

How To Play CTF

(Capture The Flag) by aria

Platform ctf : <https://ctf.ariaf.my.id>

Source code : <https://github.com/ariafatah0711/ctfs>



Daftar Isi

Daftar Isi	2
Pendahuluan	3
1.1 Apa itu CTF (Capture The Flag)	3
1.2 Tujuan dari Tutorial Ini	3
1.3 Gambaran Umum Kategori Challenge	4
Persiapan	5
2.1 Buat akun	5
2.2 Tools Yang dipersiapkan	6
Menyelesaikan Challenge	7
3.1 Join Discord	7
3.2 Read The Rules!	9
3.3 QR Vault	11
3.4 Danau	11
3.5 Base & Shift	11
3.6 exif strings	11
3.7 tebak kata	11
3.8 Leaky Login	11

Pendahuluan

1.1 Apa itu CTF (Capture The Flag)

Capture The Flag (CTF) adalah kompetisi keamanan siber di mana peserta harus menyelesaikan serangkaian tantangan (*challenges*) untuk menemukan “flag”, potongan teks unik yang menjadi bukti bahwa kamu berhasil menaklukkan tantangan tersebut.

Biasanya flag ditulis dengan format seperti:

```
CTF{this_is_an_example_flag}
```

Atau

```
FGTE{your_flag_here}
```

Konsep CTF diambil dari permainan fisik “Capture The Flag”, di mana dua tim berebut bendera lawan. Dalam dunia *cyber security*, “benderanya” adalah data rahasia yang disembunyikan di sistem, file, atau program. Peserta ditantang untuk menemukan flag dengan memanfaatkan kemampuan analisis, logika, pemrograman, dan pengetahuan keamanan siber.

Jenis CTF Berdasarkan Format Kompetisi:

a. **Jeopardy-Style CTF**

Format paling umum. Peserta menyelesaikan challenge dari berbagai kategori (Web, Crypto, Forensic, dsb.) dan mendapat poin tiap berhasil menemukan flag.

Semakin sulit challenge, semakin besar poinnya.

b. **Boot To Root**

Boot to Root adalah format CTF di mana peserta mendapatkan akses ke sebuah mesin atau sistem virtual “dari nol” (boot) dan tugasnya adalah mendapatkan **privilege tertinggi (root/administrator)** pada mesin tersebut, .

c. **Attack–Defense CTF**

Format ini biasanya dimainkan oleh tim. Setiap tim harus melindungi server sendiri sambil menyerang server tim lain untuk mencuri flag.

Cocok untuk peserta yang sudah expert di bidang network & exploitation.

1.2 Tujuan dari Tutorial Ini

Dokumen ini dibuat sebagai **panduan dasar untuk pemain baru** di dunia CTF, khususnya di platform. <https://ctf.ariaf.my.id>

Tujuannya agar peserta bisa:

- a. Memahami konsep dasar CTF.
- b. Mempelajari tools dasar yang sering digunakan.
- c. Mengerjakan contoh tantangan pertama dengan langkah-langkah yang jelas.

Jadi kalau ini pertama kalinya kamu ikut CTF — tenang, panduan ini akan nuntun kamu dari nol sampai bisa menyelesaikan challenge pertama dengan percaya diri 😊

1.3 Gambaran Umum Kategori Challenge

Setiap CTF berisi berbagai kategori tantangan, masing-masing mengasah kemampuan berbeda dalam keamanan siber. Di bawah ini penjelasan kategori-kategori yang umum ditemui — termasuk catatan khusus untuk **CTF Aria**: platform ini berjalan di Vercel + Supabase dan admin belum menyediakan server sendiri, sehingga hanya tantangan yang **dapat dijalankan tanpa backend server** yang bisa dihadirkan.

Kategori	Deskripsi	Contoh Tantangan / Tools yang Dipakai
Misc	Soal umum atau teka-teki ringan. Bisa berupa file teks aneh, QR code, encoding, atau puzzle. Fokus pada logika dan ketelitian.	Decode QR, pesan tersembunyi di file, berbagai encoding (Base64, hex)
Web	Tantangan berbasis aplikasi web ringan yang tidak membutuhkan server terpisah . Biasanya menguji bug umum seperti form injection, XSS sederhana, atau mencari direktori tersembunyi.	Login bypass sederhana, cari /hidden folder, LFI ringan (jika memungkinkan)
Forensic	Analisis file digital (gambar, audio, dump data) untuk mencari flag tersembunyi. Cocok untuk soal yang bisa diselesaikan dengan alat lokal.	strings, exiftool, binwalk, analisis steganografi
Crypto	Soal enkripsi & dekripsi — dari kriptografi klasik sampai transformasi data modern. Fokus pada teknik analisis pola dan decode.	Base64, Caesar Cipher, ROT13, frequency analysis
Reverse	Analisis program/biner secara statis atau dinamis tanpa perlu akses server. Melatih pemahaman assembly, format file, dan logika program.	Analisis file .exe/.elf (statis), dekomplilasi sederhana
Pwn	Eksplotasi memori dan remote exploitation yang biasanya membutuhkan akses server/target yang bisa dieksplotasi .	(Kategori Pwn biasanya butuh layanan/target berjalan)
OSINT	Open Source Intelligence — cari informasi dari sumber publik (web, media sosial, DNS, dsb.) untuk menemukan clue/flag.	Penelusuran web, analisis metadata publik, investigasi akun

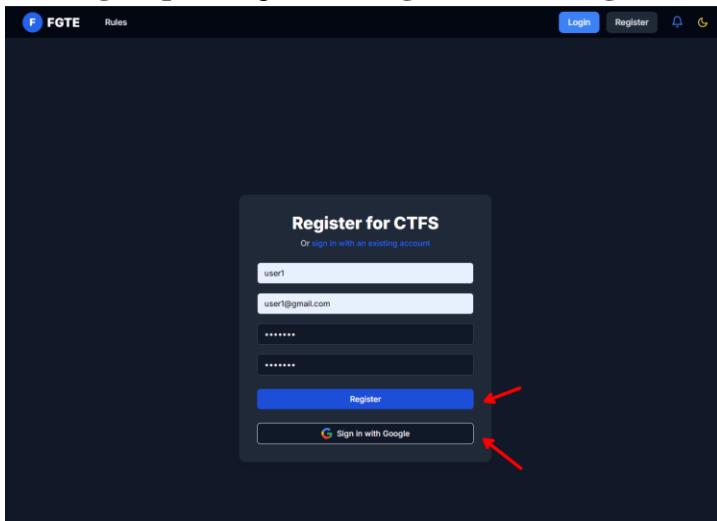
Persiapan

Sebelum mulai main, kamu butuh dua hal: **akun di platform CTF** dan **tools dasar** yang siap digunakan. Bagian ini akan bahas keduanya.

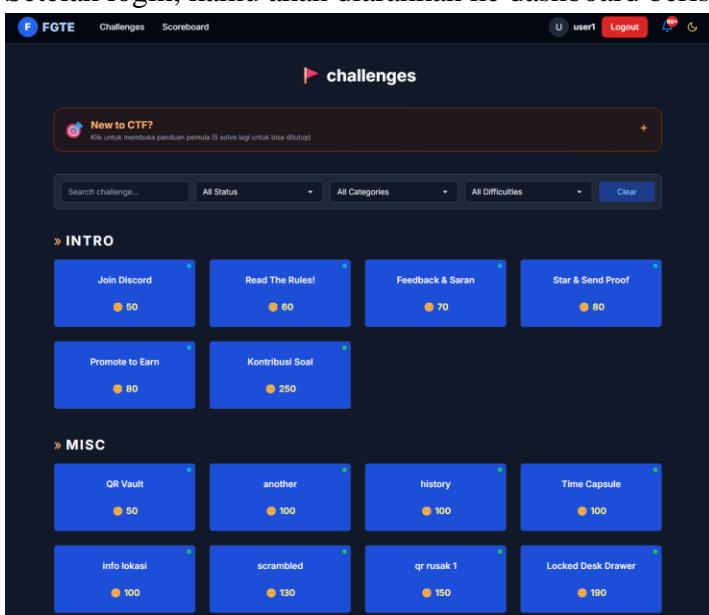
2.1 Buat akun

Langkah-langkah:

- a. Buka <https://ctf.ariaf.my.id>.
- b. Klik **Register**.
- c. Isi data berikut:
 - Username (bebas tapi unik)
 - Email valid
 - Password
- d. Klik **Sign Up**, atau gunakan **Sign in with Google** untuk cara cepat.



- e. Setelah login, kamu akan diarahkan ke dashboard berisi daftar challenge.



2.2 Tools Yang dipersiapkan

Minimal Tools yang direkomendasikan di siapkan:

1. Browser – (Wajib)
2. Web yang sekiranya bisa membantu solving – (Opsional)
 - a. Cyberchef
 - b. Reverse Image
 - c. QR Scanner
 - d. Stegno Online
 - e. dll
3. Terminal Linux (Kali, Ubuntu, Parrot) – (Opsional)
 - a. Python3
 - b. Exiftool, Strings
 - c. File, Binwalk, Steghide
 - d. xxd, hexedit

Menyelesaikan Challenge

3.1 Join Discord



Solve:

1. Klik Link Discord

Di halaman challenge, terdapat tautan menuju server Discord: <https://s.id/dev-universe>

2. Masuk ke Server Discord

Setelah masuk, kamu akan melihat beberapa channel.

Sebelum bisa mengakses semuanya, kamu **harus mengambil role** terlebih dahulu.

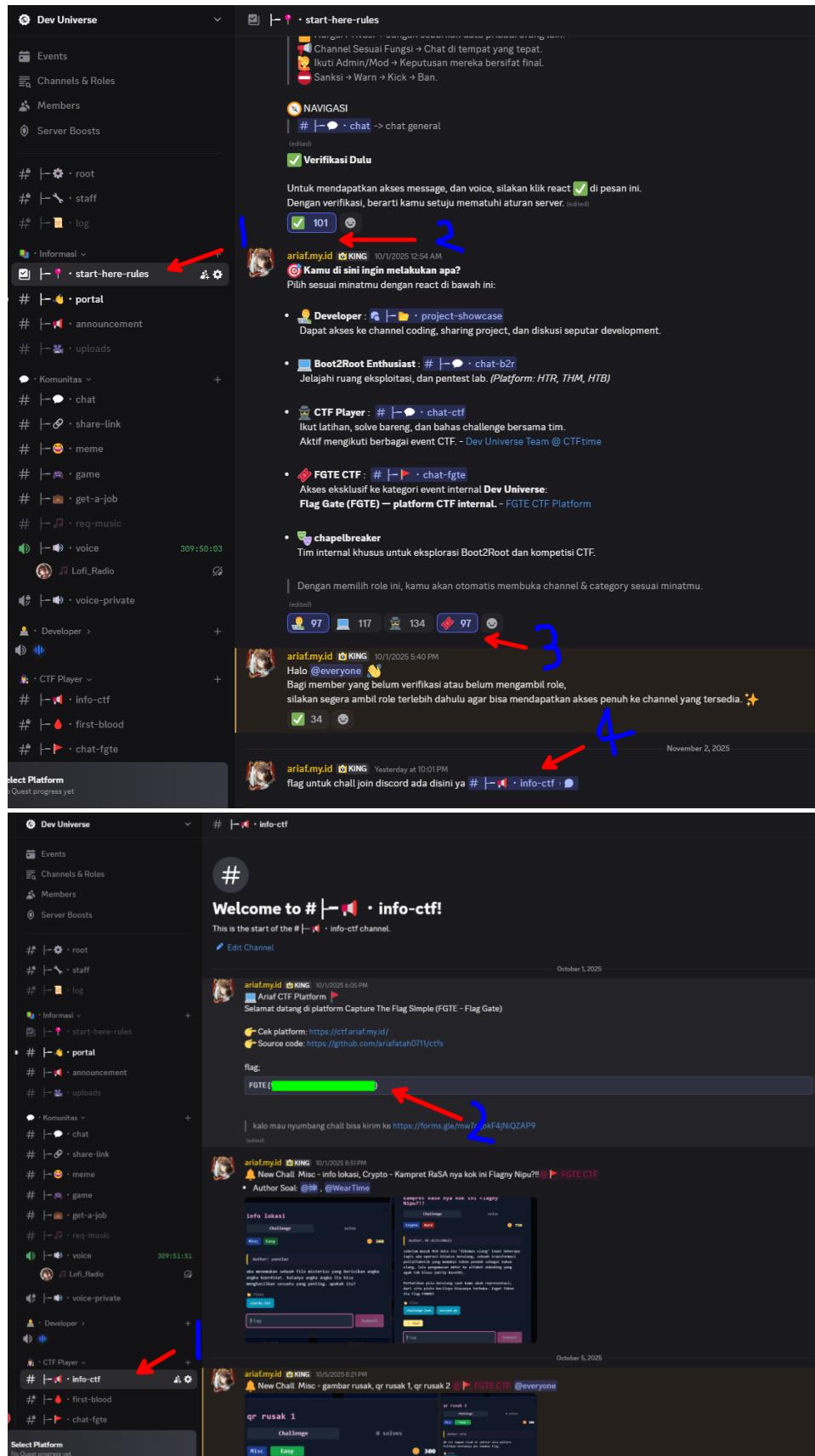
3. Ambil Role di Channel #start-here-rules

Buka channel #start-here-rules.

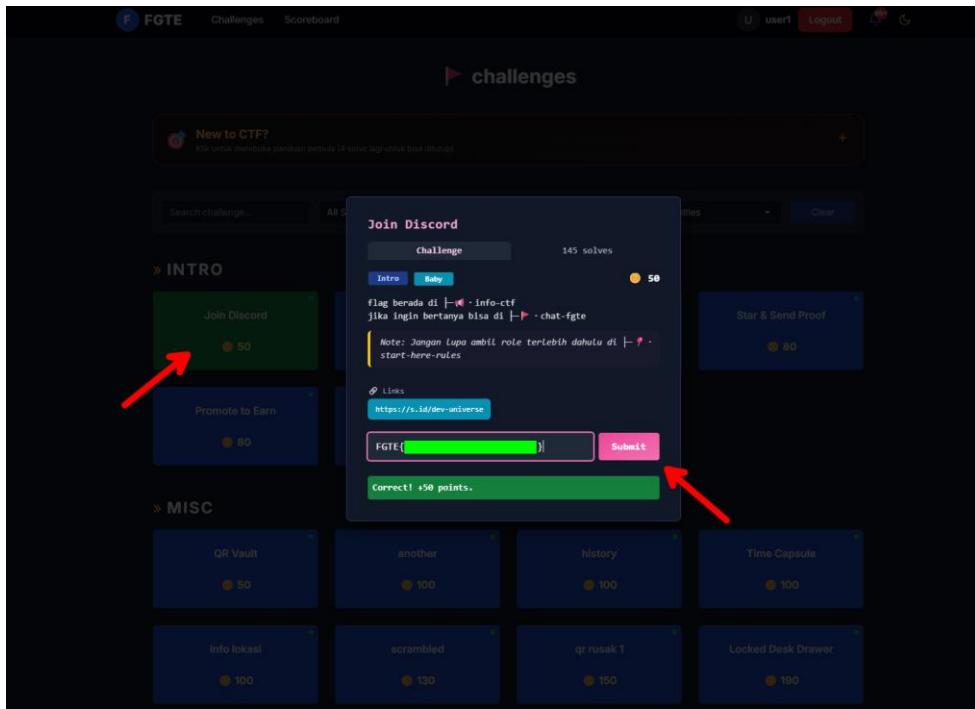
➤ Klik reaksi emoji untuk mendapatkan role fgte.

Setelah itu, channel lain seperti #info-ctf dan #chat-fgte akan terbuka.

4. Cari Flag di Channel #info-ctf di bagian paling atas, atau langsung click link di bagian #start-here-rules



Setelah copy flag nya submit ke platform ctf nya



3.2 Read The Rules!

A screenshot of the 'Read The Rules!' challenge page. It has 62 solves and a value of 60. The challenge type is 'Challenge'. The description says: 'Pastikan kamu membaca seluruh Rules di web ini dengan saksama.' Below that is a 'Links' section with a link to 'https://ctf.ariaf.my.id/rules'. At the bottom is a text input field with 'Flag' in it and a 'Submit' button.

Solve:

1. Buka halaman challenge “**Read The Rules!**” di platform.
2. Jangan buru-buru inspect element atau view page source — flag sebenarnya **sudah ada di halaman**, cuma **warnanya sama dengan background**, jadi tidak terlihat.
3. Tekan **Ctrl + A** untuk menyeleksi seluruh teks di halaman.
4. Setelah diseleksi, kamu akan melihat **kode dalam bentuk Base64** muncul.

The screenshot shows the FGTE Rules page. At the top, there are navigation links for 'Challenges' and 'Scoreboard'. On the right, there are user status indicators for 'user1' and a 'Logout' button. Below the header, the title 'Platform FGTE Rules' is displayed with a small flag icon.

A message below the title reads: 'Mohon baca dan patuh aturan berikut sebelum mengikuti challenge di CTFS Platform.'

The page lists ten rules, each with a title and a detailed description:

- Fokus ke Challenge**: Mainkan challenge untuk mencari flag. Fokus pada permainan — jangan ganggu atau eksplorasi layanan lain.
- Kolaborasi & Bantuan**: Boleh kerja sama, pakai AI, atau tanya admin/author. Tapi jangan pernah membagikan flag ke publik.
- Point**: Poin tergantung tingkat kesulitan. Sistem dynamic (turun tiap solve) dan static (tetap). Baby: 150–50–5, Easy: 300–100–10, Medium: 500–300–20, Hard: 750–500–50, Impossible: 1000–3000 (tetap).
- Writeup**: Boleh dipublikasikan 30 hari setelah rilis dan jika sudah disolve ≥10 orang. Semua flag wajib {REDACTED}.
- Akun**: Gunakan satu akun per peserta. Dilarang membuat akun ganda untuk keuntungan apa pun.
- Etika & Privasi**: Hormati peserta lain. Dilarang mengambil atau menyebarkan data pribadi.
- Larangan Serangan**: Jangan serang host, platform, atau lakukan brute force pada layanan apa pun.
- Pelaporan Bug**: Laporkan bug atau celah keamanan ke admin secepatnya.

At the bottom of the page, a red arrow points to a highlighted section of the URL: `RkdURXtZb3VfSGF2ZV9BY2NlcHRIZF9BbGxfUnVsZXNfQW5kX0V0aGljc30=`. Below the URL is a 'Back to Home' button.

At the very bottom, it says: 'Built with Next.js, TailwindCSS, Framer Motion, and hosted with Supabase and Vercel.'

5. Salin kode Base64 tersebut.
6. Buka **CyberChef**, dan masukan teks base64 ke dalam input, dan cari base64 di bagian operations, dan drag and drop ke dalam recipe, flag akan muncul di bagian output

The screenshot shows the CyberChef interface. The left sidebar has a list of operations, with 'base64' highlighted by a blue arrow labeled '2'. Below it, 'From Base64' is also highlighted by a blue arrow labeled '3'. The main area shows a 'Recipe' window with 'From Base64' selected. The 'Input' field contains the copied Base64 string: `RkdURXtZb3VfSGF2ZV9BY2NlcHRIZF9BbGxfUnVsZXNfQW5kX0V0aGljc30=`. A red arrow labeled '4' points to the 'Output' field, which displays the decrypted flag: `FGTE{}`.

3.3 QR Vault

Comming Soon

3.4 Danau

Comming Soon

3.5 Base & Shift

Comming Soon

3.6 exif strings

Comming Soon

3.7 tebak kata

Comming Soon

3.8 Leaky Login

Comming Soon