Modul 1: Introduction to Bug Bounty

Memahami ekosistem Bug Bounty, cara kerja industri ini, dan bagaimana Anda bisa mendapatkan penghasilan secara legal dari menemukan celah keamanan di sistem digital.

EDY SUSANTO - FOUNDER C-SIX SECURITY

Tujuan Pembelajaran

Apa yang Akan Anda Pelajari?

Modul ini dirancang untuk memberikan fondasi yang kuat bagi siapa saja yang ingin memulai perjalanan di dunia Bug Bounty — dari pemahaman konsep dasar hingga aturan legal yang harus dipatuhi.

🎯 Konsep Dasar

Memahami apa itu Bug Bounty, sejarahnya, dan perbedaannya dengan Ethical Hacking.

⚙️ Cara Kerja

Mengenal alur program Bug Bounty, scope, dan Rules of Engagement yang berlaku.

🏆 Reward & Pengakuan

Memahami sistem penilaian severity, jenis reward, dan Hall of Fame.

⚖️ Aspek Legal

Responsible Disclosure dan ekosistem platform Bug Bounty global.

Apa itu Bug Bounty?

Bug Bounty adalah program yang ditawarkan oleh perusahaan atau organisasi kepada para peneliti keamanan (security researcher) untuk menemukan dan melaporkan celah keamanan (vulnerability) dalam sistem mereka. Sebagai imbalannya, peneliti akan mendapatkan kompensasi berupa uang, hadiah, atau pengakuan resmi.

> Bug Bounty bukan hacking ilegal — ini adalah bentuk kolaborasi resmi antara perusahaan dan komunitas keamanan siber untuk menciptakan ekosistem digital yang lebih aman.

Sejarah Bug Bounty

Bug Bounty bukan konsep baru. Perjalanannya dimulai jauh sebelum era internet modern, berkembang dari program eksperimental menjadi industri bernilai miliaran dolar.

1

1983

Hunter & Ready menawarkan VW Beetle sebagai hadiah bagi siapa saja yang menemukan bug di sistem operasi VRTX mereka — program bug bounty pertama di dunia.

2

1995

Netscape meluncurkan program bug bounty digital pertama untuk browser Netscape Navigator 2.0 dengan hadiah uang tunai.

3

2004

Mozilla Firefox memulai program bug bounty formal untuk produk open-source mereka, membuka era baru keamanan komunitas.

4

2012

HackerOne dan Bugcrowd berdiri, menjadi platform bug bounty profesional pertama yang menghubungkan researcher dengan perusahaan secara masif.

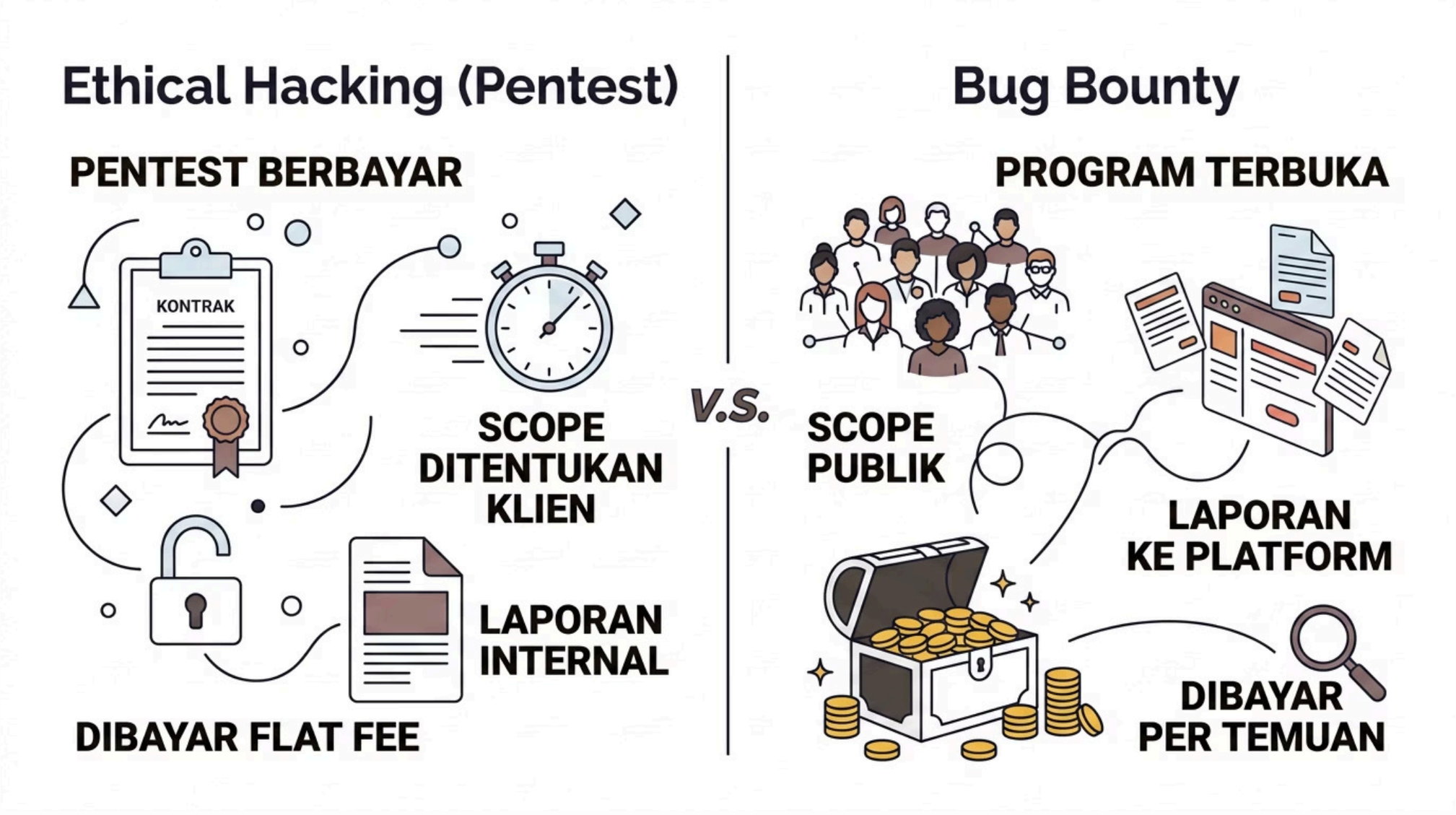
5

2020+

Industri Bug Bounty meledak. Ribuan perusahaan Fortune 500 dan pemerintah di seluruh dunia kini memiliki program resmi.

Ethical Hacking vs Bug Bounty

Dua istilah ini sering disalahartikan sebagai hal yang sama, padahal terdapat perbedaan mendasar dalam konteks, izin, dan tujuannya.



Keduanya legal dan bertujuan meningkatkan keamanan — namun Bug Bounty memberikan fleksibilitas lebih besar karena siapa saja bisa berpartisipasi kapan saja sesuai scope yang telah ditentukan program.

Bagaimana Program Bug Bounty Bekerja?

Prosesnya terstruktur dan transparan. Setiap laporan yang valid akan diverifikasi oleh tim keamanan internal perusahaan sebelum reward diberikan. Kecepatan dan kualitas laporan sangat menentukan besaran reward yang diterima.

Scope dan Rules of Engagement

Setiap program Bug Bounty memiliki **scope** yang jelas — yaitu batas-batas sistem apa saja yang boleh diuji. Melanggar scope berarti melanggar hukum, bahkan jika Anda menemukan celah yang nyata.

✅ In-Scope

- Domain dan subdomain yang disebutkan
- Aplikasi mobile yang terdaftar
- API endpoint yang ditentukan
- Fitur produk tertentu

❌ Out-of-Scope

- Infrastruktur pihak ketiga
- Serangan DoS/DDoS
- Social engineering terhadap karyawan
- Data pengguna nyata

> ⚠ Selalu baca Rules of Engagement sebelum memulai pengujian. Ignorance is not an excuse.

Responsible Disclosure

Responsible Disclosure adalah prinsip etika dan prosedur resmi dalam melaporkan celah keamanan kepada pihak yang tepat, dengan cara yang tepat, dan dalam waktu yang disepakati — sebelum informasi tersebut dipublikasikan.

→ Temukan Vulnerability

Dokumentasikan temuan Anda secara lengkap dengan bukti (screenshot, PoC) tanpa menyalahgunakan akses.

→ Laporkan ke Vendor/Platform

Kirimkan laporan melalui platform resmi atau kontak keamanan perusahaan. Jangan publikasikan dulu.

→ Tunggu Masa Remediasi

Berikan waktu kepada vendor untuk memperbaiki (umumnya 90 hari sesuai standar industri Google Project Zero).

→ Publikasi Terkoordinasi

Setelah patch dirilis, Anda dapat mempublikasikan write-up sebagai portofolio profesional Anda.

Severity Rating: CVSS

Common Vulnerability Scoring System (CVSS) adalah standar industri untuk menilai tingkat keparahan sebuah vulnerability. Skor ini menentukan besaran reward yang akan Anda terima.

🔵 Informational / None (0.0)

Temuan yang tidak memiliki dampak langsung. Biasanya tidak dibayar, namun bisa masuk ke Hall of Fame.

🟢 Low (0.1 – 3.9)

Dampak terbatas, butuh kondisi tertentu untuk dieksploitasi. Reward kecil, cocok untuk pemula.

🟡 Medium (4.0 – 6.9)

Potensi dampak moderat. Kombinasi beberapa low-severity bisa menghasilkan medium. Reward mulai signifikan.

🔴 High (7.0 – 8.9)

Dampak besar pada kerahasiaan, integritas, atau ketersediaan data. Reward besar, butuh keahlian tinggi.

🚨 Critical (9.0 – 10.0)

Eksploitasi penuh sistem tanpa autentikasi. Reward tertinggi — bisa mencapai puluhan ribu dolar.

Jenis Reward dan Hall of Fame

💰 Jenis Reward

- **Monetary (Uang Tunai)** — Dibayar via PayPal, bank transfer, atau cryptocurrency
- **Swag & Merchandise** — T-shirt, stiker, atau barang eksklusif dari perusahaan
- **Credits & Points** — Poin reputasi di platform yang meningkatkan visibilitas profil
- **Acknowledgment** — Pengakuan resmi dalam catatan keamanan perusahaan

🏆 Hall of Fame

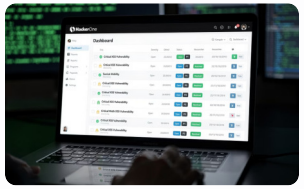
Hall of Fame adalah daftar penghargaan resmi dari perusahaan untuk researcher yang telah memberikan kontribusi keamanan. Masuk ke Hall of Fame perusahaan besar seperti Google, Apple, atau Microsoft adalah pencapaian bergengsi yang bisa memperkuat portofolio karier Anda.

Beberapa researcher Indonesia telah masuk Hall of Fame Google, Microsoft, dan Facebook!

Platform Bug Bounty

Kenali Platform Utamanya

Berikut adalah platform Bug Bounty terkemuka di dunia yang menjadi tempat bertemunya researcher dengan ribuan program dari perusahaan global.



HackerOne

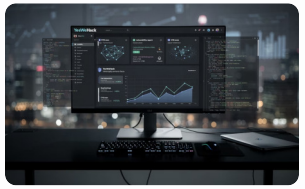
Platform terbesar di dunia dengan lebih dari 3.000 program aktif. Digunakan oleh US Department of Defense, Google, dan Twitter.

Bugcrowd

Dikenal dengan pendekatan crowd-sourced security. Memiliki sistem triage yang membantu researcher pemula belajar lebih cepat.

Intigriti

Platform asal Eropa yang berkembang pesat. Fokus pada perusahaan-perusahaan Eropa dengan standar GDPR yang ketat.



YesWeHack

Platform Eropa yang inklusif dan ramah pemula. Aktif di Asia-Pasifik dan memiliki komunitas yang supportif untuk researcher baru.

Perbandingan Platform Bug Bounty

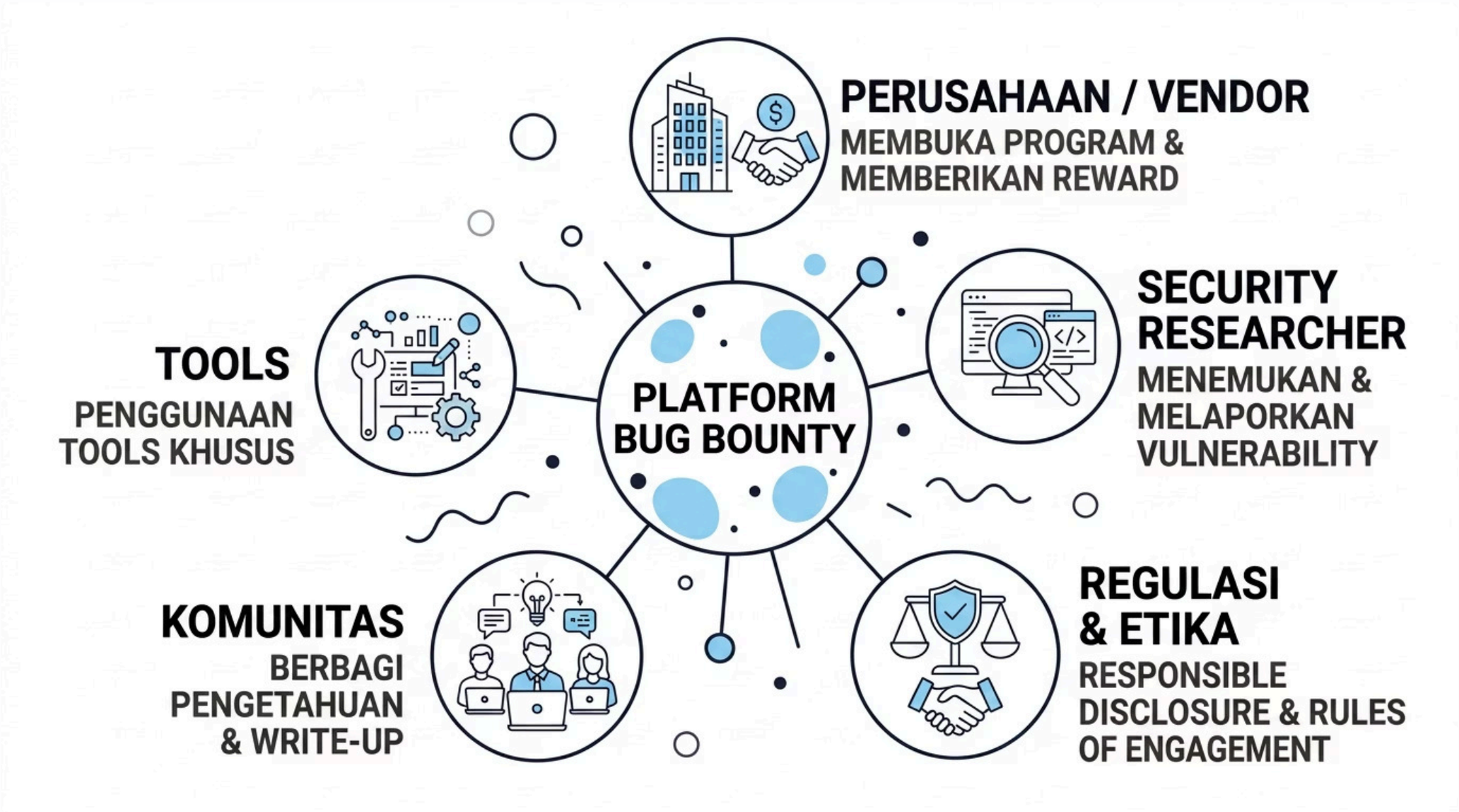
Setiap platform memiliki keunggulan masing-masing. Pilih platform yang sesuai dengan level dan fokus Anda sebagai researcher.

Aspek	HackerOne	Bugcrowd	Intigriti	YesWeHack
Jumlah Program	3.000+	1.000+	500+	400+
Ramah Pemula	Sedang	Tinggi	Sedang	Tinggi
Fokus Wilayah	Global/US	Global/US	Eropa	Eropa/Asia
Private Programs	Ya	Ya	Ya	Ya

Daftar di semua platform secara gratis dan mulailah dengan program public yang memiliki scope luas untuk membangun pengalaman.

Ekosistem Bug Bounty: Gambaran Besar

Bug Bounty adalah bagian dari ekosistem keamanan siber yang lebih luas. Memahami posisi Anda dalam ekosistem ini akan membantu Anda mengembangkan karier dengan lebih terarah.



Peluang Karier

Bug Bounty di Indonesia: Peluang Nyata

Indonesia adalah salah satu negara dengan pertumbuhan digital tercepat di Asia Tenggara, namun kesenjangan keamanan siber masih sangat besar. Ini adalah peluang emas bagi researcher lokal.

$1M+

Reward Tertinggi

Reward single bug terbesar yang pernah dibayarkan, untuk vulnerability kritis di platform global.

40K+

Researcher Aktif

Jumlah researcher aktif di HackerOne saja, bersaing secara global dari seluruh penjuru dunia.

300+

Researcher Indonesia

Estimasi researcher Indonesia yang aktif di platform global, dengan jumlah terus bertumbuh setiap tahunnya.

Kesimpulan Modul 1

Rangkuman & Langkah Selanjutnya

✅ Yang Sudah Anda Pelajari

- Definisi dan konsep dasar Bug Bounty
- Sejarah perkembangan program Bug Bounty
- Perbedaan Ethical Hacking dan Bug Bounty
- Alur kerja dan scope program
- Prinsip Responsible Disclosure
- Sistem CVSS dan jenis reward
- Platform Bug Bounty global

🚀 Langkah Selanjutnya

Setelah memahami fondasi ekosistem Bug Bounty, saatnya mempersiapkan diri secara teknis. Modul berikutnya akan membahas:

- Menyiapkan lab environment yang aman
- Tools dasar yang wajib dikuasai
- Teknik reconnaissance dan information gathering

Daftarkan diri Anda di minimal satu platform Bug Bounty hari ini — mulai eksplorasi program public yang tersedia!

EDY SUSANTO - FOUNDER C-SIX SECURITY