No	Nama Kegiatan/Pekerjaan	Tempat	Progress
1	Pengujian Keamanan Aplikasi Surat Peralihan Hak Dengan Metode White-Box Testing	Diskominfo Kabupaten Tangerang	100%

Lampiran Foto Kegiatan

Gambar disertakan pada bagian konten utama (Deskripsi)

DESKRIPSI

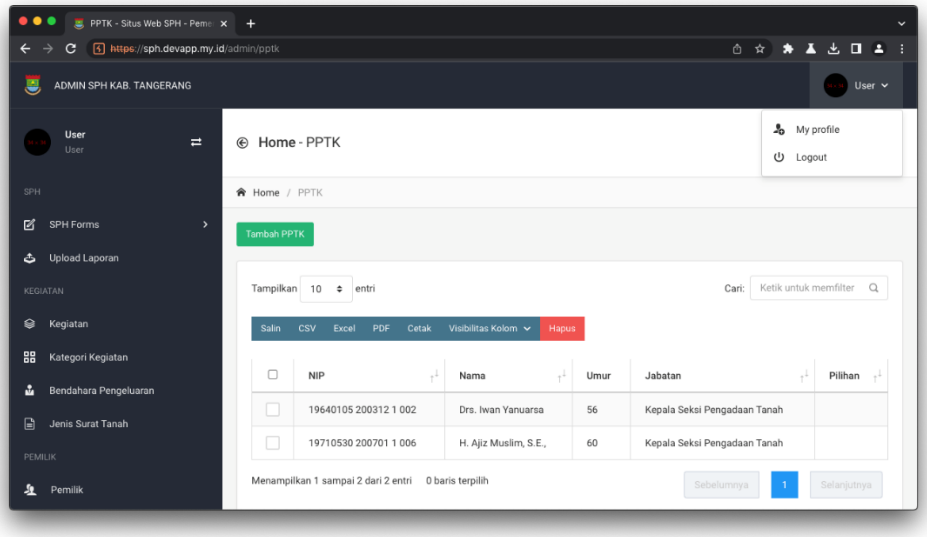
Issue / Case :

Pengujian mulai dilakukan pada tanggal 02 Mei 2023; Kegiatan ini dilakukan bertujuan untuk menguji tingkat keamanan Aplikasi Surat Peralihan Hak yang beralamat di https://sph.devapp.my.id. Pengujian dilakukan terhadap *Server Staging*, dengan metode *White-box testing*.

1.1 Broken Access Control

URL : admin/pptk
URL : admin/jabatan-pptk
URL : admin/sk-kepala-dinas
URL : admin/kejaksaan-negeri
URL : admin/dinas-terkait
URL : admin/bagian-hukum
URL : admin/kepala-pemakaman-pertanahan
METHOD : Get
THREAD LEVEL : High

Semua modul di atas masih dapat diakses oleh pengguna dengan Role “User”.



Gambar 1.1

Direct Access Modul /admin/pptk

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 :

No	Nama Kegiatan/Pekerjaan	Tempat	Progress
2	Pengujian Keamanan Aplikasi Izin Penggunaan Tanah Makam Dengan Metode White-Box Testing	Diskominfo Kabupaten Tangerang	100%

Lampiran Foto Kegiatan

Gambar disertakan pada bagian konten utama (Deskripsi)

DESKRIPSI

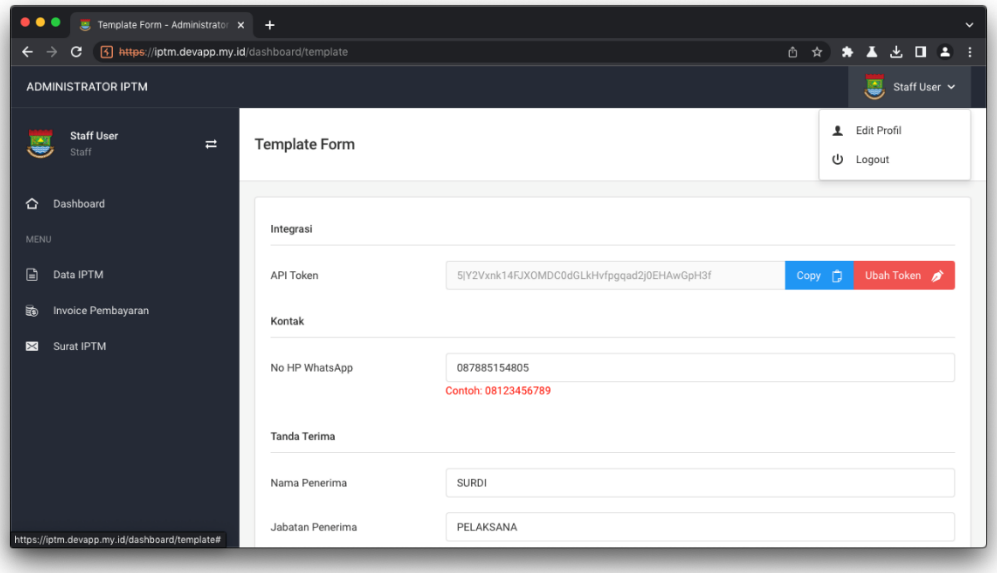
Issue / Case :

Pengujian mulai dilakukan pada tanggal 02 Mei 2023; Kegiatan ini dilakukan bertujuan untuk menguji tingkat keamanan Aplikasi Izin Penggunaan Tanah Makam yang beralamat di https://iptm.devapp.my.id. Pengujian dilakukan terhadap *Server Staging*, dengan metode *White-box testing*.

2.1 Broken Access Control

URL : /dashboard/template
METHOD : Get
THREAD LEVEL : High

Modul di atas masih dapat diakses oleh pengguna dengan Role “Staff”.



Gambar 2.1

Direct Access Modul /dashboard/template

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.

2.1.1 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);

2.1.2 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 :