
	<p align="center">LAPORAN INSIDEN CYBER SECURITY - IDOR</p>	NOMOR : MCO/09/IX/2025/006
		EDISI : 1.0
		TANGGAL : 22 Agustus 2025
		HALAMAN : 1 Dari 7 Halaman
DSS05 : MANAGED SECURITY SERVICES		

DISUSUN OLEH :

DIVISI TEKNOLOGI INFORMASI



	DISUSUN OLEH	DISETUJUI OLEH	DISAHKAN OLEH
JABATAN	MANAJEMEN KEAMANAN SISTEM APLIKASI & DATA	WS MANAGER OPERASIONAL & KEAMANAN TI	PLT VP TEKNOLOGI INFORMASI
TANDA TANGAN			

	LAPORAN INSIDEN CYBER SECURITY - IDOR	NOMOR : MCO/09/IX/2025/006
		EDISI : 1.0
		TANGGAL : 22 Agustus 2025
		HALAMAN : 2 Dari 7 Halaman
DSS05 : MANAGED SECURITY SERVICES		

Document Control

Version	Adjustment	PIC	Date
1.0	Initial Version	Rizki Adi Hidayat	22 Agustus 2025

	LAPORAN INSIDEN CYBER SECURITY - IDOR	NOMOR : MCO/09/IX/2025/006
		EDISI : 1.0
		TANGGAL : 22 Agustus 2025
		HALAMAN : 3 Dari 7 Halaman
DSS05 : MANAGED SECURITY SERVICES		

1. Point of Contact (PoC) Information

Name : Agung Prabowo
 Title : Expert Manajemen Keamanan Sistem Aplikasi & Data
 Telephone : 087822171172
 E-mail : agungp@pindad.com;

Name : Rizki Adi Hidayat
 Title : Manajemen Keamanan Sistem Aplikasi & Data
 Telephone : 082129473610
 E-mail : rizki.adi@pindad.com

2. Informasi Insiden

- **Tanggal & Waktu:** 22 Agustus 2025, 11.49 WIB
- **Sistem Terkena:** Bug IDOR pada aplikasi api milik Pindad
- **Pelapor:** Zachary Dylan (External)
- **Tanggal Laporan:** 22 Agustus 2025

3. Deskripsi Insiden

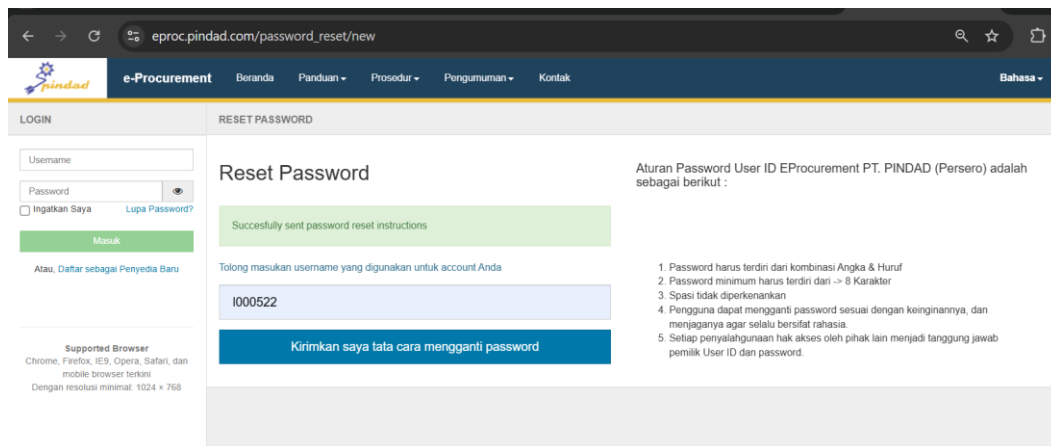
- **Jenis Insiden:** IDOR (Insecure Direct Object Reference)
- **Klasifikasi Insiden:** Cyber Security Incident – Website Compromise
- **Kritikalitas:** Tinggi (karena menyentuh layanan publik & reputasi)
- **Target Tindak Lanjut:**
 - Pemulihan layanan ≤ 1 jam
 - Patch kerentanan ≤ 7 Hari
 - Implementasi WAF ≤ 1 hari

<div><div>PT PINDAD</div></div>	<div>LAPORAN INSIDEN CYBER SECURITY - IDOR</div>	NOMOR : MCO/09/IX/2025/006
		EDISI : 1.0
		TANGGAL : 22 Agustus 2025
		HALAMAN : 4 Dari 7 Halaman
DSS05 : MANAGED SECURITY SERVICES		

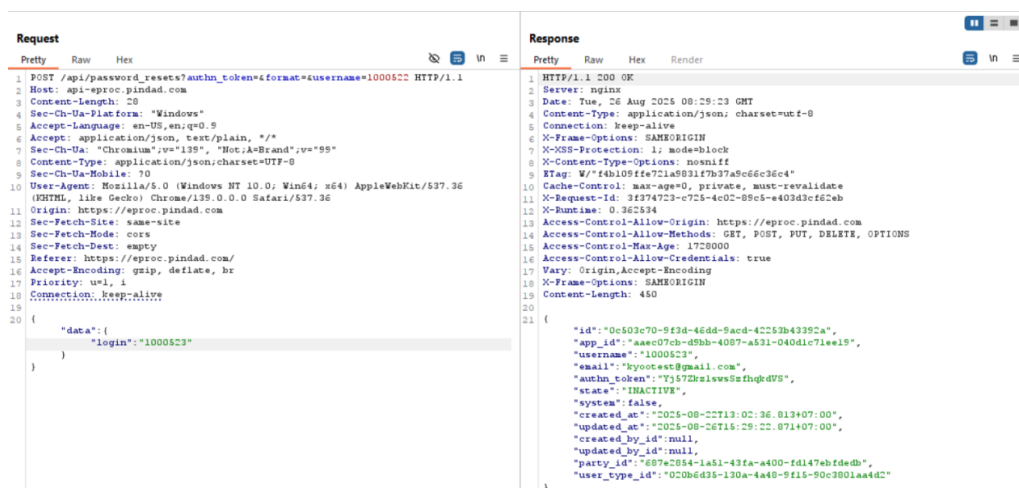
Evidence :



Gambar 1. 1 Email Report




Gambar 1. 2 IDOR pada fitur lupa password



Gambar 1. 3 IDOR untuk take over account

- Detail Insiden: Salah satu sistem api milik perusahaan terdapat kerentanan IDOR yang dapat dieksekusi untuk pencurian account.

	LAPORAN INSIDEN CYBER SECURITY - IDOR	NOMOR : MCO/09/IX/2025/006
		EDISI : 1.0
		TANGGAL : 22 Agustus 2025
		HALAMAN : 5 Dari 7 Halaman
DSS05 : MANAGED SECURITY SERVICES		

- **Lokasi:** eproc.pindad.com
- **Ringkasan:** Situs web milik eproc.pindad.com memiliki celah keamanan IDOR setelah dilakukan pengujian dan validasi. Situs ini sesuai dengan yang dilaporkan oleh pelapor lewat pesan email. Pelapor tidak menunjukkan detail api yang terdampak.
- **Gejala:** Pelapor bug melaporkan terdapat kerentanan IDOR pada salah satu api milik perusahaan namun tidak menjelaskan detail terkait kerentanan yang ada.
- **Kronologi:** Dipilah dalam 1 timeline peristiwa, yaitu:

Tabel 1 Kronologi Insiden

No.	Tanggal & Waktu	Peristiwa	Deskripsi Peristiwa
Incident			
1	22 Agustus 2025 11:49 WIB	Laporan pihak eksternal	Tim IT Security mendapatkan notifikasi email laporan bug pada salah satu api milik perusahaan
2	22 Agustus 2025 12.00 WIB	Triase & analisis awal.	Tim IT Security menerima eskalasi dan mulai melakukan investigasi
3	22 Agustus 2025 12:35 WIB	Investigasi API endpoint, indikasi IDOR ditemukan.	Tim IT Security berhasil melakukan investigasi dimana terdapat salah satu sistem milik eproc yang memiliki kerentanan IDOR sesuai dengan yang dilaporkan pelapor
4	22 Agustus 2025 13:00 WIB	Koordinasi dengan tim Dev	Dilakukan koordinasi dengan tim dev untuk penanganan jangka panjang
5	22 Agustus 2025 13:15 WIB	Pemulihan awal serta pengetatan aplikasi	Tim Security melakukan penambahan waf serta melakukan implementasi SIEM pada agent Eproc


 <div>PT PINDAD</div>	<div>LAPORAN INSIDEN CYBER SECURITY - IDOR</div>	NOMOR : MCO/09/IX/2025/006
		EDISI : 1.0
		TANGGAL : 22 Agustus 2025
		HALAMAN : 6 Dari 7 Halaman
DSS05 : MANAGED SECURITY SERVICES		

4. Dampak Insiden

- **Layanan Terpengaruh:** Website serta api eproc tidak mengalami downtime.
- **Data Terpengaruh:** Tidak ditemukan indikasi kebocoran data sensitif (database pelanggan & internal masih aman).
- **Kerugian Operasional:** Potensi kerugian bisnis akibat calon pelanggan tidak bisa mengakses informasi produk/jasa.

5. Penyebab Insiden

- **Penyebab Utama:** Eksploitasi kerentanan IDOR pada salah satu api milik perusahaan.
- **Analisis Penyebab:**
 - Berdasarkan laporan awal pelapor melaporkan terdapat kerentanan IDOR pada salah satu aplikasi milik perusahaan (pelapor tidak menunjukkan laporan lengkap serta sistem apa yang terdampak)
 - Terdapat indikasi serangan IDOR terdapat pada sistem eproc (setelah dilakukan investigasi) karena pelapor yang tidak mencantumkan domain lengkap yang terdampak. Tim melakukan investigasi menyeluruh pada beberapa aplikasi yang memiliki api.
 - Monitoring sistem pada log tidak dapat dilakukan karena serangan IDOR ini merupakan serangan yang sulit untuk dideteksi karena hampir sama dengan valid action yang dilakukan oleh user.
 - Insiden dapat dicegah jika patching dilakukan lebih cepat, serta adanya lapisan proteksi tambahan (WAF, IDS/IPS tuning, dan kebijakan akses lebih ketat).

 <div>PT PINDAD</div>	<div>LAPORAN INSIDEN CYBER SECURITY - IDOR</div>	NOMOR : MCO/09/IX/2025/006
		EDISI : 1.0
		TANGGAL : 22 Agustus 2025
		HALAMAN : 7 Dari 7 Halaman
DSS05 : MANAGED SECURITY SERVICES		

6. Tindakan yang Diambil

- **Respons Awal:** Tim Security segera melakukan investigasi ketika mendapatkan laporan kerentanan. Namun karena pelapor yang tidak menjelaskan secara detail aplikasi yang terdampak (belum ada bukti valid pada sistem yang terdampak) maka tim security melakukan Analisa terhadap beberapa sistem yang memiliki endpoint api didalamnya.
- **Pemulihan:** Melakukan penambahan WAF pada aplikasi, serta melakukan koordinasi dengan tim developer untuk patching aplikasi dalam jangka panjang dengan tim developer.
- **Mitigasi:** Implementasi Web Application Firewall (WAF) untuk memfilter serangan berbasis web, pembatasan akses aplikasi dari negara selain Indonesia, serta menetapkan jadwal patch management rutin dan vulnerability scanning berkala.

7. Rencana Pencegahan

- Melakukan update rutin patching, serta VAPT secara peiodik.
- Mengimplementasikan Web Application Firewall (WAF) sebagai lapisan proteksi tambahan.
- Mengoptimalkan SIEM/IDS/IPS untuk deteksi anomali traffic dan serangan brute force.

8. Penyelesaian Insiden

- **Tanggal Penyelesaian:** 22 Agustus 2025
- **Status Akhir:** Selesai.
- **Laporan Tambahan:** Tidak ada laporan tambahan.