

```
...use_z = False
operation == "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True
```

```
selection at the end -add
mirror_ob.select= 1
modifier_ob.select=1
context.scene.objects.active
("Selected" + str(modifier_ob))
mirror_ob.select = 0
= bpy.context.selected_object
data.objects[one.name].select
print("please select exactly")
-- 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/](https://fb.com/sonnguyen.uit/)
- TW: [@s0nnguy3n\\_](https://twitter.com/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.

# ESSENTIALS

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

	<b>Cross-Site-Scripting on <a href="http://www.tiktok.com">www.tiktok.com</a> and <a href="http://m.tiktok.com">m.tiktok.com</a> leading to Data Exfiltration</b> By <a href="#">milly</a> to <a href="#">TikTok</a>   <span>● Resolved</span>   <span>● High</span>   \$3,860.00
	<b>HEY.com email stored XSS</b> By <a href="#">jouko</a> to <a href="#">Basecamp</a>   <span>● Resolved</span>   <span>● Critical</span>   \$5,000.00
	<b>SQL Injection [unauthenticated] with direct output at <a href="https://news.mail.ru/">https://news.mail.ru/</a></b> By <a href="#">derision</a> to <a href="#">Mail.ru</a>   <span>● Resolved</span>   <span>● High</span>   \$7,500.00
	<b>Server Side Request Forgery (SSRF) at <a href="http://app.hellosign.com">app.hellosign.com</a> leads to AWS private keys disclosure</b> By <a href="#">sayaanalam</a> to <a href="#">Dropbox</a>   <span>● Resolved</span>   <span>● High</span>   \$4,913.00

# ESSENTIALS

- Hiểu sâu, nắm rõ ràng 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

# ESSENTIALS

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

Change the rating of any trip, therefore change the average driver rating

By [overjt](#) to [Uber](#)

● Resolved

● Medium

\$1,500.00



[\[api.zomato.com\]](#) Able to manipulate order amount

By [pasw](#) to [Zomato](#)

● Resolved

● High

\$4,500.00

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

Muhammad Asim  
Shahzad  
(@protector47)

# ESSENTIALS

- 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**

