PEMERINTAH KABUPATEN SIDOARJO
DINAS KOMUNIKASI DAN INFORMATIKA
Jl. Diponegoro No.139 Telp./Fax 031-8073915, fax. 031-8949231 SIDOARJO – 61213

BERITA ACARA
HASIL PENGUJIAN KEAMANAN INFORMASI
APLIKASI PROKOPIM

Nomor : 473.1/1668/438 . 5 . 14/2023

Pada hari ini Senin, 04 Desember 2023, kami yang bertanda tangan dibawah ini telah melakukan uji coba keamanan informasi pada aplikasi sebagai berikut:

Url Aplikasi	: https://prokopim.sidoarjokab.go.id/
OPD Pembuat Aplikasi	: Bagian Protokol Kabupaten Sidoarjo
Fungsi Aplikasi	: melaksanakan penyiapan pelaksanaan kebijakan, pengoordinasian pelaksanaan tugas Perangkat Daerah, pemantauan dan evaluasi pelaksanaan kebijakan daerah di bidang Protokol, Komunikasi Pimpinan, dan Dokumentasi.

Berdasarkan hasil uji coba kerentanan keamanan informasi yang dilakukan pada aplikasi tersebut, **ditemukan ancaman dengan tingkat resiko medium**, sebagaimana terlampir dalam hasil pengujian sistem, dengan ini Bidang Infrastruktur dan Keamanan TIK **dapat melakukan pemasangan** di server Dinas Komunikasi dan Informatika sampai dengan catatan dilakukannya konfirmasi/klarifikasi dan perbaikan terhadap aplikasi berdasarkan rekomendasi/saran yang diberikan.

Demikian Berita Acara ini dibuat rangkap 2 (dua) untuk dipergunakan sebagaimana mestinya.

Menyetujui,
Sub Kordinator
Keamanan Informasi dan Persandian

Ditandatangani secara elektronik oleh

KHOIRIL ERWINDRA, ST
NIP. 198210152006041007

Penguji Aplikasi,

Ditandatangani secara elektronik oleh

FAHRIZAL ARMAN, A.Md.
NIP. 199602052020121009

Mengetahui,
Kepala Bidang Infrastruktur
dan Keamanan TIK

Ditandatangani secara elektronik oleh

ERI SUDEWO, AP, MM
NIP. 197603101994121001

Lampiran Berita Acara
Nomor : 473.1/1668/438 . 5 . 14/2023
Tanggal : 04 Desember 2023

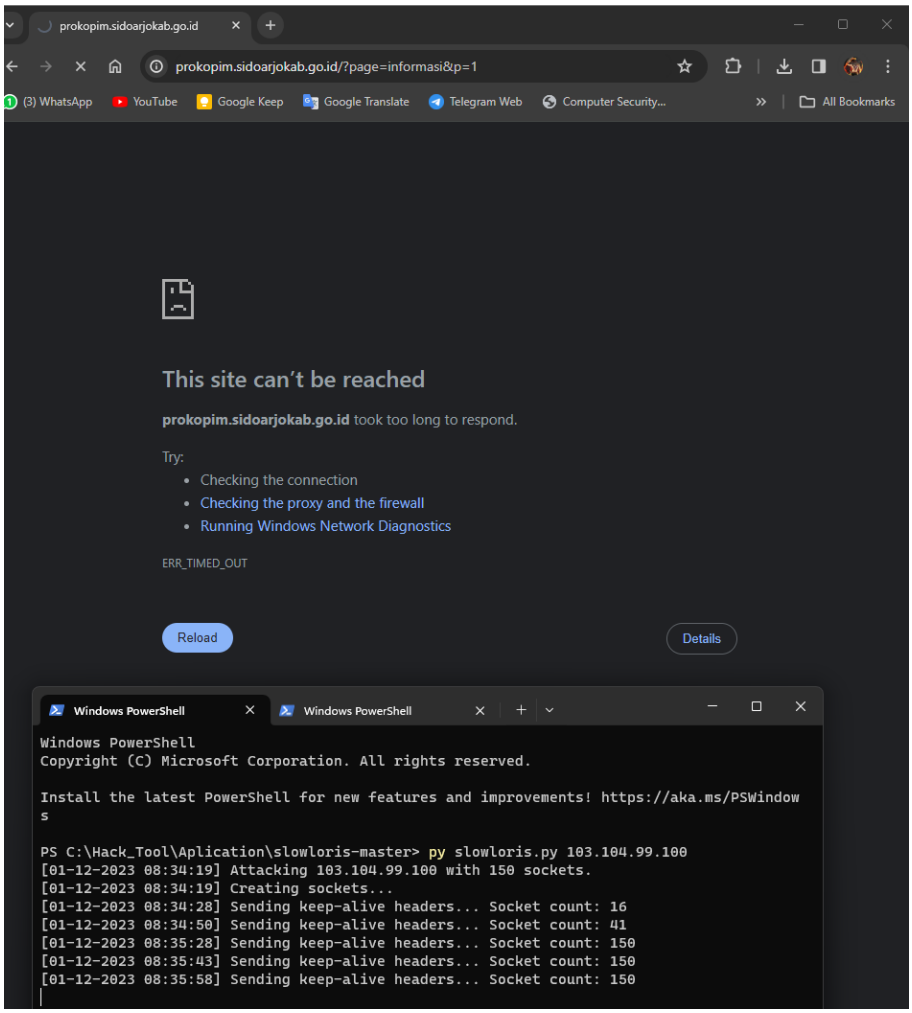
HASIL PENGUJIAN SISTEM

Terdapat 1 level ancaman (Medium) terhadap keamanan sistem yang ditemukan pada aplikasi **Prokopim** sebagaimana pada tabel berikut :

No	Hasil Pengujian	Kategori	Jumlah
1.	Slow HTTP Denial of Service Attack	Medium	1
2.	Vulnerable Package Dependencies	Medium	10
3.	Directory listings	Medium	8
4.	PHP File upload	Medium	1
Total			20

1. HTTP Denial of Service Attack

Web rentan terhadap serangan HTTP DoS (Denial of Service) yang bisa mengakibatkan website **Prokopim** down ketika serangan di aktifkan.



Saran :

1) Pada Apache server bias menggunakan `req_modetimeout`, `mod_quos`, atau `mod_security`.
2) Mengupdate package npm menjasi dersi yang terbarukan

2. Vulnerable Package Dependencies

Pada web **Prokopim** ditemukan beberapa package NPM telah kadaluarsa yang memungkinkan adanya kerentanan pada package tersebut.

- css-what 2.1.2
- debug 2.6.1
- engine.io 3.2.1
- express 4.15.2
- fresh 0.5.0
- lodash 4.17.11
- mime 1.3.4
- nth-check 1.0.2
- socket.io-parser 3.2.0
- xmlhttprequest-ssl 1.5.5

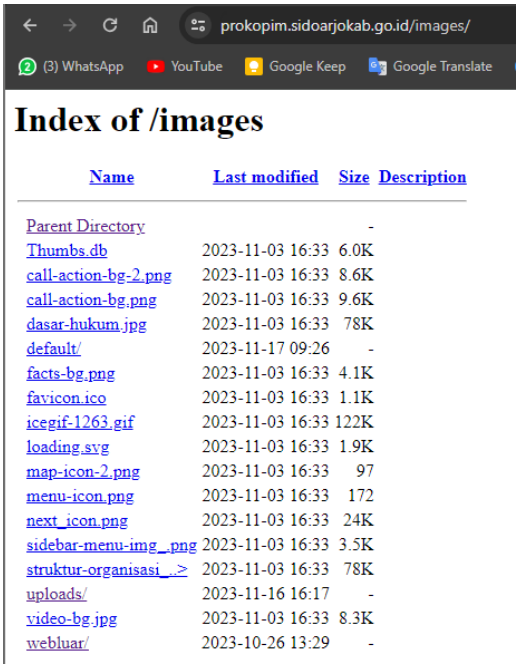
Saran :

Update package ke versi yang terbaru (`npm update`)

3. Directory listings

Direktori listing adalah fungsi server web yang menampilkan isi direktori ketika tidak ada file indeks di direktori situs web tertentu. Berbahaya untuk membiarkan fungsi ini dihidupkan untuk server web karena mengarah pada pengungkapan informasi.

https://prokopim.sidoarjokab.go.id/images
https://prokopim.sidoarjokab.go.id/pengelolaweb
https://prokopim.sidoarjokab.go.id/fonts/
https://prokopim.sidoarjokab.go.id/downloads/
https://prokopim.sidoarjokab.go.id/vendor/
https://prokopim.sidoarjokab.go.id/js/
https://prokopim.sidoarjokab.go.id/css/
https://prokopim.sidoarjokab.go.id/backend/



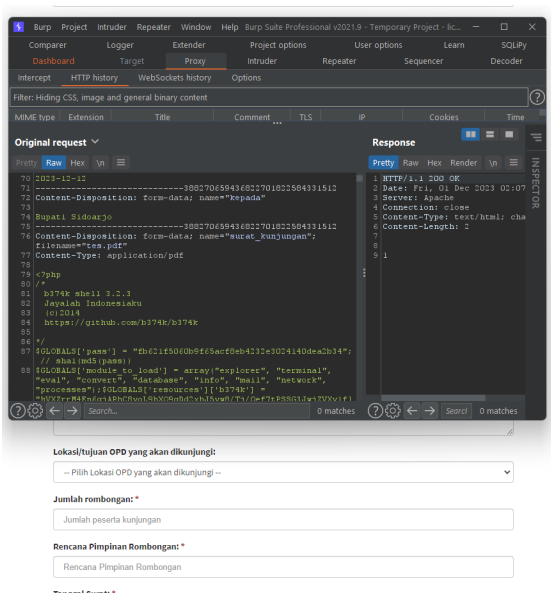
Saran :

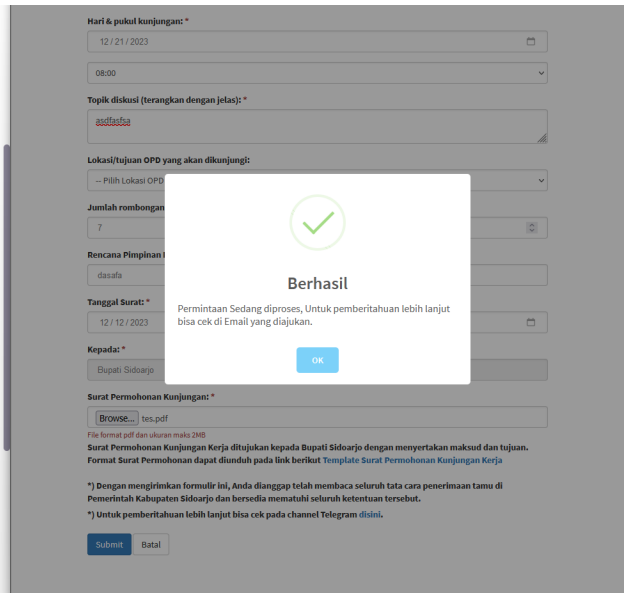
Anda harus memastikan tidak ada informasi sensitif yang diungkapkan dan membatasi akses daftar direktori dari konfigurasi server web.

4. PHP File upload

Sebuah website seharusnya hanya menerima file upload sesuai dengan kategori yang telah ditentukan, yang bertujuan untuk mencegah penyisipan file *backdoor* terutama file dengan format **php** yang marak di gunakan sebagai alat penyisipan website perjudian.

https://prokopim.sidoarjokab.go.id/kunjungan-kerja/?page=form





Lampiran Berita Acara
Nomor : 473.1/1668/438 . 5 . 14/2023
Tanggal : 04 Desember 2023

Saran :

Berikan filter pada menu file upload serta mengatur *httacces* folder file upload agar hanya menjalankan fiile yang sesuai dengan ketentuan yang di berikan (contoh : pdf,jpeg,png)

Lampiran Berita Acara
Nomor : 473.1/1668/438 . 5 . 14/2023
Tanggal : 04 Desember 2023

CHEKLIST UJI KEAMANAN APLIKASI		
	Acuan	Peraturan BSSN-04-2021
	Nama Aplikasi	Prokopim
	Revisi	00

No	Fungsi	Prosedur	Keterangan	Check
1	Autentikasi	menggunakan manajemen kata sandi untuk proses autentikasi	adanya user dan sandi yang diperlukan untuk akses akun aplikasi	√
		mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi	minimal menggunakan 8 karakter dengan kombinasi huruf besar,angka, dan karakter	-
		mengatur jumlah maksimum kesalahan dalam pemasukan kata sandi	maksimal 5x kesalahan dengan jeda 3 menit untuk memasukkan kata sandi kembali	-
		mengatur mekanisme pemulihan kata sandi	tersedia fitur reset password bagi pengguna	√
		menggunakan jalur komunikasi yang diamankan untuk proses autentikasi.	menggunakan Secure Socket Layer untuk komunikasi data	-
2	Manajemen sesi	menggunakan pengendali sesi untuk proses manajemen sesi	terdapat session control untuk mengelola sesi	√
		mengatur pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi	token sesi harus bersifat unik dan acak	√
		mengatur kondisi dan jangka waktu habis sesi	User akan logout otomatis ketika tidak ada aktifitas yang dilakukan (minimal 15 menit)	√
3	Persyaratan kontrol akses	menetapkan otorisasi pengguna untuk membatasi kontrol akses	adanya perbedaan otoritas bagi akun admin dan akun user biasa	√
		mengatur verifikasi kebenaran token ketika mengakses data dan informasi yang dikecualikan.	akun user biasa tidak dapat mengakses fitur-fitur yang hanya dapat di akses oleh akun admin	√
4	Validasi input	menerapkan fungsi validasi input pada sisi server	adanya filter untuk input yang dimasukkan oleh pengguna web	√
		menerapkan mekanisme penolakan input jika terjadi kesalahan validasi	adanya peringatan error saat input yang dimasukkan tidak sesuai	√
		memastikan runtime environment aplikasi tidak rentan terhadap serangan validasi input	lolos uji coba Pentest	√
		melakukan validasi positif pada seluruh input	mendefinisikan pola input yang dianggap valid oleh aplikasi (allow_list) dan dapat diproses	√
		menggunakan fitur kode dinamis	memberikan fitur enkripsi pada setiap parameter dan id yang digunakan	√
		melakukan pelindungan terhadap akses yang mengandung konten skrip	adanya perlindungan dari injeksi script	√
5	Kriptografi pada verifikasi statis	melakukan autentikasi data yang dienkripsi	melakukan autentikasi data yang dienkripsi	√
		membuat angka acak yang menggunakan generator angka acak kriptografi.	parameter id yang digunakan pada aplikasi harus bersifat unik dan acak	√
6	Penanganan eror dan pencatatan log	mengatur konten pesan yang ditampilkan ketika terjadi kesalahan	pesan error tidak mengandung informasi yang sensitif	√
		tidak mencantumkan informasi yang dikecualikan dalam pencatatan log	tidak menampilkan pesan yang mengandung informasi rahasia pada log	√
		mengatur pelindungan log aplikasi dari akses dan modifikasi yang tidak sah	informasi log tidak dapat di akses secara umum	√

7	Proteksi Data	melakukan pelindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi	data yang di masukkan tidak dapat di akses oleh pihak yang tidak berwenang	
		melakukan pertukaran, penghapusan, dan audit informasi yang dikecualikan	menghapus/membatasi akses informasi yang tidak diperlukan (readme.md dll)	√
8	Keamanan komunikasi	menggunakan komunikasi terenkripsi	menggunakan Secure Socket Layer untuk komunikasi data	-
		mengatur aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik.	konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik.	-
9	Pengendalian kode berbahaya	membantu dalam kontrol antiotomatisasi	adanya perlindungan dari bot dengan mengunakan captcha dan sebagainya	√
		memberikan peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa.	adanya sesor IDS yang di pasang pada aplikasi pada saat di server Diskominfo Siidoarjo	-
10	File	mengatur jumlah file untuk setiap pengguna dan kuota ukuran file yang diunggah	adanya batasan besaran file yang akan di ungah	
		melakukan validasi file sesuai dengan tipe konten yang diharapkan	file yang bisa di unggah hanya file dengan format yang telah ditetapkan	√
		melakukan konfigurasi server untuk mengunduh file sesuai ekstensi yang ditentukan	file yang di unduh sesuai dengan ekstensi yang ditentukan	√
11	Keamanan konfigurasi.	mengonfigurasi server sesuai rekomendasi server aplikasi dan kerangka kerja aplikasi yang digunakan	server terpasang sensor IDS,SSL, dan anti DDOS	√
		mendokumentasi, menyalin konfigurasi, dan semua dependensi	adanya backup konfiguransi dan disimpan dengan aman	√
		menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan	menghapus file konfigurasi seperti readme.txt, changelog.txt	√

Saran :

1. Mengupdate package NPM menjadi versi yang terbarukan.
2. Memberikan filter untuk file upload.