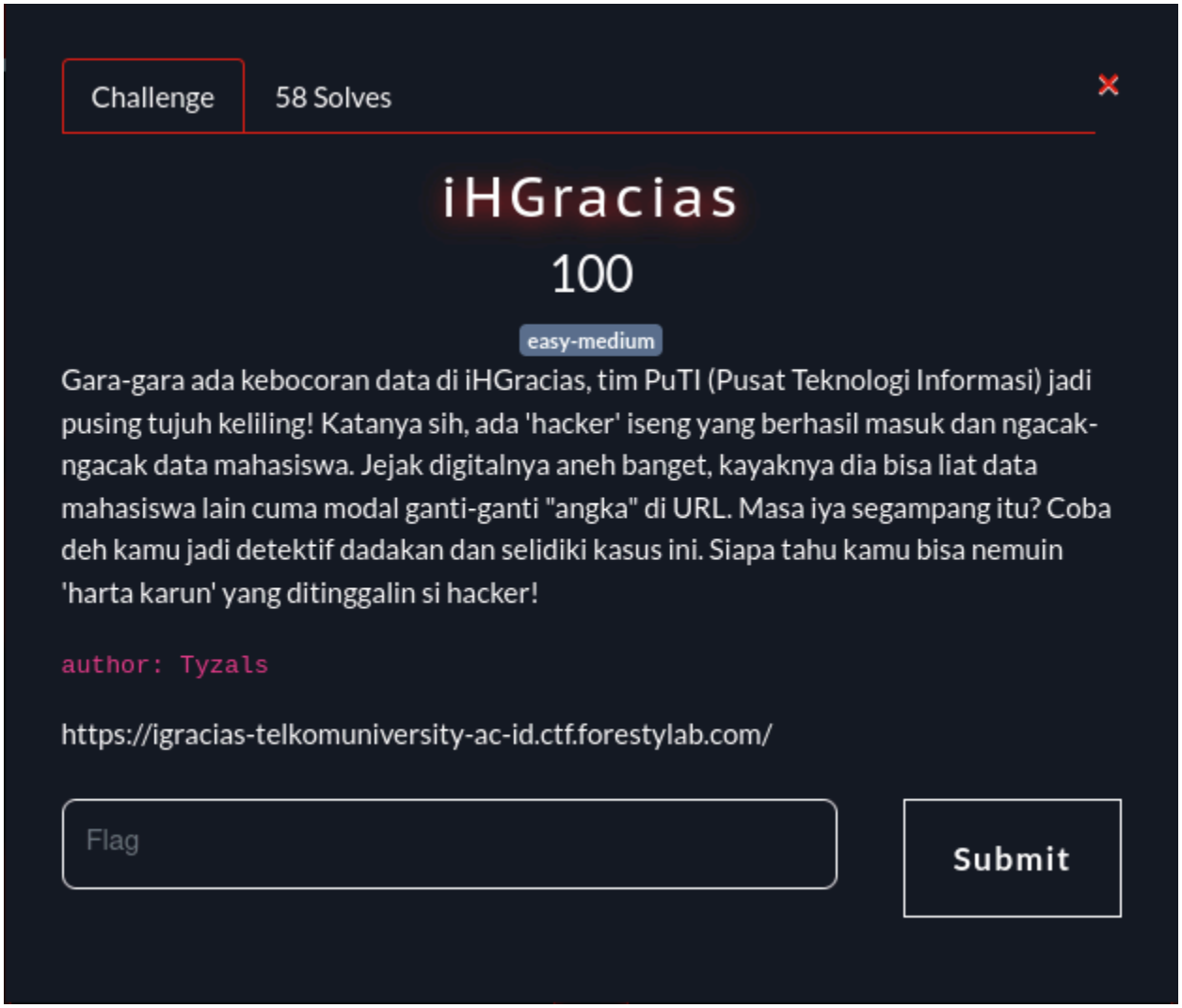
Write-up iHGracias

Player: Constantine
Kategori: Web Exploitation



Konteks Dikit

Challenge ini ngasih kita simulasi mini dari kelemahan di aplikasi web kampus, seperti credential disclosure, cookie tampering, dan IDOR di admin panel. Tujuan akhirnya nemuin flag yang disimpan di halaman profil user lain yang hanya bisa diakses admin. Cukup perhatikan source code, lalu manipulasi cookie, dan akses endpoint admin.php.

Phase 1: Recon

Kita mulai dari halaman login iGracias.
Awalnya, tampilan login kelihatan standar, form username dan password.

Namun saat aku cek View Source, aku nemu sesuatu yang *sudah sangat mencurigakan*. Di dalam komentar HTML ada kredensial test user:

```
<div class='box'><a id="link2017" style="text-transform: none !important;color:#fff; text-decoration:underline;" h
<!-- LOGIN CREDENTIAL (for Inspect Element / View-Source): username: iniAkunUser | password: iniPasswordUser -->
```

Phase 2 — Login sebagai Mahasiswa

Masuk menggunakan kredensial tersebut, dan benar, kita diarahkan ke dashboard mahasiswa biasa. Ga ada akses admin, buka admin panel malah error “you aren't allowed to view this page.” Langkah selanjutnya adalah membuka DevTools → Storage → Cookies.

Dan… jackpot. Ada cookie:

Name	Value
PHPSESS…	e4b298006aff19a226adc4420a46…
role	user
user_id	1010

Website ini enggak melakukan integrity check terhadap cookie. Artinya kalau kita ubah `role=user` menjadi `role=admin`, backend langsung percaya. Ini sejenis PrivEsc.

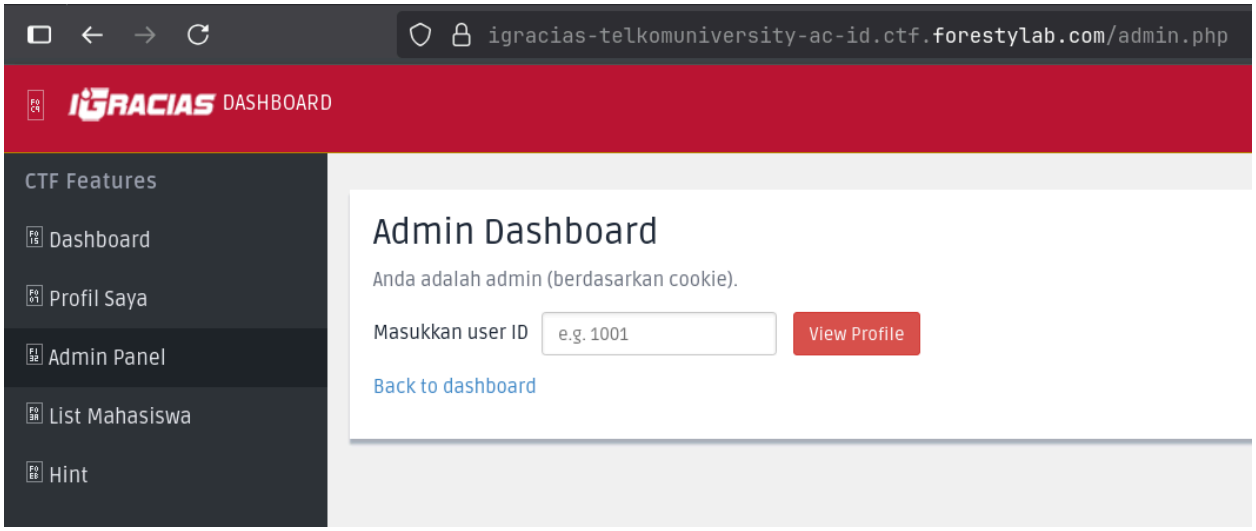
Phase 3: Cookie Tampering

Setelah cookie diubah:

Name	Value
PHPSESS…	e4b298006aff19a226adc4420a46…
role	admin
user_id	1010

Kita refresh halaman.

Menu **Admin Panel** sekarang terbuka meskipun kita bukan admin beneran.



Phase 4 IDOR

Begitu masuk Admin Panel, kita dapat form untuk memasukkan **user ID** lalu menampilkan profil user tersebut. Kita cukup fuzzing manual aja 1001 sampai 1003, kemudian klik *View Profile*.

Dan di situlah flagnya, disisipkan di kolom bio.

Flag:

FORESTY{R3ll_c4Se_iNi_W0k_elllll_cTriW_t4mpering_id0r}