

Write-up iHGracias

Player: Constantine

Kategori: Web Exploitation

Challenge 58 Solves X

iHGracias

100

easy-medium

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!

author: Tyzals

<https://igracias-telkomuniversity-ac-id.ctf.forestylab.com/>

Flag Submit

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;" href="http://iGracias.com/index.php?r=site%2Findex&u=iniAkunUser&p=iniPasswordUser">...</a>
<!-- 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.

The screenshot shows a browser window with the URL `igracias-telkomuniversity-ac-id.ctf.forestlab.com/admin.php`. The page title is "IGRACIAS DASHBOARD". On the left, there's a sidebar with "CTF Features" and links for "Dashboard", "Profil Saya", "Admin Panel" (which is highlighted in blue), "List Mahasiswa", and "Hint". The main content area is titled "Admin Dashboard" and displays the message "Anda adalah admin (berdasarkan cookie)". It has a form with an input field labeled "Masukkan user ID" containing "e.g. 1001" and a red "View Profile" button. Below the form is a link "Back to dashboard".

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.

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_eIII_ctrl+u_tampering_id0r}

Flag:

FORESTY{R3II_c4Se_iNi_W0k_eIII_cTriW_t4mpering_id0r}