Vulnerability Research as a lifestyle

Syed Faraz Abrar

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

$ whoami

- Cyber Security Undergraduate @ Curtin University

@farazsth98

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

$ whoami

- Cyber Security Undergraduate @ Curtin University
- Security Researcher @ elttam

@farazsth98

elttam.com

$ whoami

- Cyber Security Undergraduate @ Curtin University
- Security Researcher @ elttam
- Focus on low level vulnerability research

@farazsth98

elttam.com

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

What is Vulnerability Research?

- The act of studying and analyzing the internals of some specific software with the aim of finding vulnerabilities

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

What is Vulnerability Research?

- The act of studying and analyzing the internals of some specific software with the aim of finding vulnerabilities
- A subset of “Security Research”

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

What is Vulnerability Research?

- The act of studying and analyzing the internals of some specific software with the aim of finding vulnerabilities
- A subset of “Security Research”
- Usually involves:
  - Code auditing / review
  - Reverse engineering
  - Automated static analysis
  - Fuzzing

Why bother?

- Hacker mindset

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

Why bother?

- Hacker mindset
- It’s intellectually challenging

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

Why bother?

- Hacker mindset
- It’s intellectually challenging
- There’s money involved

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

Why bother?

- Hacker mindset
- It’s intellectually challenging
- There’s money involved
- It’s fun!

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

How do you get started?

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

How do you get started?

- CTFs are great

How do you get started?

- CTFs are great
  - Easier CTFs are generally not so realistic

How do you get started?

- CTFs are great
  - Easier CTFs are generally not so realistic
  - Harder CTFs are very realistic

How do you get started?

- CTFs are great
  - Easier CTFs are generally not so realistic
  - Harder CTFs are very realistic
- Teaches you how to learn

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

How do you get started?

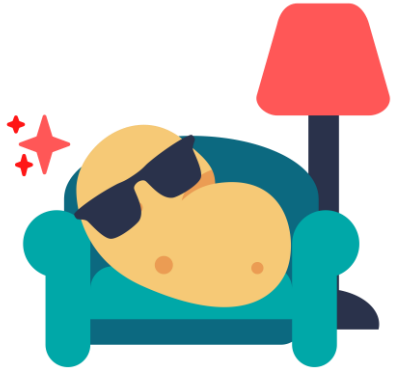
- CTFs are great
  - Easier CTFs are generally not so realistic
  - Harder CTFs are very realistic
- Teaches you how to learn
- Teaches you about bug classes

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

How do you get started?

- CTFs are great
  - Easier CTFs are generally not so realistic
  - Harder CTFs are very realistic
- Teaches you how to learn
- Teaches you about bug classes
- Focus on exploitation more than vulnerability research



COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

What next?

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

What next?

- Pick a real world target

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

What next?

- Pick a real world target
  - Any bug bounty program

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

What next?

- Pick a real world target
  - Any bug bounty program
  - Random open source Github repo

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

What next?

- Pick a real world target
  - Any bug bounty program
  - Random open source Github repo
  - Any IoT device / embedded system

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

What next?

- Pick a real world target
  - Any bug bounty program
  - Random open source Github repo
  - Any IoT device / embedded system
  - A big target

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

What next?

- Pick a real world target
  - Any bug bounty program
  - Random open source Github repo
  - Any IoT device / embedded system
  - A big target
- Read all existing research (if applicable)

What next?

- Pick a real world target
  - Any bug bounty program
  - Random open source Github repo
  - Any IoT device / embedded system
  - A big target
- Read all existing research (if applicable)
- Study past vulnerabilities (if applicable)

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

What next?

- Pick a real world target
  - Any bug bounty program
  - Random open source Github repo
  - Any IoT device / embedded system
  - A big target
- Read all existing research (if applicable)
- Study past vulnerabilities (if applicable)
- Profit!

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

Professional roles

- Security Engineer

Professional roles

- Security Engineer
- Security Researcher

Professional roles

- Security Engineer
- Security Researcher
- Security Consultant

Bug Bounty Programs

- Platforms such as Synack, HackerOne, Bugcrowd

Bug Bounty Programs

- Platforms such as Synack, HackerOne, Bugcrowd
- Bounties vary a lot

COMFYCON AU

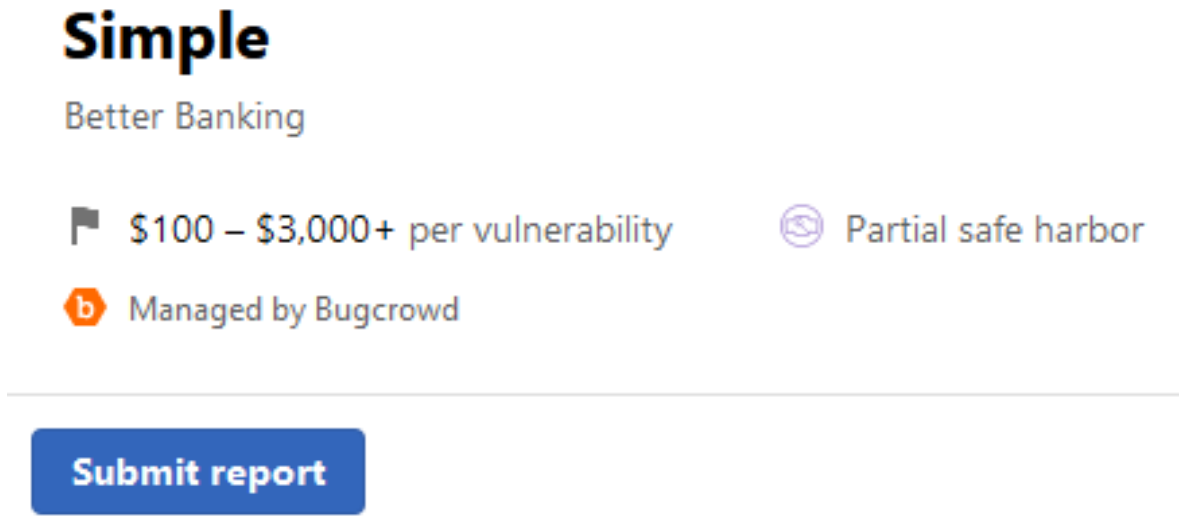
CYBER WITHOUT LEAVING YOUR ISOLATION TANK

Bug Bounty Programs

- Platforms such as Synack, HackerOne, Bugcrowd
- Bounties vary a lot
- Generally a focus on high-level vulnerabilities

Bug Bounty Programs

- Platforms such as Synack, HackerOne, Bugcrowd
- Bounties vary a lot
- Generally a focus on high-level vulnerabilities



COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

Vulnerability Rewards Programs

- Focus on low-level vulnerabilities

Vulnerability Rewards Programs

- Focus on low-level vulnerabilities
- Have their own platforms

Vulnerability Rewards Programs

- Focus on low-level vulnerabilities
- Have their own platforms
  - Chromium VRP ($500 - $30,000)

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

Vulnerability Rewards Programs

- Focus on low-level vulnerabilities
- Have their own platforms
  - Chromium VRP ($500 - $30,000)
  - MSRC Bug Bounty Program ($15,000 - $300,000)

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

Vulnerability Rewards Programs

- Focus on low-level vulnerabilities
- Have their own platforms
  - Chromium VRP ($500 - $30,000)
  - MSRC Bug Bounty Program ($15,000 - $300,000)
  - Mozilla VRP ($500 - $10,000+)

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

Vulnerability Rewards Programs

- Focus on low-level vulnerabilities
- Have their own platforms
  - Chromium VRP ($500 - $30,000)
  - MSRC Bug Bounty Program ($15,000 - $300,000)
  - Mozilla VRP ($500 - $10,000+)
  - Apple VRP ($25,000 - $1,000,000)

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

Vulnerability Rewards Programs

- Focus on low-level vulnerabilities
- Have their own platforms
  - Chromium VRP ($500 - $30,000)
  - MSRC Bug Bounty Program ($15,000 - $300,000)
  - Mozilla VRP ($500 - $10,000+)
  - Apple VRP ($25,000 - $1,000,000)
  - Trend Micro’s Zero Day Initiative

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

Vulnerability Rewards Programs

- Focus on low-level vulnerabilities
- Have their own platforms
  - Chromium VRP ($500 - $30,000)
  - MSRC Bug Bounty Program ($15,000 - $300,000)
  - Mozilla VRP ($500 - $10,000+)
  - Apple VRP ($25,000 - $1,000,000)
  - Trend Micro’s Zero Day Initiative
- There are a lot more!

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

Exploit shops

- Buys full chain exploits
  - Zerodium

Exploit shops

- Buys full chain exploits
  - Zerodium
  - Exodus Intel’s Research Sponsorship Program

Exploit shops

- Buys full chain exploits
  - Zerodium
  - Exodus Intel’s Research Sponsorship Program
- Usually pay a lot more than any VRP

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

Exploit shops

- Buys full chain exploits
  - Zerodium
  - Exodus Intel’s Research Sponsorship Program
- Usually pay a lot more than any VRP
- Only disadvantage – requires full chain exploits

ZERODIUM Payouts for Desktops/Servers*

Windows
macOS
Linux/BSD
Any OS

RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape

Up to $1,000,000									1.001 Win RCE Zero Click (Win)
Up to $500,000							3.001 Chrome RCE+LPE (Win)	2.001 Apache RCE (Linux)	2.002 MS IIS RCE (Win)
Up to $250,000					5.001 MS Outlook RCE (Win)		4.001 MS Exchange RCE (Win)	2.003 OpenSSL RCE (Linux)	2.004 PHP RCE (Linux)
Up to $200,000	6.001 VMware ESXi VME	5.002 Thunderbird RCE (Win/Linux)		4.002 Sendmail RCE (Linux)	4.003 Postfix RCE (Linux)		4.004 Dovecot RCE (Linux)	4.005 Exim RCE (Linux)	2.005 nginx RCE (Linux)
Up to $100,000		3.002 Safari RCE+LPE (Mac)	3.003 Edge RCE+LPE (Win)	3.004 Firefox RCE+LPE (Win)	5.003 Word/Excel RCE (Win)	7.001 WordPress RCE (Linux)	7.002 cPanel/WHM RCE (Linux)	7.003 Plesk RCE (Linux)	7.004 Webmin RCE (Linux)
Up to $80,000	6.002 VMware WS VME (Win/Linux)					5.004 Adobe PDF RCE+SBX (Win)	5.005 WinRAR RCE (Win)	5.006 7-Zip RCE (Win)	6.003 Windows LPE/SBX (Win)
Up to $50,000	6.004 USB LPE (Win/Mac)	8.001 Antivirus RCE (Win)		5.007 WinZip RCE (Win)	5.008 tar RCE (Linux)	6.005 macOS LPE/SBX (Mac)		6.006 Linux LPE (Linux)	6.007 BSD LPE (BSD)
Up to $10,000	9.001 Routers RCE	8.002 Antivirus LPE (Win)	7.005 phpBB RCE (Linux)	7.006 vBulletin RCE (Linux)	7.007 MyBB RCE (Linux)	7.008 Joomla RCE (Linux)	7.009 Drupal RCE (Linux)	7.010 Roundcube RCE (Linux)	7.011 Horde RCE (Linux)

*All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

Competitions

- Researchers showcase exploits

Competitions

- Researchers showcase exploits
- Competition organisers pay for exploits

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

Competitions

- Researchers showcase exploits
- Competition organisers pay for exploits
- Tianfu Cup

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

Competitions

- Researchers showcase exploits
- Competition organisers pay for exploits
- Tianfu Cup
- Pwn2Own

COMFYCON AU

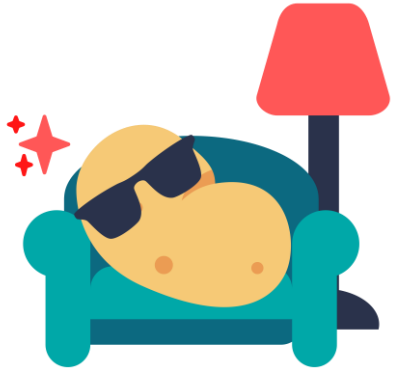
CYBER WITHOUT LEAVING YOUR ISOLATION TANK

Competitions

- Researchers showcase exploits
- Competition organisers pay for exploits
- Tianfu Cup
- Pwn2Own
- TyphoonPWN

Competitions

- Researchers showcase exploits
- Competition organisers pay for exploits
- Tianfu Cup
- Pwn2Own
- TyphoonPWN
- And a couple others



COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

Thank you!

COMFYCON AU

CYBER WITHOUT LEAVING YOUR ISOLATION TANK

@farazsth98