PEMERINTAH KABUPATEN TANGERANG
DINAS KOMUNIKASI DAN INFORMATIKA
Jl.H. Somawinata Nomor 1 Tigaraksa – Tangerang
Tlp. (021) 59944530 - 5994531-5994532 (Hunting) Fax (021) 5990604
Kode Pos 15720

Tigaraksa, 09 Juni 2023

Nomor : 330 / 1172 - Diskominfo
Sifat : Biasa
Lampiran : 1 (satu) lembar
Perihal : Tindak Lanjut Permohonan Domain dan VPS (*Virtual Private Server*)

Kepada :
Yth. Kepala Dinas Bina Marga dan Sumber Daya Air Kabupaten Tangerang
di -
Tempat

Dipermaklumkan dengan hormat, menindaklanjuti Surat Kepala Dinas Bina Marga dan Sumber Daya Air Kabupaten Tangerang tanggal 13 Maret 2023 perihal Permohonan Domain dan VPS (*Virtual Private Server*) *arsip-binamarga.tangerangkab.go.id*, maka dapat kami sampaikan beberapa hal sebagai berikut:

1. Berdasarkan hasil pengujian keamanan Aplikasi E-Arsip Dinas Bina Marga dan Sumber Daya Air dengan metode *White-Box Testing* dengan total *resume threat level* yang ditemukan dengan Level *High* sebanyak 1.
2. Permohonan domain *arsip-binamarga.tangerangkab.go.id* pada Aplikasi E-Arsip Dinas Bina Marga dan Sumber Daya Air belum dapat diberikan atau belum lulus pengujian, sehingga kami merekomendasikan agar dilakukan perbaikan/penambalan terhadap kerentanan yang berhasil ditemukan.
3. Mengingat banyaknya permintaan permohonan *penetration testing*, dimohon untuk segera memperbaiki atau menutup celah keamanan hingga batas waktu yang diberikan maksimal selama 30 (tiga puluh) hari kedepan tertanggal 11 Juli 2023. Jika dalam batas waktu yang telah ditentukan aplikasi belum diperbaiki atau belum menindaklanjuti surat ini, maka aplikasi sementara akan dinonaktifkan/*down*.
4. Pengujian kembali terhadap hasil perbaikan aplikasi akan segera dilakukan berdasarkan surat laporan perbaikan aplikasi yang disertai dengan melampirkan data atau hasil perbaikan tersebut.

Demikian pemberitahuan ini, atas perhatian dan kerjasamanya disampaikan terima kasih

Kepala Dinas Komunikasi dan Informatika
H. NONO SUDARNO, ST, M.Si
NIP.196312231983031005

Dokumen ini ditandatangan secara elektronik menggunakan Sertifikat Elektronik BSrE - BSSN

No	Nama Kegiatan/Pekerjaan	Tempat	Progress
1	Pengujian Keamanan Aplikasi E-Arsip Dinas Bina Marga dan Sumber Daya Air Dengan Metode White-Box Testing	Diskominfo Kabupaten Tangerang	100%

Lampiran Foto Kegiatan

Gambar disertakan pada bagian konten utama (Deskripsi)

DESKRIPSI

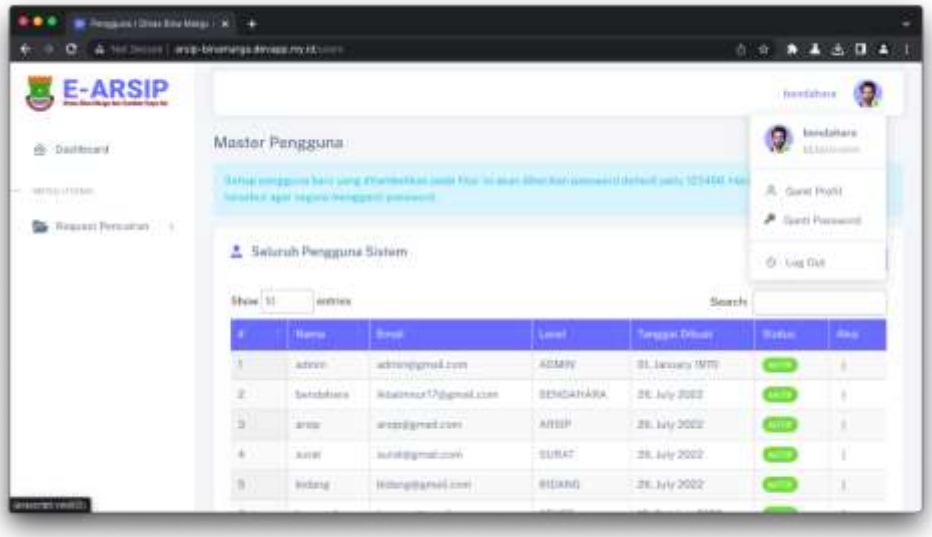
Issue / Case :

Pengujian mulai dilakukan pada tanggal 16 Mei 2023; Kegiatan ini dilakukan bertujuan untuk menguji tingkat keamanan Aplikasi E-Arsip Dinas Bina Marga dan Sumber Daya Air yang beralamat di http://arsip-binamarga.devapp.my.id. Pengujian dilakukan terhadap *Server Staging*, dengan metode *White-box testing*.

1.1 Broken Access Control

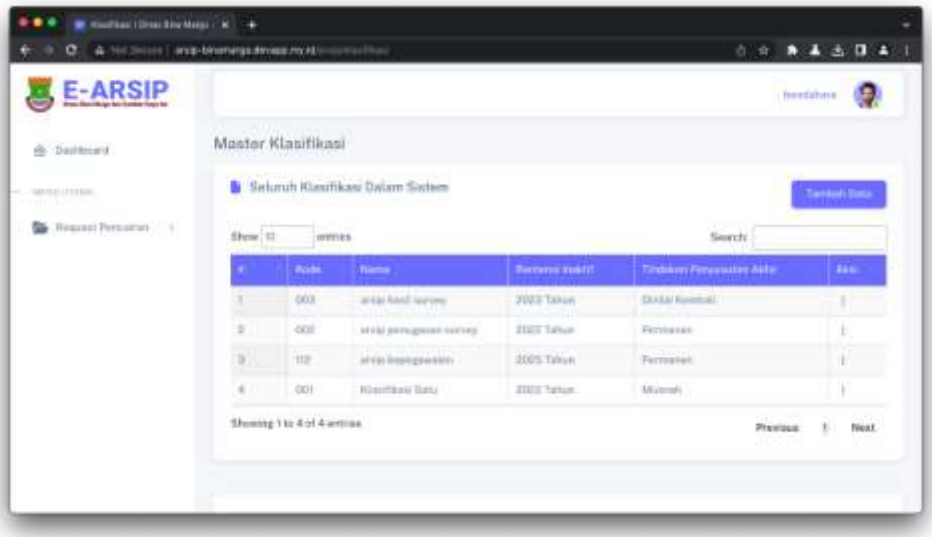
URL : /users
URL : /bidang
URL : /sub-bidang
URL : /vendor
URL : /dokumen-kontrak
URL : /dokumen-pencairan
URL : /program
URL : /kegiatan
URL : /arsip/klasifikasi
URL : /arsip/tingkat-keaslian
URL : /arsip/media-arsip
URL : /arsip/kondisi-arsip
URL : /arsip/penyimpanan
URL : /arsip/daftar-arsip
URL : /arsip/laporan-arsip
URL : /jenis-surat
URL : /boks-surat
URL : /klsf
URL : /pengirim-surat
URL : /surat-masuk
URL : /surat-keluar
URL : /request-pengarsipan-surat

METHOD : Get
THREAD LEVEL : High



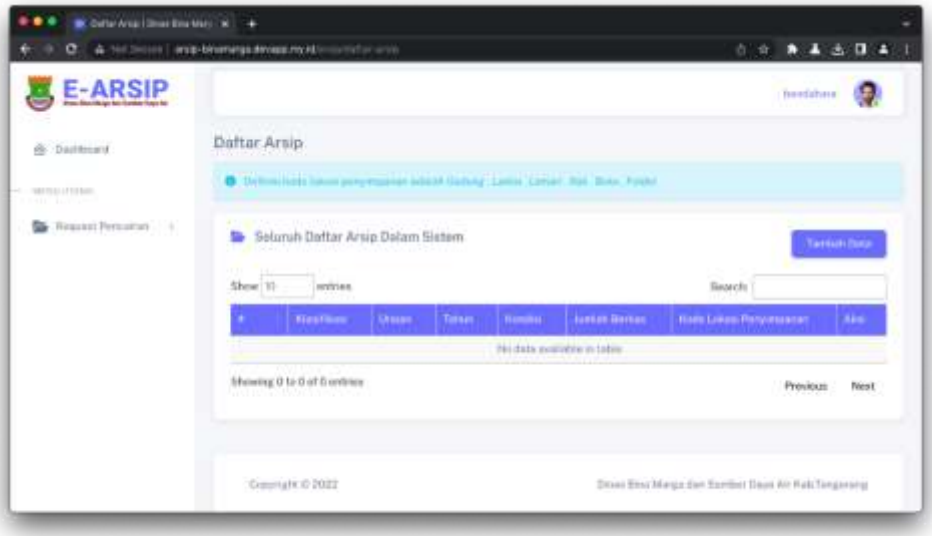
Gambar 1.1

*Pengguna Bendahara Direct Access ke Modul /*users



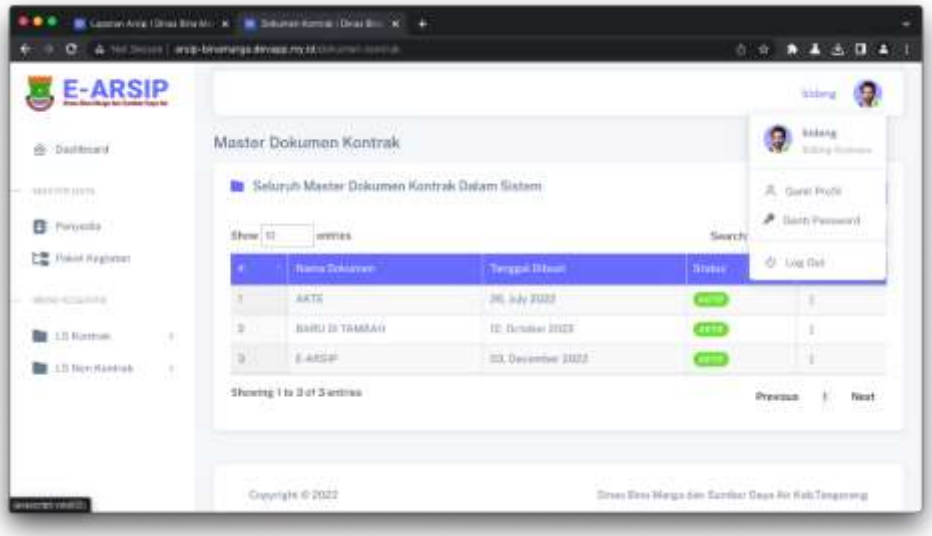
Gambar 1.2

*Pengguna Bendahara Direct Access Ke Modul /arsip /*klasifikasi



Gambar 1.3

*Pengguna Bendahara Direct Access Ke Modul /*arsip/daftar-arsip



Gambar 1.4

*Pengguna Bendahara Direct Access Ke Modul /*dokumen-kontrak

Kontrol akses memberlakukan kebijakan sehingga pengguna tidak dapat bertindak di luar izin yang dimaksudkan. Kegagalan biasanya menyebabkan pengungkapan informasi yang tidak sah, modifikasi, atau penghancuran semua data atau melakukan fungsi bisnis di luar batas pengguna. Kerentanan kontrol akses umum meliputi:

- Pelanggaran prinsip hak istimewa paling rendah atau penolakan secara default, di mana akses hanya boleh diberikan untuk role atau pengguna tertentu, tetapi tersedia untuk siapa saja;

- Mengabaikan pemeriksaan kontrol akses dengan memodifikasi URL (pengubahan/tampering parameter) atau dengan menggunakan attack tool yang memodifikasi API request;
- Mengizinkan melihat atau mengedit akun orang lain, dengan memberikan pengenal uniknya (insecure direct object references);
- Mengakses API dengan kontrol akses yang hilang untuk POST, PUT, dan DELETE;
- Ketinggian hak istimewa. Bertindak sebagai pengguna tanpa login atau bertindak sebagai admin saat login sebagai pengguna;
- Manipulasi metadata, seperti memutar ulang atau merusak token kontrol akses JSON Web Token (JWT) atau cookie yang dimanipulasi untuk meningkatkan hak istimewa;
- Force browsing ke halaman yang diautentikasi sebagai pengguna yang tidak diautentikasi atau ke halaman yang diistimewakan sebagai pengguna standar.

1.1.1 Rekomendasi

Kontrol akses hanya efektif dalam pemrograman server-side atau server-less API, di mana penyerang tidak dapat mengubah pemeriksaan kontrol akses atau metadata.

- Kecuali untuk publik, deny by default;
- Kontrol akses model harus menerapkan kepemilikan rekaman daripada menerima bahwa pengguna dapat membuat, membaca, memperbarui, atau menghapus rekaman apa pun;
- Nonaktifkan daftar direktori server web dan pastikan metadata file (misal: .git) dan file cadangan tidak ada dalam root web;
- Catat kegagalan kontrol akses, beri tahu admin bila perlu (misal: kegagalan berulang);

1.1.2 Referensi

- https://owasp.org/www-project-application-security-verification-standard
- https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/05-Authorization_Testing/README
- https://cheatsheetseries.owasp.org/cheatsheets/Access_Control_Cheat_Sheet.html
- https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html
- https://www.oauth.com/oauth2-servers/listing-authorizations/revoking-access/

To Do :

- Koordinasi dengan tim pengembang sistem untuk melakukan mitigasi berupa penambalan terhadap kerentanan sistem yang ditemukan.
- Melakukan pengujian ulang terhadap kerentanan- kerentanan yang berhasil ditemukan; setelah mendapatkan konfirmasi penyelesaian proses mitigasi dari developer.

Notes :