

iHGracias

Player: constantine

Kategori: Web Exploitation

The screenshot shows a challenge card for the 'iHGracias' challenge. At the top left is a red-bordered button labeled 'Challenge'. To its right is the text '58 Solves'. In the top right corner is a small red 'X' icon. The challenge title 'iHGracias' is centered at the top in a large white font. Below it is the point value '100' in a large white font. Underneath the point value is a blue rectangular button labeled 'easy-medium'. The challenge description is written in white text: 'Gara-gara ada kebocoran data di iHGracias, tim PuTI (Pusat Teknologi Informasi) jadi pusing tujuh keliling! Katanya sih, ada 'hacker' iseng yang berhasil masuk dan ngacak-ngacak data mahasiswa. Jejak digitalnya aneh banget, kayaknya dia bisa liat data mahasiswa lain cuma modal ganti-ganti "angka" di URL. Masa iya segampang itu? Coba deh kamu jadi detektif dadakan dan selidiki kasus ini. Siapa tahu kamu bisa nemuin 'harta karun' yang ditinggalin si hacker!' Below the description is the author information 'author: Tyzals' in purple text. A URL 'https://igracias-telkomuniversity-ac-id.ctf.forestlab.com/' is provided. At the bottom left is a large button labeled 'Flag' and at the bottom right is a button labeled 'Submit'.

Phase 1: Recon

Kita mulai dari halaman login.



Halaman terlihat normal, form username & password tanpa indikasi bug mencolok, karena belum ada interaksi yg berarti, lanjut buka **View Page Source**.

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

Pada komentar HTML terdapat kredensial user uji coba, ini memberikan akses awal menuju dashboard mahasiswa biasa.

Phase 2: Login sebagai Mahasiswa

Setelah login menggunakan kredensial yang muncul di source:

Hari Winata (2108101008)

Username	hari
TTL	Tasikmalaya, 2001-12-03
Gender	Male
Program Studi	Rekayasa Perangkat Lunak
GPA	3.12
Blood Type	A
Email	hari.winata@student.telkomuniversity.ac.id
Phone	+62-811-1008-0008
Address	Jl. Raya Tasik No.9, Tasikmalaya
Parent Contact	+62-811-2008-0008 (Ayah Slamet)
Bio	Suka hiking dan membangun aplikasi mobile.

Kita hanya mendapatkan akses user biasa.

Admin panel tidak dapat dibuka dan menampilkan pesan "*you aren't allowed to view this page.*" Langkah berikutnya adalah memeriksa **Cookies** melalui DevTools → Application → Storage.

Name	Value
PHPSESS...	174ccb2167e72843532adb8c7d86...
role	user
user_id	1008

Aplikasi tidak melakukan integrity check pada cookie.

Ketika kita ubah `role=user` menjadi `role=admin`, server langsung percaya, ini adalah **Privilege Escalation** melalui **cookie tampering**.

Phase 3: Cookie Tampering

Setelah kita ubah cookie:

Filter Items	
Name	Value
PHPSESS...	174ccb2167e72843532adb8c7d86...
role	admin
user_id	1008

Setelah refresh, menu **Admin Panel** muncul meskipun kita bukan admin sungguhan. Aplikasi ini tidak memvalidasi role di server, murni mengandalkan client-side cookie.

Phase 4: IDOR

Masuk ke Admin Panel.

Admin Dashboard

Anda adalah admin (berdasarkan cookie).

Masukkan user ID e.g. 1001

View Profile

[Back to dashboard](#)

Admin dapat memasukkan user ID untuk melihat profil siapa pun. Namun tidak ada validasi apakah admin berhak mengakses data user tersebut. Ini adalah **Insecure Direct Object Reference (IDOR)**.

Kita mulai fuzz ID 1001, 1002, 1003... hingga menemukan profil yang berisi flag.

Admin Dashboard

Anda adalah admin (berdasarkan cookie).

Masukkan user ID

e.g. 1001

[View Profile](#)

Profile for ID 1003

Username: citra

Bio: Penyuka kopi dan penggemar UI/UX.

FLAG: FORESTY{R1II_c4Se_iNi_Wok_eIIII_ctrl+u_tampering_id0r}

[Back to dashboard](#)

Flag disisipkan pada kolom bio user admin-target.

Karena tidak ada pembatasan akses, flag dapat dilihat bebas setelah cookie tampering.

Final Flag

FORESTY{R3II_c4Se_iNi_W0k_eIIII_cTriW_t4mpering_id0r}