



## RISK ASSESSMENT VULNERABILITY REPORT

---

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

---

### Contents

#### **INTRO**

#### ***IDOR (Insecure Direct Object Reference)***

##### ***Description***

##### ***Impact***

##### ***References***

##### ***Step to reproduce:***

1. *Step 1 – Mengunjungi halaman*
2. *Step 2 – Membuat aduan*
3. *Step 3 - Memeriksa Endpoint*
4. *Step 4 - Membuat akun target*
5. *Step 5 - Simulasi penghapusan data*
6. *Step 6 - Hasil simulasi*

##### ***Screenshots/Logs:***

##### ***System/Environment Detail:***

##### ***Severity:***

##### ***Recommendation/Fix***

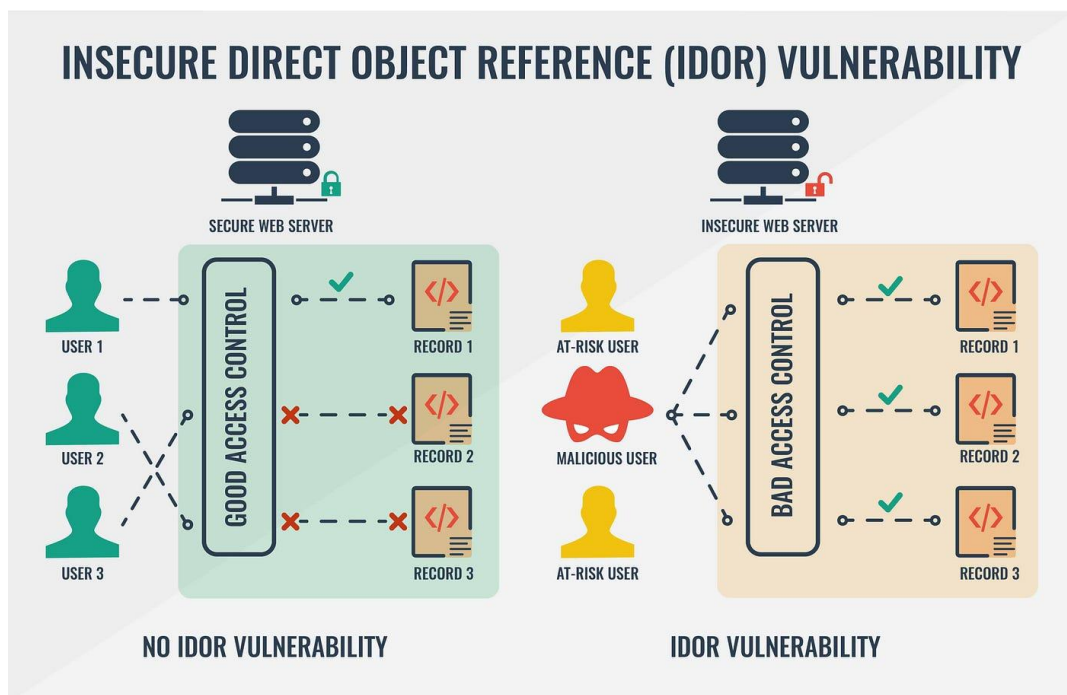
## INTRO

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://wbs.kominfo.go.id/>

## IDOR (Insecure Direct Object Reference)



## Description

*Insecure Direct Object Reference (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 bencana besar. Di bawah ini adalah beberapa cara IDOR dapat berdampak pada kerahasiaan, Integritas, dan Ketersediaan data client:*

1. *Kerahasiaan – 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 adalah jika itu data pribadi para pengguna seperti nama lengkap, alamat lengkap, alamat, no hp, email dll.*
2. *Integritas – Dalam beberapa kasus, penyerang mungkin dapat menggunakan IDOR untuk memodifikasi data, biasanya jenis serangan ini memanipulasi parameter dalam permintaan 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:***

***Medium***

***STATUS:***

***Unsolved***

***Endpoint:***

- [https://wbs.kominfo.go.id/pengaduan\\_wbs/destroy/\(id\)](https://wbs.kominfo.go.id/pengaduan_wbs/destroy/(id))

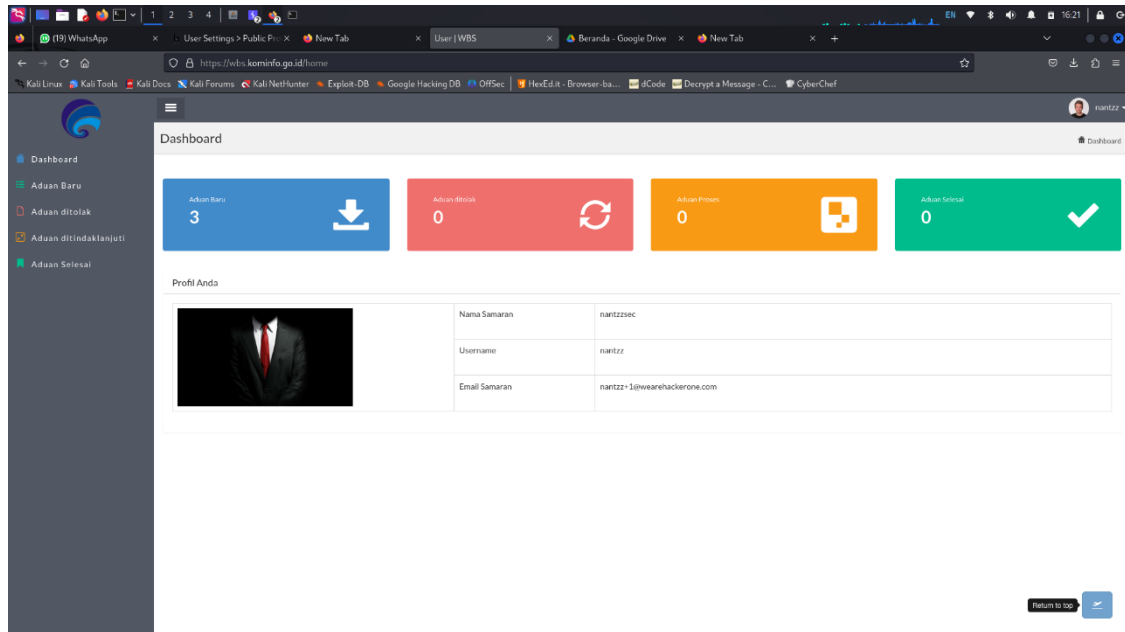
***Video PoC***

- <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 mencoba membuat aduan baru dan mengisi semua kolom yang ada untuk mendapatkan scope di burpsuite

Input Data WBS

Unit Utama: Direktorat Jenderal Sumber Daya Dan Perangkat Pos Dan Informatika

Perihal: dawdsa

Nama pejabat terduga terlibat: asdaweda

Lokasi Kejadian: awdas

Tanggal Kejadian: 31-05-2024

Urutan: dachwad

File Bukti: cat.jpg

Ekstensi yang diizinkan: JPG/JPEG/PNG/MP4/MP3

### 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

https://wbs.kominfo.go.id	GET	/pengaduan_wbs/245/detail_aduan	2
https://wbs.kominfo.go.id	GET	/pengaduan_wbs?draw=1&column...	2
https://wbs.kominfo.go.id	GET	/pengaduan_wbs/244/detail_aduan	2
https://wbs.kominfo.go.id	GET	/pengaduan_wbs/destroy/244	2
https://wbs.kominfo.go.id	GET	/pengaduan_wbs?draw=1&column...	2
https://wbs.kominfo.go.id	POST	/logout	3

### 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

Pretty	Raw	Hex	Pretty	Raw	Hex	Render
1 GET /pengaduan_wbs/destroy/250 HTTP/1.1			1 HTTP/1.1 200 OK			
2 Host: wbs.kominfo.go.id			2 date: Thu, 16 May 2024 09:35:42 GMT			
3 Cookie: visid_incap_2796514=3NB0ZeMnSSKSeupC+qtFN62oRwYAAAAQUIPAAAAAD8skz6Z6tmqXNqKu4UNY7Z; visid_incap_2815255=04faS0IKRJkKp5c2w8DIcuyoRwYAAAAQUIPAAAAAADv02z1g0dduohZbghz09o0; XSRF-TOKEN=			3 server: Apache/2.4.41 (Ubuntu)			
			4 cache-control: no-cache, private			
			5 set-cookie: XSRF-TOKEN=			

Pretty	Raw	Hex	Pretty	Raw	Hex	Render
1 GET /pengaduan_wbs/destroy/253 HTTP/1.1			1 HTTP/1.1 200 OK			
2 Host: wbs.kominfo.go.id			2 date: Thu, 16 May 2024 09:36:11			
3 Cookie: visid_incap_2796514=3NB0ZeMnSSKSeupC+qtFN62oRwYAAAAQUIPAAAAAD8skz6Z6tmqXNqKu4UNY7Z; visid_incap_2815255=04faS0IKRJkKp5c2w8DIcuyoRwYAAAAQUIPAAAAAADv02z1g0dduohZbghz09o0; XSRF-TOKEN=			3 server: Apache/2.4.41 (Ubuntu)			
			4 cache-control: no-cache, private			
			5 set-cookie: XSRF-TOKEN=			

## 6. Step 6 - Hasil simulasi

Ketika melakukan sending Endpoint ternyata laporan dari victim akan terhapus dari tabel aduan

The screenshot displays a web application interface. On the left, a REST client shows a GET request to `/pengaduan_wbs/destroy/253`. The response is a 200 status code. On the right, the application's dashboard is visible, showing a table with one entry. The entry is highlighted in red, indicating it has been deleted. The table has columns for 'No', 'No Aduan', 'Tanggal Masuk', 'Pelapor', 'Perihal', 'Unit', and 'Aksi'.

No	No Aduan	Tanggal Masuk	Pelapor	Perihal	Unit	Aksi
1	0252/WBS/05/2024	16-05-2024	nantzz+2	wadawd	Inspektorat Jenderal	<span style="color: red;">X</span>

## Screenshoot and log:

<https://drive.google.com/drive/folders/1boI0McMF3ttGBU87KQhgZFszPc1F3PCM?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 memungkinkan bisa di eksploitasi
- 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 terdeteksi

Best Regards,  
Gede Ananda