Mulai bug bounty dari bekal CTF

Memilih program, memilih target, dan peran keberuntungan

CTF dan bug bounty adalah permainan berbeda

CTF

- Bug pasti ada
- Soal terbatas dan bisa diselesaikan
- Hasil hampir tanpa keberuntungan

Bug bounty

- Banyak target tanpa bug yang mudah
- Scope besar, titik mulai ditentukan sendiri
- Ribuan hunter mencoba hal yang sama

Perubahan mindset

Dari "bagaimana cara exploit ini?" menjadi "asumsi developer apa yang bisa saya langgar?"

Bug yang paling sering valid

- Broken access control dan IDOR
- Auth bypass
- Logic flaw di alur bisnis
- Misconfiguration
- SSRF, race condition, JWT dan OAuth yang lemah

Jarang berupa exploit yang rumit.

Algoritma memilih program

1. Tentukan profil: stack, waktu, tujuan
2. Kumpulkan 10 sampai 20 kandidat
3. Buang yang gagal filter keras
4. Beri skor, maksimal 100
5. Smell test 2 sampai 3 jam per program
6. Komit 2 sampai 4 minggu pada 1 sampai 2 program
7. Pantau perubahan scope secara berkala

Skor program, maksimal 100

Kriteria	Bobot
Kebaruan	25
Luas scope	20
Kompleksitas aplikasi	20
Kecepatan dan keadilan program	15
Kecocokan skill	10
Kompetisi	10

Di atas 70 layak dicoba. 50 sampai 70 watchlist. Di bawah 50 lewati.

Yang dicek di sebuah program

Tab Scope

- Aset baru atau wildcard
- Eligible for bounty
- Max severity per aset
- Daftar out-of-scope

Policy dan statistik

- Response efficiency
- Tabel bounty
- Reports resolved
- Tanggal launch
- Safe harbor

Lima kolom untuk menyaring program

Kolom	Cara membacanya
Launch date	Makin baru makin menarik
Reports resolved	Gambaran kompetisi
Response efficiency	Triage cepat, kamu betah lama
Bounty minimum	Low severity juga dibayar?
Last updated scope	Buka tab Scope, cari aset baru

Peluang bug valid per jenis target

Target	Peluang	Catatan
Web dan API	Tertinggi	Paling padat, duplicate tinggi
Android	Tinggi	Banyak bug ada di API belakang
Desktop	Sedang	Electron paling masuk akal
Kernel dan OS	Terendah	Butuh berbulan-bulan

Kalau web terasa jenuh

Cari titik temu antara bug masih ada dan sedikit yang mengincar.

1. Android lewat reversing, cari endpoint tersembunyi
2. Electron dan desktop app
3. Source code review proyek open source
4. Program kecil, baru, atau VDP

Recon subdomain

Kenapa dilakukan

- Aplikasi utama paling ketat dijaga
- Staging, dev, admin, dan API lama sering terlupakan
- Subdomain baru muncul terus

Keunggulan sebenarnya

- Daftar subdomain bukan keunggulan, semua punya
- Pelajari subdomain membosankan yang punya fungsi bisnis
- Pantau perubahan lebih cepat
- Cek scope sebelum menguji

Skala penilaian

0

Murni skill

10

Murni keberuntungan

Penilaian subjektif, bukan hasil pengukuran.

Peran keberuntungan per situasi

Situasi	Luck (0 sampai 10)
CTF	1
Satu laporan tertentu	7 sampai 8
Bug pertama dalam 1 sampai 2 bulan	6 sampai 7
Hasil 6 sampai 12 bulan	3 sampai 4
Hunter konsisten bertahun-tahun	2 sampai 3

Kenapa angkanya turun seiring waktu

Keberuntungan

Acak per kejadian. Makin banyak sampel, makin saling menetralkan.

Skill

Menumpuk lewat kebiasaan. Pengaruhnya makin besar di jangka panjang.

Di mana keberuntungan berperan

Besar

- Timing menguji fitur baru
- Duplicate
- Pilihan target
- Siapa triager-nya

Hampir tidak ada

- Kedalaman memahami aplikasi
- Konsistensi di satu target
- Kualitas laporan
- Kemampuan memilih target

Situasimu sekarang

6 dari 10

Skill sudah cukup untuk punya peluang. Kapan bug pertama muncul masih banyak ditentukan timing dan pilihan target.

Yang bisa dikendalikan

1. Perbanyak jam di target yang tepat
2. Pilih target baru, sepi, atau niche
3. Pantau scope dan rilis fitur baru
4. Jangan berhenti terlalu cepat