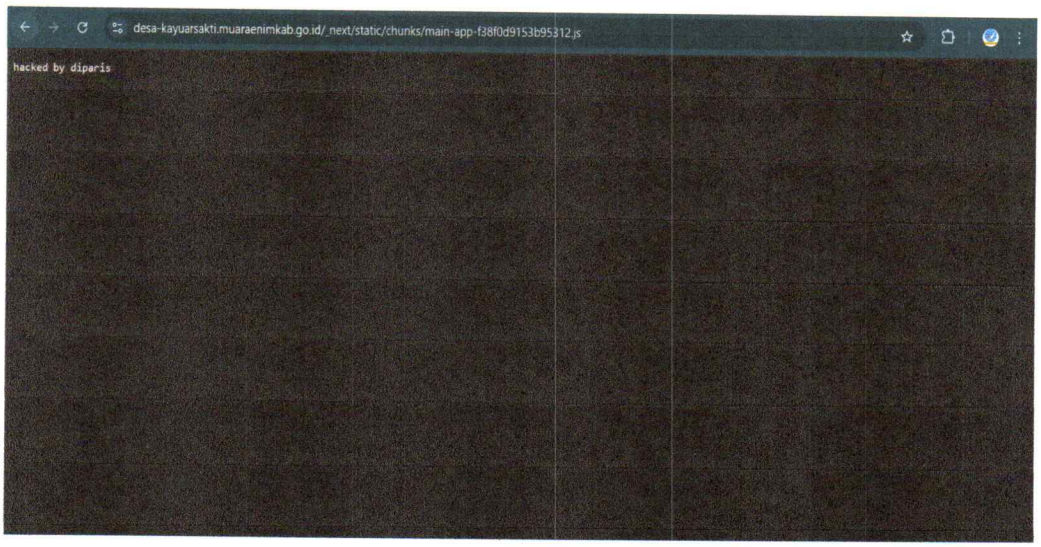
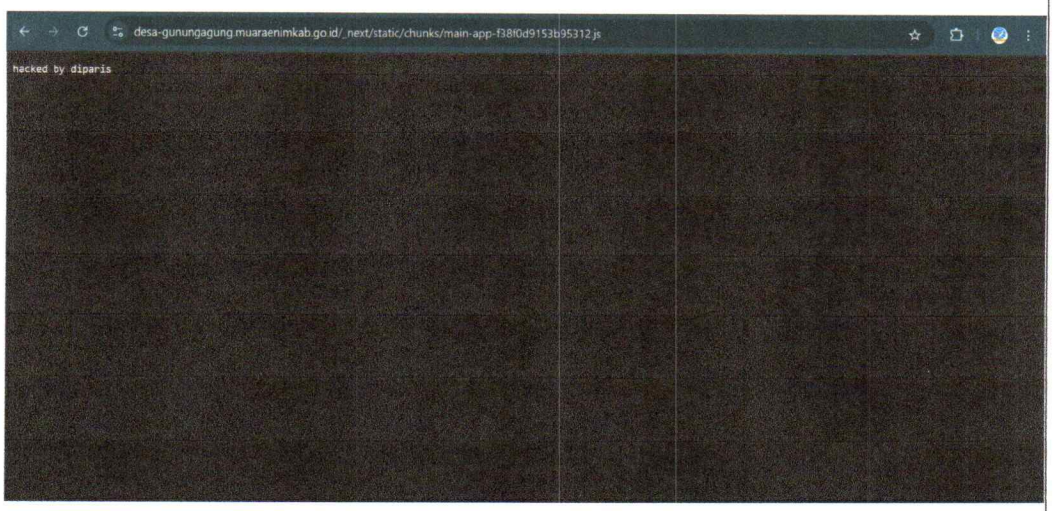
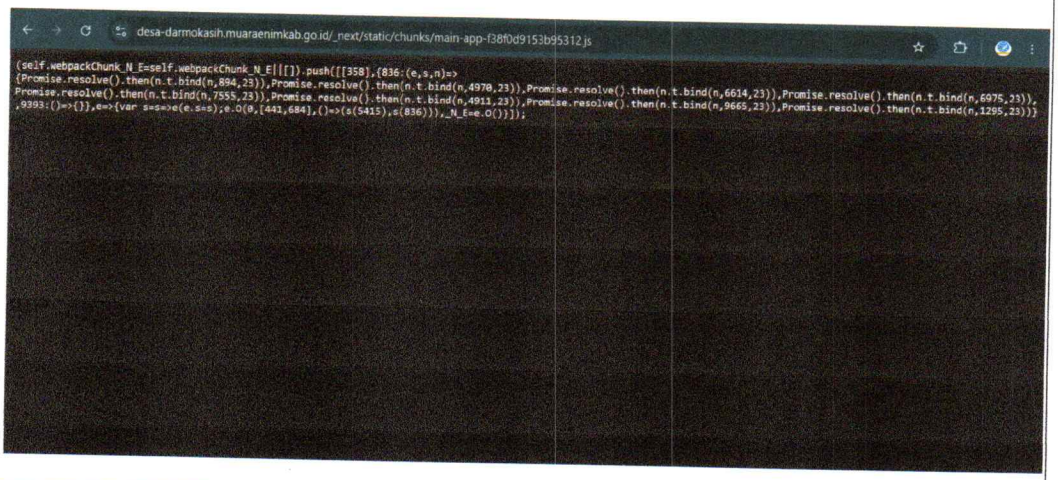
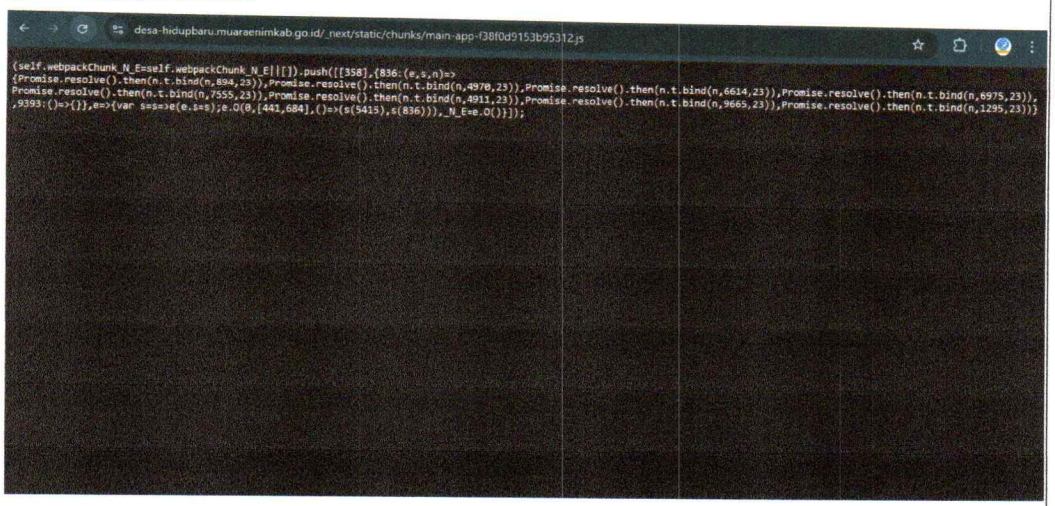
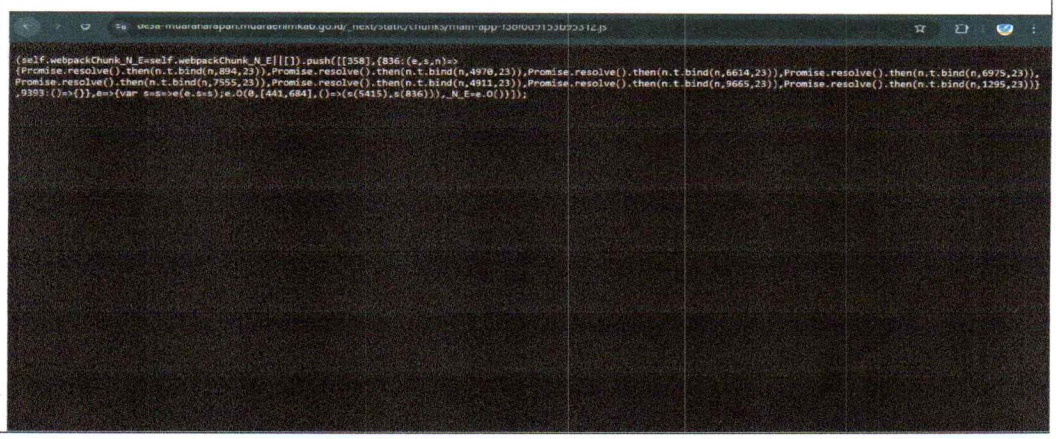
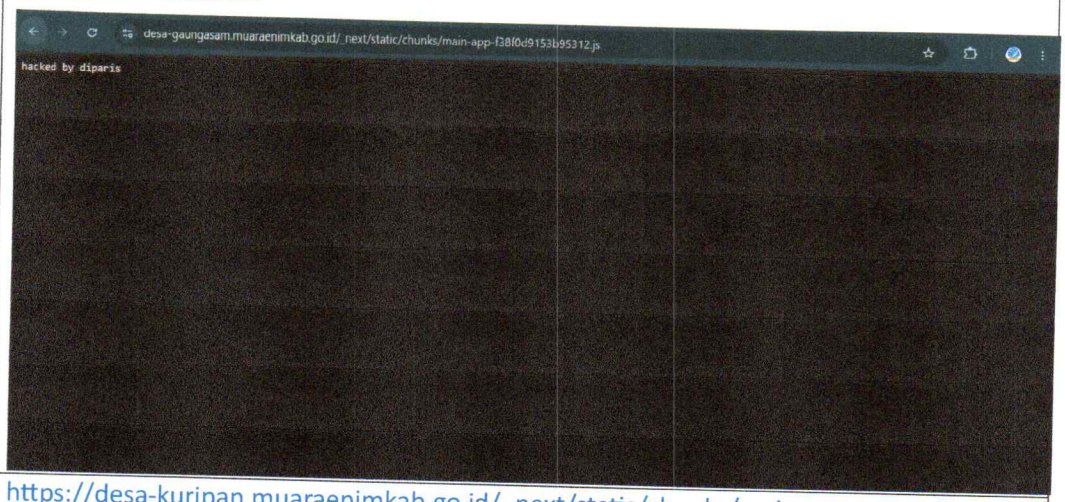
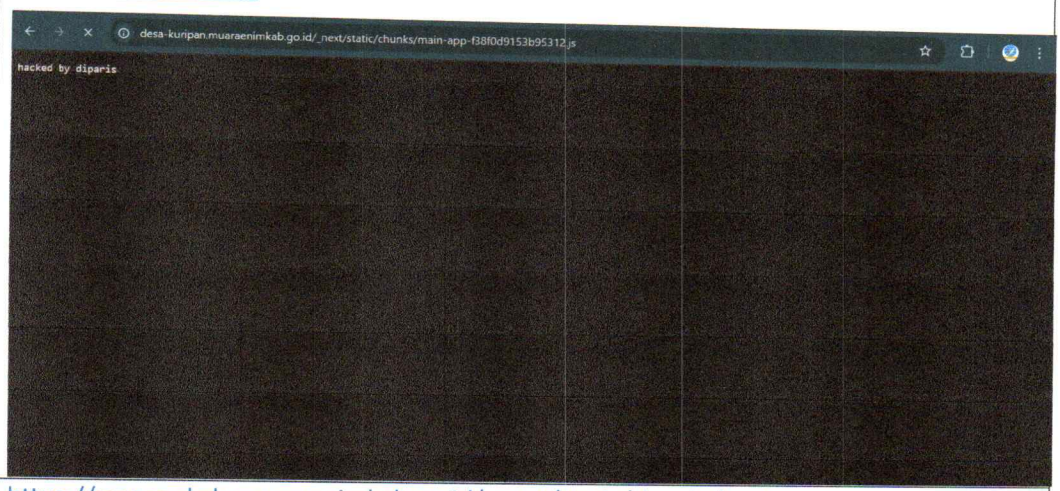
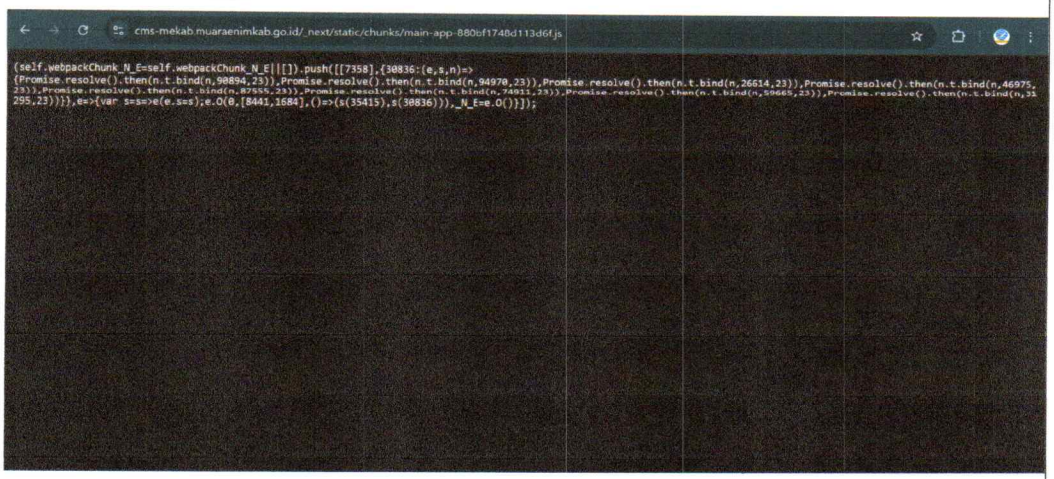
Laporan Insiden Siber Aset Pemkab Muara Enim

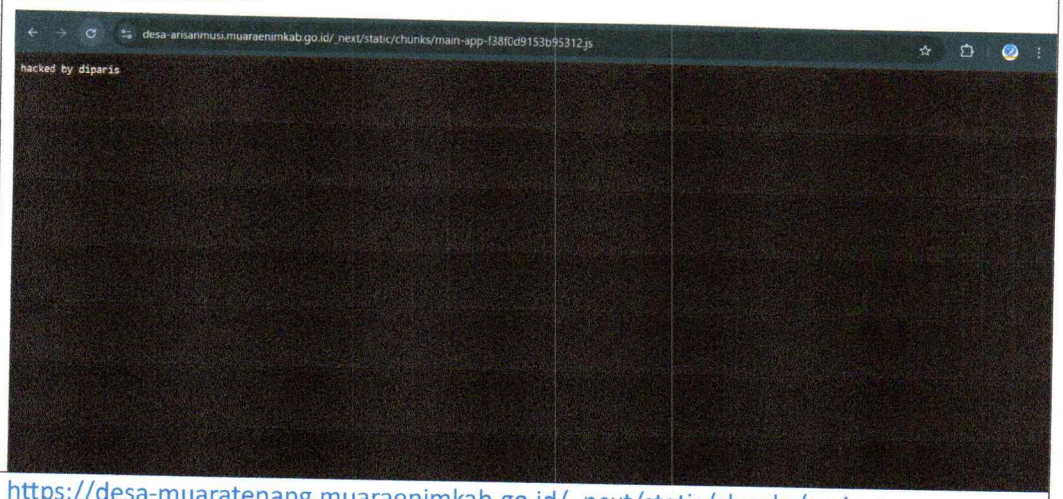
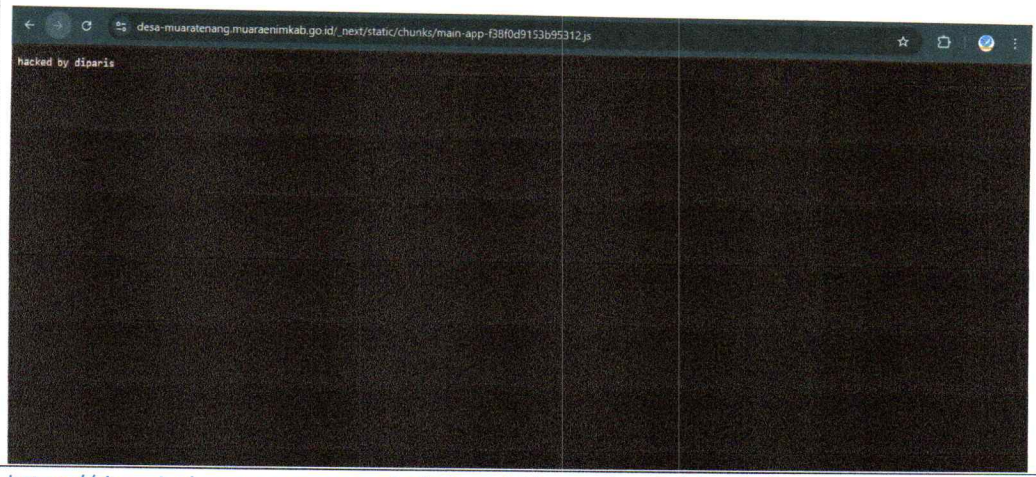
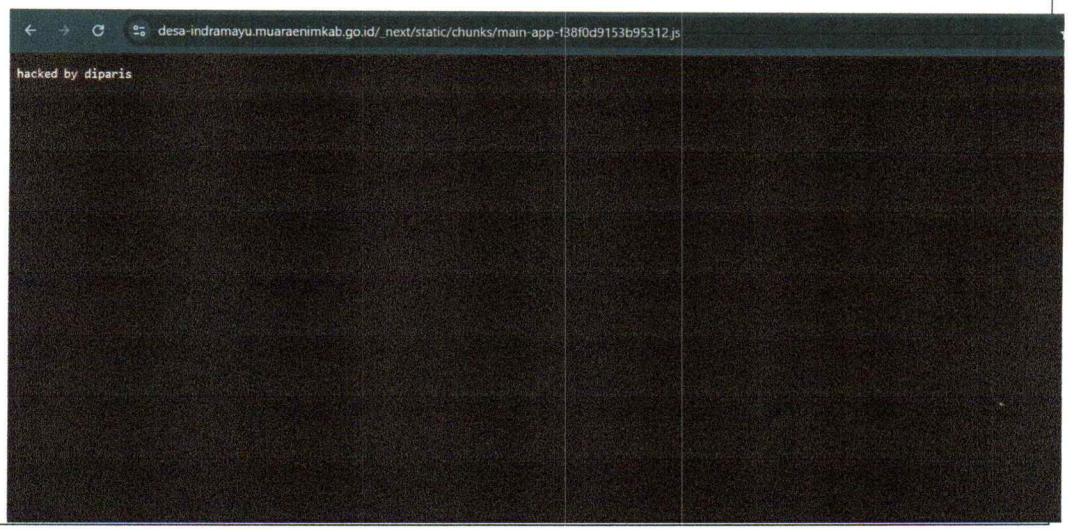
Tanggal Temuan Insiden : 07 Januari 2026
Jenis Insiden : Mass Defacement

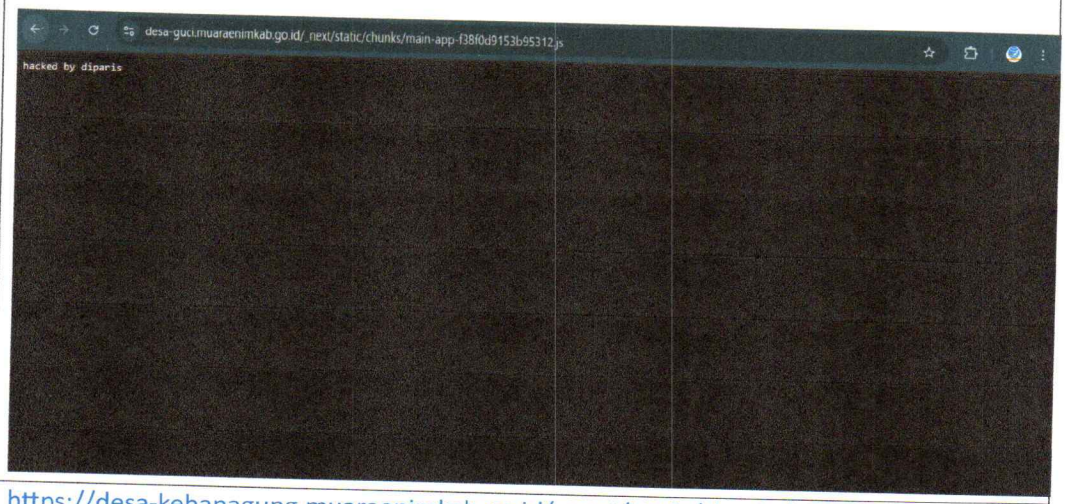
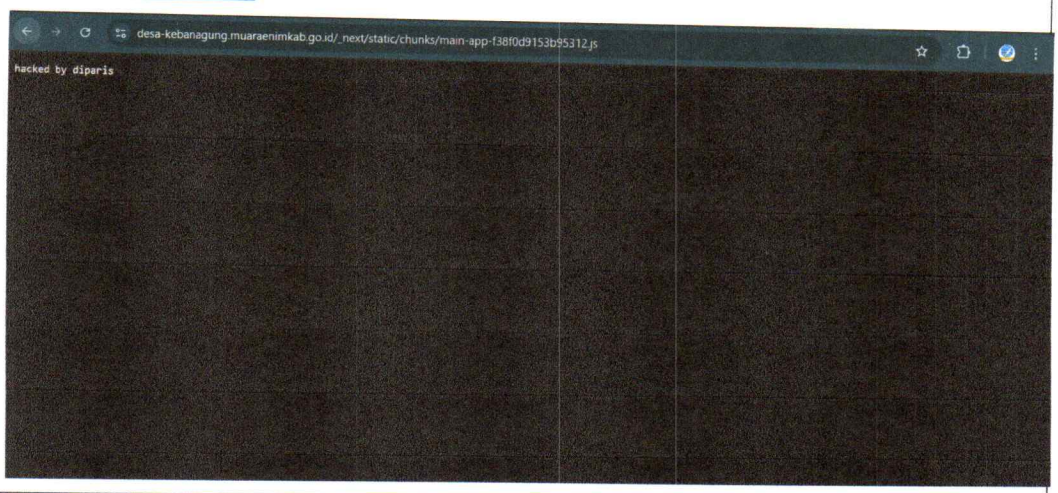
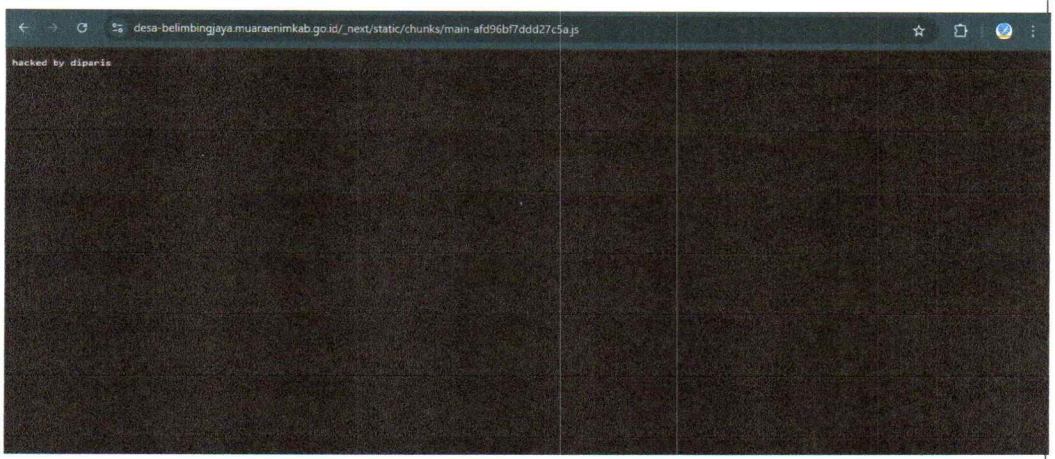
Bersama ini kami sampaikan laporan insiden keamanan terkait subdomain resmi milik Pemerintah Kabupaten Muara Enim yang terindikasi mengalami pembajakan (Mass Defacement). Subdomain yang dimaksud adalah:

1	https://desa-kayuarsakti.muaraenimkab.go.id/_next/static/chunks/main-app-f38f0d9153b95312.js 
2	https://desa-gunungagung.muaraenimkab.go.id/_next/static/chunks/main-app-f38f0d9153b95312.js 

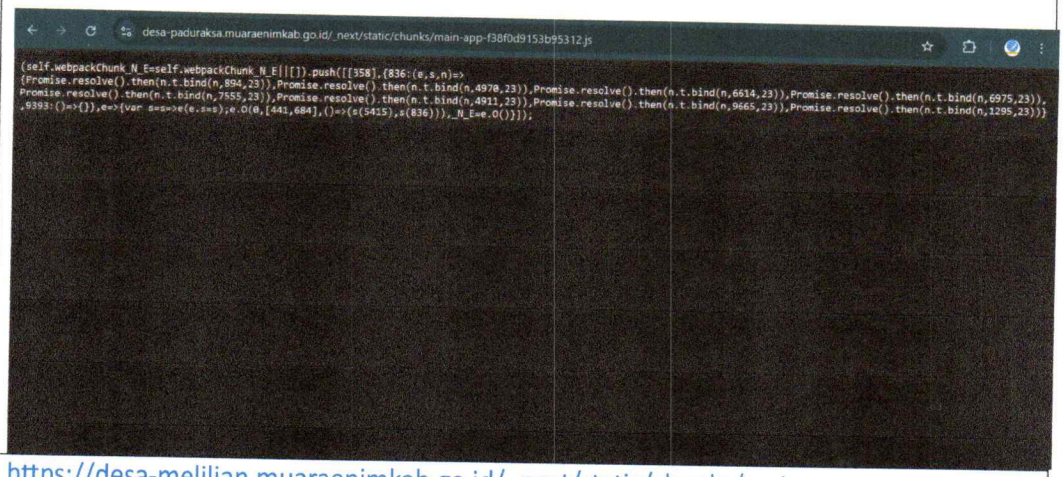
3	https://desa-darmokasih.muaraenimkab.go.id/_next/static/chunks/main-app-f38f0d9153b95312.js 
4	https://desa-hidupbaru.muaraenimkab.go.id/_next/static/chunks/main-app-f38f0d9153b95312.js 
5	https://desa-muaraharapan.muaraenimkab.go.id/_next/static/chunks/main-app-f38f0d9153b95312.js 

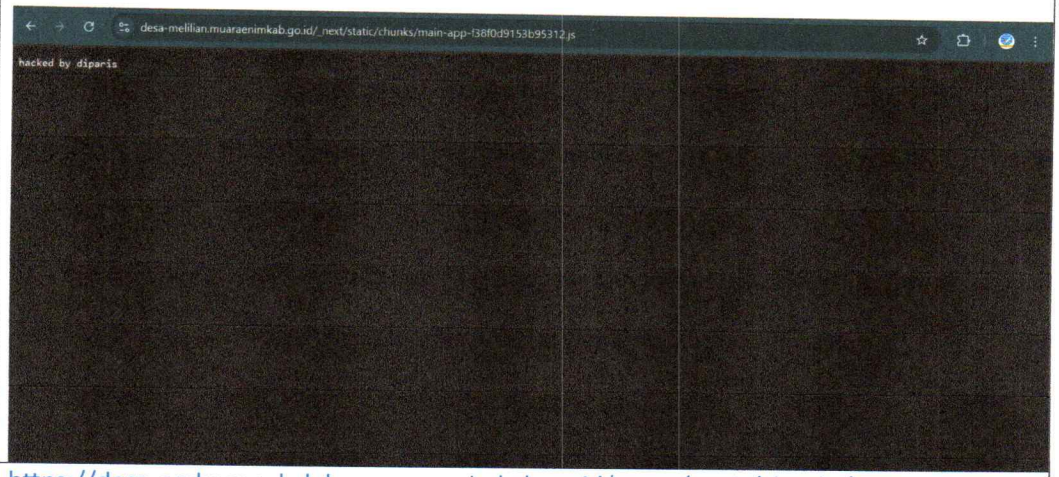
6	https://desa-gaungasam.muaraenimkab.go.id/_next/static/chunks/main-app-f38f0d9153b95312.js 
7	https://desa-kuripan.muaraenimkab.go.id/_next/static/chunks/main-app-f38f0d9153b95312.js 
8	https://cms-mekab.muaraenimkab.go.id/_next/static/chunks/main-app-880bf1748d113d6f.js 

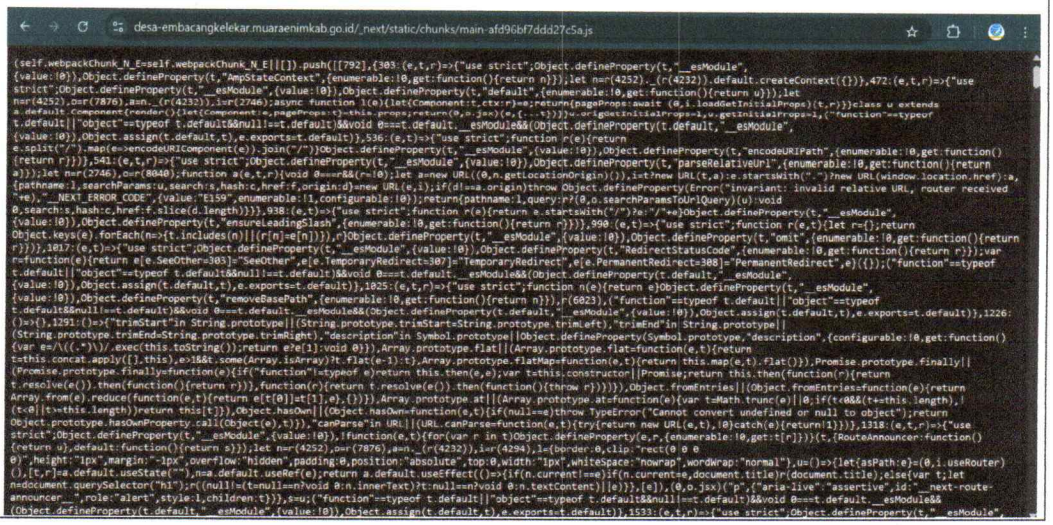
9	https://desa-arisanmusi.muaraenimkab.go.id/_next/static/chunks/main-app-f38f0d9153b95312.js 
10	https://desa-muaratenang.muaraenimkab.go.id/_next/static/chunks/main-app-f38f0d9153b95312.js 
11	https://desa-indramayu.muaraenimkab.go.id/_next/static/chunks/main-app-f38f0d9153b95312.js 

12	https://desa-guci.muaraenimkab.go.id/_next/static/chunks/main-app-f38f0d9153b95312.js 
13	https://desa-kebanagung.muaraenimkab.go.id/_next/static/chunks/main-app-f38f0d9153b95312.js 
14	https://desa-belimbingjaya.muaraenimkab.go.id/_next/static/chunks/main-afd96bf7ddd27c5a.js 

15	https://desa-paduraksa.muaraenimkab.go.id/_next/static/chunks/main-app-f38f0d9153b95312.js
16	https://desa-melilian.muaraenimkab.go.id/_next/static/chunks/main-app-f38f0d9153b95312.js
17	https://desa-embacangkelekar.muaraenimkab.go.id/_next/static/chunks/main-afd96bf7ddd27c5a.js







1. Ringkasan Kejadian

Pada tanggal 7 Januari 2026, diketahui bahwa subdomain tersebut menampilkan "***hacked by diparis***".

2. Potensi Penyebab

- Subdomain mengarah ke layanan hosting eksternal (CDN) yang sudah tidak dikelola
- Celah Keamanan CMS & Plugin
- Terjadi subdomain takeover oleh pihak ketiga yang memanfaatkan celah konfigurasi DNS
- Belum adanya sistem monitoring subdomain aktif pada domain `muaraenimkab.go.id`

3. Dampak

- Reputasi Pemerintah Daerah sangat terancam
- Mengganggu Pemerintah Desa dan masyarakat dalam mengakses website
- Risiko malware/phishing pada masyarakat yang mengakses
- Kepercayaan publik terhadap sistem digital pemerintah terganggu

4. Rekomendasi

- Segera hapus, takedown atau perbaiki konfigurasi DNS subdomain
- Audit dan pemantauan semua subdomain aktif
- Penerapan sistem alert DNS/subdomain agar insiden serupa tidak terjadi
- Koordinasi dengan CSIRT Pemkab Muara Enim dan Pengelola Website

5. Penutup

Demikian laporan ini kami sampaikan agar menjadi perhatian dan segera dapat ditindaklanjuti. Atas perhatian dan kerjasamanya, kami ucapkan terima kasih.

Muara Enim, 07 Januari 2026

Penelaah Teknis Kebijakan

SEPTA PUTRA ANGGARA

NIP. 199009122019021005

Kepala Bidang Persandian dan Keamanan Informasi

Dinas Kominfo SP Kab. Muara Enim

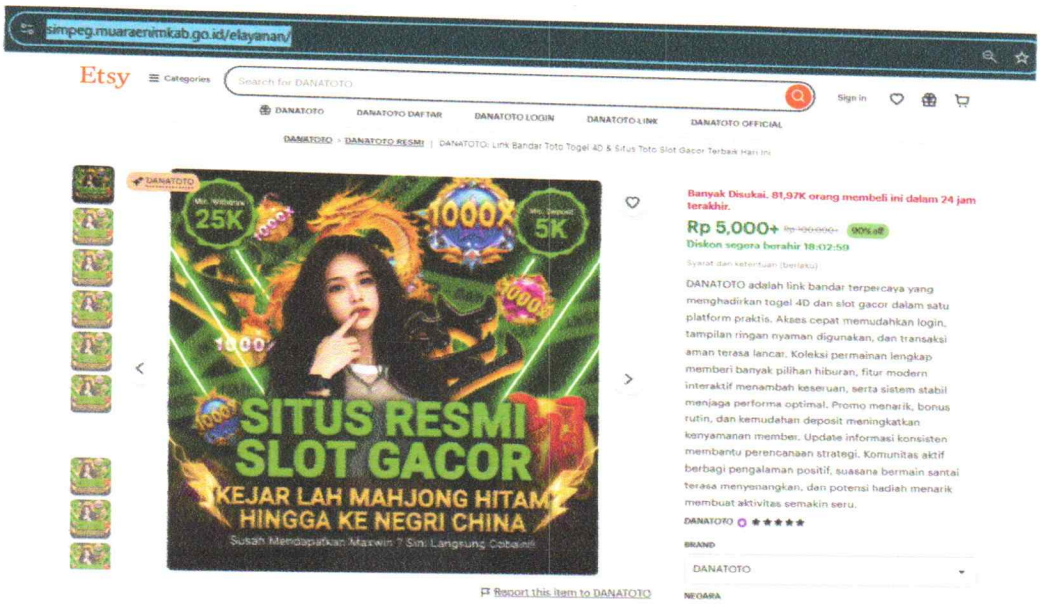
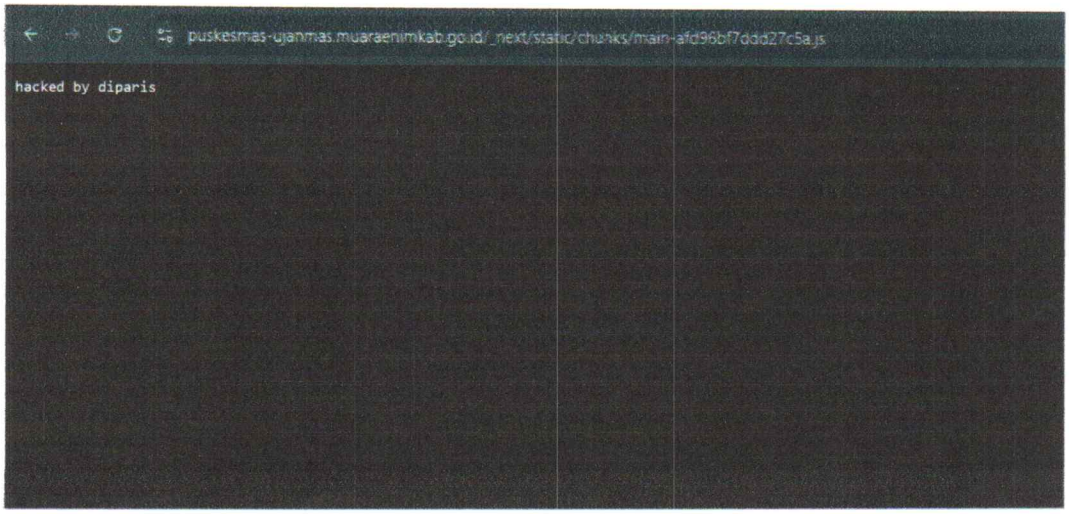
YULIANI INDRIANI, S. H

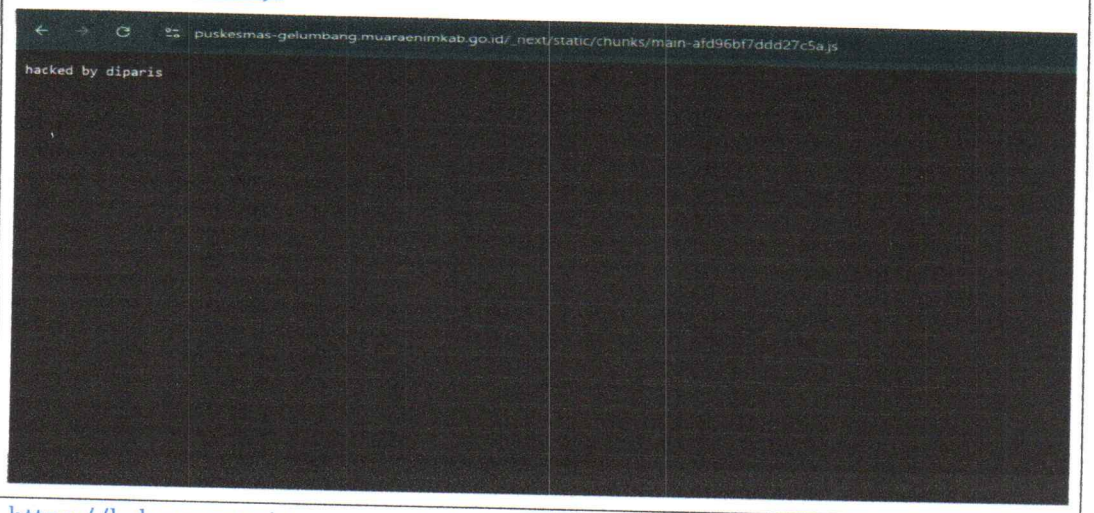
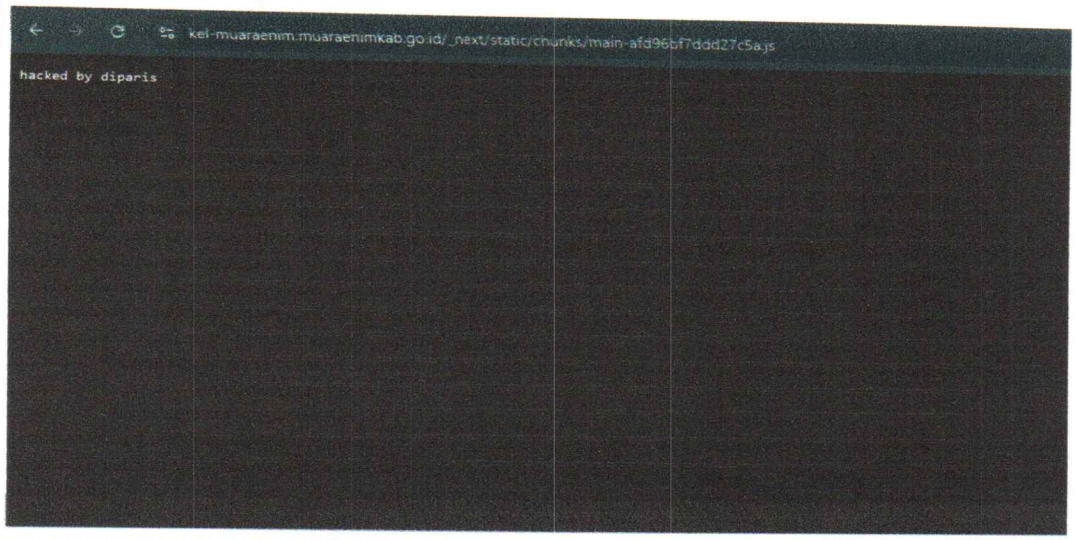
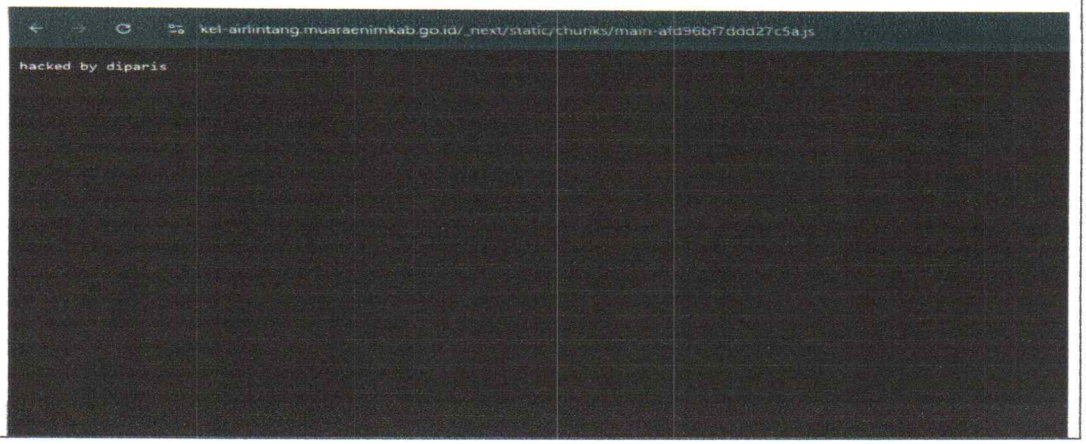
NIP. 197907152006042020

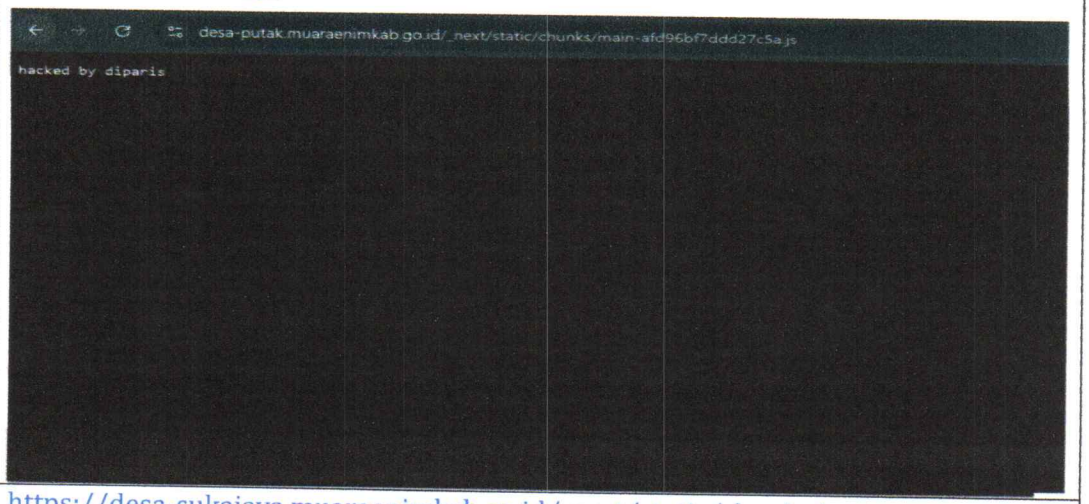
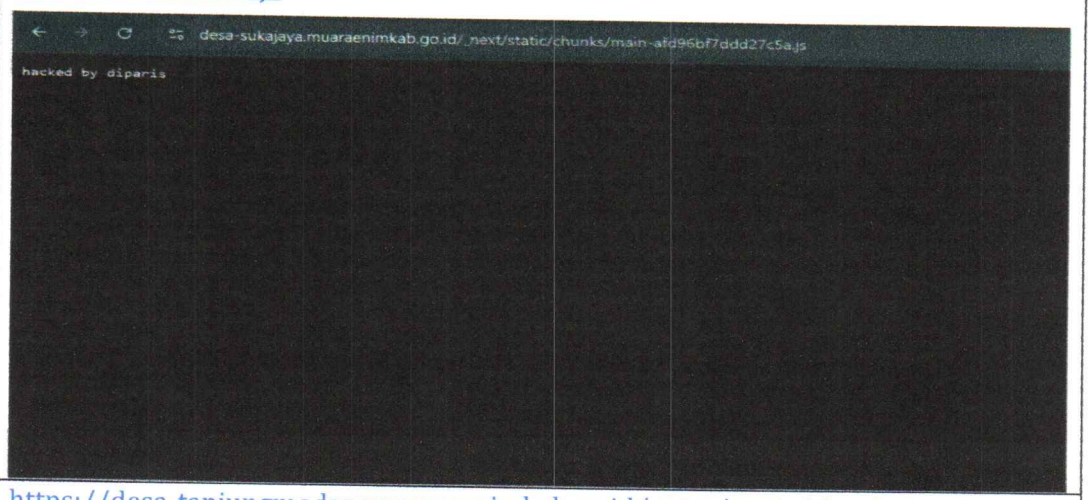
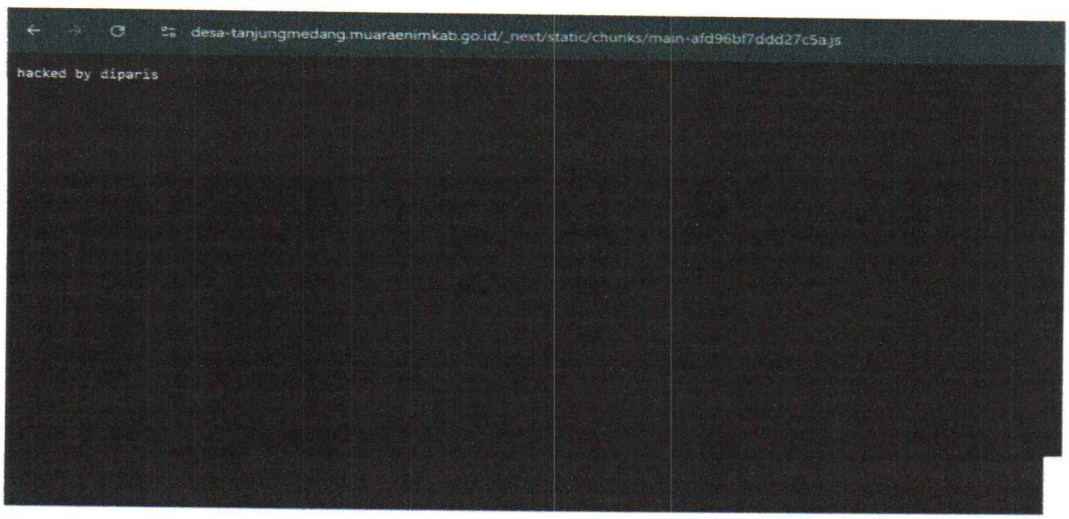
Laporan Insiden Siber Aset Pemkab Muara Enim

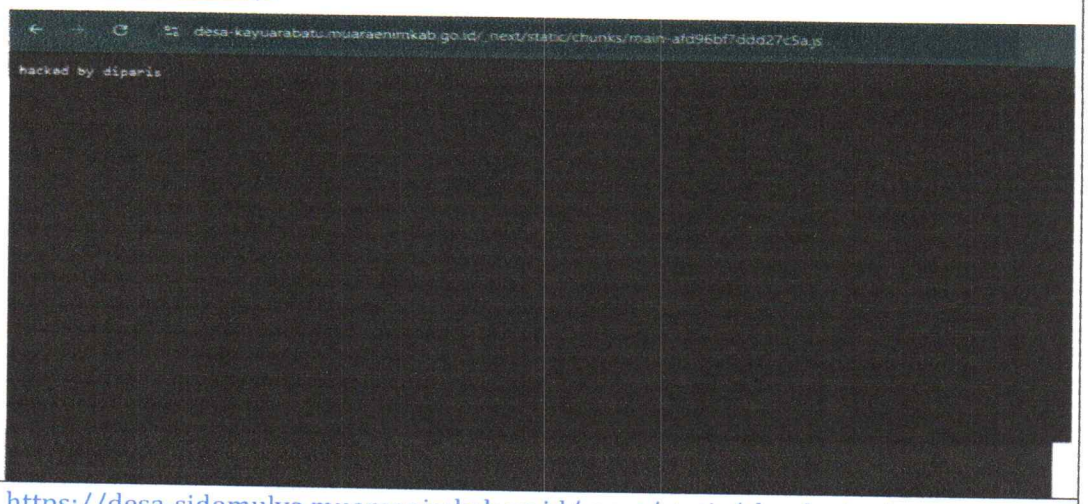
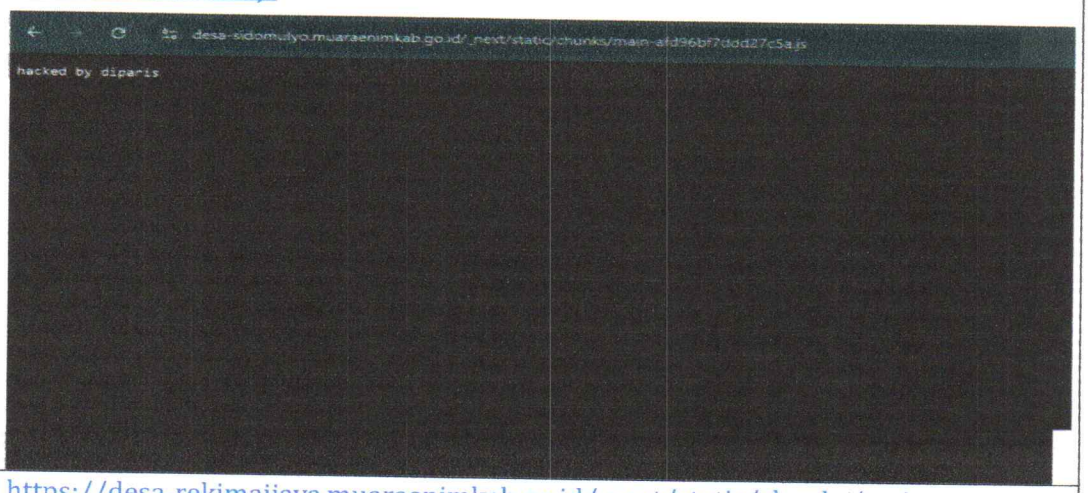
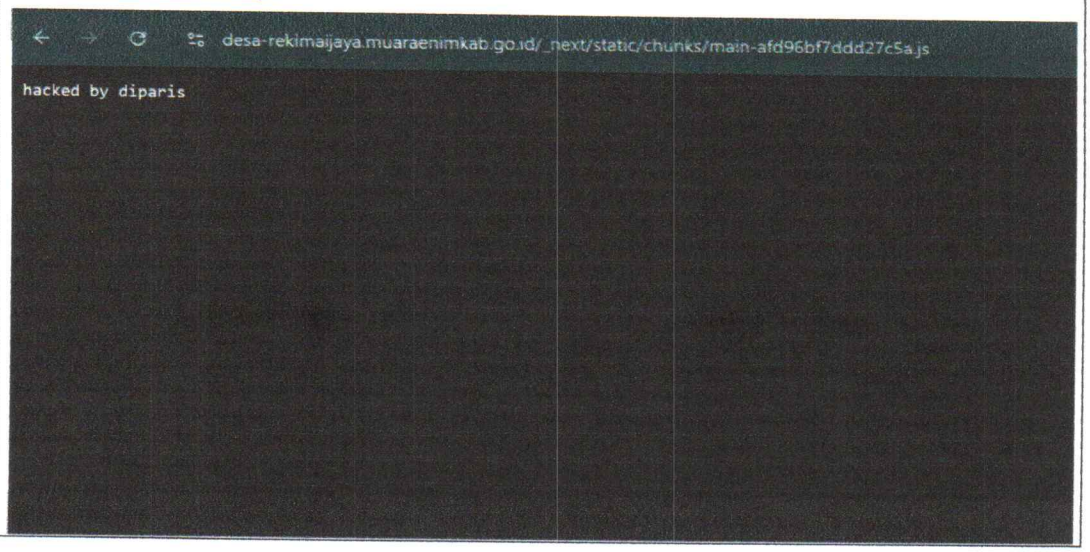
Tanggal Temuan Insiden : 26 Januari 2026
Jenis Insiden : Slot Gacor dan Mass Defacement

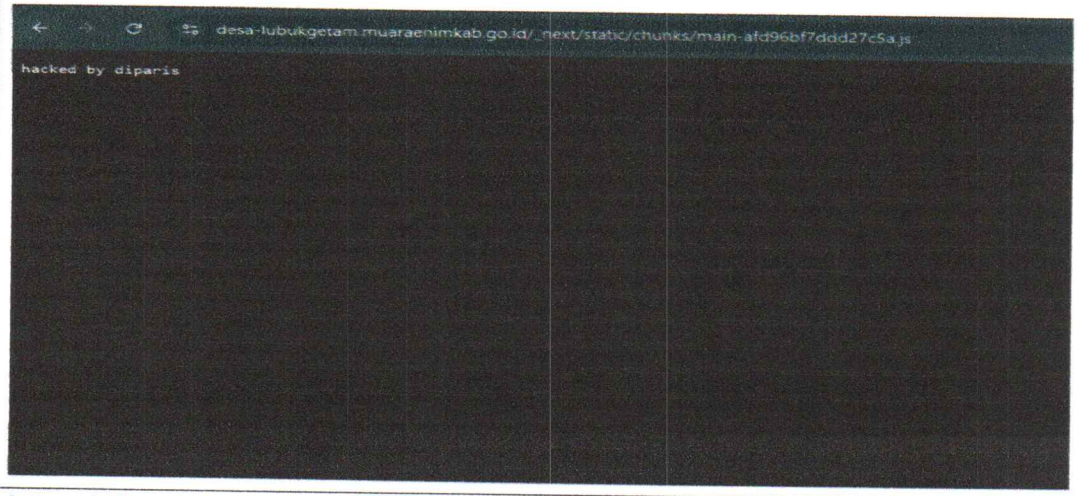
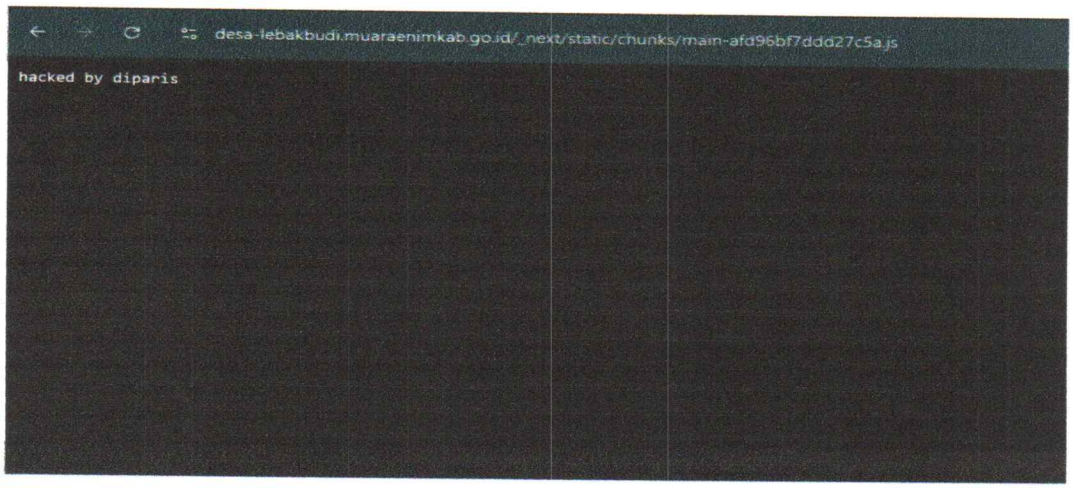
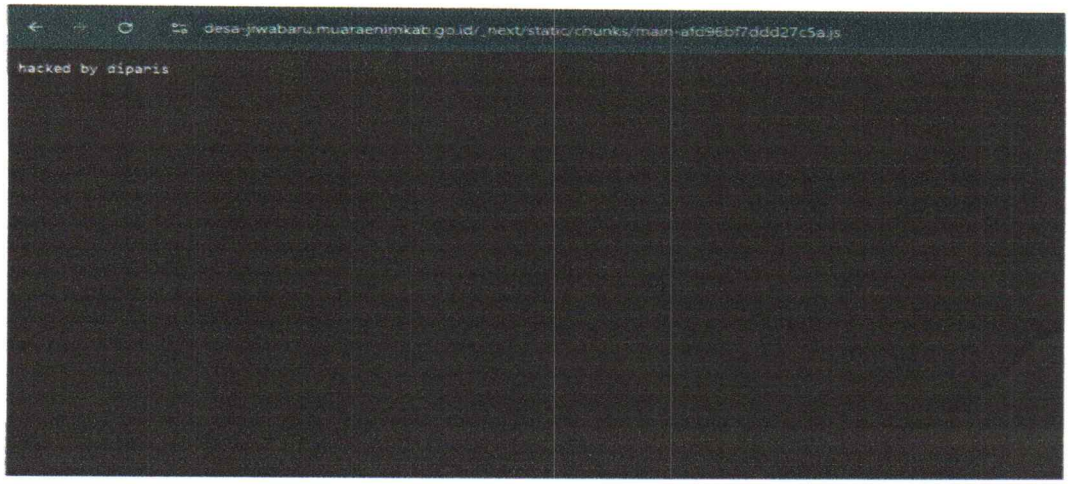
Bersama ini kami sampaikan laporan insiden keamanan terkait subdomain resmi milik Pemerintah Kabupaten Muara Enim yang terindikasi mengalami pembajakan (Mass Defacement). **Subdomain yang dimaksud adalah:**

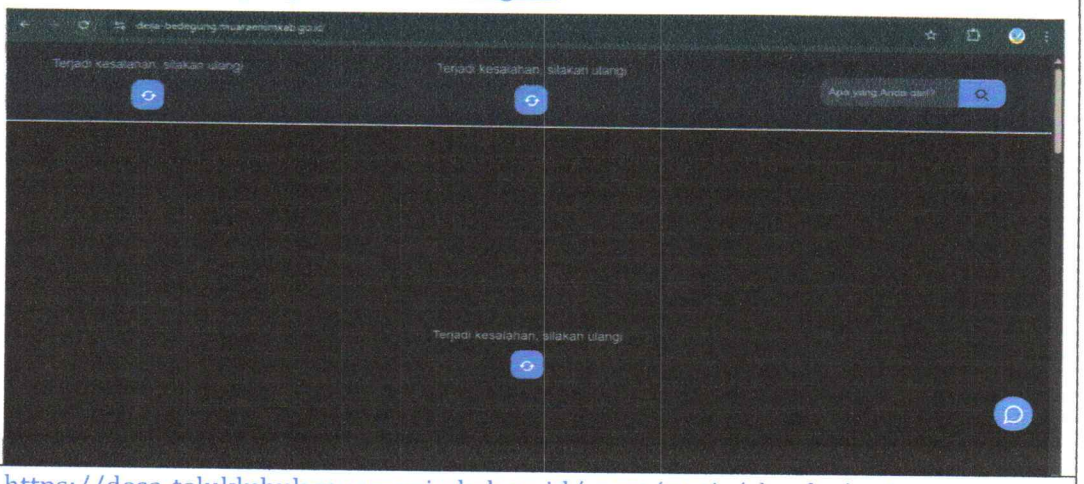
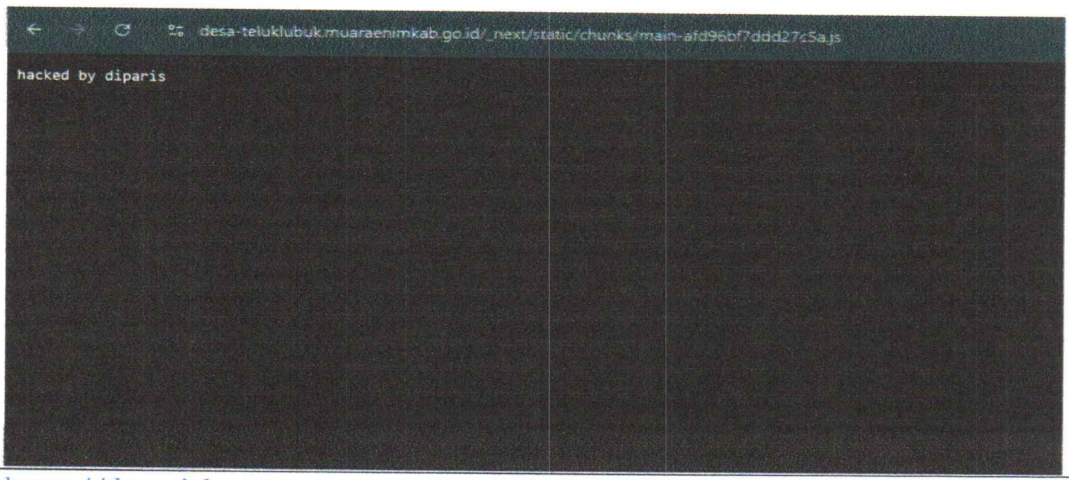
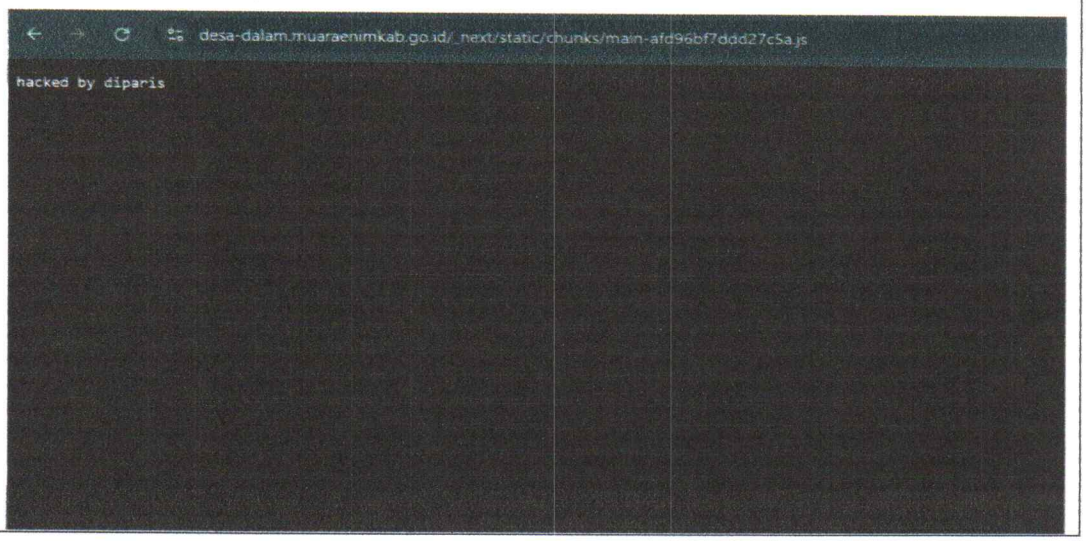
1	https://simpeg.muaraenimkab.go.id/elayanan/ 
2	https://puskesmas-ujanmas.muaraenimkab.go.id/_next/static/chunks/main-afd96bf7ddd27c5a.js 

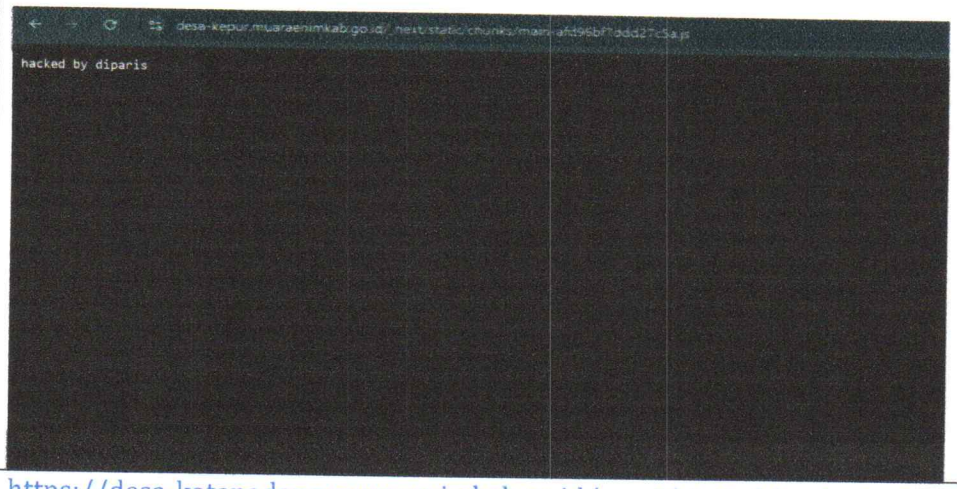
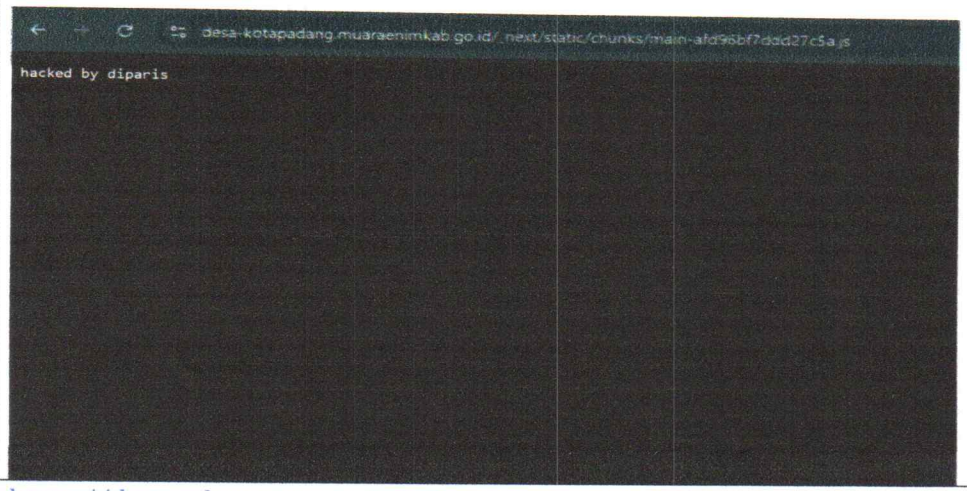
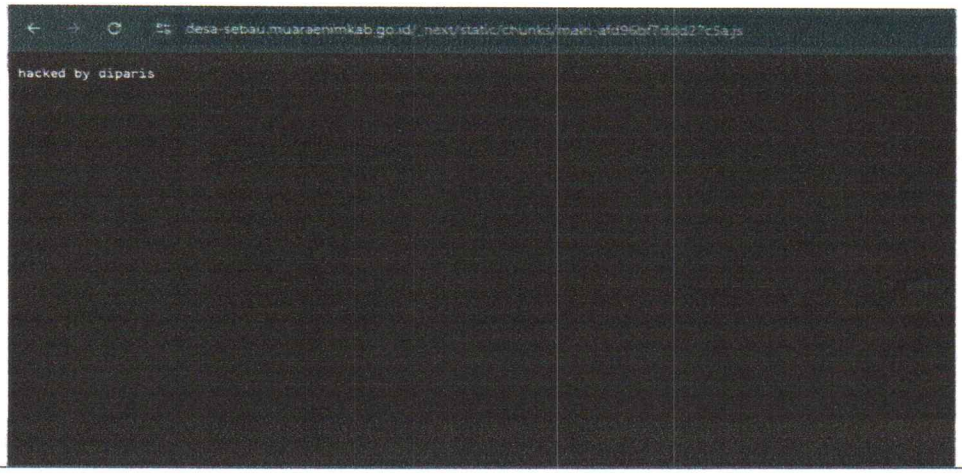
3	https://puskesmas-gelumbang.muaraenimkab.go.id/_next/static/chunks/main-afd96bf7ddd27c5a.js 
4	https://kel-muaraenim.muaraenimkab.go.id/_next/static/chunks/main-afd96bf7ddd27c5a.js 
5	https://kel-airlintang.muaraenimkab.go.id/_next/static/chunks/main-afd96bf7ddd27c5a.js 

6	https://desa-putak.muaraenimkab.go.id/_next/static/chunks/main-afd96bf7ddd27c5a.js 
7	https://desa-sukajaya.muaraenimkab.go.id/_next/static/chunks/main-afd96bf7ddd27c5a.js 
8	https://desa-tanjungmedang.muaraenimkab.go.id/_next/static/chunks/main-afd96bf7ddd27c5a.js 

9	https://desa-kayuarabatu.muaraenimkab.go.id/_next/static/chunks/main-afd96bf7ddd27c5a.js 
10	https://desa-sidomulyo.muaraenimkab.go.id/_next/static/chunks/main-afd96bf7ddd27c5a.js 
11	https://desa-rekimaijaya.muaraenimkab.go.id/_next/static/chunks/main-afd96bf7ddd27c5a.js 

12	https://desa-lubukgetam.muaraenimkab.go.id/_next/static/chunks/main-afd96bf7ddd27c5a.js 
13	https://desa-lebakbudi.muaraenimkab.go.id/_next/static/chunks/main-afd96bf7ddd27c5a.js 
14	https://desa-jiwabaru.muaraenimkab.go.id/_next/static/chunks/main-afd96bf7ddd27c5a.js 

15	https://desa-bedegung.muaraenimkab.go.id 
16	https://desa-teluklubuk.muaraenimkab.go.id/_next/static/chunks/main-afd96bf7ddd27c5a.js 
17	https://desa-dalam.muaraenimkab.go.id/_next/static/chunks/main-afd96bf7ddd27c5a.js 

18	https://desa-kepur.muaraenimkab.go.id/_next/static/chunks/main-afd96bf7ddd27c5a.js 
19	https://desa-kotapadang.muaraenimkab.go.id/_next/static/chunks/main-afd96bf7ddd27c5a.js 
20	https://desa-sebau.muaraenimkab.go.id/_next/static/chunks/main-afd96bf7ddd27c5a.js 

1. Ringkasan Kejadian

Pada tanggal 26 Januari 2026, diketahui bahwa subdomain tersebut menampilkan "***hacked by diparis***"dan tampilan Promosi judi online slot gacor .

2. Potensi Penyebab

- Celah Keamanan CMS & Plugin
- Terjadi subdomain takeover oleh pihak ketiga yang memanfaatkan celah konfigurasi DNS
- Belum adanya sistem monitoring subdomain aktif pada domain `muaraenimkab.go.id`

3. Dampak

- Reputasi Pemerintah Daerah sangat terancam
- Mengganggu Pemerintah Desa dan masyarakat dalam mengakses website
- Risiko malware/phishing pada masyarakat yang mengakses
- Kepercayaan publik terhadap sistem digital pemerintah terganggu

4. Rekomendasi

- Segera hapus, takedown atau perbaiki konfigurasi DNS subdomain
- Audit dan pemantauan semua subdomain aktif
- Penerapan sistem alert DNS/subdomain agar insiden serupa tidak terjadi
- Koordinasi dengan CSIRT Pemkab Muara Enim dan Pengelola Website

5. Penutup

Demikian laporan ini kami sampaikan agar menjadi perhatian dan segera dapat ditindaklanjuti. Atas perhatian dan kerjasamanya, kami ucapkan terima kasih.

Muara Enim, 26 Januari 2026

Penelaah Teknis Kebijakan

SEPTA PUTRA ANGGARA
NIP. 199009122019021005

Kepala Bidang Persandian dan Keamanan Informasi
Dinas Kominfo SP Kab. Muara Enim

YULIANI INDRIANI, S. H
NIP. 197907152006042020

PEMERINTAH KABUPATEN MUARA ENIM
DINAS KOMUNIKASI, INFORMATIKA, STATISTIK DAN PERSANDIAN
Jalan Jenderal A Yani No. 14 Kel. Pasar I Muara Enim Kode Pos 31311
Telpon (0734) 421175 – Email: diskominfo@muaraenimkab.go.id

Muara Enim, 24 Juni 2025

Nomor : 500.12.10/12/DISKOMINFO/2025
Sifat : Penting
Lampiran : -
Hal : Insiden Slot Gacor Website DPMPTSP

Yth. Dinas Penanaman Modal dan Pelayanan
Terpadu Satu Pintu (DPMPTSP)
Kab. Muara Enim
di -
Tempat

Sehubungan dengan temuan indikasi serangan siber berupa slot gacor pada aset Pemkab Muara Enim yang dikelola oleh DPMPTSP dengan rincian sebagaimana terlampir, terkait hal tersebut diatas, kami dari Dinas Kominfo SP mohon untuk dilakukan penghapusan file pada index dimaksud agar website tersebut dapat kembali diaktifkan aksesnya.

Untuk Informasi lebih lanjut dapat menghubungi sdr. Ruslim Anwar, S. Kom (Manggala Informatika Muda) Nomor HP. 081271778819 dan Septa Putra Anggara, S. Kom (Analis Persandian) Nomor HP. 081272427629

Demikian disampaikan dan diucapkan terima kasih.

KEPALA DINAS KOMUNIKASI, INFORMATIKA,
STATISTIK DAN PERSANDIAN

ARDIAN ARIFANARDI, AP., M. Si
Pembina Utama Muda
NIP. 197407201993111001.

Tembusan :

1. Kabid E-Government Diskominfo SP Kab. Muara Enim

Lampiran : Surat Kepala Dinas Komunikasi, Informatika, Statistik dan Persandian
Nomor : 500.12.10/12/DISKOMINFO/2025
Tanggal : 24 Juni 2025

TEMUAN INSIDEN SIBER SLOT GACOR ASET PEMKAB MUARA ENIM TAHUN 2025

Tanggal Temuan Insiden : 04 Juni 2025
Jenis Insiden : Slot Gacor

No	Link terdampak	Tindak Lanjut	Keterangan
1	https://dpmptsp.muaraenimkab.go.id/docs/index.php?ez=GACOR-ANTI-RUNGKAD-RTP	Sudah di take down	DPMPTSP
2	https://dpmptsp.muaraenimkab.go.id/docs/index.php?ez=APA-ITU-GACOR	Sudah di take down	DPMPTSP
3	https://dpmptsp.muaraenimkab.go.id/docs/index.php?ez=BO-OLYMPUS-GACOR-2024	Sudah di take down	DPMPTSP
4	https://dpmptsp.muaraenimkab.go.id/docs/index.php?ez=BO-OLYMPUS-GACOR-RTP	Sudah di take down	DPMPTSP
5	https://dpmptsp.muaraenimkab.go.id/docs/index.php?ez=SCATTER-MUDAH-LOGIN	Sudah di take down	DPMPTSP
6	https://dpmptsp.muaraenimkab.go.id/docs/index.php?ez=ZEUS-SCATTER-WAP	Sudah di take down	DPMPTSP

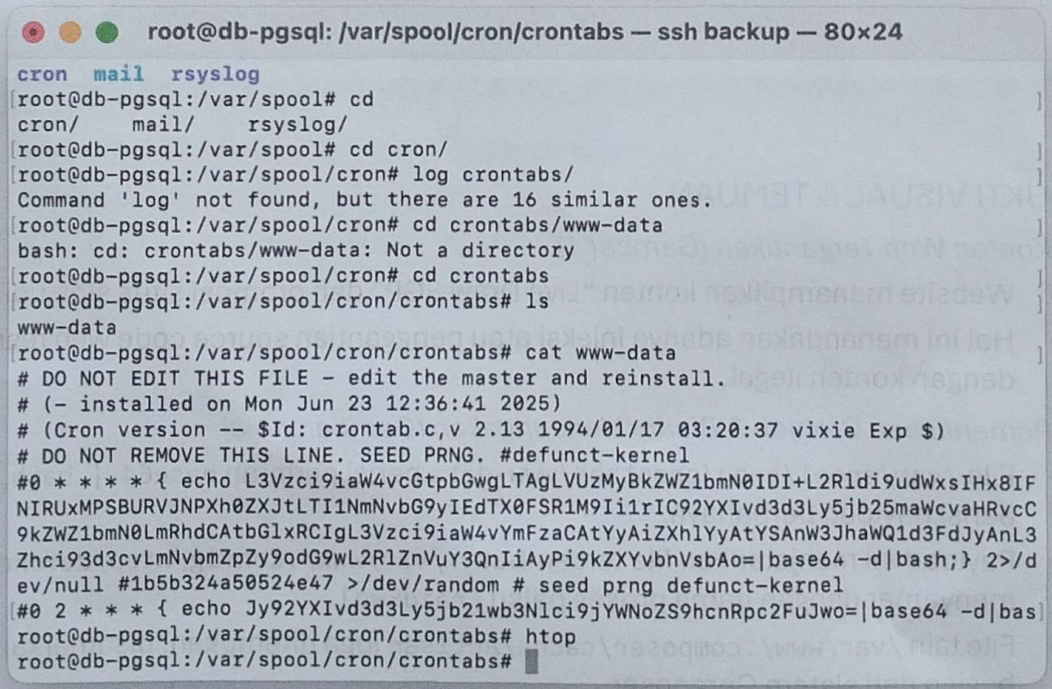
LAPORAN INSIDEN KEAMANAN SISTEM

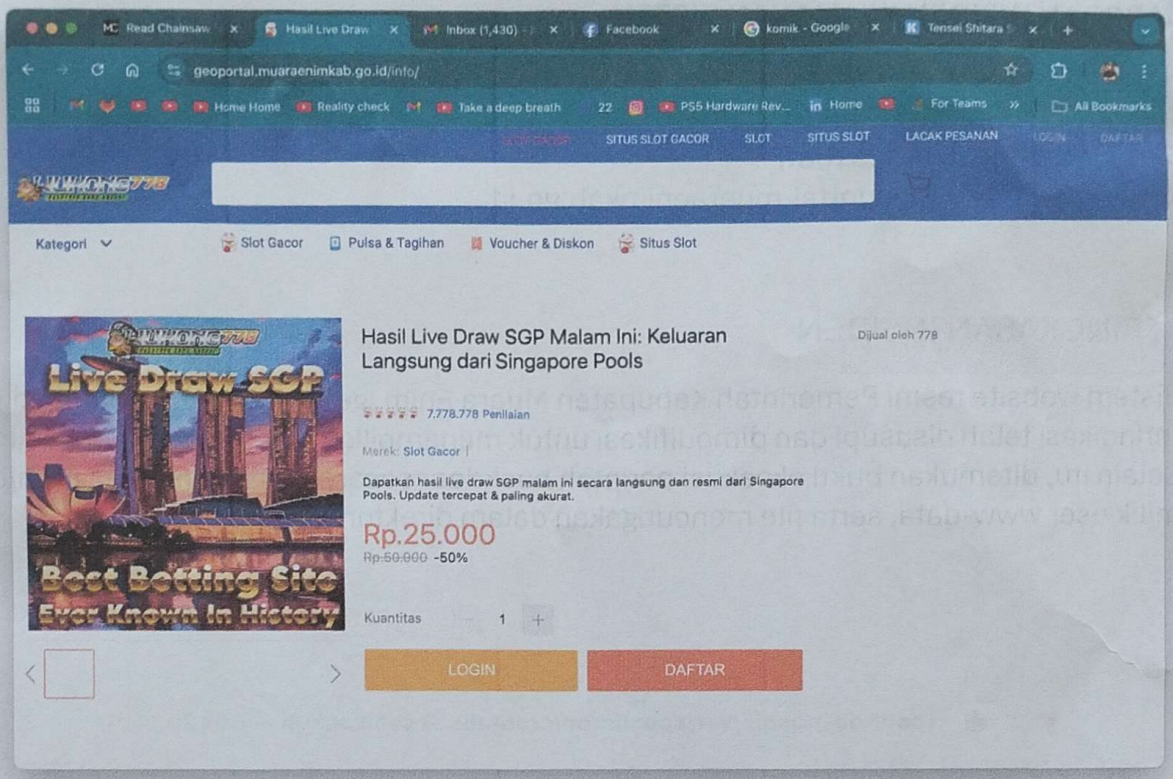
Nama Sistem: geoportal.muaraenimkab.go.id
Tanggal Deteksi: 3 Juli 2025
Server: db-pgsql (akses root)
Lokasi: /var/www/geoportal.muaraenimkab.go.id

---

1. RINGKASAN INSIDEN

Sistem website resmi Pemerintah Kabupaten Muara Enim (geoportal.muaraenimkab.go.id) terindikasi telah disusupi dan dimodifikasi untuk menampilkan konten perjudian online. Selain itu, ditemukan bukti eksekusi perintah backdoor secara periodik melalui cronjob milik user www-data, serta file mencurigakan dalam direktori sistem.





2. BUKTI VISUAL & TEMUAN

2.1. Konten Web Tergantikan (Gambar 1)

- Website menampilkan konten "Live Draw SGP" dan promosi situs slot judi.
- Hal ini menandakan adanya injeksi atau penggantian source code web resmi dengan konten ilegal.

2.2. Pemeriksaan Cronjob & Binary Mencurigakan (Gambar 2 & 3)

- File `/var/spool/cron/crontabs/www-data` berisi perintah `base64 | bash`, yang berisi payload berbahaya.
- Payload ini menjalankan file tersembunyi `/var/www/.config/htop/defunct` dan menyamar dengan nama proses palsu `[raid5wq]`.
- File lain `/var/www/.composer/cache/artisan` juga ditemukan, disamarkan seolah bagian dari sistem Composer.

2.3. Kegagalan Utilitas Standar

- Tools standar seperti `netstat`, `proftpd`, `crontab -e` tidak tersedia/berfungsi, menandakan kemungkinan sistem telah dimodifikasi oleh penyerang.

---

3. ANALISIS INSIDEN

- Penyerang berhasil memperoleh akses tulis pada sistem, kemungkinan melalui celah upload file atau injeksi web.
- Malware mempertahankan keberadaannya melalui cronjob user www-data.
- Teknik penyembunyian meliputi obfuscation base64, penggunaan nama proses palsu, dan peletakan binary di lokasi tidak wajar.

---

4. TINDAKAN YANG DIREKOMENDASIKAN

4.1. Isolasi

- Cabut koneksi internet dari server terindikasi.
- Backup penuh seluruh sistem untuk keperluan forensik.

4.2. Eliminasi Ancaman

- Hapus cronjob user www-data.
- Karantina file:
  - `/var/www/.config/htop/defunct`
  - `/var/www/.composer/cache/artisan`
- Hentikan proses aktif mencurigakan.

4.3. Audit & Recovery

- Cek integritas semua file sistem dan aplikasi.
- Re-deploy dari source yang bersih.
- Ganti seluruh kredensial (SSH, DB, dll).
- Tambahkan proteksi WAF, monitoring cron, dan file integrity checker (AIDE, etc).

---

5. STATUS DAN LANGKAH LANJUT

- Status: KRITIS (kompromi penuh web server).
- Rencana: Format ulang server dan deployment ulang sistem. Lanjutkan investigasi potensi penyusupan dari aplikasi.

Disusun oleh:
Bryan Wahyu
Diskominfo Muara Enim
Tanggal: 3 Juli 2025