

Nama : Rifko Satrio Rahmadani

Email : [ikosatriorahmadani@gmail.com](mailto: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**

```

http
No. Time Source Destination Protocol Length Info
39 2.934440592 192.168.95.248 192.168.95.247 HTTP 529 GET /DVWA/logout.php HTTP/1.1
41 2.935478426 192.168.95.247 192.168.95.248 HTTP 403 HTTP/1.1 302 Found
43 2.937743077 192.168.95.248 192.168.95.247 HTTP 528 GET /DVWA/login.php HTTP/1.1
44 2.939331812 192.168.95.247 192.168.95.248 HTTP 1047 HTTP/1.1 200 OK (text/html)
102 6.677692221 192.168.95.248 192.168.95.247 HTTP 717 POST /DVWA/login.php HTTP/1.1 (application/x-www-form-urlencoded)
103 6.681589768 192.168.95.247 192.168.95.248 HTTP 541 HTTP/1.1 302 Found
105 6.684459745 192.168.95.248 HTTP 528 GET /DVWA/Index.php HTTP/1.1
106 6.685505383 192.168.95.247 192.168.95.248 HTTP 2884 HTTP/1.1 200 OK (text/html)
109 10.692841102 192.168.95.248 192.168.95.247 HTTP 529 GET /DVWA/logout.php HTTP/1.1
178 10.693765089 192.168.95.247 192.168.95.248 HTTP 402 HTTP/1.1 302 Found
171 10.696334892 192.168.95.248 192.168.95.247 HTTP 528 GET /DVWA/login.php HTTP/1.1
172 10.697843851 192.168.95.247 192.168.95.248 HTTP 1046 HTTP/1.1 200 OK (text/html)
256 17.709843618 192.168.95.248 192.168.95.247 HTTP 717 POST /DVWA/login.php HTTP/1.1 (application/x-www-form-urlencoded)
258 17.712042197 192.168.95.247 192.168.95.248 HTTP 542 HTTP/1.1 302 Found
266 17.730708926 192.168.95.248 192.168.95.247 HTTP 528 GET /DVWA/Index.php HTTP/1.1
261 17.731881675 192.168.95.247 192.168.95.248 HTTP 2870 HTTP/1.1 200 OK (text/html)

> Frame 102: Packet, 717 bytes on wire (5736 bits), 717 bytes captured (5736 bits) on interface
> Ethernet II, Src: VMware_90:a2:99 (00:0c:29:90:a2:99), Dst: VMware_f3:5e:7b (00:0c:29:90:a2:99)
> Internet Protocol Version 4, Src: 192.168.95.248, Dst: 192.168.95.247
> Transmission Control Protocol, Src Port: 58444, Dst Port: 80, Seq: 926, Ack: 1319, Len: 717
> Hypertext Transfer Protocol
> HTML Form URL Encoded: application/x-www-form-urlencoded
> Form item: "username" = "admin"
> Form item: "password" = "password"
> Form item: "Login" = "Login"
> Form item: "user_token" = "50133d1123f960bb58f29afad28fc463"

0018 02 d9 98 7c 40 00 40 06 5e 7c c8 a8 5f f8 c8 a8 ... |...|...|...|...
0020 5f f7 c5 0c 00 58 95 1d 21 54 fa 9b 08 63 80 18 ... |...|...|...|...
0030 00 f9 43 f2 00 00 01 01 08 0a f6 5b 00 0a 4f ... |...|...|...|...
0040 5b 04 50 4f 53 54 20 2f 44 56 57 41 2f 6c 6f 67 V-POST / DVWA/log
0050 69 6e 2e 70 68 70 20 48 54 54 50 2f 31 2e 31 ed in.php H TTP/1.1
0060 00 48 6f 73 74 3a 20 31 39 32 2e 31 36 38 20 39 Host: 192.168.9
0070 35 2e 32 34 37 0d 0a 55 73 65 72 2d 41 67 65 6e 5.247-U ser-Agen
0080 74 3a 20 44 6f 7a 69 6c 62 61 2f 35 2e 30 20 28 t: Mozilla/5.0 (
0090 5d 31 31 30 28 4c 69 6e 75 78 28 38 36 5f 36 36 X-Forwarded-For: 192.168.9.6
00a0 34 34 34 34 34 34 34 34 34 34 34 34 34 34 34 34 4: ru/14.0.4.6c
00b0 6b 6f 2f 32 32 32 32 32 32 32 32 32 32 32 32 32 ko/20109.107.Fire
00c0 66 6f 78 2f 31 34 30 2e 30 0d 0a 41 63 63 65 70 fox/149.0. Accep
00d0 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 78 t: text/html.app
00e0 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 location:/html<x
00f0 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 m_appli_cation/x
0100 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2b 3b 71 3d 30 m1:qz@0.9 .*/:qz@0
0110 2c 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 .8 - Acc pt-Langu
0120 61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d age: en-US,en;q=
0130 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 0.5 - Acc ept-Enc
0140 64 69 66 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c ding: gz ip, defl
0150 61 74 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 ate -Content-Type

```

- No. Paket 256

Kredensial:

**username=gordonb&password=abc123&Login=Login&user\_token=c3019b9aa6e1d5d2e185782f128f4e7c**

No.	Time	Source	Destination	Protocol	Length	Info
102	6.677692221	192.168.95.248	192.168.95.247	HTTP	717	POST /DVWA/login.php HTTP/1.1 (application/x-www-form-urlencoded)
103	6.681589768	192.168.95.247	192.168.95.248	HTTP	541	HTTP/1.1 302 Found
105	6.684459745	192.168.95.248	192.168.95.247	HTTP	528	GET /DVWA/index.php HTTP/1.1
106	6.6856585383	192.168.95.247	192.168.95.248	HTTP	2884	HTTP/1.1 200 OK (text/html)
109	10.692841182	192.168.95.248	192.168.95.247	HTTP	529	GET /DVWA/logout.php HTTP/1.1
170	10.693705008	192.168.95.247	192.168.95.248	HTTP	402	HTTP/1.1 302 Found
171	10.696334892	192.168.95.248	192.168.95.247	HTTP	528	GET /DVWA/login.php HTTP/1.1
172	10.697843851	192.168.95.247	192.168.95.248	HTTP	1046	HTTP/1.1 200 OK (text/html)
256	17.798845618	192.168.95.248	192.168.95.247	HTTP	717	POST /DVWA/login.php HTTP/1.1 (application/x-www-form-urlencoded)
258	17.712042197	192.168.95.247	192.168.95.248	HTTP	542	HTTP/1.1 302 Found
260	17.738708926	192.168.95.248	192.168.95.247	HTTP	528	GET /DVWA/index.php HTTP/1.1
261	17.731881675	192.168.95.247	192.168.95.248	HTTP	2876	HTTP/1.1 200 OK (text/html)
431	28.374325517	192.168.95.248	192.168.95.247	HTTP	529	GET /DVWA/logout.php HTTP/1.1
433	28.376866744	192.168.95.247	192.168.95.248	HTTP	403	HTTP/1.1 302 Found
435	28.379977899	192.168.95.248	192.168.95.247	HTTP	528	GET /DVWA/login.php HTTP/1.1
436	28.381857094	192.168.95.247	192.168.95.248	HTTP	1048	HTTP/1.1 200 OK (text/html)

## - 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.