Nama : Rhio Bimo Prakoso S
NIM : 13523123

Distract and Destroy

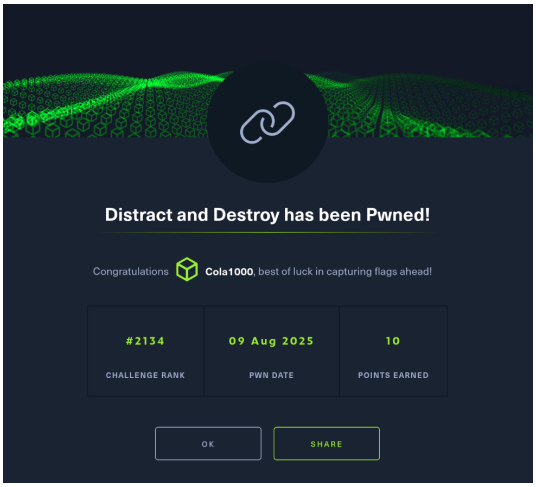
CVSS:
AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:L
(Tbh, I don't learn too much in how to fill the CVE rating/score)

Problem Statement

After defeating her first monster, Alex stood frozen, staring up at another massive, hulking creature that loomed over her. She knew that this was a fight she couldn't win on her own. She turned to her guildmates, trying to come up with a plan. "We need to distract it," Alex said. "If we can get it off balance, we might be able to take it down." Her guildmates nodded, their eyes narrowed in determination. They quickly came up with a plan to lure the monster away from their position, using a combination of noise and movement to distract it. As they put their plan into action, Alex drew her sword and waited for her chance.

POC:
Dari file .Sol harus membuat Creature.balance=0. Itu dapat dilakukan jika 'tx.origin != msg.sender' dan darah monsternya 0. Bisa membuat contract di tengah Creature.sol dan EOA (misal solve.sol) dimana jika memanggil function darinya dia akan *call* attack function di creature selagi dia 'distracted' dan tinggal loot.

Flag:
HTB{tx.0r1gin_c4n_74k3_d0wn_4_m0n5732}



What I Learn:

- Apa itu dan cara pakai foundry
- Apa itu contract :v

Remediation:

Masalah utama pada tantangan HTB Distract & Destroy adalah penggunaan tx.origin untuk logika otorisasi, yang memungkinkan peretas melewati proteksi dengan memasukkan kontrak perantara sehingga tx.origin tetap EOA awal, tetapi msg.sender berbeda. Teknik remediasi yang tepat meliputi:

1) Hentikan penggunaan tx.origin untuk kontrol akses dan ganti dengan msg.sender yang dipadukan dengan pola akses eksplisit seperti Ownable atau AccessControl;

2) Jangan mengandalkan perbedaan EOA vs kontrak untuk logika keamanan, gunakan peran atau tanda tangan kriptografi (misal EIP-712) untuk multi-aktor;

3) Desain alur multi-aktor secara eksplisit, misal dengan menyimpan alamat yang berhak bertindak atau memverifikasi persetujuan off-chain;

4) Ikuti praktik aman untuk interaksi dan pembayaran, seperti checks-effects-interactions dan pull-payment pattern;

5) Otomatisasi deteksi melalui linting (tx.origin), analisis statis (Slither), dan fuzzing (Echidna/Foundry) untuk mencegah bypass melalui kontrak perantara.

Contoh Kasus:

Contoh kasus nyata serupa terjadi pada THORChain (2021), di mana kontrak token RUNE menggunakan tx.origin sehingga peretas dapat menguras token korban melalui kontrak jembatan, menunjukkan risiko nyata pola yang sama. Dengan demikian, lesson HTB mengajarkan bahwa logika berbasis jalur panggilan (tx.origin) rapuh dan harus diganti dengan kontrol akses eksplisit berbasis msg.sender dan tanda tangan kriptografi.

Agriweb

CVSS:

Problem Statement
Digital farmlands lie ruined as drones spin out of control and greenhouses overheat; the white-hats must infiltrate the corrupted AgriWeb interface and bring the fields back to life.

POC:
Harus masuk ke interface websitenya dengan juga modif si payloadnya.

Flag:

What I Learn:

Remediation:

Contoh Kasus:

Help aku gak sempet :v