

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

The screenshot shows the Wireshark interface with packet 102 selected. The 'Packet Details' pane on the left shows the 'HTML Form URL Encoded' section expanded, displaying the following fields:

- > Form item: "username" = "admin"
- > Form item: "password" = "password"
- > Form item: "Login" = "Login"
- > Form item: "user_token" = "50133d1123f960bb58f29afad28fc463"

The 'Packet Bytes' pane on the right shows the raw data of the packet, which is a POST request to /DWa/login.php.

- 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	6.685505383	192.168.95.247	192.168.95.248	HTTP	2884	HTTP/1.1 200 OK (text/html)
169	10.692841102	192.168.95.248	192.168.95.247	HTTP	529	GET /DVWA/logout.php HTTP/1.1
170	10.693705009	192.168.95.247	192.168.95.248	HTTP	482	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	17.708843618	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	17.730708926	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)
431	28.374325517	192.168.95.248	192.168.95.247	HTTP	529	GET /DVWA/logout.php HTTP/1.1
433	28.376086746	192.168.95.247	192.168.95.248	HTTP	483	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	1046	HTTP/1.1 200 OK (text/html)

> Frame 256: Packet, 717 bytes on wire (5736 bits), 717 bytes captured (5736 bits) on interface 0	0010 02 bf 07 0a 80 0c 40 06 ef ee c0 a8 5f f8 c0 a8 ..U..e.....
> Ethernet II, Src: VMware_08:00:27:9d:12:19, Dst: VMware_f3:5e:7b:00:0c:29:10	0020 5f f7 a0 64 00 50 da ff a7 38 41 98 a1 eb 80 18 ...dP...8A....
> Internet Protocol Version 4, Src: 192.168.95.248, Dst: 192.168.95.247	0030 00 fb 43 f2 00 00 01 01 08 0a f6 5b 2f f8 0a 4f ...C.....[+...O
> Transmission Control Protocol, Src Port: 80, Seq: 1, Ack: 1, Len: 651	0040 90 69 50 4f 53 54 20 2f 44 56 57 41 2f 6c 6f 67 ...iPOST / DVWA/log
> Hypertext Transfer Protocol	0050 69 6e 2e 70 68 70 20 48 54 54 50 2f 31 2e 31 8d ...in.php H TTP/1.1
> HTML Form URL Encoded: application/x-www-form-urlencoded	0060 0a 48 6f 73 74 3a 20 31 39 32 2e 31 36 38 2e 39 ...Host: 1 92.168.9
> Form item: "username" = "gordonb"	0070 35 2e 32 34 37 0d 0a 55 73 65 72 2d 41 67 65 6e ...5.247: U ser-Agen
> Form item: "password" = "abc123"	0080 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 ...t: Mozill la/5.0 (
> Form item: "Login" = "Login"	0090 58 31 31 3b 20 4c 69 6e 75 78 20 78 38 36 5f 36 ...Xll; Lin ux x86.6
> Form item: "user_token" = "c3019b9aa6e1d5d2e185782f128f4e7c"	00a0 34 3b 20 72 76 3a 31 34 30 2e 30 29 20 47 65 63 ...4; rv:14 0.0) Gec
	00b0 66 6f 78 2f 31 34 30 2e 30 6d 0a 41 63 63 65 70 ...ko/20100 101 Fire
	00c0 66 6f 78 2f 31 34 30 2e 30 6d 0a 41 63 63 65 70 ...fox/140. 0 Accep
	00d0 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 ...t: text/ html,app
	00e0 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 ...lication /xhtml+x
	00f0 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 ...ml,appli cation/x
	0100 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b 71 3d 30 ...ml;q=0.9 ,*/;q=0
	0110 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 ...8 Acce 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-Enco
	0140 64 69 6e 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 Con tent-Typ

- No. Paket 499
- Kredensial:

username=pablo&password=letmein&Login=Login&user_token=3b529b1d260fa34ee1d9ac15cddf7a92

No.	Time	Source	Destination	Protocol	Length	Info
170	10.693705009	192.168.95.247	192.168.95.248	HTTP	482	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	17.708843618	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	17.730708926	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)
431	28.374325517	192.168.95.248	192.168.95.247	HTTP	529	GET /DVWA/logout.php HTTP/1.1
433	28.376086746	192.168.95.247	192.168.95.248	HTTP	483	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	1046	HTTP/1.1 200 OK (text/html)
499	32.986669223	192.168.95.248	192.168.95.247	HTTP	716	POST /DVWA/login.php HTTP/1.1 (application/x-www-form-urlencoded)
500	32.988632609	192.168.95.247	192.168.95.248	HTTP	541	HTTP/1.1 302 Found
502	32.991220982	192.168.95.248	192.168.95.247	HTTP	528	GET /DVWA/index.php HTTP/1.1
503	32.992669197	192.168.95.247	192.168.95.248	HTTP	2867	HTTP/1.1 200 OK (text/html)

> Frame 499: Packet, 716 bytes on wire (5728 bits), 716 bytes captured (5728 bits) on interface 0	0010 02 be 55 9d 80 0c 40 06 a1 5c c0 a8 5f f8 c0 a8 ..U..e.....
> Ethernet II, Src: VMware_08:00:27:9d:12:19, Dst: VMware_f3:5e:7b:00:0c:29:10	0020 5f f7 95 22 00 50 79 79 55 92 89 13 b5 3e 80 18 ...Py U...>..
> Internet Protocol Version 4, Src: 192.168.95.248, Dst: 192.168.95.247	0030 00 f9 43 f1 00 00 01 01 08 0a f6 5b 67 a5 0a 4f ...C.....[g...O
> Transmission Control Protocol, Src Port: 80, Seq: 926, Ack: 1318, Len: 651	0040 ba 1b 50 4f 53 54 20 2f 44 56 57 41 2f 6c 6f 67 ...iPOST / DVWA/log
> Hypertext Transfer Protocol	0050 69 6e 2e 70 68 70 20 48 54 54 50 2f 31 2e 31 8d ...in.php H TTP/1.1
> HTML Form URL Encoded: application/x-www-form-urlencoded	0060 0a 48 6f 73 74 3a 20 31 39 32 2e 31 36 38 2e 39 ...Host: 1 92.168.9
> Form item: "username" = "pablo"	0070 35 2e 32 34 37 0d 0a 55 73 65 72 2d 41 67 65 6e ...5.247: U ser-Agen
> Form item: "password" = "letmein"	0080 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 ...t: Mozill la/5.0 (
> Form item: "Login" = "Login"	0090 58 31 31 3b 20 4c 69 6e 75 78 20 78 38 36 5f 36 ...Xll; Lin ux x86.6
> Form item: "user_token" = "3b529b1d260fa34ee1d9ac15cddf7a92"	00a0 34 3b 20 72 76 3a 31 34 30 2e 30 29 20 47 65 63 ...4; rv:14 0.0) Gec
	00b0 66 6f 78 2f 31 34 30 2e 30 6d 0a 41 63 63 65 70 ...ko/20100 101 Fire
	00c0 66 6f 78 2f 31 34 30 2e 30 6d 0a 41 63 63 65 70 ...fox/140. 0 Accep
	00d0 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 ...t: text/ html,app
	00e0 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 ...lication /xhtml+x
	00f0 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 ...ml,appli cation/x
	0100 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b 71 3d 30 ...ml;q=0.9 ,*/;q=0
	0110 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 ...8 Acce 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-Enco
	0140 64 69 6e 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 Con tent-Typ

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.