



CYBERKARTA



# Web Security Slides

Kelas Premium Web Security - Cyberkarta





# Penetration Test, Bug Bounty, dan VDP



# Offensive Security

- Sering dianggap sebagai red team
- Bekerja dengan melakukan hacking ke sistem
- Mencari celah sebelum ditemukan oleh “bad actor”
- Sulit, tetapi rewarding



# Penetration Test

- Percobaan peretasan secara legal untuk mencari celah secara menyeluruh pada layanan.
- Menggunakan kontrak.



# Bug Bounty

- Sayembara untuk menemukan celah pada layanan. Hadiahnya berupa bounty (uang) yang diberikan secara langsung per celah yang ditemukan.
- Organisasi dapat mencari top talent dengan memberikan hadiah yang lebih besar.

Severity	Payout Range
Critical	\$10,000 - \$15,000
High	\$3,000 - \$10,000
Medium	\$500 - \$3,000
Low	\$100 - \$500
Informative	\$0 - \$0



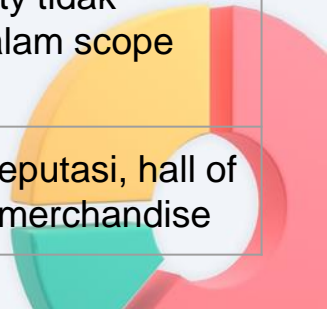
# Vulnerability Disclosure Program (VDP)

- Metode terstruktur tentang bagaimana ethical hacker dapat melaporkan celah secara mudah dan aman.
- Organisasi terkadang memberikan hadiah terhadap celah yang ditemukan, namun tidak membayar per celah yang ditemukan



# Penetration Test, Bug Bounty, VDP

Perbedaan	Penetration Test	Bug Bounty	VDP
Kontrak	Melakukan kontrak secara formal sebelum melakukan testing	Menggunakan sayembara dengan aturan main	Menggunakan aturan main
Phishing	Terkadang phishing termasuk ke dalam scope testing	Phishing tidak termasuk ke dalam scope	Phishing tidak termasuk ke dalam scope
Physical security	Terkadang physical security termasuk ke dalam scope testing	Physical security tidak termasuk ke dalam scope	Physical security tidak termasuk ke dalam scope
Reward	Dibayarkan berdasarkan kontrak kerja	Dibayarkan berdasarkan temuan celah	Mendapatkan reputasi, hall of fame, ataupun merchandise









# Panduan Melakukan Penetration Test



# Penetration Test (Pentest)

- Percobaan peretasan secara legal untuk mencari celah secara menyeluruh pada layanan.
- Menggunakan kontrak.



# Tip Penetration Test

- Black box
- Grey box
- White box



# Step dari Pentest

1. Pre-engagement
2. Reconnaissance
3. Vulnerability Assessment
4. Exploitation
5. Post Exploitation
6. Reporting



# Pre-Engagement

- Koordinasi proyek
- Dokumen
  - Kontrak
  - Scope
  - Non-Disclosure Agreement (NDA)



# Reconnaissance

- “Berkenalan” dengan layanan
  - Open port
  - API
  - Sensitive information
  - IP address dan domain
  - Penggunaan HTTP header



# Vulnerability Assessment

- Menggunakan data yang didapatkan pada fase reconnaissance untuk mengidentifikasi kemungkinan celah dan teknik eksploitasinya.



# Exploitation

- Dari data yang didapatkan pada fase reconnaissance dan vulnerability assessment, pentester melakukan percobaan eksploitasi untuk mendapatkan akses ke server.
- Fase yang paling riskan pada proses pentesting.





# Post Exploitation

- Penetration tester mencoba mencari objektif yang terekspos dari proses eksploitasi
  - Sensitive data
  - Unauthorized process
  - Privilege escalation



# Reporting

- Melaporkan segala jenis hasil penetration test yang ditemukan pada laporan.
- Tujuan: mengurangi resiko memiliki layanan IT







# Panduan Mencari Target Bug Bounty dan VDP



# Bug Bounty

- Sayembara untuk menemukan celah pada layanan. Hadiahnya berupa bounty (uang) yang diberikan secara langsung per celah yang ditemukan.
- Organisasi dapat mencari top talent dengan memberikan hadiah yang lebih besar.

Severity	Payout Range
Critical	\$10,000 - \$15,000
High	\$3,000 - \$10,000
Medium	\$500 - \$3,000
Low	\$100 - \$500
Informative	\$0 - \$0




# Vulnerability Disclosure Program (VDP)

- Metode terstruktur tentang bagaimana ethical hacker dapat melaporkan celah secara mudah dan aman.
- Organisasi terkadang memberikan hadiah terhadap celah yang ditemukan, namun tidak membayar per celah yang ditemukan



# Public Bug Bounty Program

Program bug bounty yang dibuka kepada publik.

**Starbucks**  
Inspiring and nurturing the human spirit -- one person, one cup, one neighborhood at a time.  
<http://www.starbucks.com> · @Starbucks

[Submit report](#)

**Bug Bounty Program**  
Launched on Nov 2016  
Managed by HackerOne  
Includes retesting ⓘ  
Bounty splitting enabled ⓘ

Reports resolved  
**1541**

Assets in scope  
**35**

Average bounty  
**\$300-\$500**

[Policy](#) [Scope](#) [New!](#) [Hacktivity](#) [Thanks](#) [Updates \(2\)](#) [Collaborators](#)

This program requires two-factor authentication enabled to participate in.

**Rewards**

Low 0.1 - 3.9	Medium 4.0 - 6.9	High 7.0 - 8.9	Critical 9.0 - 10.0
\$200	\$800	\$2,000	\$6,000
\$100	\$500	\$1,000	\$4,000

**Response Efficiency**  
**7 hrs**  
Average time to first response  
**3 days**  
Average time to triage  
**12 days**  
Average time to bounty



# Public Bug Bounty Program (3rd Party)

- BugCrowd
- HackerOne
- YesWeHack
- RedStorm
- CyberArmy





# Public Bug Bounty Program (self-managed)

- Google
- Tokopedia
- Traveloka



# Private Bug Bounty Program

Dengan menggunakan invitation, biasanya dilihat dari reputasi bug bounty hunter dari public bug bounty program.







# Penutup





# Congratulations

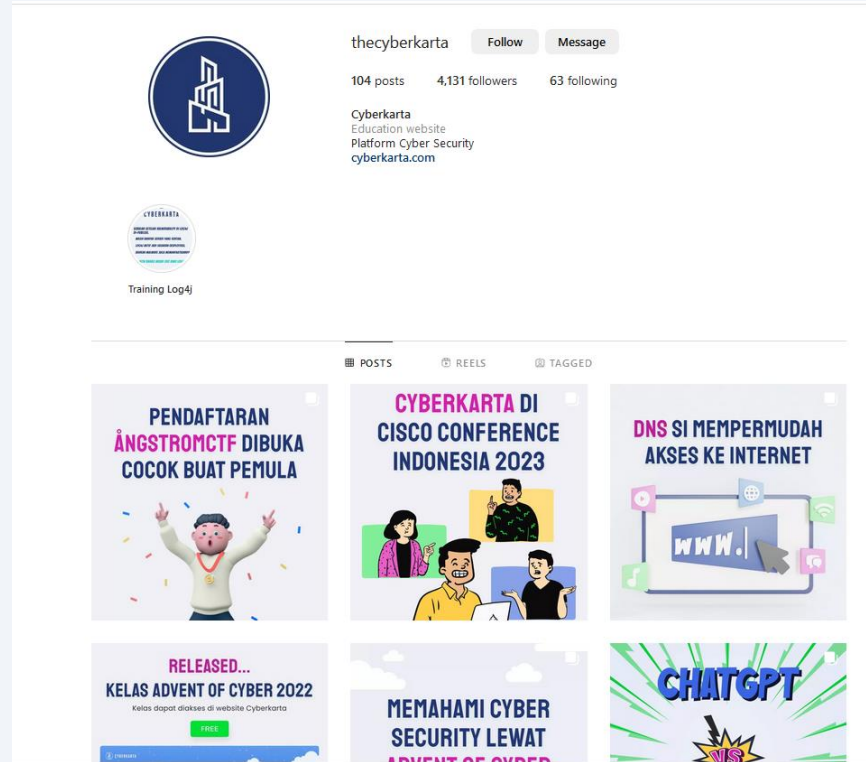




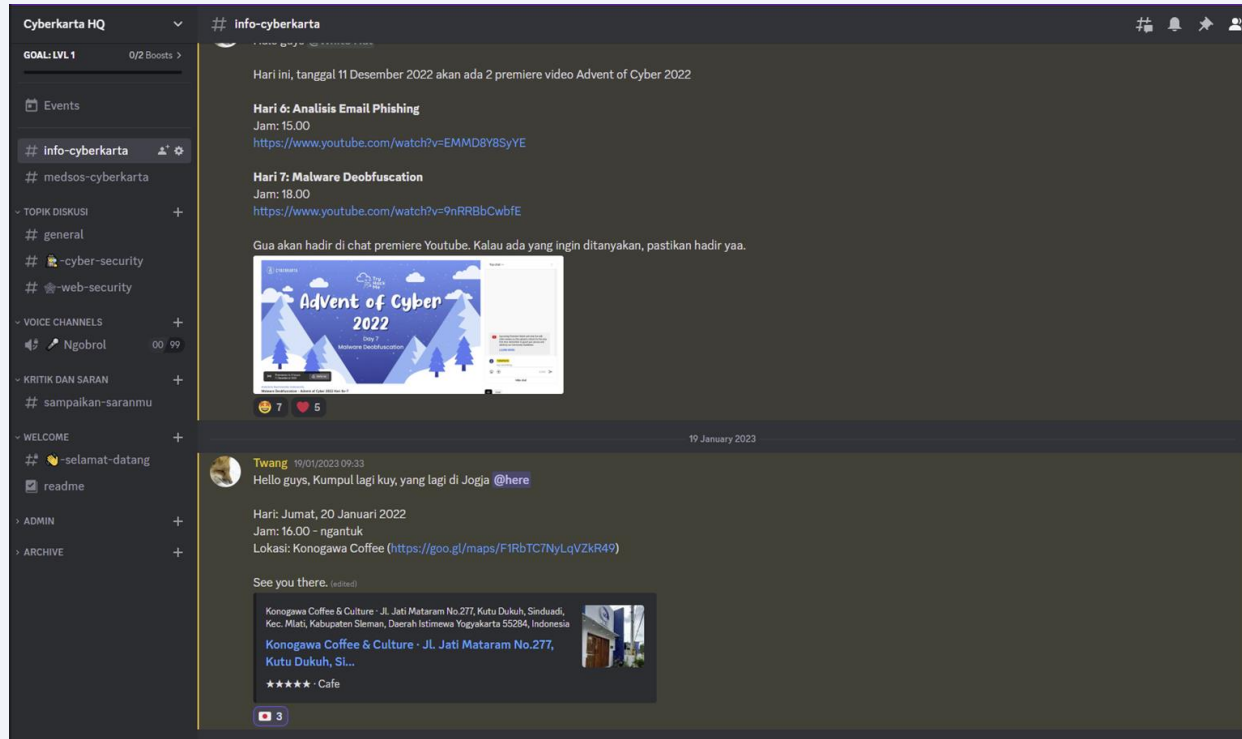
# Start Now



# Instagram



# Discord





# Penutup





Terima Kasih



