```
operation == "MIRROR_Y"
Irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
 operation == "MIRROR_Z";
 rror_mod.use_x = False
 rror_mod.use_y = False
 rror_mod.use_z = True
melection at the end -add
  _ob.select= 1
 er ob.select=1
  ntext.scene.objects.action
 "Selected" + str(modified
  irror ob.select = 0
bpy.context.selected_obj
 lata.objects[one.name].sel
int("please select exaction
 OPERATOR CLASSES ----
```

HOW TO BECOME A PENTESTER: THE ESSENTIALS

SONNGUY3N

WHO AM I?

- Son Nguyen ATTT2015
- Senior Security Engineer of ZaloPay (VNG Corp)
- Lead of Infrastructure security, R&D
- FB: fb.com/sonnguyen.uit/
- TW: @s0nnguy3n_

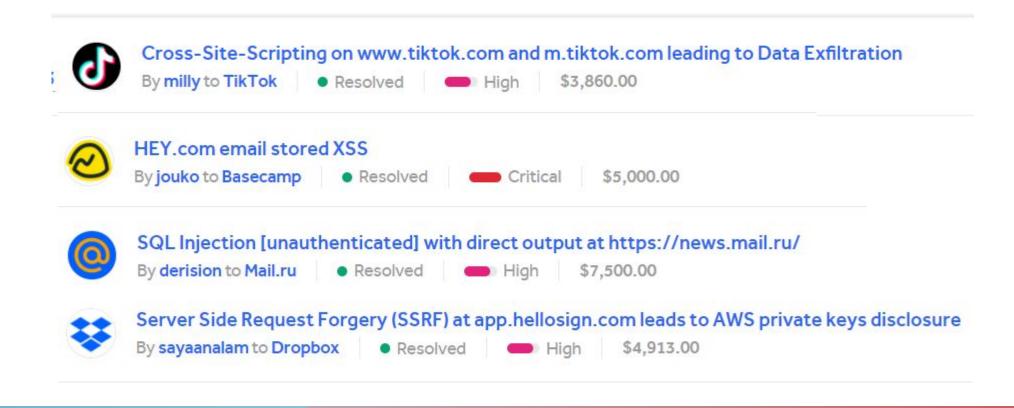
AGENDA

- Overview
- Essentials
- Practice
- Career
- Q&A

OVERVIEW

- Kiểm tra tính an toàn của Ứng dụng web và mobile.
- Trên thực tế thì kiểm thử ứng dụng web và mobile gần như giống nhau, đều kiểm thử dựa trên request/response.
- Tùy vào yêu cầu sẽ có những phương pháp kiểm thử riêng như blackbox, graybox hay whitebox.
- Phần lớn ở VN là kiểm thử blackbox.

- Nắm rõ các lỗ hổng thường gặp (TOP 10 OWASP) BẮT BUỘC
 - Fact: Thường thì các pentester chỉ nắm vững một số lỗi sở trường thôi...



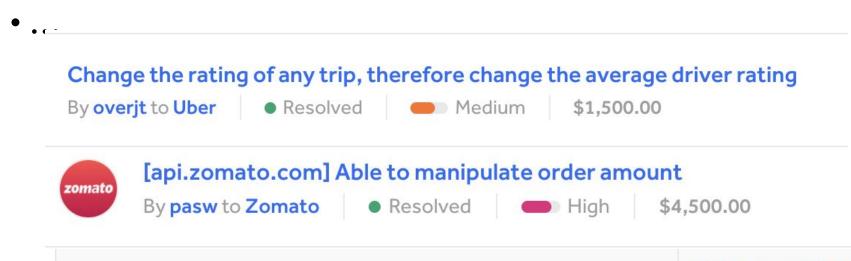
- Hiểu sâu, nắm rõ rãng về ứng dụng web/mobile cần kiểm thử.
 - Workflow
 - Technology
 - Sensitive data

An attacker can run pipeline jobs as arbitrary user
By u3mur4 to GitLab Resolved Critical \$12,000.00

Arbitrary file read via the UploadsRewriter when moving and issue
By vakzz to GitLab Resolved Critical \$20,000.00

Spring Actuator endpoints publicly available and broken authentication
By kazan71p to LINE Resolved Critical \$12,500.00

- Logic bugs (Business logic)
 - Numerical Bug
 - Payment



Bounty \$1000 — Critical Business Logic Flaw leads to Account Takeover & Product Order Amount Manipulation

Muhammad Asim Shahzad (@protector47)

- TOOL
 - BurpSuite + extensions (*)
 - Acunetix
 - Dirsearch

•



ESSENTIALS (Level cao cấp, có thể bỏ qua)

- Advanced bug
 - Web cache poisoning
 - HTTP request smuggling
 - Deserialization (top trending)
 - China blog
 - RCE bug
 - Java(*), Php, Ruby...

PRACTICE

- CTF (base)
- Lab (Hackthebox, Tryhackme) + Cert (OSCP..)
- Twitter (Tip + Trick)
- Web Security Lab of PortSwigger
 - https://portswigger.net/web-security
- Bug Bounty
 - Safevuln.com , Whitehub.net (Viet Nam)
 - Bug Crowd (https://www.bugcrowd.com/)
 - Hackerone (https://www.hackerone.com/)

CAREER

- Cơ hội nghề nghiệp cực nhiều
- · Có hai dạng công ty chính:
 - Dịch vụ chuyên đi kiểm thử cho các công ty, tổ chức khác
 - Bên A phục vụ cho bản thân công ty, đảm bảo an toàn cho hệ thống của chính mình.
- Đối với các bạn sinh viên, các nhà tuyển dụng sẽ dựa vào thành tích CTF,
 profile bug bounty để đánh giá năng lực khi tuyển dụng.
- Các pentester thu nhập cao, có thể kiếm thêm rất nhiều từ việc tìm lỗi (bug bounty) (*)

BONUS - CV ấn tượng cho nhà tuyển dụng

•

- Blog/writeup
- Thành tích trong các hội thảo, cuộc thi CTF, Coding, Hacking...
- Certification (CEH + OSCP)
- Profile Bug bounty
- · Một lời giới thiệu từ anh em bạn bè trong lĩnh vực ATTT.

BONUS - COMPANIES

- VNG (Zalo, Zalopay, VNG Cloud,...)
- Viettel
- Vincss
- Techlab
- VNPT
- FPT (Ftel...)
- Bank (TCB, VIB, HBBANK...)
- •

Q&A

