizaciones

UNDEF Universidad de la Defensa Nacional IUA

Universidad de la Defensa Nacional

HACKERSPACE CÓRDOBA

Qué motivadores hay para el hacker para iniciar en BB?

- Hobby /entretenimiento / diversión
- Sentirse desafiado (nunca llegar a saber todo)
- Aprender (incorporación gradual y permanente de conocimiento)
- Catapultar a mejores trabajos “tradicionales” / acelerar carrera laboral
- “Responsabilidad social”, “hacer el mundo un lugar mejor”
- Ganar networking personal y team-up con otros hackers
- Ganar plata!!

UNDEF Universidad de la Defensa Nacional IUA

Universidad de la Defensa Nacional

HACKERSPACE CÓRDOBA

***Qué motivadores hay para el hacker para iniciar en BB?* (continuación)**

- Paraguas legal (siempre que se cumpla la policy!).
- Reputación y badges ganadas.
- Garantía de cobro (si el bounty era monetario)
- Facilitación para el pago:
  - PayPal
  - Bitcoin vía Coinbase
  - Bank Transfer vía Currencycloud
- Posibilidad de hacer splitting del pago entre varios hackers.

UNDEF Universidad de la Defensa Nacional IUA
Universidad de la Defensa Nacional

HACKERSPACE CÓRDOBA

Qué tengo que saber como hacker para el BB?

- Habilidades técnicas
  - Seguridad informática
  - Desarrollo de software
  - Lenguajes de programación
  - Redes
  - Auditoría
  - Etc.
- Gran capacidad de reporting y anclaje a evidencia
- GRAN CAPACIDAD DE RESISTENCIA A LA FRUSTRACIÓN ☺

UNDEF Universidad de la Defensa Nacional IUA

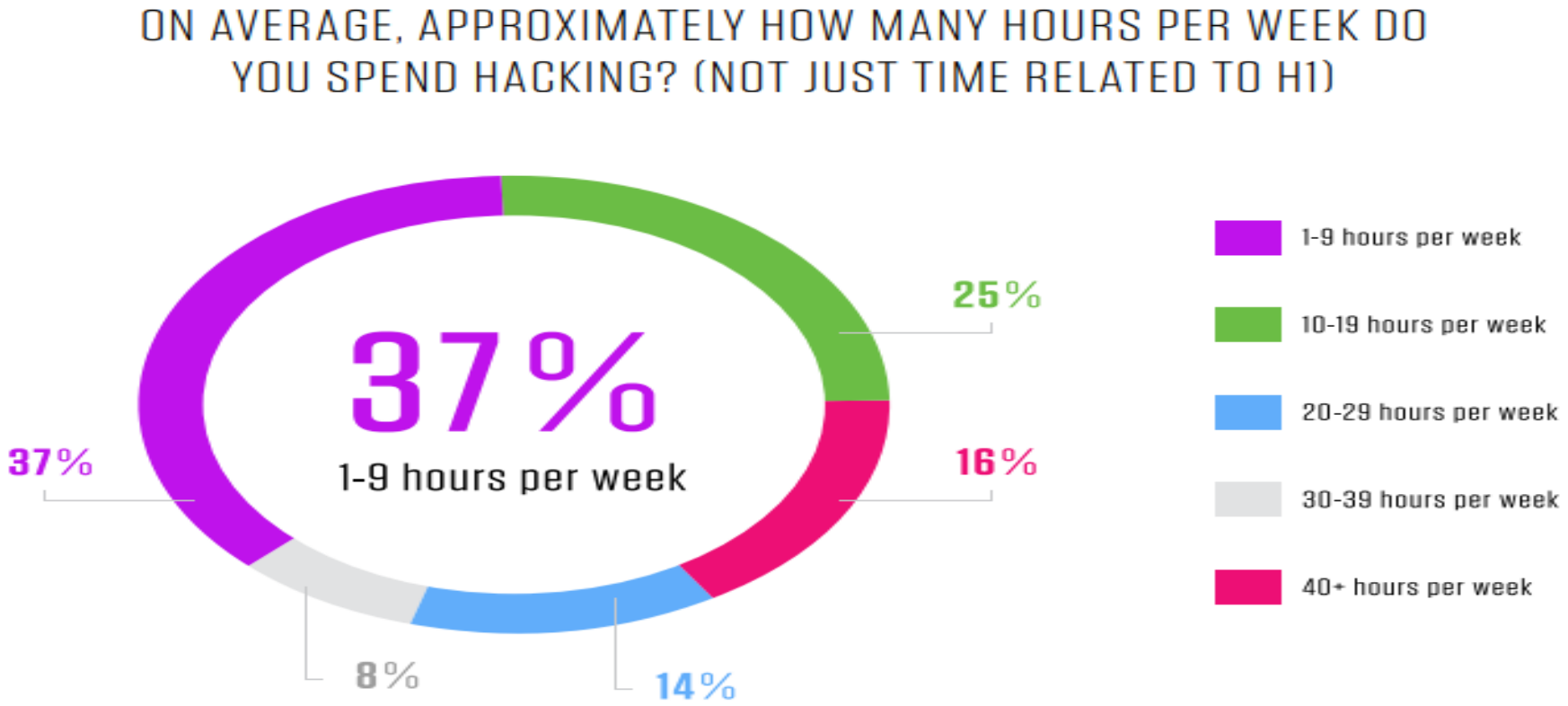
Universidad de la Defensa Nacional

HACKERSPACE CÓRDOBA

Cuánto tiempo le tengo que dedicar al BB?

"...the more...the better..."

"...something is better than nothing..."



Fuente: https://www.hackerone.com/lp/resources/2020-hacker-report

UNDEF Universidad de la Defensa Nacional IUA

Universidad de la Defensa Nacional

HACKERSPACE CÓRDOBA

Me decidí, ahora cómo arranco??!!

Una idea general del proceso puede ser:

1) **Sign-up en plataforma.**
2) **CTF, learning**
3) **Program tour**
4) **Selección de programas**
5) **Recon**
6) **Tests…eventualmente bugs!!**
7) **Triage**
8) **Reporte…eventualmente cash!!**

UNDEF Universidad de la Defensa Nacional IUA
Universidad de la Defensa Nacional

HACKERSPACE CÓRDOBA

Ya empecé, pero ahora cómo sigo??!!

“Hace semanas que no avanzo, no entiendo, no logro nada…” ☹

- Ya con el esfuerzo de entender se logra algo
- Quizás se debe utilizar otro material de estudio
- Se puede revisar enfoque distinto de otro hacker de referencia
- Se puede “tomar un descanso” de una vulnerabilidad para pasar a otras (Síndrome de Burnout)
- Efecto túnel, necesidad de esparcimiento
- Networking personal
- Participación en CTF y plataformas de e-learning de Bug Bounty.
- Administración del tiempo

☺

UNDEF Universidad de la Defensa Nacional IUA

Universidad de la Defensa Nacional

HACKERSPACE CÓRDOBA

Empezando por Recon y siguiendo…

a) Leer bien las reglas y scope del programa
b) Comprender el alcance y contexto
c) Automatización
d) Obtención de contenido
e) Leer write-ups de otros
f) Investigación manual
g) Mantener un historial/documentación
h) Aprender de otros, no parar de aprender!
i) Animarse y reportar!

INTERNET ARCHIVE WayBackMachine

MASSCAN

MassDNS

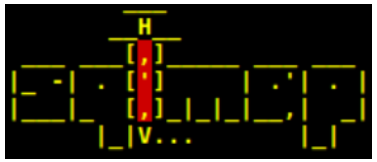
lazys3

webscreenshot.py

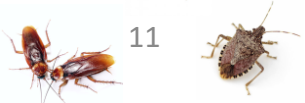
OWASP DirBuster

VPS!!
(ej. Digital Ocean)

BURPSUITE



SecLists



UNDEF Universidad de la Defensa Nacional IUA

Universidad de la Defensa Nacional

HACKERSPACE CÓRDOBA

Beneficios desde el punto de vista de las empresas…

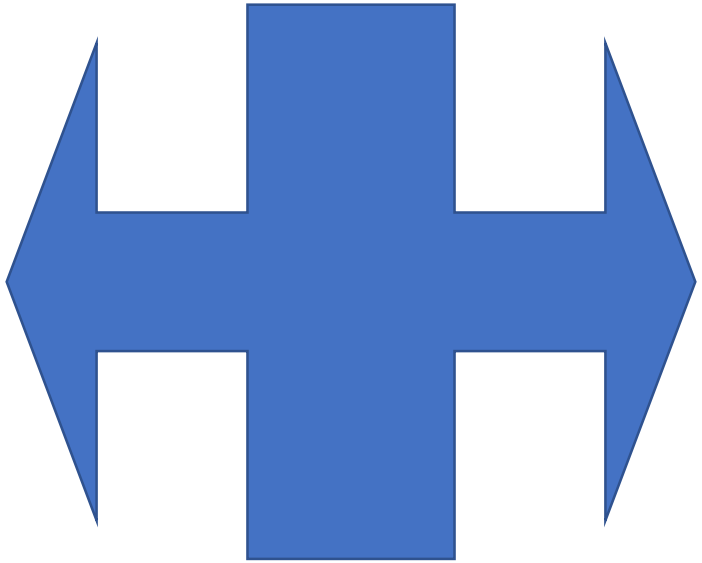
- Testeo más efectivo y veloz de bug
- Posibilidad de hacer un programa público
- Posibilidad de hacer un programa privado y elegir los hackers
- Posibilidad de establecer el alcance y evidencia necesaria para dar como válido un bug
- Posibilidad de establecer reglas de Non-disclosure
- Background check
- Posibilidad de establecer vínculos con los hackers para anclar ciclos de desarrollo de software
- Canal de retroalimentación que sirva de educación en bugs comunes para el equipo de desarrollo.
- Seguridad

UNDEF Universidad de la Defensa Nacional IUA
Universidad de la Defensa Nacional

HACKERSPACE CÓRDOBA

Variantes para las empresas…

- Recurrir a plataforma de Bug Bounty.
- Esquema organizado



- Programa de Bug Bounty propio.
- Total claridad de los targets
- Total claridad sobre la evidencia
- Información sobre qué forma de contraprestación

UNDEF Universidad de la Defensa Nacional IUA

Universidad de la Defensa Nacional

HACKERSPACE CÓRDOBA

Concepto de Triage de bugs reportados…

- Ya sea en Programa de Bug Bounty propio y vía plataforma de Bug Bounty, debe haber un proceso de triage.
- Evaluación de si el bug hallado cumple con alcance y evidencia necesarios.
- Verificación de que no se trata de un duplicado.

UNDEF Universidad de la Defensa Nacional IUA

Universidad de la Defensa Nacional

HACKERSPACE CÓRDOBA

Reflexiones para las empresas…

- Vencer miedos
- Abrazar una forma de trabajo ágil y efectiva
- Tener top-hacker de nuestro lado
- Descansar en una plataforma de bug bounty
- Conocer empresas que ya lo hacen

UNDEF Universidad de la Defensa Nacional IUA
Universidad de la Defensa Nacional

HACKERSPACE CÓRDOBA

Empresas que ya lo hacen…

- Verizon
- AT&T
- PayPal
- Xbox
- GM
- Snapchat
- Cisco
- Dropbox
- Apple
- Facebook
- Google
- Vimeo
- Twitter
- Github
- Uber
- Mercadolibre
- UN GRAN ETC.

UNDEF Universidad de la Defensa Nacional IUA
Universidad de la Defensa Nacional

HACKERSPACE CÓRDOBA

Mercadolibre y su política en Hackerone…

hackerone FOR BUSINESS FOR HACKERS HACKTIVITY COMPANY TRY H

Please consider that the bugs submitted through this directory page will/may not be eligible for bounties, and the invites into our private program are at the discretion of the MercadoLibre Security Team.

Responsible Disclosure

To encourage coordinated disclosure, MercadoLibre does not intend to initiate any legal action or law enforcement investigation against security researchers as long as they adhere to the following guidelines:

- Researchers will report details of a discovered security issue to Mercadolibre without making any information or details of the vulnerability public until mutual agreement is made or with the explicit authorization of MercadoLibre.
- Researchers will allow Mercado Libre reasonable time to resolve the issue before publishing any information or details about the vulnerability or other making such information generally known. Mercado Libre will do their our best to follow the HackerOne disclosure guidelines which committing to open communication, providing an initial response to the researcher within 30 days and providing a disclosure timeline to the researcher to be mutually agreed upon.
- Researchers will make all reasonable attempts in good faith to avoid destroying, stealing, modifying, damaging, violating or otherwise jeopardizing the personal data or privacy of any Mercadolibre's customer or Mercadolibre's data. This includes disrupting or degrading Mercadolibre's products and service to its customers.

The following are expressly prohibited and are not covered under the above Coordinated Disclosure Policy:

- Physical attacks against Mercado Libre employees, offices, and data centres.
- Social engineering of Mercado Libre employees, contractors, vendors, or service providers, including phishing.
- Pursuing vulnerabilities which send unsolicited bulk messages (spam).
- Pursuing vulnerabilities through the compromise of a Mercadolibre customer or employee account – (e.g. do not attempt

UNDEF Universidad de la Defensa Nacional IUA
Universidad de la Defensa Nacional

HACKERSPACE CÓRDOBA

Comentarios de cierre…

Hacker o empresa

- Animarse!
- Estudiar!
- Planificar!
- Hacer Networking!

UNDEF Universidad de la Defensa Nacional

HACKERSPACE CÓRDOBA

Preguntas/dudas?

UNDEF Universidad de la Defensa Nacional IUA
Universidad de la Defensa Nacional

HACKERSPACE CÓRDOBA

Contactos:

Eduardo Casanovas: ecasanovas@iua.edu.ar - @IngCasanovasOk

Carlos Tapia - ctapia@iua.edu.ar - @carlitostapia