LFG!

FORMING A BUG BOUNTY HUNTING PARTY

HARRISON RICHARDSON (RSON)

WHO I AM NOT

HIGH-SPEED OPERATOR

I am NOT a super secret NSA hacker/operator who's here to teach you how to break into the Pentagon

"MILLION DOLLAR" HACKER

I am NOT a 1337 hacker who crush you all at any CTF when I'm not racking up fully automated $10k bugs

100X CODER (ONLY VIM)

I am NOT a 100x coder that knows every langage, built my own compiler, and actually uses vim as their IDE

WHO I AM

I ♥ BUG BOUNTY HUNTING

I am someone who genuinely loves the idea of being able to legally “hack” a company, get paid for it. It’s easy to put 10,000 hours in when it doesn’t feel like work.

UNIQUE CAREER PATH

I have worked in a wide range of security jobs, including federal & civilian, offensive & defensive, freelance & traditional, with some consulting and sales for good measure.

PASSION FOR TEACHING

I get an enormous amount of joy and purpose from sharing my skills with the community and watching members of that community succeed.

YOUTUBE.COM/@R5ON_LIVE

GITHUB.COM/R-5ON

"I WOULD *LOVE* TO WORK IN CYBER SECURITY, BUT THERE'S NO WAY I'M SMART ENOUGH..."

— HARRISON RICHARDSON (2013)

WORKSHOP OVERVIEW

PURPOSE

Build a formal methodology for forming a group of like-minded bug bounty hunters to collaborate with.

WHY?

Working with a group *dramatically* increases your chances of long-term success.

I get private messages 5+ times a week from aspiring researchers who don't know where to start.

TAKE AWAYS:

- Repeatable Process to Form a Balanced Group
- Skills & Tools Needed to Effectively Collaborate
- Ways to Maximize Return on Investment (ROI)
- My Full Bug Bounty Hunting Methodology
- New Bug Bounty Hunting Friends!

LET'S FORM OUR GROUPS!

We will be splitting up into groups of six (give or take) based on three criteria.

Can anyone guess what the first and most important criteria is?

EXERCISE 1

YOUR DEFINITION OF "SUCCESS"

What are your goals, and how can you use Bug Bounties to achieve them?

In order to create win-win scenarios collaborating with other bug bounty hunters, you **must** be sure that your goals are aligned.

What's worse, some goals are incompatible with other goals. If researchers with incompatible goals try to hunt together, one will eventually be pulled further away from accomplishing their goal.

HOW YOU HUNT

Someone who only tests for Race Conditions as part of a research project working with someone who wants passive income

WHEN YOU HUNT

Someone who works as a full-time developer learning AppSec at night working with someone who sprays for new CVE's when they drop

WHY YOU HUNT

Someone who needs to make $10k for medical bills working with someone interested in casually learning in their free time

MY VERSION OF SUCCESS

1 LEARNING

Bug bounties allow you to legally practice and learn offensive security techniques against live, real-world applications

2 PERSONAL BRAND

Building a positive personal brand in the bug bounty community is a fantastic way to open doors in all aspects of cybersecurity

3 ADVANCE CAREER

To be successful in bug bounties, you must have a great “toolkit” of real-world skills that can provide a lot of value to large organizations

4 POSITIVE IMPACT

Your bug bounty submission, especially to a small business, could mean the difference between their success and bankruptcy

5 MAKE MONEY

Not everyone can make good money with bug bounties, but there is almost no barrier of entry or earnings cap

6 FUN & RELAXING

There’s nothing better then a Flow State, and many find it easy to find that state with some good music and bug bounties

CORE GROUP TYPES

BIG MONEY

Is your **primary goal** to make money through bug bounties?

CYBER PROFESSIONAL

Do you want to leverage bug bounties to start or advance your career in cybersecurity?

CONTENT CREATOR

Do you want to leverage bug bounties to build your personal brand?

EARN WHILE YOU LEARN

Do you want to use bug bounties as a controlled way to learn offensive security?

DECISION POINT

1/4

Take a few minutes to meet the other members of your group! Share why you chose this group and a bit about your experience.

Do you feel like your goals are aligned? Does anyone feel like they ended up in the wrong place?

BALANCING THE TEAMS

Before we move on, we want to make sure our teams are balanced based on skill level, work experience, and passion for a specific hunting style.

EXERCISE 2

OFFENSIVE OR DEFENSIVE

Bug bounty hunting requires a *wide* range of skills and knowledge. Working with researchers that have an opposite and complementary skillset naturally develops feedback loops that help both participants grow exponentially.

RED TEAM

Knows how an attacker thinks. Can identify vulnerabilities and effectively articulate the impact of weaponizing that vulnerability

BLUE TEAM

Understands how applications are built, how they work, and how security teams apply controls to protect the application's data

EXPERIENCE LEVELS

All bug bounty researchers can be put into one of three categories based on experience level. NOTE: Hunting groups do NOT need to have anyone in the “Mastering” phase, they simply need ONE researcher in the “Applying” phase

MASTERING

Hunters at the “Mastering” phase have found some level of success with bug bounties and are comfortable teaching some bug bounty topics

APPLYING

Hunters at the “Applying” phase are able to perform bug bounty hunting on their own and answer basic questions about the steps they are taking

LEARNING

Hunters at the “Learning” phase are not able to perform bug bounty hunting on their own but they have a basic understanding of web technology and are eager to learn

LET'S ASSIGN GROUP ROLES!

Now that we have our teams aligned by their goals and well balanced, we need to define how we will work together. Formalized roles make this easier!

EXERCISE 3

TEAM ROLES

AUTOMATION

SUPPORT

RED TEAMER

HUNTER

MENTOR

LEADER

BLUE TEAMER

HUNTER

SCRIBE

SUPPORT

TEAM DYNAMICS

MENTORS SUPPORT EVERYONE

Mentors do less active hunting, spending most of their time supporting other roles, answering questions, and removing blockers

RED TEAMER LEARNS DEFENSE

When a Red Teamer sees unusual behavior or needs insight into how an application works, they reach out to a Blue Teamer

BLUE TEAMER LEARNS OFFENSE

When a Blue Teamer is unsure how an attacker would approach a specific technology or workflow, they reach out to a Red Teamer

TEAM DYNAMICS

SCRIBE DOCUMENTS & LEARNS

Scribe is the least experienced, supports and maintains documents for all other roles, as well as conducting automated scanning

AUTOMATION ENG. SOLVES PROBLEMS

Automation engineers build scripts that automate time-consuming and/or challenging workflows the team faces while hunting

HUNT TOGETHER, WIN TOGETHER

While the majority of the team's hunting will probably be async, hunting live as a full team = HUGE exponential growth

ROI BY ROLE

MENTOR

Mentor collaborates on most submissions without doing the bulk of the work (more passive income), learns from a wide range of questions

HUNTERS

Hunters learn from each other's unique skillset, grow quickly, and find bugs that specialized researchers miss

SCRIBE

Scribes learn from experienced researchers, as well as by taking notes, and collaborate on some reports

AUTOMATION

Automation collaborates on most submissions without doing active hunting, spends a lot of time developing async in flow state

IDEAL TEAM OF SIX

MINIMUM SKILLS NEEDED

DECISION POINT

2/4

Talk with your new team and decide on roles for each member. Be sure to share why you chose your role, that insight will be helpful to other members of your group!

LET'S PLAN OUR HUNT!

We now have balanced teams of bug bounty hunters with clearly defined roles and responsibilities. Each member also knows how to bring and get value from their group by working together. All that's left is "How?"

EXERCISE 4

HUNTING STYLES

RECON HEAVY

Hunters do a wide range of automated scanning to discover hidden domains, endpoints, and/or attack vectors that other researchers have not targeted

SAAS APP DEEP DIVE

SaaS apps are almost always highly complex with authentication and multiple roles and/or access control systems. Hunters look for logic flaws

FUTURE BUGS

Don't just aim for where your target is, aim at where it is going. When a domain is spun up, a new feature is added, or a new CVE drops, these hunters go to work

RECON HEAVY

PROGRAMS WITH A WIDE SCOPE

This style of hunting focuses on finding the targets and vulnerabilities that others miss

Programs with a wide open scope (Tesla, DoD) are the best option for groups that chose this strategy

Programs that have several wildcard domains are also great targets for this strategy

Bugs are less consistent, but groups typically find multiple bugs from a single undiscovered target

This style of hunting is the closest to how real-world attackers target organizations (w/o social engineering)

Automated tools like Amass and Nuclei are mandatory for this style of hunting

Recon Heavy hunting is a great option for groups with less experienced members

SAAS APP DEEP DIVE

SOFTWARE AS A SERVICE (SAAS)

SaaS companies provide customers with a web application to manage a complex system or process.

PROGRAMS W/ A SINGLE LARGE APP

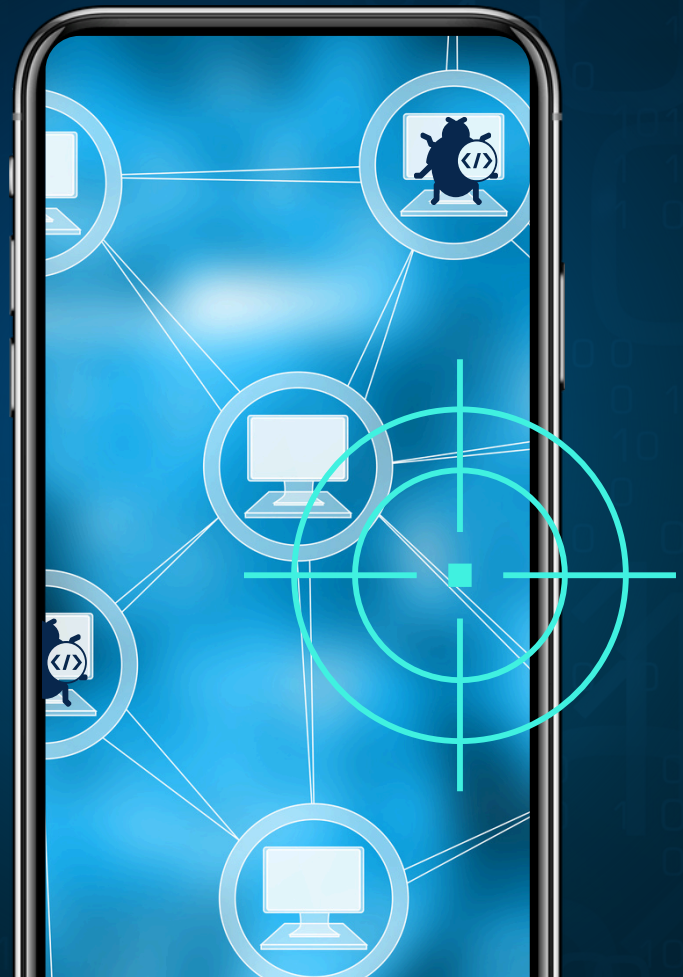
This style of hunting is slow, methodical, and tedious. However, it is also the best way to get consistent bugs

Hunters start by learning everything they can about the SaaS company's core application and offerings

All SaaS apps have authentication and most have complex access control systems, making them perfect for testing IDORs and ACVs

SaaS apps are changing constantly, with new bugs being introduced every day

This style is perfect for teams with more blue team experience, especially for developers with experience on the tech stack



FUTURE BUGS

ALL PROGRAMS, ALL PLATFORMS

This style of hunting requires the group to use a wide range of automation systems to identify various changes

The success of this team is dependent on their speed and technical expertise

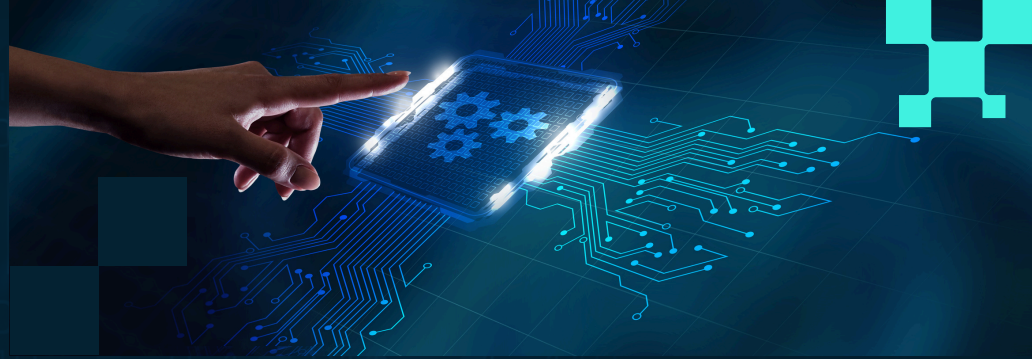
When new public programs launch, the group is notified and swarms to find the bugs before others

When a new CVE is released, the group builds a tool to scan a wide range of targets for this new bug

When a new domain is discovered or feature is released, the team aims to be the first to test it

This style of hunting is entirely dependent on the decision of others

This style is perfect for hunters who want to maximize income but terrible for Security Professionals



DECISION POINT

3 / 4

Decide as a group what hunting style you will use and find a program to match. Remember that these are just examples, feel free to get creative and come up with your own styles!

COMMUNICATION STRATEGIES

SYNCHRONOUS

The group meets at a specific time and place, either online or in person, to work together as a team and find bugs. A member w/ the Mentor role leads the hunting while others support

ASYNCHRONOUS

Each member of the group hunts on a specific target at different times. As new information is gathered, it is shard with the group and another member uses that info to inform their next steps

SYNCHRONOUS TOOLS

ZOOM

Great collaboration tools and good performance, but the free version only allows for meetings up to 45 minutes.

★★★

DISCORD VC

Very easy to use, decent performance, great collaboration tools, and has no time limit. Can be used for async as well.

★★★★★

GOOGLE MEET

Great performance, decent collaboration tools, and free meetings up to an hour. One on one meetings can go up to 24 hours.

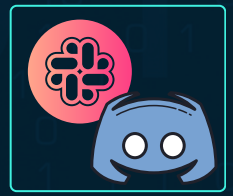
★★★★

ASYNCHRONOUS TOOLS

GOOGLE DOCS

Great for writing processes and long-term notes about hunting methodologies. They are also free, easy to share, and has great RBAC

★★★★



SLACK/DISCORD

Both tools are a *must* for any hunting group, it's just a matter of preference. Discord's message limit can be a challenge.

★★★★★

CONFLUENCE

Has many features that Google Docs does not have that allow you to write dynamic processes. A bit less accessible, though.

★★★

LET'S BUILD A METHODOLOGY

If you brought a laptop, you can clone the repo from my GitHub. Otherwise, raise your hand and I'll bring over a paper copy of the methodology. The repo will be public, so you can always clone it later if you want!

EXERCISE 5

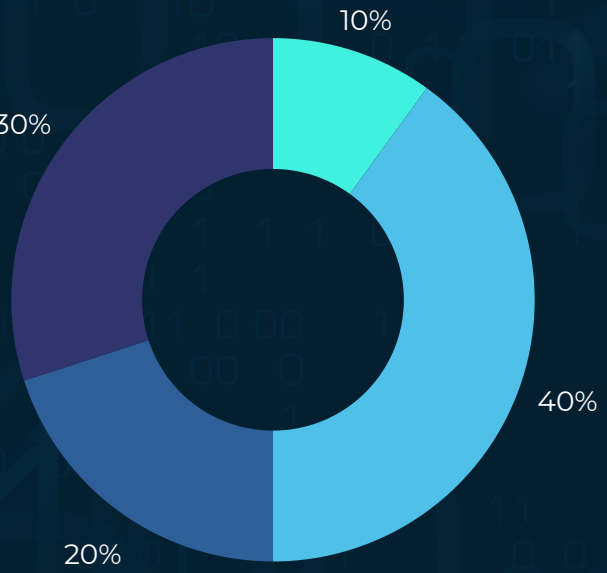
METHODOLOGY OVERVIEW

RECON

Apex Domains, Subdomains, IP Addresses, Open Ports, Live URLs, Endpoints, Parameters, HTTP Verbs, Leaked Secrets

INJECTION

Cross-Site Scripting, Prototype Pollution, SQL Injection, Server-Side Template Injection, XPath Injection, XML External Entity



CLOUD

Code -> Cloud Service, Infrastructure, Known Misconfigurations, DNS, WAF, TLS Certs, Request Smuggling, HTTP2

LOGIC

OAuth Misconfig, IDOR, Access Control Violations, Payment Process, Password Reset, Race Conditions, SAML Misconfiguration

FINAL EXERCISE

METHODOLOGY

Working as a team, divide blocks of rs0n's methodology between the members of your group and develop a plan of execution.

HARRISON RICHARDSON (RS0N)

YOUTUBE
youtube.com/@rs0n_live

GITHUB
github.com/R-s0n

WEBSITE
ars0nsecurity.com

SECURITY ENGINEERING MANAGER @ #FloQast

THANK YOU

HAPPY HUNTING!