KOMINFO

RISK ASSESSMENT VULNERABILITY REPORT

Nama	: Gede Ananda
Phone no	: 085896873540
Email	: gedeananda03@gmail.com
Endpoint	: https://wbs.kominfo.go.id/pengaduan_wbs/destroy/(id)
Date Report	: 16 Mei 2024

Contents

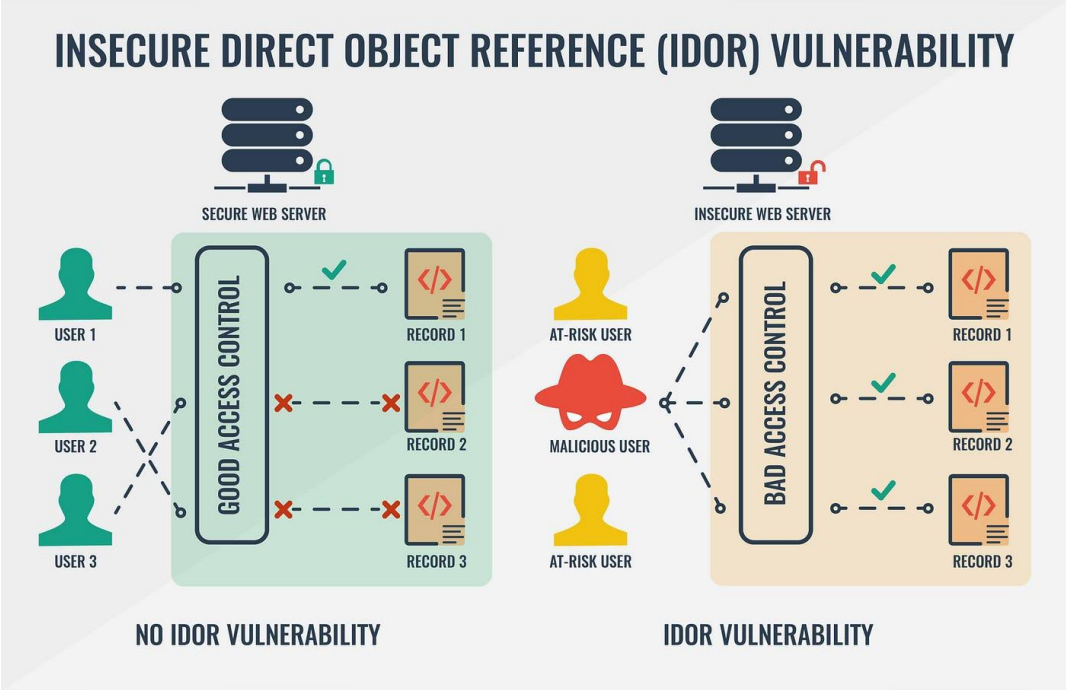
INTRO

Assalamu'alaikum Wr. Wb. Shalom, Om Swastiastu, Namo Budaya, Salam Kebajikan. Selamat Sejahtera bagi kita semua.

Yth.Bapak/Ibu

Perkenalkan nama saya Gede Ananda pada tanggal 16 mei 2024 , Jam 21.13 WIB saya ingin melaporkan kerentanan pada website https: https://wbs.kominfo.go.id/

IDOR (Insecure Direct Object Reference)



Description

Insecure Direct Object Refrence (IDOR) memungkinkan penyerang untuk memotong otorisasi dan mengakses sumber daya secara langsung dengan memodifikasi nilai paramater yang digunakan untuk mengarahkan langsung ke objek. Sumber daya semacam itu bisa menjadi entri database milik pengguna lain, file dalam sistem, dan banyak lagi. Hal ini disebabkan oleh fakta bahwa aplikasi tersebut memasukan input yang dipasok pengguna dan menggunakannya untuk mengambil objek tanpa melakukan pengecekan otoriasasi yang memadai.

Impact

Kerentanan IDOR dapat dieksploitasi dengan mudah, tetapi dampak dari jenis serangan ini berpotensi menjadi menjadi bencana besar. Di bawah ini adalah beberapa cara IDOR dapat berdamapak pada kerahasiaan, Integritas, dan Ketersediaan data clint:

1. *Kerasahasiaan – Serangan IDOR yang berhasil memberikan penyerang akses ke suatu yang seharusnya tidak bisa mereka lihat. Ini bisa berupa apa saja, mulai dari kode diskon untuk pembeli yang sering berbelanja hingga lebih parahnya adalaha jika itu data pribadi para pengguna seperti nama lengkap,alamat lengkap, alamat, no hp, email dll.*
2. *Integritas – Dalam beberapa kasusu, penyerang mungkin dapat menggunakan IDOR untuk memodifikasi data, biasanya jenis serangan ini memanipulasi parameter dalam perminataan HTTP POST*
3. *Ketersediaan – IDOR juga dapat disalahgunakan untuk memperngaruhi ketersediaan sumber daya. Bayangkan sebuah fungsi dalam aplikasi PHP yang menghapus dokumen berdasarkan nama file, tanpa pemeriksaan otorisasi yang tepat, penyerang mungkin dapat mengubah nama file dan menghapus dokumen yang bahkan tidak mereka akses!*

References

- https://portswigger.net/web-security/access-control/idor

Discovered Vulnerability Details

Vulnerability #1

IDOR (Insecure Direct Object Reference)

SEVERITY:	***STATUS:***
Medium	***Unsolved***

Endpoint:

- https://wbs.kominfo.go.id/pengaduan_wbs/destroy/(id)

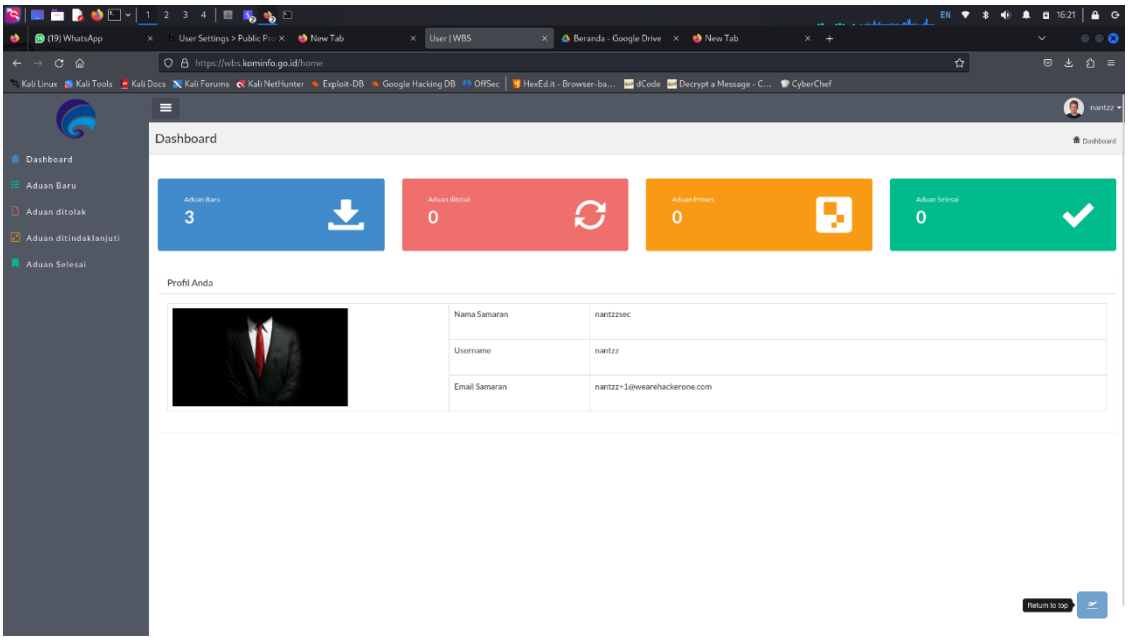
Video PoC

- https://drive.google.com/drive/folders/1boI0McMF3ttGBU87KQhqZFszPc1F3PCM?usp=sharing

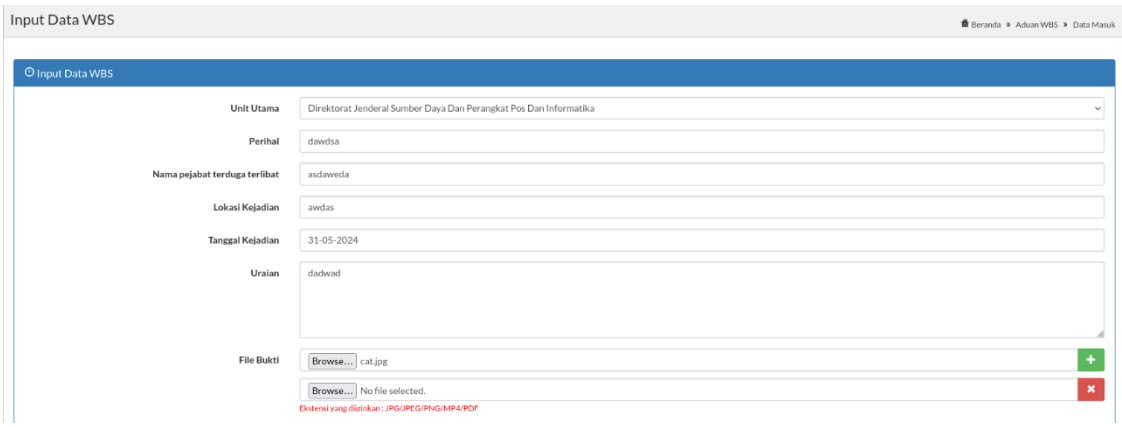
Step to reproduce:

1. Step 1 – Mengunjungi halaman

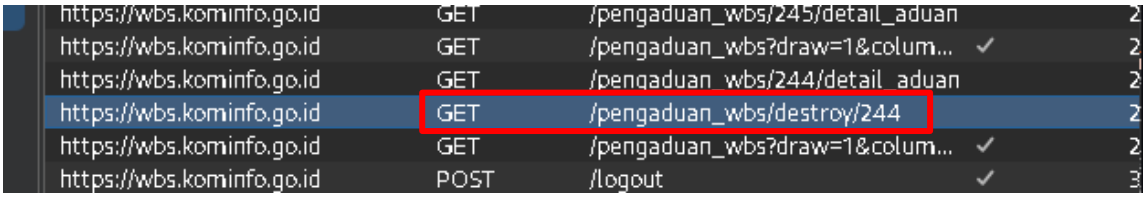
   Saya mengunjungi web https://wbs.kominfo.go.id/ dan melakukan pendaftaran di website tersebut



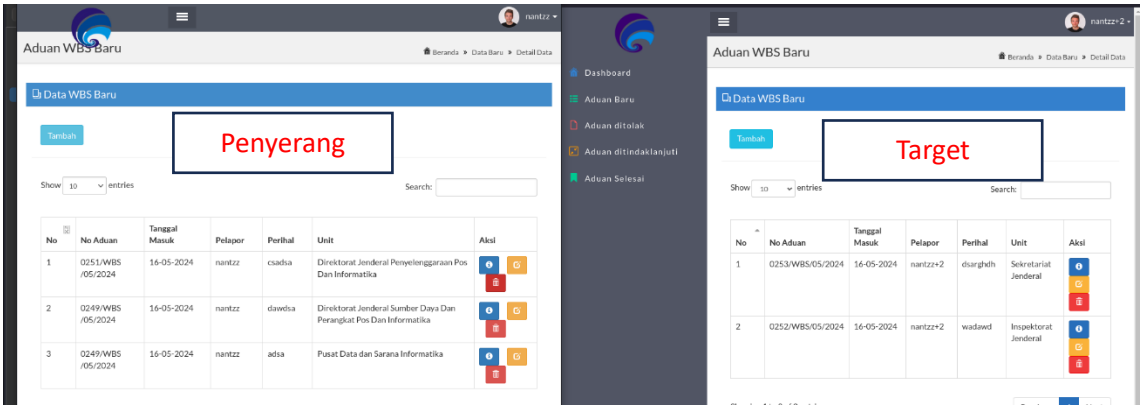
2. Step 2 – Membuat aduan
   Saya memcoba membuat aduan baru dan mengisi semua kolom yang ada untuk mendapatkan scope di burpsuite



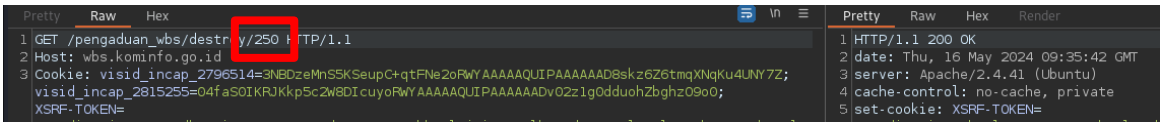
3. Step 3 - Memeriksa Endpoint
   Setelah masuk di burp suite saya tertarik dengan data post dan saya mencoba untuk menghapus salah satu laporan, muncul sebuah endpoint destroy dan tertarik dengan endpoint ini, karena memiliki id seperti gambar di bawah

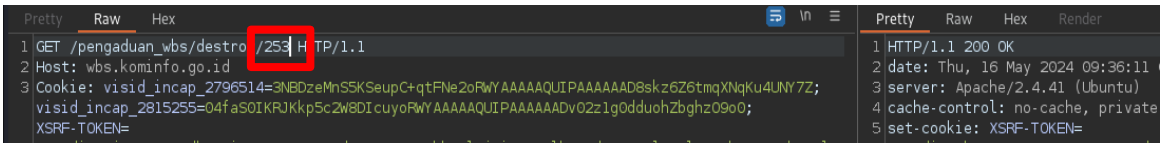


4. Step 4 - Membuat akun target
   Saya curiga adanya sebuah bug Idor pada endpoint tersebut dan mencoba untuk membuat akun kedua sebagai target seperti gambar di bawah

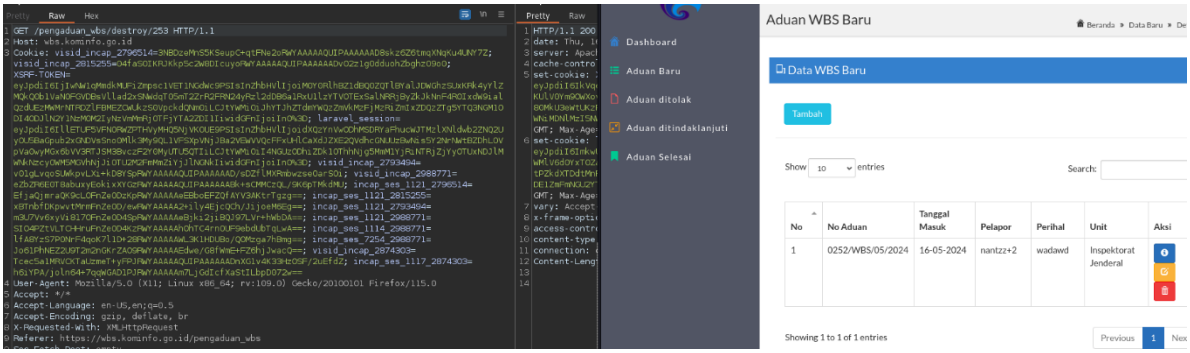


5. Step 5 - Simulasi penghapusan data
   Attacker akan menghapus data miliknya dan akan merubah id penghapusan menjadi id milik korban, 250 sebagai id attacker dan 252 sebagai id victim dan endpoint berjalan dengan normal dan ternyata benar adanya bug Idor





6. Step 6 - Hasil simulasi
   Ketika melakukan sending Endpoint ternyata laporan dari victim akan terhapus dari tabel aduan



Screenshoot and log:
https://drive.google.com/drive/folders/1boI0McMF3ttGBU87KQhqZFszPc1F3PCM?usp=sharing
Video Dokumentasi PoC untuk melengkapi dokumentasi laporan.

Recommendation/Fix

Memulikan Kerentanan IDOR

- Pengembang harus menghindari menampilkan refrensi objek pribadi seperti id user atau kunci lainnya yang memungkin kan bisa di exploitasi
- Melakukan Enkripsi pada paramater id_user yang digunakan pengguna
- Validasi parameter harus diterapkan dengan benar
- Verifikasi semua objek yang direferensikan harus diperiksa
- Token harus dibuat sedemikian rupa sehingga hanya dapat dipetakan ke pengguna dan tidak bersifat public
- Pastikan kueri dicakup ke pemilik sumber daya / data
- Hindari hal-hal seperti menggunakan UUID(pengenal unik universal) melalui ID Berurutan karena UUID sering kali membiarkan kerentanan IDOR tidak terdekteksi

Best Regards,
Gede Ananda