RAHASIA

LAPORAN KERENTANAN PADA APLIKASI SIMKAH4.KEMENAG.GO.ID (*Broken Object Level Authorization/Insecure Direct Object Reference-IDOR*)

TIM TANGGAP INSIDEN SIBER KEMENAG
(KEMENAG-CSIRT) 2023

RAHASIA

A. Dasar

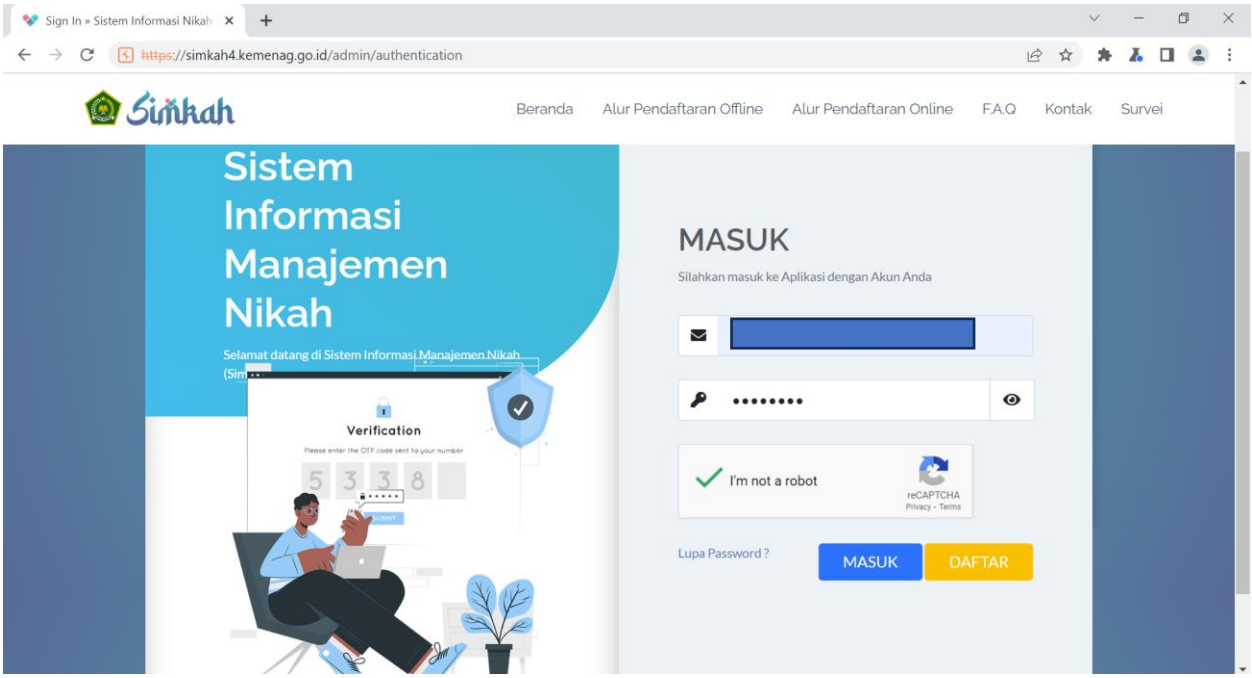
Keputusan Menteri Agama (KMA) Nomor 86 Tahun 2023 Tentang Tim Tanggap Insiden Siber Pada Kementerian Agama Tahun 2023.

B. Proof of Concept (PoC) Kerentanan

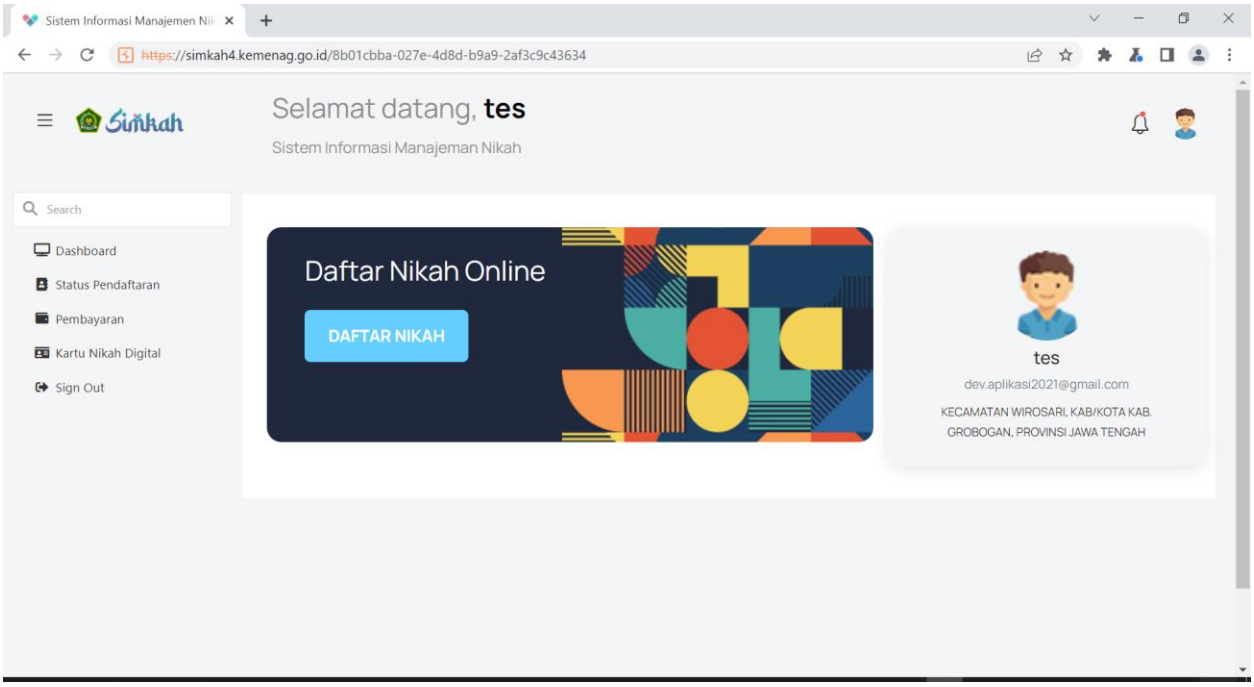
Nama Kerentanan	:	*Broken Object Level Authorization/Insecure Direct Object Reference* (IDOR)
Kategori OWASP 10	:	A01:2023 *Broken Object Level Authorization*
Lokasi URL	:	https://simkah4.kemenag.go.id
Tingkat *Severity*	:	*Critical*
Resiko	:	Kebocoran Data Aplikasi SIMKAH dan Perusakan Data pada Aplikasi
Dampak Hukum	:	Undang Undang No 27 Tahun 2022 tentang Perlindungan Data Pribadi

1. Penguji melakukan *Reconnaissance, Information Gathering dan Analysis* sehingga di dapatkan akun dan *credential* yang valid.

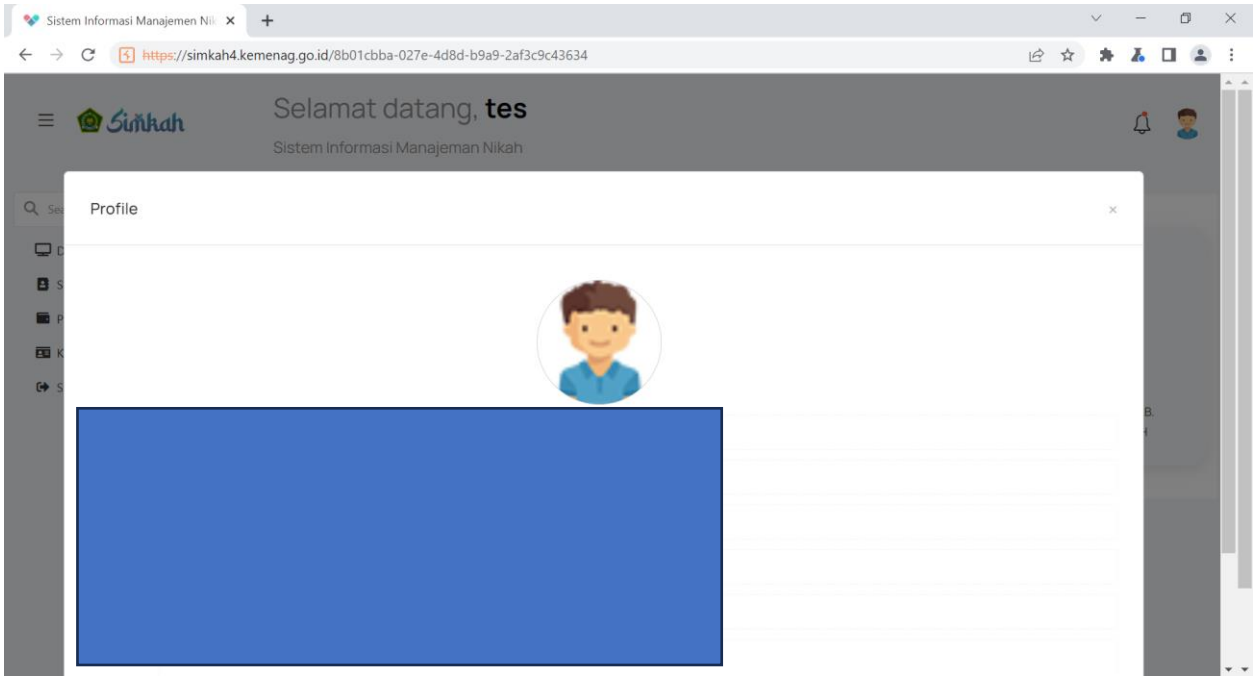
2. Penguji melakukan uji coba *login* ke aplikasi target yaitu simkah4.kemenag.go.id

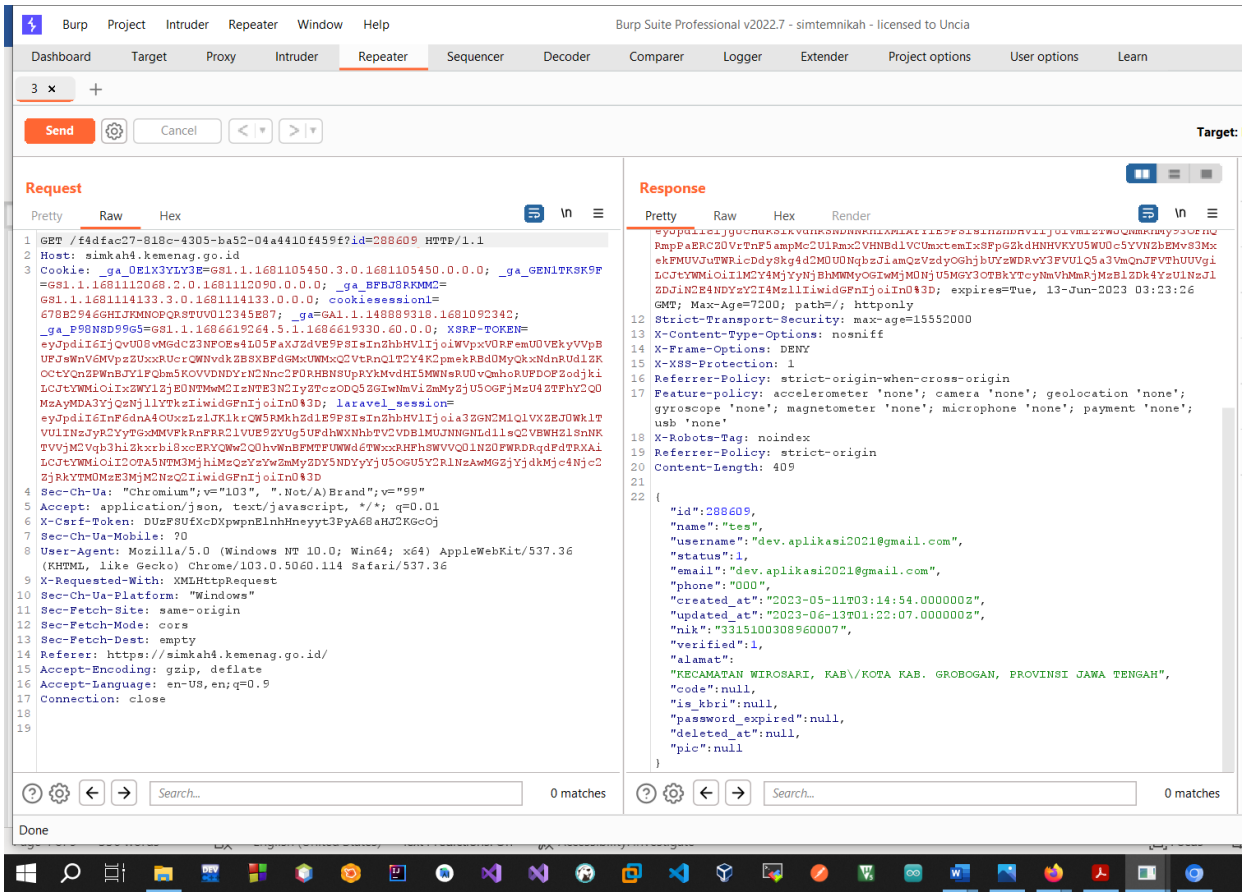


3. Penguji berhasil masuk dengan salah satu *role user*

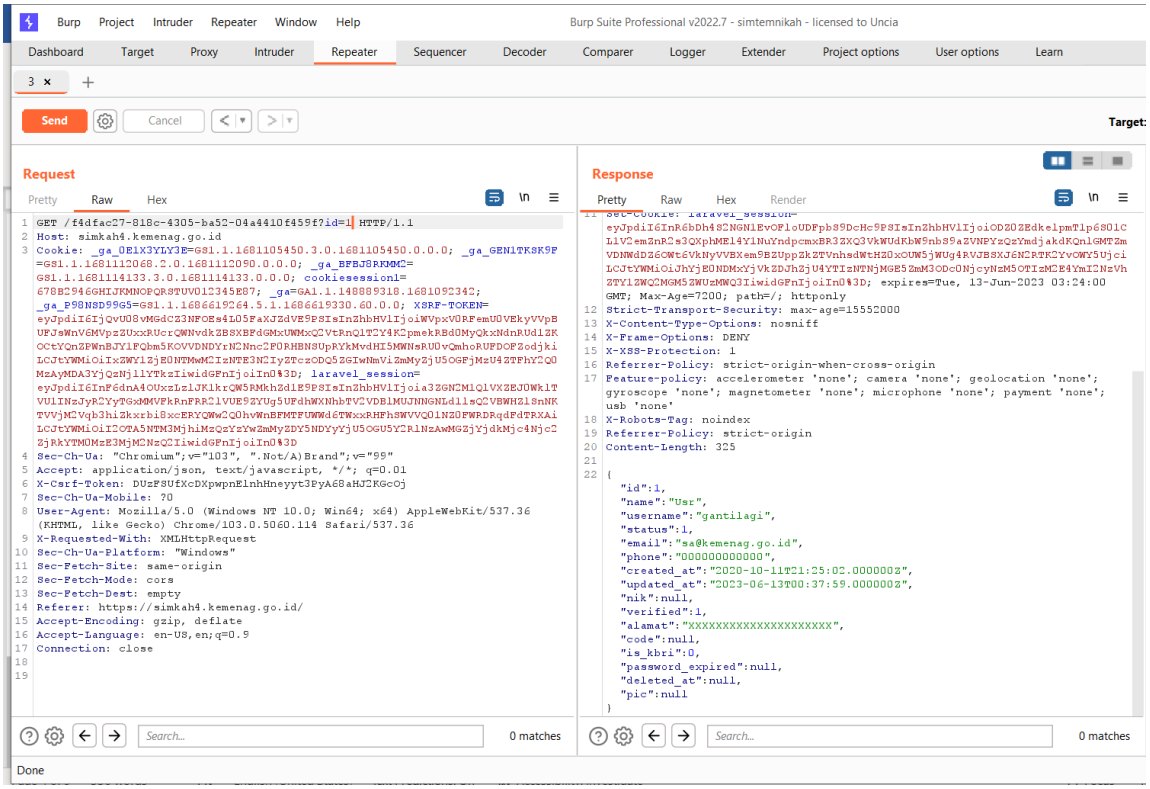


4. Penguji melakukan *proxy request* dengan menggunakan *burpsuite* dan didapatkan hasil *request* berisi informasi data siswa pada URL https://simkah4.kemenag.go.id/f4dfac27-818c-4305-ba52-04a4410f459f?id= 288609 Angka 288609 dibelakang URL menunjukan ID dari data.





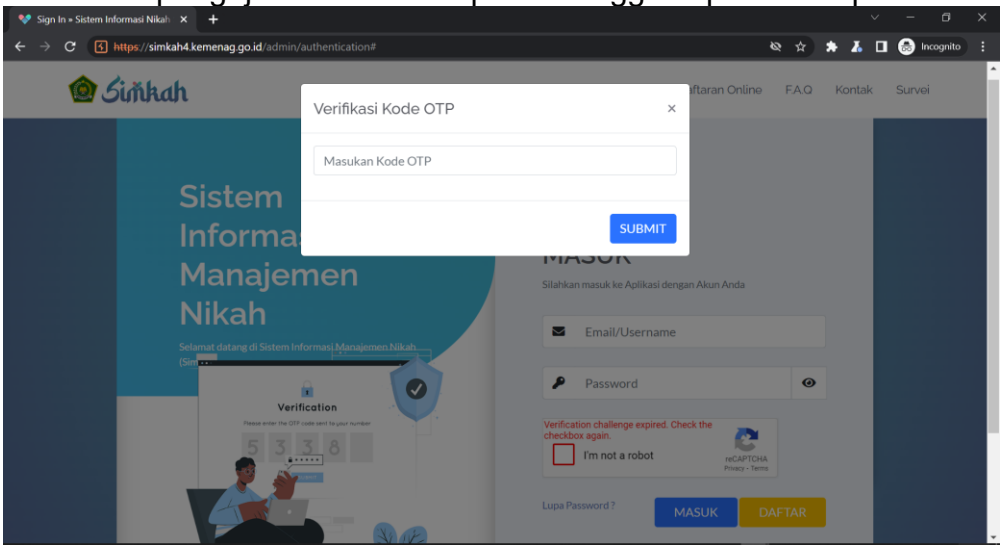
5. Kemudian penguji melakukan request Kembali dengan ID URL dibelakang angka selanjutnya yaitu 1. https://simkah4.kemenag.go.id/f4dfac27-818c-4305-ba52-04a4410f459f?id=1



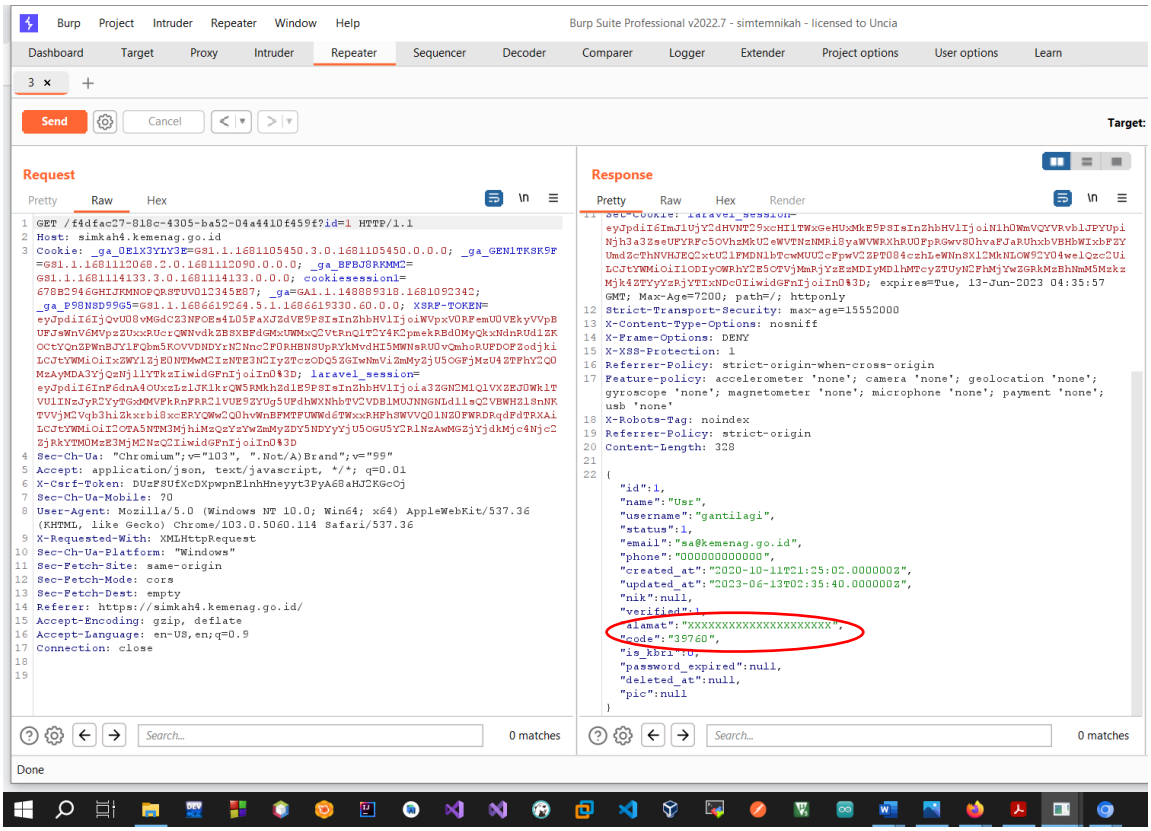
Penguji berhasil mendapatkan data Adminyang seharusnya tidak bisa di dapatkan dengan menggunakan *role user* yang ada.

Penguji mendapatkan informasi admin mulai username, email, dll.

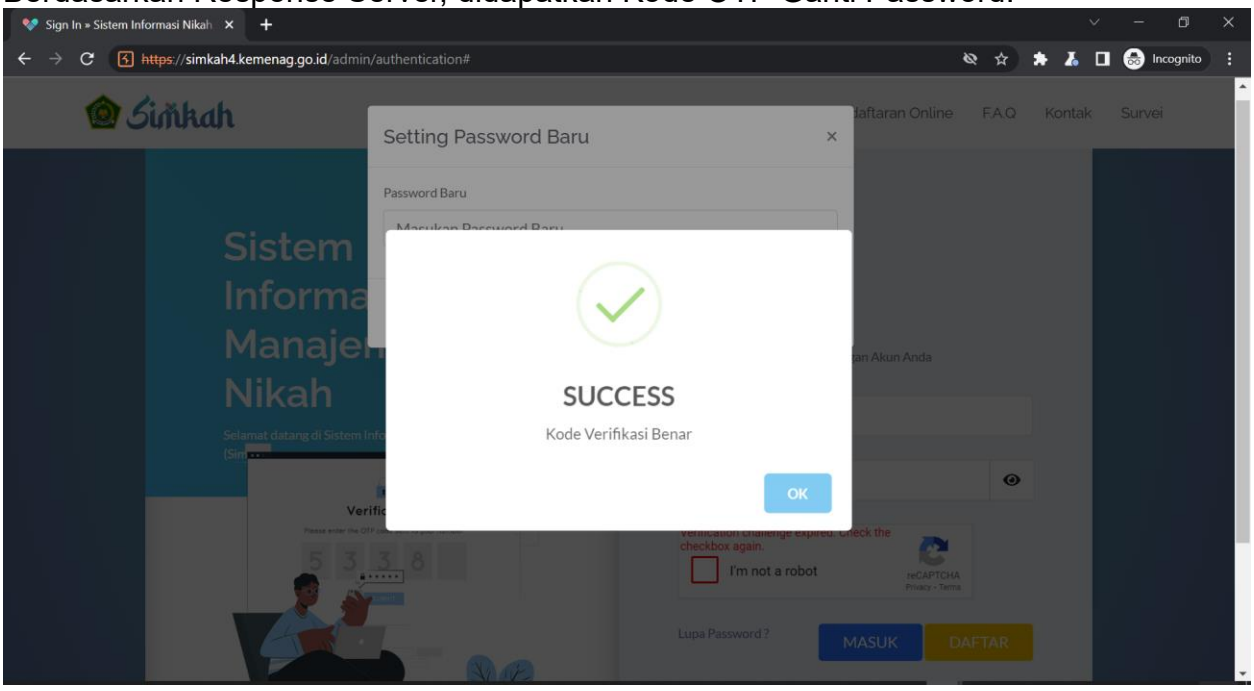
6. Kemudian penguji melakukan request mengganti password pada email admin.

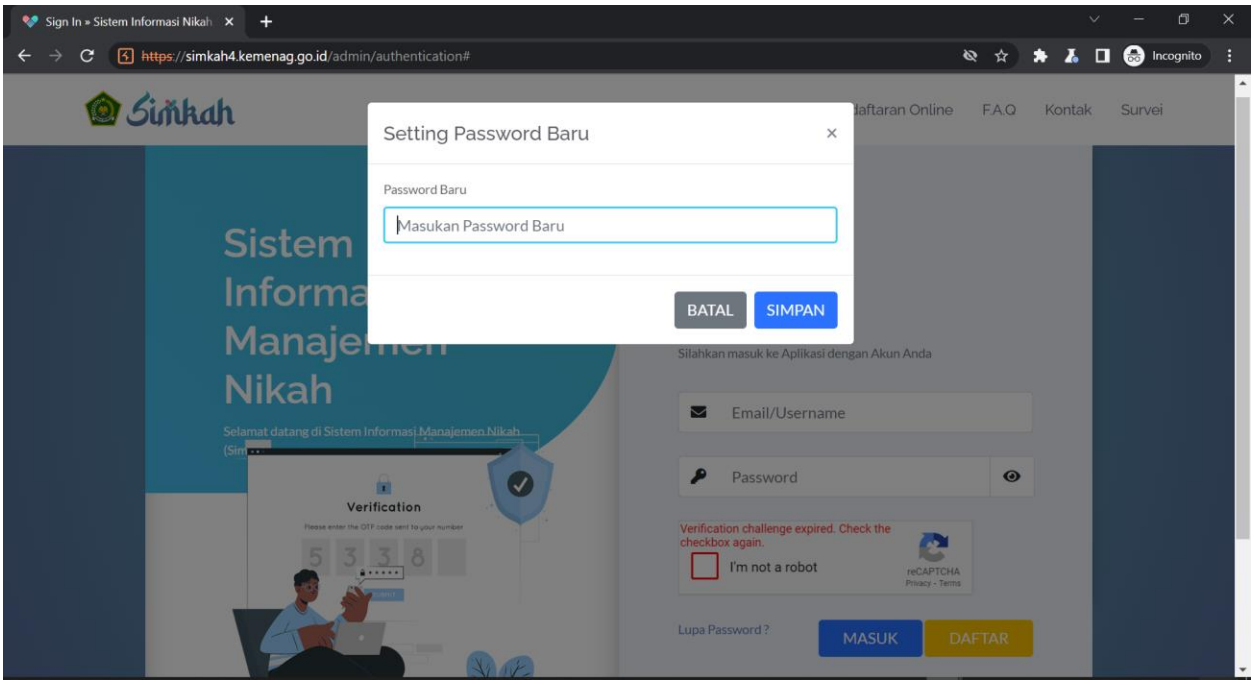


RAHASIA

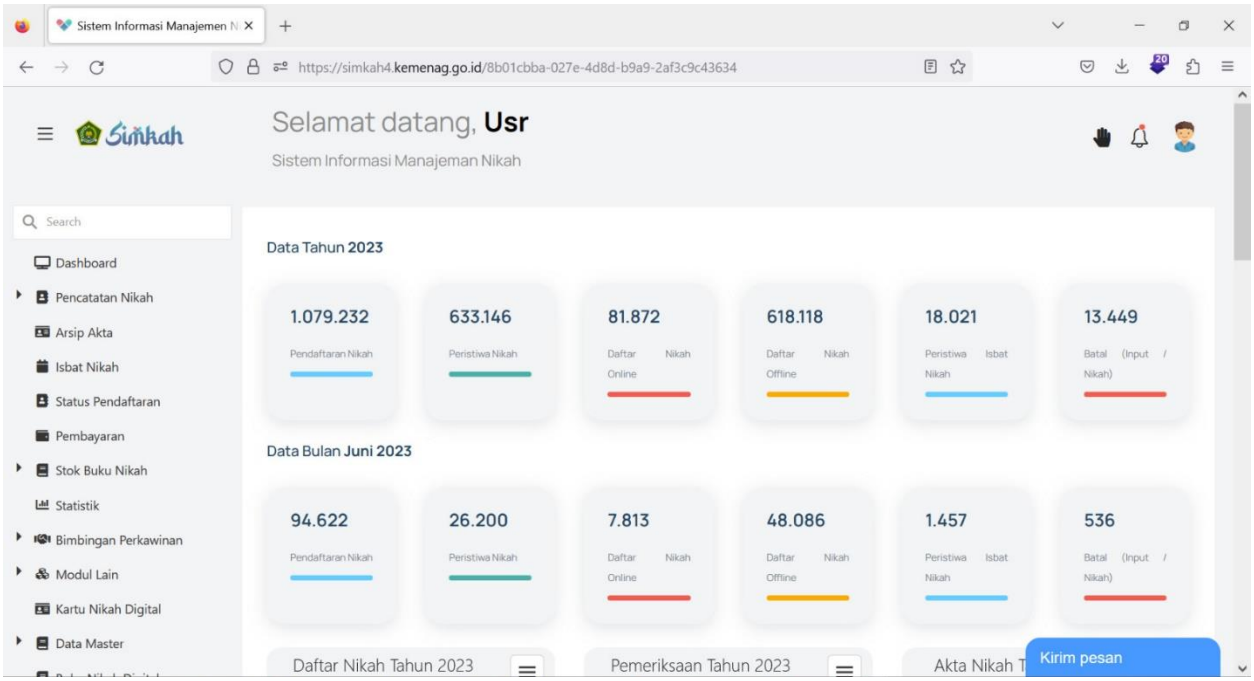


Berdasarkan Response Server, didapatkan Kode OTP Ganti Password.



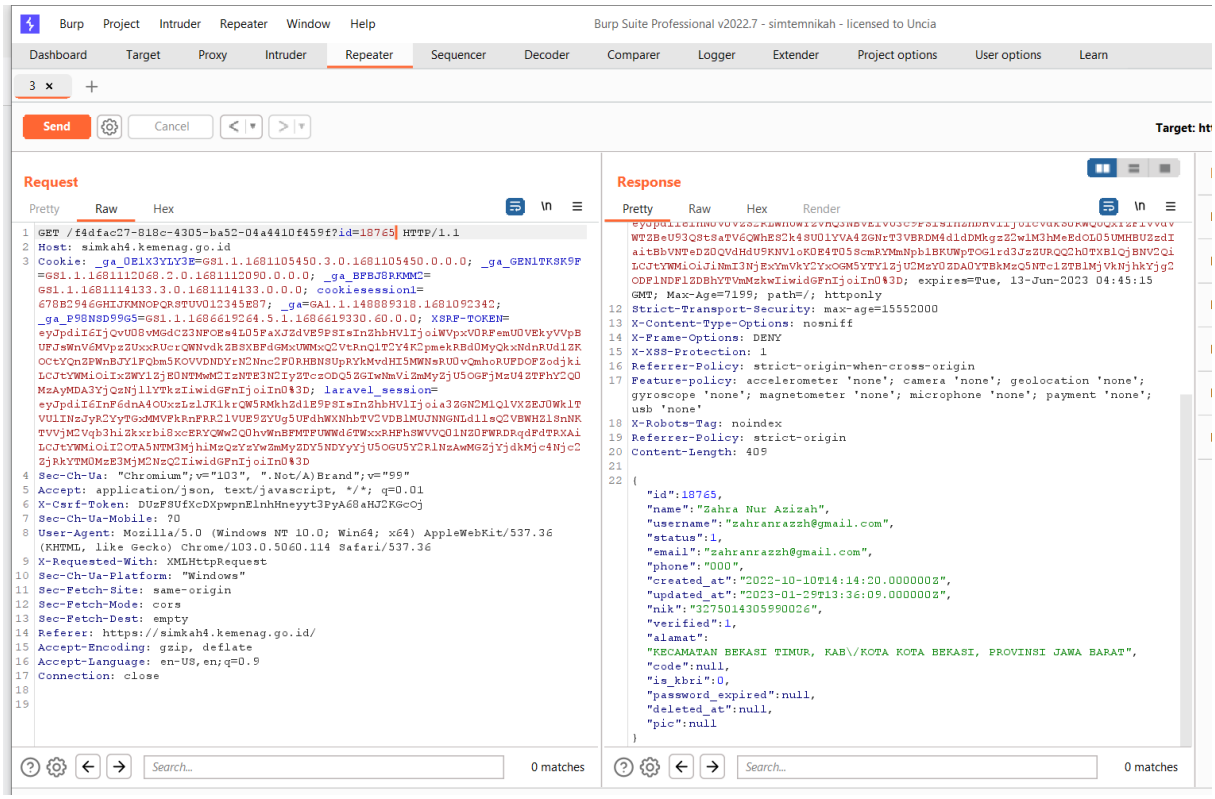


7. Kemudian penguji masuk sebagai admin



Dari fitur Admin Penguji dapat Mengubah, Menambah, dan Mengunduh Semua Data.

8. Penguji bisa mendapatkan informasi user lain



C. Mitigasi Kerentanan

1. Menutup aplikasi sementara waktu untuk perbaikan jika dimungkinkan.
2. Melakukan Review keseluruhan terhadap source code Aplikasi
3. Melakukan Pentest/IT Security Assestmen secara berkala
4. Menerapkan mekanisme otorisasi yang tepat yang bergantung pada kebijakan dan hierarki pengguna
5. Penggunaan ID acak dan tidak dapat ditebak seperti GUID untuk ID rekaman
6. Otorisasi setiap permintaan yang dibuat oleh pengguna.
7. Membatasi Session hanya beberapa menit, untuk membatasi akses.

RAHASIA