Nama : Rifko Satrio Rahmadani

Email : ikosatriorahmadani@gmail.com

Pekerjaan : Mahasiswa

Nama Instansi/Sekolah : Politeknik Negeri Bandung

Challenge Keamanan Aplikasi:

Laporan Hasil Analisa dan Langkah-Langkah Traffic pcap Menggunakan WireShark untuk Menemukan "Username" dan "Password" dari Awal sampai Akhir

I. Pendahuluan

Tugas ini bertujuan untuk menganalisis file pcap dengan Wireshark guna menemukan username dan password yang dikirimkan melalui jaringan. Analisis dilakukan menggunakan fitur-fitur dasar Wireshark seperti filter HTTP dan pemeriksaan isi paket POST untuk melihat bagaimana kredensial dapat terbaca secara plaintext jika tidak melalui protokol yang aman.

II. File & Tools yang digunakan

- Laptop dengan sistem operasi Windows
- Wireshark
- File lalulintaas.pcapng

III. Langkah-Langkah Analisis & Fitur Wireshark

Berikut adalah langkah-langkah analisis file pcap menggunakan Wireshark beserta fitur yang digunakan untuk menemukan username dan password:

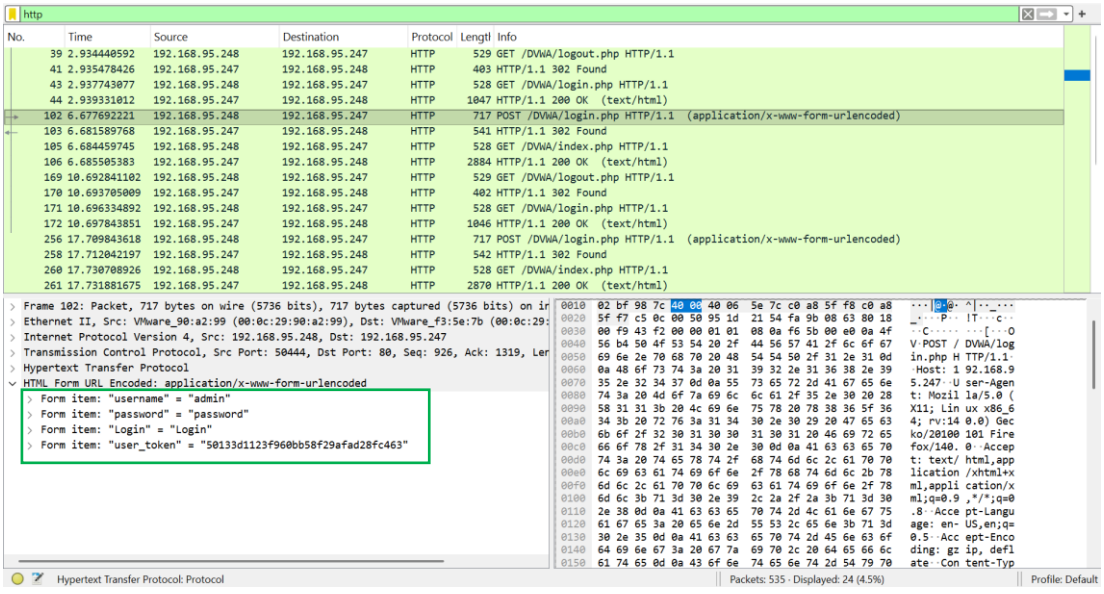
1. Membuka file pcap
   Fitur: File lalulintaas.pcapng → Open pilih → lalulintaas.pcapng
   Saya membuka file *lalulintaas.pcapng* ke dalam Wireshark untuk melihat seluruh traffic jaringan yang terekam.
2. Menggunakan Display Filter "http"
   Fitur: Display Filter Bar
   Filter yang digunakan: `http`
   Saya menggunakan filter "http" untuk menampilkan paket yang memakai protokol HTTP. Indikasinya, setelah filter diterapkan seluruh paket yang muncul memiliki protokol HTTP pada kolom Protocol.
3. Mencari paket POST secara manual
   Saya memeriksa kolom Info untuk menemukan paket dengan metode: `POST /DVWA/login.php HTTP/1.1`

Indikasi paket login:Metode *POST*, Destination menuju halaman login, dan Content-Type: *application/x-www-form-urlencoded*
Paket ini membawa form data berisi username dan password.

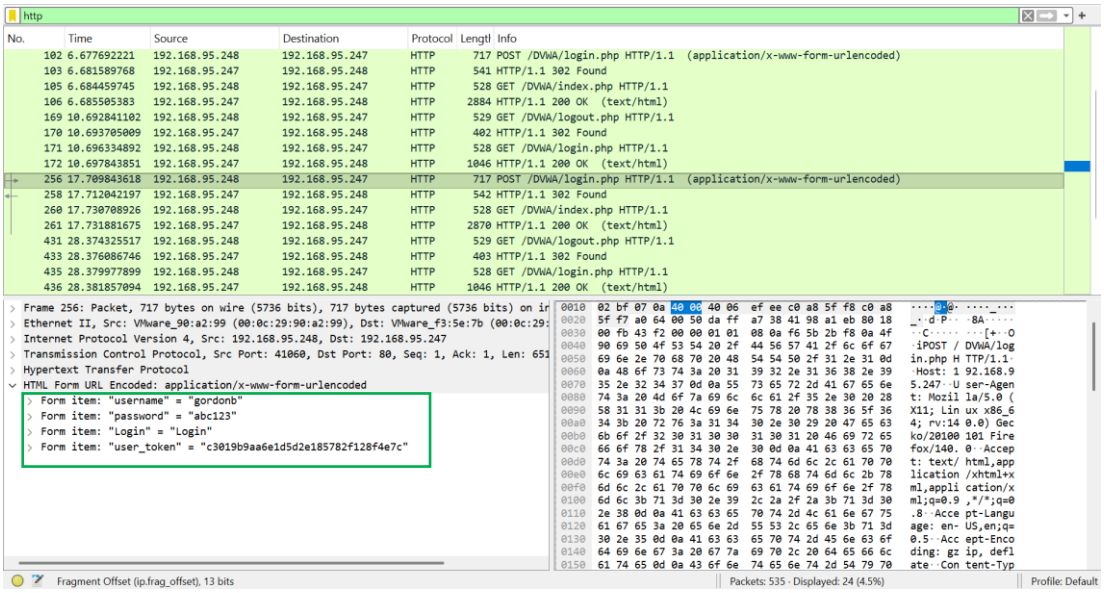
4. Melihat isi Form Data pada paket POST
   Fitur: Packet Details → HTML Form URL Encoded
   Saya mengklik paket *POST* lalu membuka panel *Packet Details*. Setelah itu, saya mengekspand bagian *HTML Form URL Encoded*
   Indikasi data kredensial:
   - Ada field *username =.....*
   - Ada field *password =.....*
   - Formatnya plaintext (tidak terenkripsi)
5. Memvalidasi menggunakan Follow TCP Stream
   Fitur: Right-click → Follow → TCP Stream
   Menampilkan seluruh isi komunikasi HTTP dalam satu tampilan untuk memastikan kredensial benar dikirimkan.

IV. Hasil Laporan

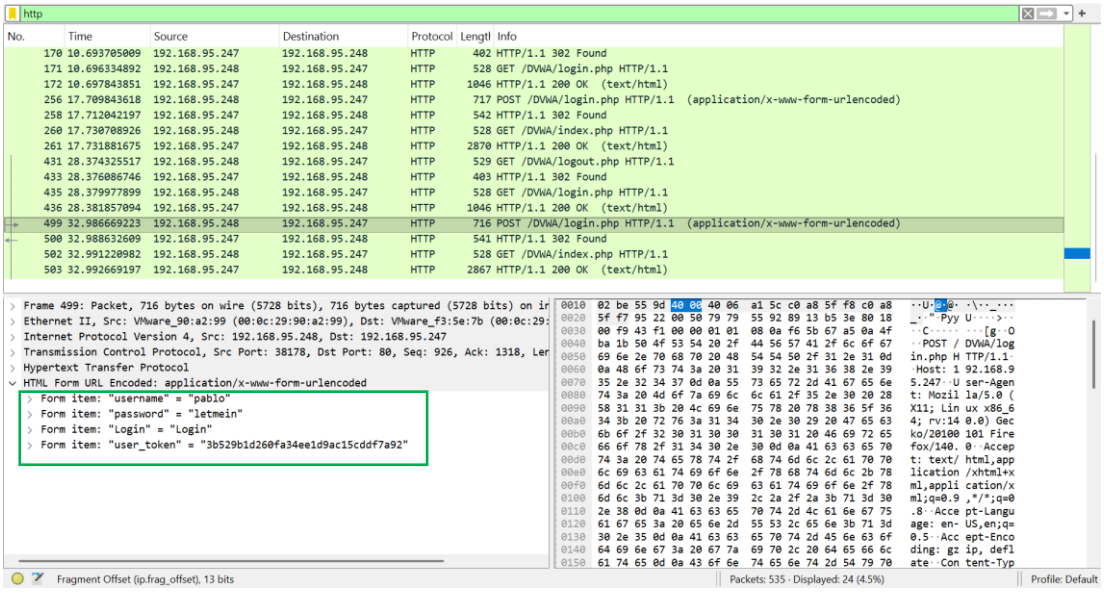
- No. Paket 102
  Kredensial:
  `username=admin&password=password&Login=Login&user_token=50133d1123f960bb58f29afad28fc463`



- No. Paket 256
  Kredensial:
  `username=gordonb&password=abc123&Login=Login&user_token=c3019b9aa6e1d5d2e185782f128f4e7c`



- No. Paket 499
  Kredensial:
  `username=pablo&password=letmein&Login=Login&user_token=3b529b1d260fa34ee1d9ac15cddf7a92`



V. Kesimpulan

Dari analisis file pcap menggunakan Wireshark, saya berhasil menemukan username dan password yang terkirim melalui paket HTTP POST. 3 Kredensial dapat terlihat jelas karena data dikirimkan dalam bentuk plaintext tanpa enkripsi. Hal ini menunjukkan bahwa protokol HTTP tidak aman untuk mengirimkan informasi sensitif dan seharusnya diganti dengan protokol yang terenkripsi seperti HTTPS.