PEMPROV SULTENG
DISKOMINFOSANTIK
DINAS KOMUNIKASI, INFORMATIKA, PERSANDIAN DAN STATISTIK

DOKUMEN TERBATAS

# PANDUAN PENANGANAN

## *Data Exposure*

Jl. R.A. Kartini, Kel. Lolu Selatan
Kec. Palu Timur, Kota Palu
Sulawesi Tengah, 94235



2024

## Tabel Versi Dokumen

| No | Versi | Tanggal | Deskripsi Perubahan |
|---|---|---|---|
| 1 | 1.0 | 2024-12-10 | Versi awal dokumen |

## Tabel Anggota Tim

| No | Nama | Peran |
|---|---|---|
| 1 | Tatin Supriatin, S.Kom. | Proofreader |
| 2 | Ir. Moh. Arham Rahim, S.Kom. | Content Writer |
| 3 | Nael Amany, S.Kom. | Graphic Designer |
| 4 | Muhammad Adi Agum, S.Kom. | Layout Editor |

## CATATAN

*Sebelum melanjutkan ke tahap ini, sangat disarankan untuk melakukan backup guna menghindari hal-hal yang tidak diinginkan.*

## DESKRIPSI

***Data Exposure*** merujuk pada keadaan di mana informasi sensitif atau pribadi dapat diakses oleh pihak yang tidak berwenang. *Data Exposure* terjadi ketika data pengguna yang sensitif (seperti nama pengguna, email, atau informasi lainnya) dapat diakses tanpa perlindungan yang cukup, atau oleh pihak yang tidak seharusnya melihatnya. Berikut adalah beberapa contoh metode atau teknologi yang dapat menjadi sumber *Data Exposure*, diantaranya sebagai berikut:

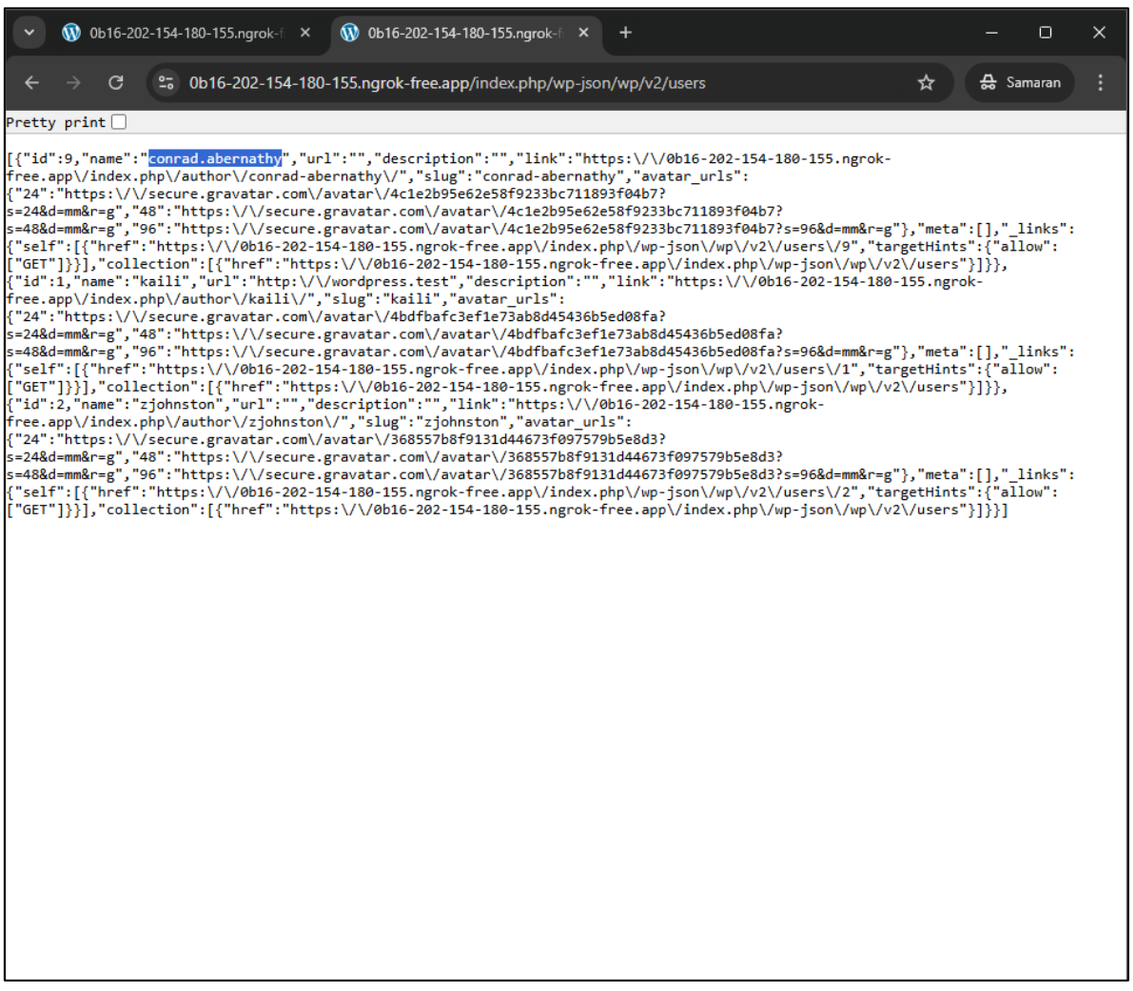
## PROOF OF CONCEPT

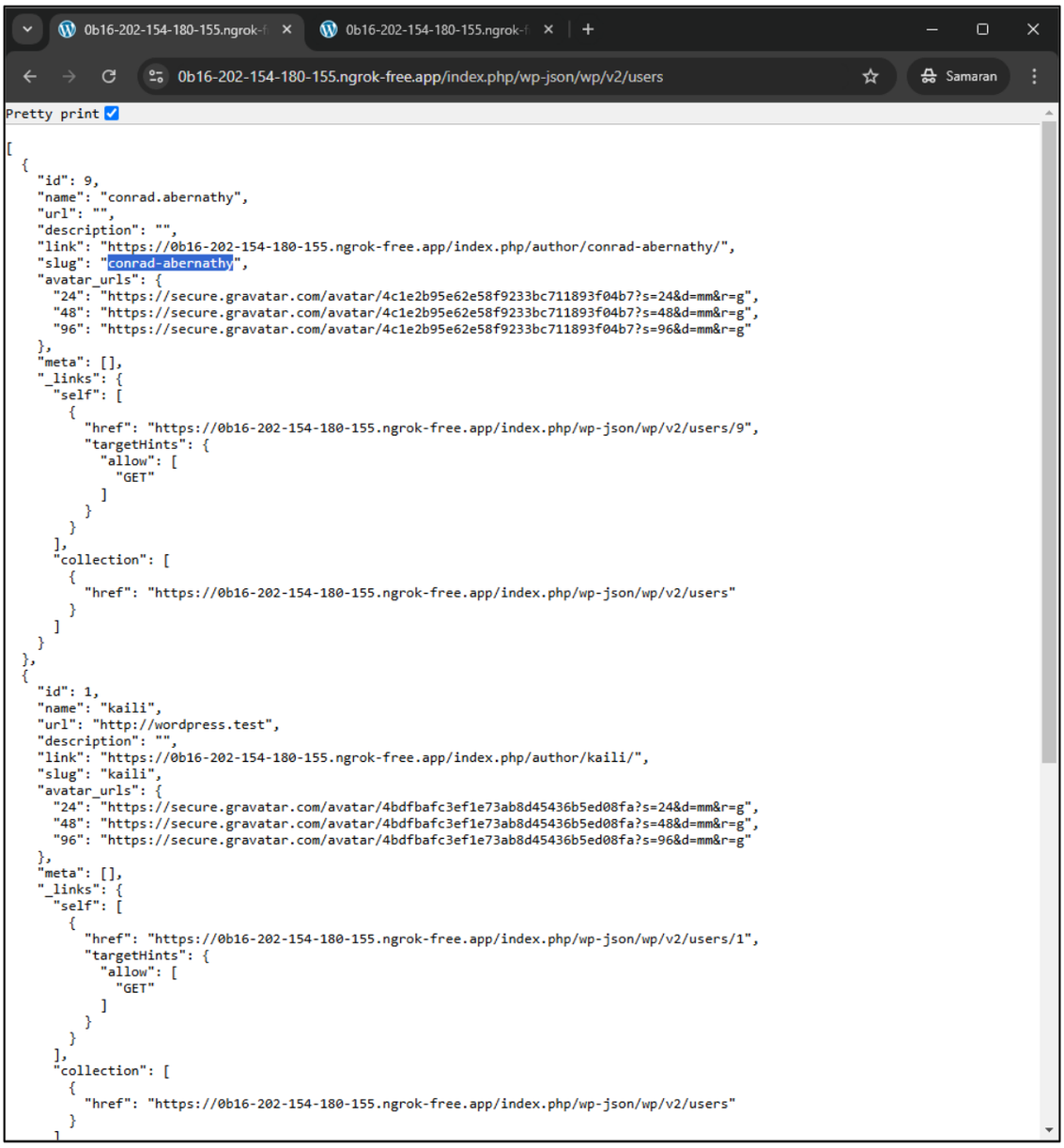
- **WORDPRESS JSON API**

  Akses URL utama *web wordpress* dan tambahkan akses ke sub direktori **/wp-json/wp/v2/users**. Contohnya seperti berikut

  https://url-web-profile-anda.com/index.php/wp-json/wp/v2/users

  https://url-web-profile-anda.com/wp-json/wp/v2/users





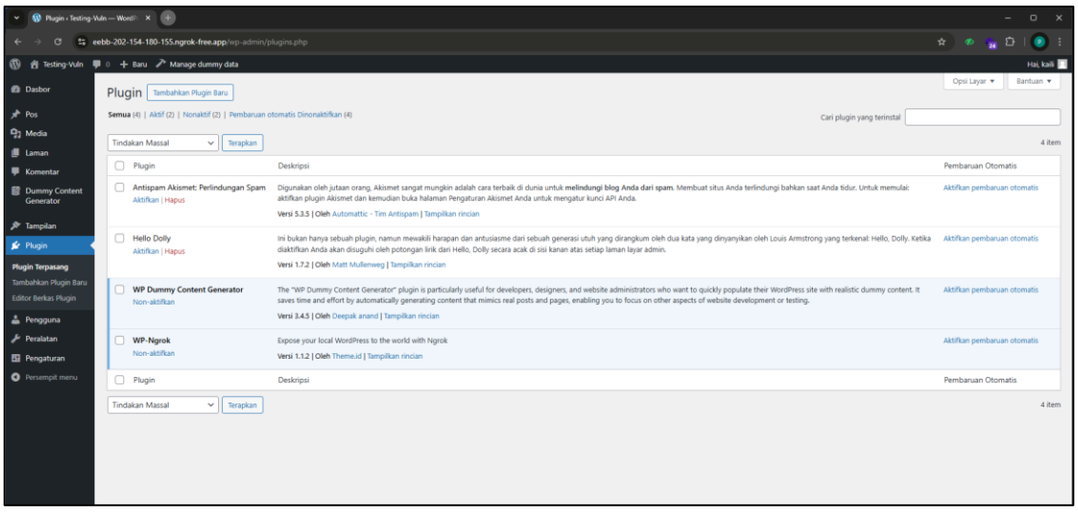


```
[
  {
    "id": 9,
    "name": "conrad.abernathy",
    "url": "",
    "description": "",
    "link": "https://0b16-202-154-180-155.ngrok-free.app/index.php/author/conrad-abernathy/",
    "slug": "conrad-abernathy",
    "avatar_urls": {
      "24": "https://secure.gravatar.com/avatar/4c1e2b95e62e58f9233bc711893f04b7?s=24&d=mm&r=g",
      "48": "https://secure.gravatar.com/avatar/4c1e2b95e62e58f9233bc711893f04b7?s=48&d=mm&r=g",
      "96": "https://secure.gravatar.com/avatar/4c1e2b95e62e58f9233bc711893f04b7?s=96&d=mm&r=g"
    },
    "meta": [],
    "_links": {
      "self": [
        {
          "href": "https://0b16-202-154-180-155.ngrok-free.app/index.php/wp-json/wp/v2/users/9",
          "targetHints": {
            "allow": [
              "GET"
            ]
          }
        }
      ],
      "collection": [
        {
          "href": "https://0b16-202-154-180-155.ngrok-free.app/index.php/wp-json/wp/v2/users"
        }
      ]
    }
  },
  {
    "id": 1,
    "name": "kaili",
    "url": "http://wordpress.test",
    "description": "",
    "link": "https://0b16-202-154-180-155.ngrok-free.app/index.php/author/kaili/",
    "slug": "kaili",
    "avatar_urls": {
      "24": "https://secure.gravatar.com/avatar/4bdfbafc3ef1e73ab8d45436b5ed08fa?s=24&d=mm&r=g",
      "48": "https://secure.gravatar.com/avatar/4bdfbafc3ef1e73ab8d45436b5ed08fa?s=48&d=mm&r=g",
      "96": "https://secure.gravatar.com/avatar/4bdfbafc3ef1e73ab8d45436b5ed08fa?s=96&d=mm&r=g"
    },
    "meta": [],
    "_links": {
      "self": [
        {
          "href": "https://0b16-202-154-180-155.ngrok-free.app/index.php/wp-json/wp/v2/users/1",
          "targetHints": {
            "allow": [
              "GET"
            ]
          }
        }
      ],
      "collection": [
        {
          "href": "https://0b16-202-154-180-155.ngrok-free.app/index.php/wp-json/wp/v2/users"
        }
      ]
```

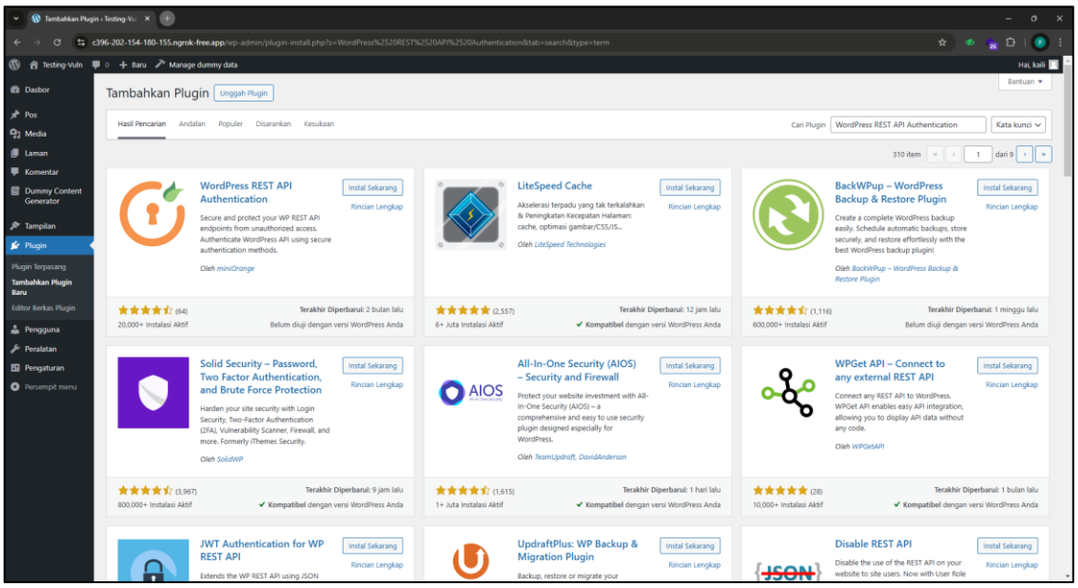

# REMEDIASI

## A. MENGGUNAKAN *WORDPRESS PLUGIN*

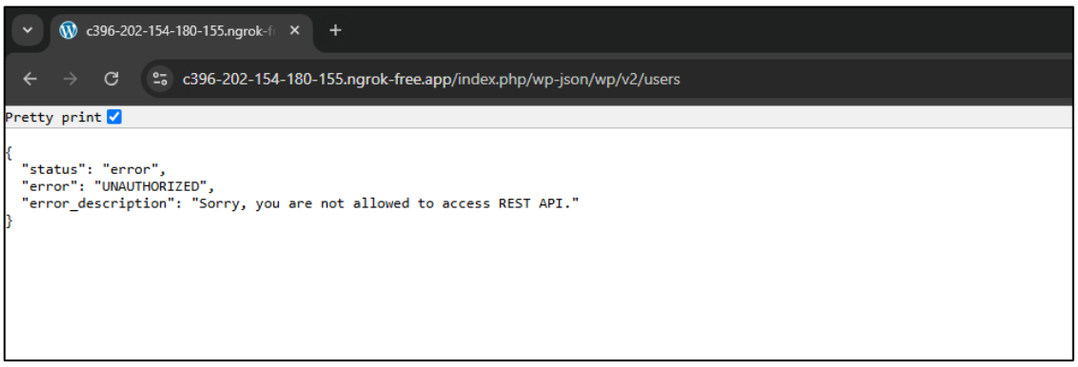
1. *Login* ke *wordpress*, kemudian pergi ke menu *Plugin* dan pilih “Tambah *Plugin* Baru”.



2. Lakukan pencarian “*WordPress* REST API *Authentication*” , kemudian klik "Install Sekarang” dan klik “Aktifkan”.

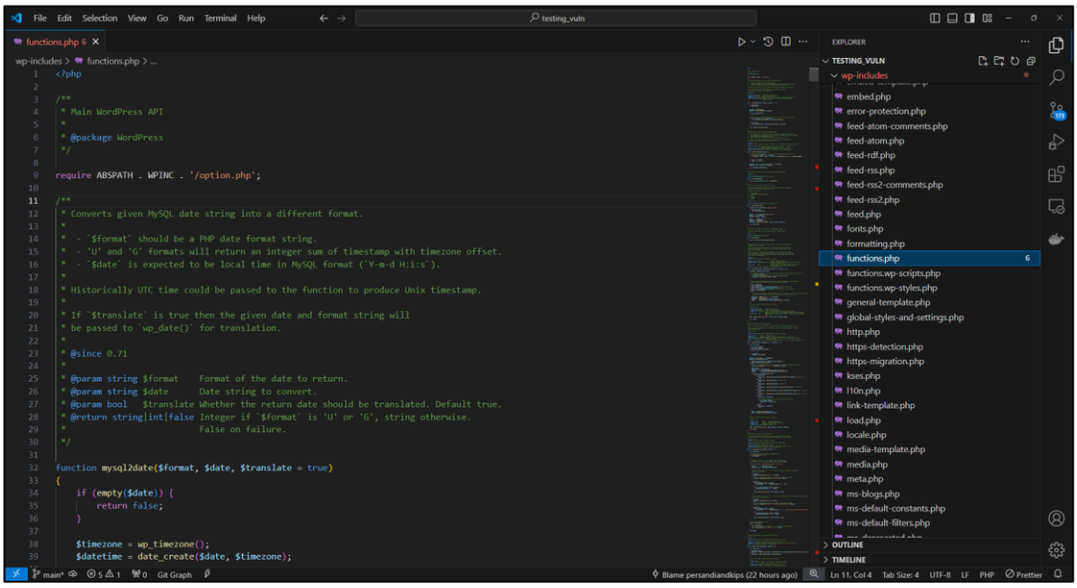



3. Setelah itu, coba akses kembali URL *website* dengan sub direktori wp-json/wp/v2/users atau index.php/wp-json/wp/v2/users dalam kondisi *logout* atau keluar dari sistem. Diharapkan akan muncul *error* seperti yang terlihat pada gambar berikut.




## B. KONFIGURASI SECARA MANUAL LEWAT SCRIPT CODE

1. Buka *file* “function.php” yang berada dalam folder “wp-includes”

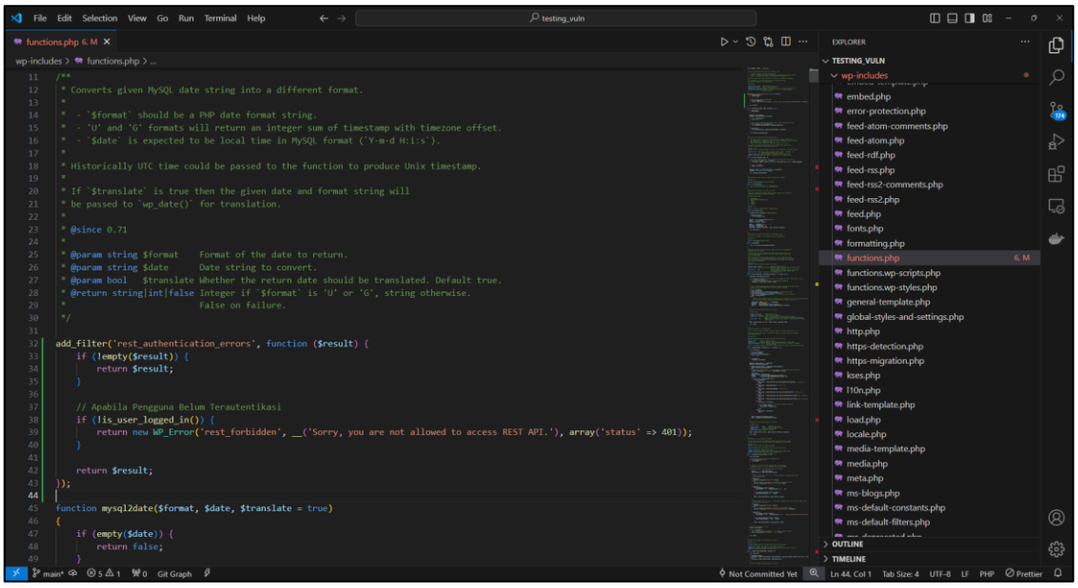


2. Tambahkan *script* berikut pada *file* function.php, sehingga akan terlihat seperti pada gambar berikut.

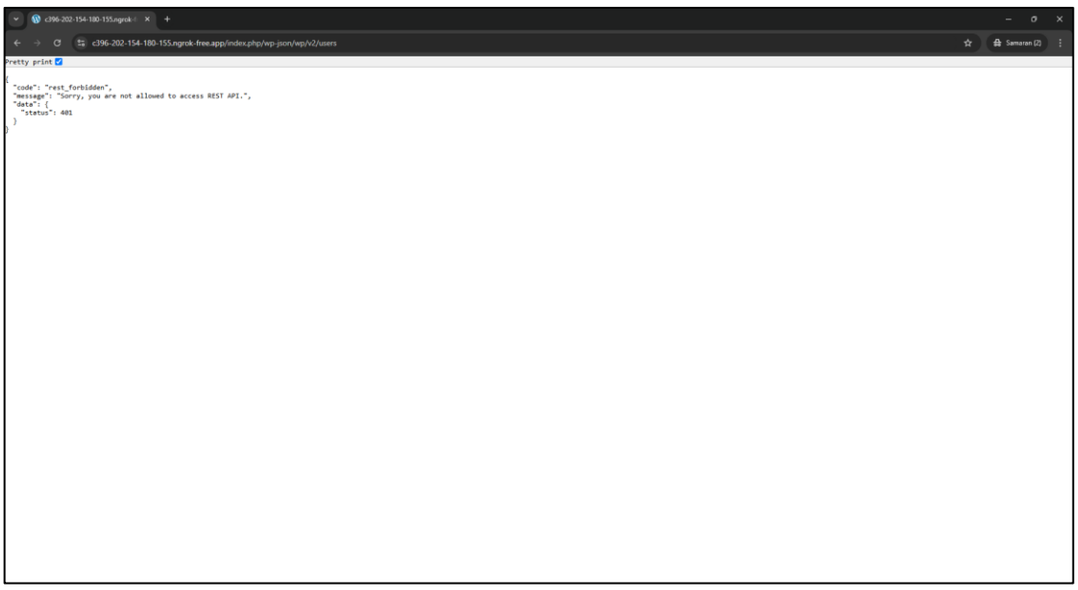
```
add_filter('rest_authentication_errors', function ($result) {
      if (!empty($result)) {
            return $result;
       }

        // Apabila Pengguna Belum Terautentikasi
       if (!is_user_logged_in()) {
             return new WP_Error('rest_forbidden', __('Sorry, you are not
             allowed to access REST API.'), array('status' => 401));
        }

       return $result;
});
```



3. Setelah itu, coba akses kembali URL *website* dengan sub direktori wp-json/wp/v2/users atau index.php/wp-json/wp/v2/users dalam kondisi *logout* atau keluar dari sistem. Diharapkan akan muncul *error* seperti yang terlihat pada gambar berikut.



## REKOMENDASI

1. Setiap akses ke REST API, terutama yang melibatkan data sensitif seperti /wp/v2/users, harus dilindungi dengan autentikasi yang memadai. Anda dapat menggunakan *plugin* seperti "*WordPress* REST API *Authentication*" untuk memastikan bahwa hanya pengguna yang terautentikasi yang dapat mengakses *endpoint* tersebut. Hal ini akan membantu mencegah akses yang tidak sah dan melindungi data sensitif di situs Anda.
2. Jika ada *endpoint* API yang tidak diperlukan, seperti /wp/v2/users, sebaiknya nonaktifkan untuk mengurangi risiko eksposur data sensitif kepada pihak yang tidak berwenang. Anda bisa menonaktifkan *endpoint* ini baik menggunakan *plugin* atau dengan menambahkan kode manual di *file* functions.php, sesuai dengan kebutuhan situs Anda.
3. Pastikan semua komunikasi antara klien dan server dilakukan melalui HTTPS. Penggunaan HTTPS akan mengenkripsi data yang ditransfer dan mencegah potensi serangan *Man-in-the-Middle* (MitM), sehingga data yang ditransfer antara server dan pengguna tetap aman.
4. Terapkan kontrol akses berbasis peran pengguna untuk membatasi akses ke data sensitif. Misalnya, hanya pengguna dengan peran administrator yang diperbolehkan mengakses *endpoint* seperti /wp/v2/users, sedangkan pengguna lain yang tidak memiliki hak akses yang sesuai akan diblokir.
5. Pemantauan akses API secara rutin sangat penting untuk mendeteksi adanya percakapan mencurigakan atau upaya akses yang tidak sah. Anda dapat menggunakan alat pemantauan keamanan seperti **Wordfence** atau **Sucuri** untuk membantu mendeteksi dan mencegah potensi ancaman terhadap situs Anda.
6. Pertimbangkan untuk menggunakan autentikasi berbasis *token*, seperti **JWT (JSON Web Tokens)**, untuk setiap permintaan API. Dengan menggunakan *token*, Anda dapat mengurangi ketergantungan pada sesi *login* standar dan memperkuat kontrol akses API.
7. Selalu lakukan pembaruan rutin pada *WordPress* dan *plugin* yang digunakan. Pembaruan ini sering kali mencakup perbaikan keamanan yang menutup celah yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mengeksploitasi API atau bagian lain dari situs Anda.
8. Gunakan *firewall* aplikasi web (WAF) untuk melindungi situs dari serangan API yang dapat mengeksploitasi celah keamanan. Layanan seperti **Cloudflare** atau *plugin* **Wordfence** dapat membantu menghalau serangan sebelum mencapai server, menjaga situs Anda tetap aman dari potensi ancaman.