RED BIRD

Seguridad Ofensiva

GAME OVER

- BugBounty Tips
- Herramientas
- Recursos

BUGBOUNTY

Los BugHunters son los mercenarios de la CiberSeguridad

BugBounty para Todos


BUGBOUNTY
GAME OVER

10 - Reportes 25

Introducción ¿BugBounty?

El “BugBounty” es un programa de recompensas el cual tiene como propósito premiar o reconocer a las personas/usuarios quienes lograron encontrar vulnerabilidades, fallos o Bugs en el software o hardware de las empresas, ya sean sus plataformas de servicios, productos de hardware o soluciones en software.

Los usuarios/personas que encuentran estas vulnerabilidades tienen una amplia experiencia y conocimientos, relacionados a las Pruebas de Penetración o Pentesting y las propias metodologías para realizar pruebas de penetración.

Para que los usuarios, puedan recibir algún tipo de recompensa primero deben pasar por un proceso como el siguiente:

1. Registrarse en algún programa o plataforma BugBounty
2. Identificar la vulnerabilidad y explotarla.
3. Documentar la vulnerabilidad (POC).
4. Reportar la vulnerabilidad.

Generalmente ese es el proceso a seguir en todos los programas BugBounty, sin embargo, también es importante tener en cuenta otros factores tales como:

- Las normas/reglas del programa BugBounty.
- La no difusión de la vulnerabilidad, hasta ser verificada y corregida.

Las normas son muy importantes, ya que estas indican los tipos de vulnerabilidades que la empresa busca en su programa BugBounty y cuáles no, los tipos de “ataques” permitidos y cuáles no, en resumen, son las reglas del programa. En cuanto a la no difusión, es una de las partes fundamentales y básicas en todo programa BugBounty, se ha de aclarar que esta parte está enfocada a no divulgar los datos técnicos que permitan a otros usuarios poder identificar y explotar esta vulnerabilidad.

Sin embargo, también existen X límites de tiempo, el los cuales, si no recibes una respuesta por parte de la empresa, ya una vez reportada, la vulnerabilidad se hace pública.

¿Merece la pena?

Los programas de BugBounty, son muy beneficiosos para ambas partes, tanto como para las empresas ya que mejoran la calidad y seguridad de su tecnología como para los participantes, quienes mejoran sus habilidades, y pueden recibir algún tipo de recompensa por “Hackear” de forma completamente legal.

Incluso, si eres un usuario, quien ya tiene práctica y conocimiento técnico obtenido por practicar en entornos controlados como laboratorios de pruebas de penetración o retos de Captura la Bandera (CTF) y quieres “hackear” los sitios web de grandes empresas, sin meterte en problemas legales, los programas BugBounty son los indicados.

¿Y dónde están las recompensas?

La parte fundamental de los programas de BugBounty son las recompensas y existen diferentes tipos de recompensas, de las cuales hablaremos rápidamente. Las recompensas pueden ser las siguientes:

1. Recompensas Monetarias
    a. Las que buscan todos, en estas puedes recibir dinero, la cantidad dependerá de varios factores, entre ellos, el tipo de vulnerabilidad o riesgo que representa la vulnerabilidad para la empresa, o si ya existe una cantidad fija.
2. Recompensas con Productos o Servicios
    a. Algunas empresas en lugar de pagar con dinero, regalan sus productos u ofrecen licencias premium de su software.
3. Recompensas y Reconocimientos
    a. Otras empresas otorgan algo que la mayoría de los Bug Hunters (Cazadores de Bugs) buscan y es el reconocimiento, ya sea por medio de algún certificado de logro o ser incluidos en algo llamado “Salones de la Fama”.
4. Recompensas con Trabajo
    a. No todas las empresas lo ofrecen, pero lo han hecho. Ofrecen un empleo para los Bug Hunters, ya sea en sus equipos de seguridad TI o como consultores en desarrollo e implementación de software, pero son raras las empresas que lo hacen.

Tipos de Programas BugBounty

Como tal, no existen tipos ya que todas son exactamente lo mismo en un principio, sin embargo, las podemos clasificar en 3 tipos, esto en base a la forma en que presentan el programa BugBounty.

1. **Plataformas de BugBounty**. Estas son las más populares, pues son sitios web, en los cuales las empresas, se registran y ofrecen sus programas BugBounty a una comunidad de Bug Hunters, estas plataformas suelen funcionar como intermediarios entre la empresa y el Bug Hunter. Tenemos por ejemplo a la plataforma HackerOne (www.hackerone.com).
2. **Programas BugBounty Propios de una empresa y públicos**. Estos son programas propios de las empresas, completamente ajenos a las plataformas BugBounty, por ejemplo el programa de BugBounty de Facebook, "BugBounty WhiteHat" (www.facebook.com/whitehat)
3. **Programas BugBounty Propios de una empresa, pero privados**. Al igual que el anterior, con la única diferencia en donde el Bug Hunter debe registrarse y satisfacer una serie de requisitos o experiencia para poder ser admitido o simplemente ser invitado por la empresa.

1 - Lo que debes saber antes de iniciar

Pues bien, hasta este punto conocemos de forma teórica los tipos de programas BugBounty así como las recompensas a las que podemos acceder gracias a estos. Sin embargo, antes de decidir iniciarte en el mundo del BugBounty debemos tener en cuenta una serie de puntos.

Estos puntos puedes tomarlos como consejos, en base a las vivencias de varios Bug Hunters que ya tienen más de 3 años laborando en el ámbito.

1.- BugBounty = Pentesting
El BugBounty a grandes rasgos son pruebas de penetración, es decir para poder participar en estos programas debes tener conocimientos sobre las pruebas de penetración.

2.- Pruebas de Penetración y Metodologías
Debes de tener con total claridad cuáles son las fases de una prueba de penetración, así como emplear y tener conocimiento de alguna metodología,

3.- Conocimientos Técnicos
Esta es una de las partes importantes, los conocimientos técnicos te permitirán desarrollar exploits, payloads o incluso tus propias herramientas o scripts. Dependiendo el tipo de tecnología la cual estas auditando serán los conocimientos, por ejemplo, si haces BugBounty en programas donde el objetivo son plataformas web, debes saber desarrollar o programar en lenguajes tales como: JavaScript, PHP, XML, etc.

4.- Dominar Herramientas
Hoy día, existe una gran infinidad de herramientas, algunas muy complejas, otras muy simples o básicas, lo importante es poder dominar en su totalidad un grupo selecto de herramientas, no es necesario usar 5 herramientas que explotan una vulnerabilidad, cuando puedes ser un experto utilizado una o dos.

5.- Corregir vulnerabilidades
Muy bien, ahora que encontraste una vulnerabilidad, la explotaste con éxito, creaste un reporte, puede que tengas un trabajo extra, si quieres aumentar tu recompensa o recibirla, es corregir la vulnerabilidad, para esto, funges como un consultor o asesor o directamente trabajas sobre el código y la corriges, entonces, así como es de importante saber explotar una vulnerabilidad, es importante saber cómo se corrige.

6.- No todo es Bueno
Desgraciadamente una de las situaciones que más tienden a repetirse y al mismo tiempo enfada a muchos Bug Hunters es cuando son ignorados y sus reportes no son atendidos a pesar de que la vulnerabilidad exista o no son recompensados por su trabajo.

Generalmente tiende a crearse estas situaciones:

1. Ignoren el reporte. En algunos casos, después de encontrar la vulnerabilidad y reportarla nunca revisas el reporte.
2. No hay ningún tipo de bonificación, ni las gracias. En ocasiones no te pagan, ni las gracias te dan por el trabajo.
3. Problemas técnicos para reproducir la vulnerabilidad. Por lo regular cuando reportas una vulnerabilidad y si esta no puede ser reproducida, no te pagan.
4. La vulnerabilidad ya fue reportada por otro Bug Hunter.
5. Recompensas muy mínimas.
6. Incumplimiento de pagos.
7. Pagos excesivamente lentos.
8. Requerimientos Excesivos e innecesarios. Algunas compañías, piden un reporte muy excesivo, tanto así que suelen compartir una guia sobre como debes de reportar las vulnerabilidades, una acción de tres o 5 pasos por mucho, ellos lo quieren en 20 pasos.

7.- Debes de leer las normas/políticas
Es de mucha importancia que leas las normas o políticas de los programas bugbounty todos son completamente diferentes. Las políticas o normas de los programas, son a grandes rasgos las reglas de la cacería de vulnerabilidades. Dentro de estas puedes encontrar información como:

1. Requerimientos Generales/Específicos.
2. Requerimientos Generales/Específicos del testeo.
3. Recompensas.
4. Objetivos dentro y fuera del Alance.
5. Vulnerabilidades Excluidas/Aceptadas.
6. Técnicas de explotación aceptadas y excluidas

8.- No todos los programas de BugBounty pagan

Dependiendo del programa, las recompensas son muy variables y el valor de la recompensa dependerá de la gravedad de la vulnerabilidad reportada.

Program	Launch date ↓	Reports resolved	Bounties minimum	Bounties average	
Ramp	03 / 2020	7	-	-	☆
Orion Labs Managed	03 / 2020	-	-	-	☆
Helium	02 / 2020	8	$25	$125	☆
Kindred Group Managed	02 / 2020	152	$150	$150	☆

9.- El BugBounty y el status de los Hackers

Aunque se pueda conseguir una recompensa, muchos de los bugs hunters realmente están más interesados por el status, poder decir que han descubierto una vulnerabilidad en las tecnologías de grandes empresas.

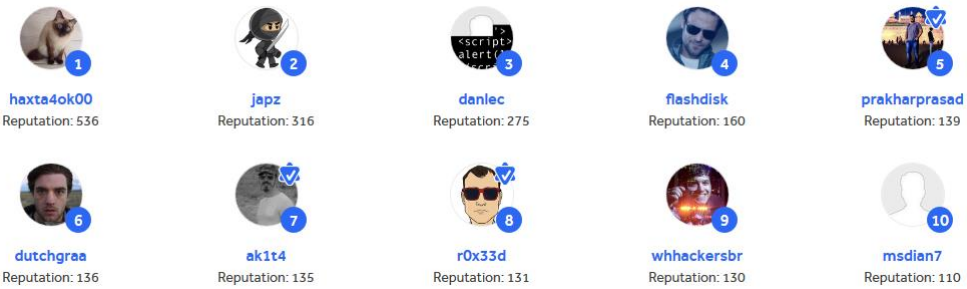
TOP-50 Researchers

Security Researcher	Helped Patch	Recommendations	Badges
calv1n	17416	37	12
Spam404	16363	69	11
login_denied	7926	76	8

TOP-50 VIP Researchers

Security Researcher	Helped Patch	Recommendations	Badges
dim0k	2404	21	10
Spam404	1580	69	11
Kenan	1133	6	8

Los investigadores de vulnerabilidades buscan incansablemente estar en las listas del Top 10 de los programas o plataformas de BugBounty. Por otro lado algunos realizan la práctica del BugBounty como un deporte.



10.- ¿Puedo vivir solo de BugBounty?
Muchos usuarios pueden ganar dinero cansado vulnerabilidades en programas BugBounty, incluso existen casos de jóvenes que se hicieron millonarios, pero la realidad es otra, requieres de una gran habilidad y ser muy constante, de forma simple, dedicarte 24/7 a buscar vulnerabilidades en los programas de BugBounty.

Se recomienda, que el BugBounty sea tomado como un pasatiempo o una forma de obtener ingresos extra.

11.- ¿Puedo ser millonario haciendo BugBounty?
Como lo mencionamos anteriormente, no decimos que no se pueda, pero es un proceso muy complicado y tardado. Es más favorable que el BugBounty sea visto como un pasatiempo o una forma alternativa para generar ingresos extras.

2 - Programas BugBounty

Los programas de BugBounty tienen como fin otorgar recompensas y reconocimientos a quienes descubren vulnerabilidades en sistemas, aplicaciones web, redes, etc. Hoy en día contamos con muchas empresas que toman la decisión de crear sus propios programas de BugBounty y abrirlos, compartirlos con la comunidad, para mejorar la detección y corrección de vulnerabilidades, las cuales puedan atentar contra la privacidad de sus usuarios o clientes, así como mejorar la calidad de la seguridad de la información de los mismos.

Los programas de BugBounty son necesarios hoy en día y muchos expertos consideran que en unos años las empresas deberán de contar con sus equipos de RedTeam, BlueTeam y programas BugBounty, esto debido a que no existe ningún sistema o aplicación completamente seguro, ni los mejores ingenieros ni las mejores metodologías de desarrollo de software, así como las buenas prácticas pueden asegurar que exista un sistema completamente seguro.

Incluso con los programas de BugBounty se espera persuadir a los cibercriminales a que en lugar de crear exploits y venderlos de forma ilegal, reporten la vulnerabilidad y el propio exploit.

También es el incentivo para la creación de nuevos modelos de negocio, como lo son las plataformas de BugBounty, las cuales tienen como fin ofrecer los servicios y soportes necesarios para aquellas empresas que no cuentan con los recursos, para crear su propio programa.

Programas de BugBounty Atractivos

Google Vulnerability Rewards Program

El programa de recompensas de vulnerabilidades de Google es uno de los más famosos y codiciados, los sitios que se encuentran registrados en este programa con: [Clic Aqui]

1. Google.com
2. YouTube.com
3. Blogger.com

Category	Examples	Applications that permit taking over a Google account [1]	Other highly sensitive applications [2]	Normal Google applications	Non-integrated acquisitions and other sandboxed or lower priority applications [3]
Vulnerabilities giving direct access to Google servers					
Remote code execution	*Command injection, deserialization bugs, sandbox escapes*	$31,337	$31,337	$31,337	$1,337 - $5,000
Unrestricted file system or database access	*Unsandboxed XXE, SQL injection*	$13,337	$13,337	$13,337	$1,337 - $5,000
Logic flaw bugs leaking or bypassing significant security controls	*Direct object reference, remote user impersonation*	$13,337	$7,500	$5,000	$500
Vulnerabilities giving access to client or authenticated session of the logged-in victim					
Execute code on the client	Web: *Cross-site scripting* Mobile / Hardware: *Code execution*	$7,500	$5,000	$3,133.7	$100
Other valid security vulnerabilities	Web: *CSRF, Clickjacking* Mobile / Hardware: *Information leak, privilege escalation*	$500 - $7,500	$500 - $5,000	$500 - $3,133.7	$100

Microsoft Online Services Bug Bounty program

El programa de BugBounty de Microsoft. [Clic Aquí]

Security Impact	Report Quality	Severity			
		Critical	*Important*	*Moderate*	*Low*
Remote Code Execution	High Medium Low	$20,000 $15,000 $10,000	$15,000 $10,000 $5,000	$0	$0
Elevation of Privilege	High Medium Low	$8,000 $4,000 $3,000	$5,000 $2,000 $1,000	$0	$0
Information Disclosure	High Medium Low	$8,000 $4,000 $3,000	$5,000 $2,000 $1,000	$0	$0
Spoofing	High Medium Low	N/A	$3,000 $1,200 $500	$0	$0
Tampering	High Medium Low	N/A	$3,000 $1,200 $500	$0	$0
Denial of Service	High/Low	Out of Scope			

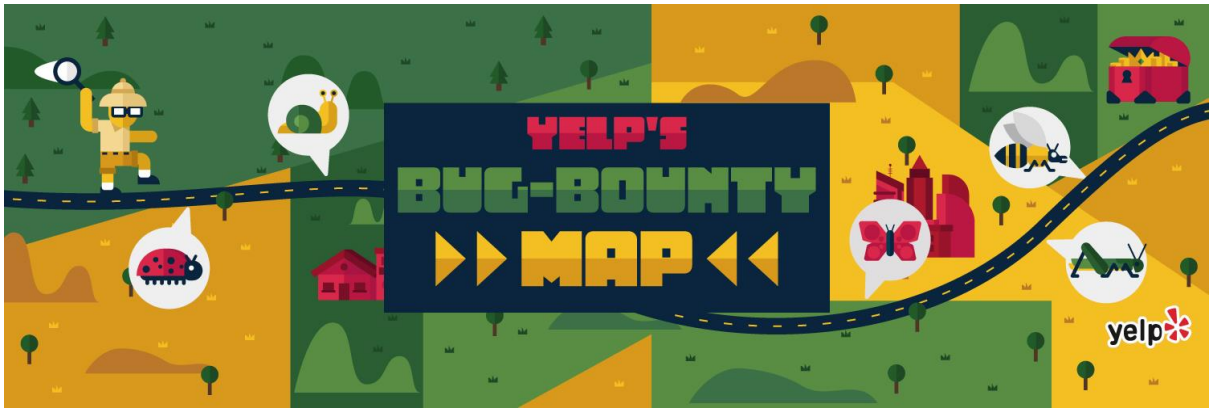
Facebook WhiteHat BugBounty Program

Facebook también maneja su programa de recompensas de BugBounty, actualmente se tiene en consideración que el pago mínimo es de $500 dólares y no existe límite para las recompensas [Clic Aquí]

Productos o servicios	Válidos	No válidos
Facebook	Sitios web: facebook.com, fb.com, fb.me, messenger.com, thefacebook.com y accountkit.com Aplicaciones: Administrador de anuncios, Facebook, Facebook Lite, Workplace de Facebook, Grupos, Hello, Mentions, Messenger, Moments, Administrador de páginas, Paper (de Facebook) y Work Chat	Sitios web: events.fb.com, fbsbx.com, investor.fb.com, media.fb.com, newsroom.fb.com, research.fb.com, search.fb.com, work.fb.com, research.fb.com, madebykorea.fb.com Aplicaciones: Facebook para Blackberry y Facebook para Windows
Instagram	Sitios web: instagram.com Aplicaciones: Boomerang, Hyperlapse, Instagram y Layout	Sitios web: blog.instagram.com
Internet.org	Sitios web: freebasics.com e internet.org Aplicaciones: Free Basics	

Yelp's Bug-Bounty Map

Tal vez Yelp no es muy conocido por algunos usuarios, pero tiene una gran cantidad de sitios donde podemos buscar vulnerabilidades, la recompensa mínima por exploit es de $100 Cuenta con un mapa donde comparte todas sus plataformas registradas en el programa bugbounty [Clic Aqui]



Lo anterior son solo algunos de los programas de recompensas por vulnerabilidades que han destacado por sus lucrativos pagos, recompensas muy interesantes. Sin embargo, no son los únicos, existen muchas empresas que no tienen la capacidad de poder establecer un programa BugBounty, entonces se registran a plataformas de BugBounty que administran casi todos los aspectos técnicos.

3 - Plataformas BugBounty

Las plataformas de BugBounty son sitios, en los cuales las empresas se registran y crean sus programas de BugBunty, de hecho, en estas plataformas, es donde se encuentran la mayoría de las empresas, con sus diversas recompensas.

Plataformas BugBounty Públicas/Registro	
HackerOne	https://www.hackerone.com/
Bugcrowd	https://www.bugcrowd.com/
BountyFactory	https://bountyfactory.io/
Intigriti	https://intigriti.be/
Bugbountyjp	https://bugbounty.jp/
Safehats	https://safehats.com/
BugbountyHQ	https://www.bugbountyhq.com/
Hackerhive	https://hackerhive.io/
Hackenproof	https://hackenproof.com/
Hacktrophy	https://hacktrophy.com/
CESPPA	https://www.cesppa.com/

Plataformas de BugBounty Privadas/Basadas en Invitaciones	
Synack	https://www.synack.com/red-team/
Cobalt	https://cobalt.io/
Zerocopter	https://zerocopter.com/
Yogosha	https://www.yogosha.com/
Bugbountyzone	https://bugbountyzone.com/
Antihack.me	http://www.antihack.me/
Vulnscope	https://www.vulnscope.com/

4 - CTF y Entornos Controlados

Uno de los consejos importantes a tener en cuenta, es la constancia, práctica y ser muy autodidacta, en todos los aspectos de la vida y en Ciberseguridad no existen las excepciones ni mucho menos.

Muchos expertos del ámbito de pruebas de penetración aseguran ciertamente que se debe practicar de forma constante en entornos controlados. En nuestro Blog compartimos una recopilación de más de 30 sitios CTF y laboratorios de pruebas de penetración que recomendamos, y aunque no son todos los que existen, tienden a ser los más interesantes.

No son las únicas plataformas en las cuales puedes practicar, y mejorar tus habilidades, existen laboratorios muy específicos.

Principales Plataformas de Entrenamiento Recomendadas					
Pentesterlab	XSS Game	Hack This Site	Root-Me	HackTheBox	Hack Me
CTF 365	Google Gruyere	OWASP Juice Shop	Hack Yourself First	flAWS Cloud	bWAPP

5 - Retroalimentación en Twitter

Ya son varios posts que hacemos, tanto en nuestra cuenta de instagram como en nuestra página de Facebook.

Es importante estar todo el tiempo, actualizado con nuevas técnicas, exploits, vulnerabilidades y herramientas que van apareciendo para tener un repositorio de “trucos” para hacer nuestro trabajo.

Para lograr tener una continua fuente de información, de actualizaciones, podemos contar con la red social Twitter.
Twitter es la red social de los Micro-Blogs donde podemos encontrar información relacionada al BugBounty y otros aspectos muy interesantes. Para poder tener acceso a esa información debemos hacer un seguimiento de los Hashtag, claro solo los hashtags adecuados.

Nosotros te recomendamos busques los siguientes Hashtag en Twitter:

#bugbountytip #bugbountytips #pentesting #hackingtools #hackingtips #redteaming #redteamingtips #pentestingtips

Evidentemente no son los únicos hashtags que puedes seguir, existe una gran cantidad, todo depende de la especialización que tengas

6 - Aprende de otros BugHunters “Consejos/Tips”

Las vulnerabilidades más buscadas y presentes en programas BugBounty

Vulnerabilidades más presentes en Programas de BugBounty WEB

XSS	SQL INJECTION	SSRF	LFI/RFI
XXE	RCE	OPEN REDIRECT	TEMPLATE & CONTENT INJECTION
CSRF	IMPROPER ACCESS CONTROL	INFORMATION LEAK	BY PASS

En plataformas de BugBounty como lo es HackerOne puedes reportar hasta 150 diferentes tipos de vulnerabilidades

Lee todo el tiempo

Es importante estar estudiando, un consejo fundamental es leer y estudiar todo lo que puedas, no importa si es contenido para principiantes o para expertos, debes leer, solo de esta forma, podrás apreciar como, existen cientos de formas, para explotar una vulnerabilidad; como consejo utiliza las técnicas de búsqueda avanzada de Google para buscar contenido con mayor precisión.

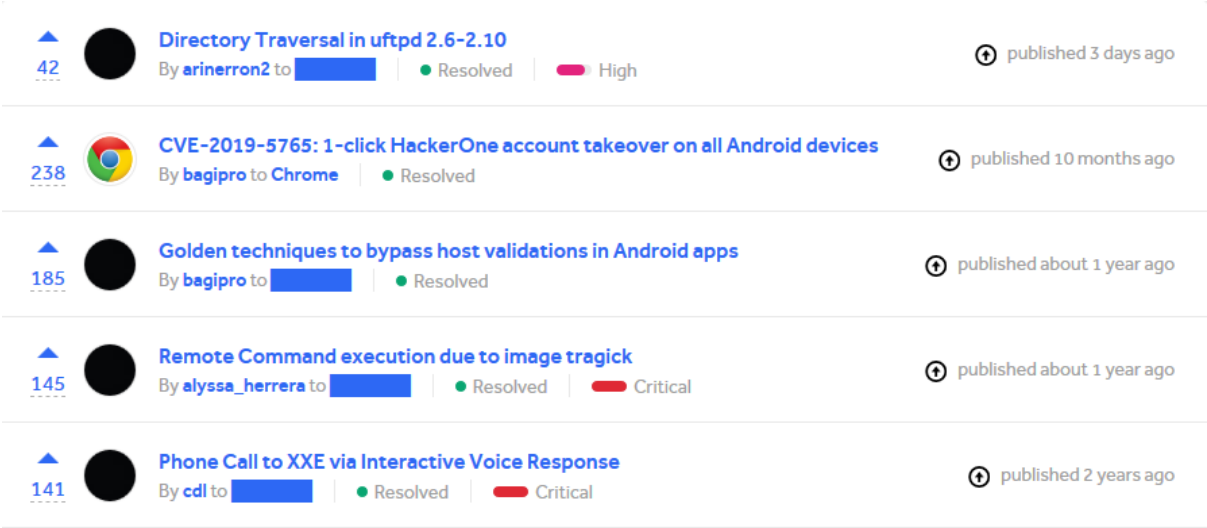
Estos son los Blogs o Foros recomendados;

- ✓ RedBird Blog
- ✓ El Lado Del Mal
- ✓ HackPlayers
- ✓ Underc0de
- ✓ BlackPloit
- ✓ PortSwigger Research

WriteUps & PoC

Los writeups y los PoC (Pruebas de Concepto) son claves para tus estudios, a grandes rasgos son los reportes, liberados creados por pentesters o bug hunters donde explican paso a paso cómo fue que lograron identificar la vulnerabilidad, explotarla y las herramientas empleadas.

Cada reporte dependiendo de la plataforma tiene una fecha en la cual este se mantiene en privado y al finalizar esta fecha pasa a ser público. Sus beneficios, son muchos, pero el más destacable, es que puedes aprender trucos totalmente nuevos, y formas de hacer el trabajo.



Algunos Bug Hunters y Pentesters tienen sus propios blogs, muchos otros escriben libros (por favor compra sus libros). Ahora ¿Dónde puedo tener acceso a los PoC o WriteUps?

1. Plataformas de BugBounty, revisando los reportes.
2. En los Foros.
3. En los sitios donde comparten vulnerabilidades y exploits.

Te compartimos el siguiente lInk de GitHub donde encontraras una gran cantidad de PoC y Writeups
Link: **Awesome Writeups and POCs by. dhaval17**

Este repositorio en GitHub tiene una gran colección de PoCs y Writeup de HackerOne clasificados en base al tipo de vulnerabilidad o tipo de programa.
Link: **HackerOne Reports: Top disclosed reports from HackerOne by. reddelexc**

Libros Recomendados

En la mayoría de las ocasiones nos solicitan recomendaciones de libros tanto digitales como físicos con los cuales podemos incrementar considerablemente nuestras habilidades. Pues bien, en la actualidad existen cientos de libros por los cuales podemos iniciar, sin embargo, nosotros te recomendamos los siguientes:

1. Real Word Bug Hunting [LINK]
2. Bug Bounty Hunting for Web Security: Find and Exploit Vulnerabilities in Web Sites and Applications [LINK]
3. Hacking: The Art of Exploitation [LINK]
4. Rtfm: Red Team Field Manual [LINK]
5. The Hacker Playbook: Practical Guide To Penetration Testing [LINK]
6. Black Hat Python: Python Programming for Hackers and Pentesters [LINK]
7. Fuzzing: Brute Force Vulnerability Discovery [LINK]

En nuestro Blog compartimos una recopilación de eBooks, de diversos temas, todas en su mayoría centrados en la Seguridad Informática, Seguridad ofensiva. [LINK]

7 - Herramientas y Recursos

En esta sección tenemos muchas cosas para compartir HERRAMIENTAS y RECURSOS online que debes tener si o si en tu repertorio al igual que una serie de consejos de expertos en el ámbito de la ciberseguridad.

Antes que nada se tiene que tener en claro los siguientes aspectos:

- Las herramientas de BugBounty son exactamente las mismas herramientas de Pentesting.
- No es necesario manejar cientos de herramientas. “En mi experiencia he manejado más de 8 herramientas para explotar vulnerabilidades XSS, pero lo mejor es saber manejar una o dos, y poder sacar el máximo potencial” - Drok3r

Nuestra serie “Armas Para Hacking”

En nuestro blog en RedBird tenemos una serie llamada Armas Para Hacking la cual tiene un solo propósito, recopilar nuevas herramientas para pruebas de penetración, cada lunes compartimos un nuevo capítulo con diversas herramientas o exploits.

[Armas Para Hacking]

Sitios Online de Herramientas para Pruebas de Penetración

Tener un repositorio de herramientas, para diversos trabajos es parte del trabajo. Cada X tiempo salen nuevas herramientas, algunas tienen actualizaciones otras mejoran sus procesos.

⚒ Sitios Online de Herramientas para Pruebas de Penetración ⚔			
HackingResources - CyberSecurity	PentestTools - Penetration Testing Tools.	CyberPunk	KitPloit
https://code.nsa.gov/	Concise Courses | Hacker Tools & Growth Marketing Tools	Penetration Testing • Information Security	Armas para Hacking

Recursos Online

Los recursos ONLINE tienden a ser herramientas que nos pueden ser de ayuda para nuestros trabajos de Pruebas de Penetración, en su momento, en RedBird teníamos de forma interna una discusión sobre un tema un tanto peculiar, **¿Se pueden realizar pruebas de penetración, sin la necesidad de descargar herramientas en nuestros equipos?**

Al comienzo, se pensó en juego y en la problemática que tuvimos en una auditoría “flash” o muy rápida, en la cual no contábamos en ese momento con las herramientas adecuadas y a disposición para el trabajo. Sin embargo en busca de soluciones, nuestro equipo CyberSecurityRecon nos propuso intentar realizar el trabajo aprovechándonos de las herramientas online.

“El futuro de las tecnologías y los servicios está 100% enfocado en la nube”

De este modo, nos dimos a la tarea de crear un apartado al que llamamos “**Recursos Online**” sin embargo este presenta una serie de inconvenientes, los cuales explicaremos a fondo en un futuro.

GitHub

Herramientas, exploits, vulnerabilidades, etc.
Link: https://github.com

Pastes

Son un sitio muy interesante donde podemos encontrar información muy interesante, en algunos casos DataLeaks, Exploits y Payloads.

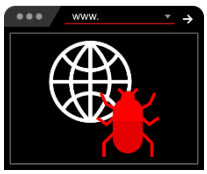
RedBird PasteBin
En nuestra cuenta de PasteBin tenemos una recopilación de Payloads para explotar vulnerabilidades XSS, Dorks para Google Hacking con los cuales podemos encontrar sitios web vulnerables, dorks de Shodan y mucho más.
Link: https://pastebin.com/u/RedBirdTeam

Exploit Wordpress 5.3 - User Disclosure
Payload XSS - Steal Cookie
JavaScript Keylogger Code
Dorks Para Detectar Servidores
CookieLogger.php | Codigo para robar Coockies
SQL INJECTION | WAF Bypass
Com Fabrik #Dork y #Exploit - ¿Upload webshell?
Dorks para encontrar Botnets
Payloads LFI
20 mil Dorks | 3er
DORKS | 2do
DORKS | 1er
Shodan Filtros para búsquedas.
Lista de E-Mails utilizados en Fraudes (eBay,Facebook, Amazon)
33737 Dorks (LISTA)
Bangladesh Cyber Army Shell (BCA Private Shell)
Default User and Pass For Services Unhash
Cámaras Foscam y dispositivos de red claves codifi...
Bypass Login Web - SQL Strings List
Introducción a los troyanos en PHP
Phishing Técnica: Tab Napping Short Code
XSS PAYLOAD CROSS SITE SCRIPTING LIST
Payloads XSS Filter Bypass List
Más de 4000 Dorks - SQL INJECTION

Sitios recomendados
Link: https://pastebin.com
Link: https://pastelink.net/

Recopilar información de Sitios Web (Information Gathering)

La siguiente recopilación de herramientas online, con las cuales podemos recopilar información de sitios web, como lo puede ser el tipo de CMS, versiones y tecnología con la cual fue desarrollado el sitio web.



- ✓ Sitio 1: https://w3techs.com/sites (Escáner de sitios Web)
- ✓ Sitio 2: https://urlscan.io/ (Escáner de URL)
- ✓ Sitio 3: https://sitecheck.sucuri.net/ (Escáner de SUCURI)
- ✓ Sitio 4: https://www.wpthemedetector.com/ (WordPress)
- ✓ Sitio 5: http://onlinewebtool.com/ (Conjunto de Herramientas de Análisis Web)
- ✓ Sitio 6: https://wpsec.com/ (Escáner de Vulnerabilidades en Sitios WordPress)
- ✓ Sitio 7: https://pentest-tools.com/home (Conjunto de Herramientas de Pentesting Online)

Vulnerabilidades, Exploits, Payloads y PoC

Sitios en los cuales puedes encontrar vulnerabilidades, exploits, PoC y mucha más información.

💣 **Sitios Web de Vulnerabilidades y PoC** 💣			
Exploit Database	https://vulmon.com/	CVE security vulnerability database	Vulnerabilidades | INCIBE-CERT
Exploit Collector	https://insecure.org/	Homepage | CISA	http://www.exploit4arab.org/

Motores de Búsqueda recomendamos para Pruebas de Penetración

Los mejores motores de búsqueda, para la recopilación de información, algunos de ellos nos facilitan la búsqueda de Exploits, fugas de información y vulnerabilidades

🔍 **Motores de Búsqueda para Pruebas de Penetración** 🔎			
Censys	Greynoise	https://zoomeye.org/	https://fofa.so/
https://onyphe.io/	https://app.binaryedge.io/login	https://hunter.io/	https://www.shodan.io/

8 - Metodologías de Pruebas de Penetración

OWASP (*Open Web Application Security Project*)

Es un proyecto abierto dedicado a la investigación de vulnerabilidades en aplicaciones web, desde la documentación de todas las vulnerabilidades, las diversas técnicas de explotación, desarrollo de herramientas, exploits hasta las formas de como corregir y prevenir dichas vulnerabilidades. Actualmente cuentan con un Top 10 de vulnerabilidades en aplicaciones web y una guía de pruebas de penetración.

Sitio Oficial de OWASP [www.owasp.org]
Guía de Pruebas de Penetración [LINK]
Top 10 de Vulnerabilidades OWASP en Español [LINK]

OSSTMM (*Open Source Security Testing Methodology Manual*)

El Manual de Metodología de Pruebas de Seguridad de Código Abierto es una metodología completa para pruebas de penetración y seguridad, análisis de seguridad y la medición de la seguridad operacional para construir las mejores defensas de seguridad posibles para su organización.

Sitio [LINK]
Guía OSSTMM [LINK]

PTES (*Penetration Testing Execution Standard*)

El estándar de ejecución de pruebas de penetración consta de siete (7) secciones principales. Estos cubren todo lo relacionado con una prueba de penetración, desde la comunicación inicial y el razonamiento detrás de un pentest, pasando por la recopilación de inteligencia y las fases de modelado de amenazas donde los evaluadores trabajan detrás de escena para obtener una mejor comprensión de la organización probada, a través de la investigación de vulnerabilidades, explotación y post explotación, donde la experiencia técnica en seguridad de los probadores juega y se combina con la comprensión comercial del compromiso, y finalmente con la presentación de informes, que captura todo el proceso, de una manera que tiene sentido para el cliente y proporciona el más valor para ello.

Sitio [LINK]
Guia PTES [LINK]

9 - Guía ISO 29147

La guía ISO 29147 establece como las organizaciones, empresas o gobiernos puedes integrar y gestionar la divulgación de vulnerabilidades en sus procesos comerciales normales.

ISO 29147 proporciona pautas para la divulgación de vulnerabilidades potenciales en productos y servicios en línea. Detalla los métodos que un proveedor debe usar para abordar los problemas relacionados con la divulgación de vulnerabilidades.

- Proporciona pautas para los proveedores sobre cómo recibir información sobre posibles vulnerabilidades en sus productos o servicios en línea,
- Proporciona pautas para los proveedores sobre cómo difundir información de resolución sobre vulnerabilidades en sus productos o servicios en línea,
- Proporciona los elementos de información que deben producirse a través de la implementación del proceso de divulgación de la vulnerabilidad de un proveedor, y
- Proporciona ejemplos de contenido que deben incluirse en los elementos de información.

A principios del 2019 en nuestra página en Facebook habíamos compartido un post sobre esta guía donde explicamos un poco sobre esta y su función. Después de haberla compartido una serie considerable de usuarios, desconocían de su existencia y los beneficios. Te recomendamos encarecidamente que cuando tengas tiempo la estudies. Da clic en el icono para descargar.

DESCARGA

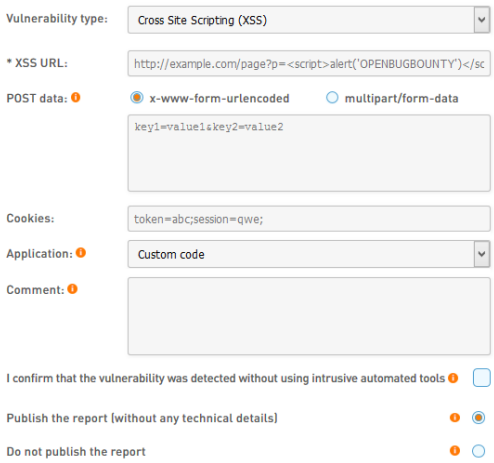
10 - Reportes

Los reportes son extremadamente importantes en el ámbito, tener conocimiento de su redacción, así como las partes que lo conforman son de mucha importancia.

Sin embargo, debes de saber, que ya no es tan necesario saber cómo hacer un reporte ¿Por qué?

Las plataformas de BugBounty ya cuentan con un formulario interactivo el cual solo debes llenar con los datos solicitados y listo. El contenido del reporte dependerá del tipo de vulnerabilidad y de los requisitos solicitados por la empresa, generalmente las partes de un reporte son:

1. El objetivo o software vulnerable.
2. El tipo de vulnerabilidad.
3. Una estimación del riesgo que representa la vulnerabilidad.
4. La prueba de concepto (POC) - Es importante destacar esta sección ya que debes ser lo más claro posible, ya que en este apartado describiremos los pasos de como llegaste a esa vulnerabilidad, las herramientas empleadas y como puede ser replicada.



✓ Herramienta | Generador de Reportes
Link: https://github.com/fransr/template-generator
✓ Ejemplo de Reporte de Pruebas de Penetración
Link: Sample Penetration Test Report
✓ Ejemplo de Reporte de Pruebas de Penetración
Link: PENTEST REPORT

Muchas gracias por leer nuestro e-book, esperamos te sea de gran ayuda, si nuestro trabajo es útil para ti, estaríamos muy agradecidos si nos ayudas dándonos tu sincera opinión en nuestra pagina de Facebook, no tienes idea lo mucho que nos ayudas.

¿Tienes dudas?
Ponte en contacto con nosotros
redbirdoficial@protonmail.com

¿Quieres recibir contenido especial?
Responde nuestro pequeño cuestionario
Cuestionario

Nuestras Tiendas Online

Leanpub

Leanpub – Beneficios
✓ Pagas el Precio que Quieras
✓ Actualizaciones Gratuitas

payhip

PayHib - Beneficios
✓ Ofertas mensuales
✓ Gran Variedad de Contenido

RED BIRD
Seguridad Ofensiva

Twitter | Facebook | Instagram | Blog