e-ISSN 2962-6129
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 20 Agustus 2022

Analisis Keamanan Website LEADS UPNVJ Terhadap Serangan SQL Injection & Sniffing Attack

Dimas Perdana Putranto, Jayanta, S.Kom., M.Si., Bayu Hananto, S.Kom., M.Kom.
Informatika / Fakultas Ilmu Komputer
Universitas Pembangunan Nasional Veteran Jakarta
Jl. RS. Fatmawati Raya, Pd. Labu, Depok , Jawa Barat 12450
[1]dimaspp@upnvj.ac.id, [2]jayanta@upnvj.com, [3]bayuhananto@upnvj.ac.id

Abstrak. LEADS UPNVJ adalah sistem yang dirancang untuk keperluan pembelajaran elektronik bagi mahasiswa, yang dapat diakses secara *online* menggunakan *Website*. Pada *website* LEADS UPNVJ terdapat data yang penting dan harus dijaga keamanannya karena terdapat informasi-informasi yang bersifat privasi. Jenis-jenis serangan yang sering digunakan untuk menyerang sebuah website adalah SQL *injection* & *Sniffing Attack*. SQL *injection* adalah sebuah serangan injeksi SQL yang dapat menimbulkan ancaman keamanan serius terhadap sebuah website, yang mana SQL *injection* mengizinkan penyerangnya untuk mendapatkan akses ke *database* sebuah *website* yang dapat menyebabkan kebocoran data yang membuat hilangnya kerahasiaan data terutama untuk informasi yang bersifat sensitif. *Sniffing Attack* adalah penyadapan dan pencurian data dengan cara menangkap dan memonitor lalu lintas paket data jaringan internet. Yang bertujuan untuk memperoleh data dan informasi yang bersifat sensitif. Oleh karena itu melalui penelitian ini, diharapkan dapat diperoleh analisis yang baik untuk mengukur tingkat keamanan dari *website* LEADS UPNVJ. Sehingga jika terdapat kelemahan pada *website* akan dianalisa dan diperoleh solusi untuk menciptakan keamanan *website* yang lebih kuat.

Kata Kunci: LEADS UPNVJ, *website,* serangan, keamanan, SQL *Injection, Sniffing attack, database,* dan paket data.

1 Pendahuluan

Pada saat ini kebutuhan akan suatu *website* menjadi sangat penting, *website* bukan lagi hanya menjadi sarana penyedia informasi, melainkan sudah menjadi media komunikasi, media transaksi, media pembelajaran, dan lain-lain. Karena peran *website* sangat penting dan mencakup banyak aspek, maka banyak terjadi kasus pencurian data, penyadapan, dan lain-lain yang dilakukan oleh *hacker*. untuk itu sistem keamanan pada suatu *website* menjadi hal yang sangat penting untuk menghindari terjadinya hal-hal yang tidak diinginkan yang disebabkan oleh serangan *hacker*.

Serangan yang sering digunakan dan yang berbahaya adalah SQL *injection* & *Sniffing attack*. serangan SQL *injection* adalah teknik yang dapat mengeksploitasi kueri dari *structured query language* (SQL) untuk bisa menembus menuju *back-end* dari *database*, jika sudah menembus *database,* penyerang mendapat keleluasaan dalam mendapatkan informasi sensitif yang terdapat pada database tersebut, seperti *username*, *password*, nama, alamat, nomor telepon, dan lain-lain. Lalu *sniffing attack* adalah ketika *packet* melakukan lalu lintas melalui jaringan *internet*, lalu lintas data tadi dapat dianalisis untuk mendapatkan data dan informasi yang bersifat sensitif. Lalu lintas data tadi bisa ditangkap menggunakan bantuan alat *sniffing*.

LEADS UPNVJ merupakan sistem pembelajaran elektronik berbasis *web* yang dapat diakses kapan saja dan dimana saja. LEADS UPNVJ digunakan oleh seluruh mahasiswa & dosen di UPNVJ. Kegiatan-kegiatan pembelajaran yang bisa dilakukan di LEADS UPNVJ meliputi pemberian materi, pelaksanaan ujian, absensi, penugasan, penilaian, dan lain-lain.

Mengetahui bahwa SQL *injection* & *Sniffing attack* merupakan serangan yang berbahaya dan dapat mengancam privasi dari penggunanya. maka penulis memutuskan untuk mengangkat tema ini dengan mengambil judul "Analisis Keamanan Website LEADS UPNVJ Terhadap Serangan SQL Injection & Sniffing Attack".

2 Landasan Teori

Pada penelitian ini memperlukan teori-teori untuk memperkuat dasar dari penelitian yang dilakukan, berikut merupakan landasan teori yang digunakan pada penelitian ini.

2.1 SQL

SQL (*Structured Query Language*) adalah bahasa *database* komputer yang dirancang untuk mengelola data di dalam sebuah sistem manajemen basis data relasional [3]. SQL merupakan bahasa komputer standar yang dikembangkan oleh IBM, banyak hal yang bisa dilakukan oleh SQL seperti, menambahkan *database* baru, melakukan *update* pada *database* baru, menghapus data pada *database*, dan lain-lain. Walaupun SQL merupakan bahasa yang menjadi standar untuk sistem *database*, tetapi banyak sistem *database* yang mengimplementasikan bahasa SQL versinya sendiri-sendiri seperti, Microsoft SQL Server, MySQL, Microsoft Access, Sybase, dan lain-lain.

2.2 SQL Injection

SQL *Injection* merupakan suatu teknik eksploitasi dengan cara melakukan modifikasi perintah sql pada *form input* suatu aplikasi yang nantinya akan memungkinkan penyerang untuk mengirimkan sintaks atau perintah kepada *database* suatu aplikasi [2].

2.3 Sniffing Attack

Sniffing attack adalah teknik penyadapan melalui proses penangkapan aliran paket data yang melalui jaringan tertentu dengan menggunakan alat *sniffing*. Informasi yang ditangkap bisa berupa informasi yang sensitif seperti *username*, *password*, dan lain-lain.

2.4 Kerentanan

Kerentanan adalah kelemahan suatu sistem yang dieksploitasi oleh penyerang, biasanya dilakukan untuk mendapatkan akses ke beberapa aset. banyaknya keadaan yang secara tidak sengaja menciptakan kelemahan di dalam sistem, mereka dibagi menjadi tiga area : layanan, aplikasi, tindakan yang dilakukan oleh user [4].

2.5 Website

Website merupakan apa yang anda lihat melalui *browser*, sedangkan definisi dari *web* adalah sebuah aplikasi *web*, karena disana kita akan melakukan perintah tertentu dan membantu anda dalam melakukan aktifitas tertentu [6].

2.6 Serangan Siber

Serangan siber (*cyber attack*) adalah serangan dunia maya, baik yang ditujukan untuk menyerang maupun bertahan yang menjadi alasan sebagai penyebab kematian seseorang atau kerusakan suatu objek yang dituju [5].

2.7 Basis Data

Database adalah kumpulan informasi yang disimpan pada komputer dengan cara yang sistematik sehingga dapat diperiksa dengan menggunakan program komputer agar dapat memperoleh informasi [1].

2.8 Web Application Firewall

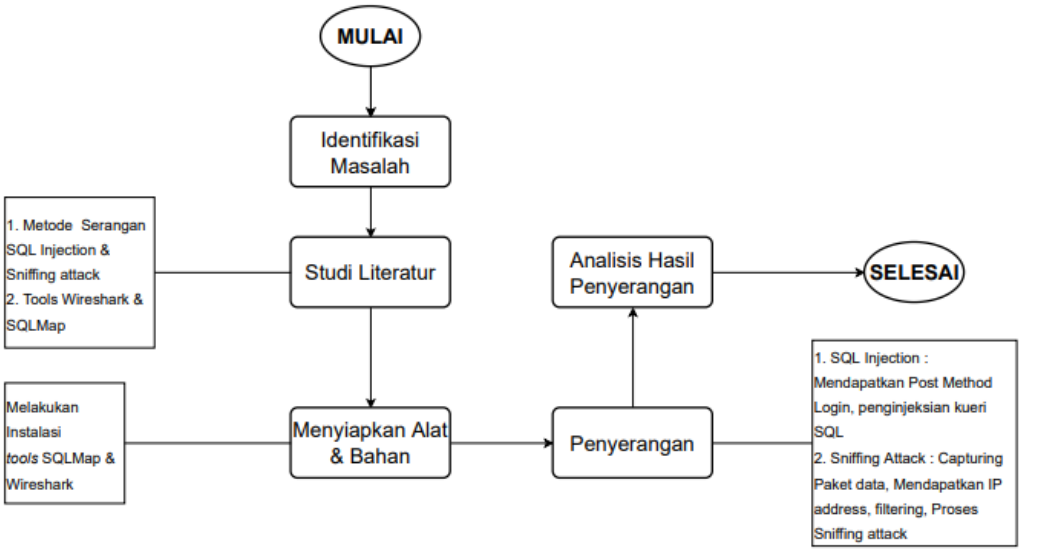
Web Application Firewall (WAF) adalah bentuk lain dari *firewall* yang bertugas mengidentifikasi, menyaring, dan menahan aliran data yang dianggap mencurigakan dari *client* menuju *server* dari suatu *website.* Berikut merupakan gambaran dari cara kerja dari WAF.

2.9 Transport Layer Security

Transport layer security (TLS) merupakan protokol kriptografi yang berfungsi mengamankan komunikasi paket data yang dikirimkan antara *client* dan *server*, sehingga isi dari paket data yang dikirimkan tadi bisa dilindungi privasi dan kerahasiaannya agar terjalin komunikasi yang aman pada jaringan *internet.*

3 Hasil

Pada pengujian ini akan dilakukan sesuai dengan alur penelitian yang sudah dibuat. Berikut merupakan gambar dari alur penelitian yang akan dilakukan.



Gambar 1. Gambar kerangka pikir penelitian

Berikut ini merupakan tahapan-tahapan yang akan dilakukan dalam penelitian ini :

1. Identifikasi Masalah, dalam tahap ini penulis mencoba mencari masalah dan menegaskan masalah yang akan diangkat pada penelitian ini.
2. Studi Literatur, dalam tahap ini penulis mengumpulkan sumber literatur dari mulai buku, jurnal, artikel, dan lain-lain untuk menunjang penelitian ini.
3. Menyiapkan Alat dan bahan, dalam tahap ini penulis menyiapkan alat dan bahan berupa perangkat keras dan perangkat lunak yang akan digunakan untuk membantu penelitian ini.

4. Penyerangan, dalam tahap ini penulis akan mencoba melakukan penyerangan SQL *Injection* dan *Sniffing Attack* untuk serangan SQL *injection* memiliki tahapan seperti berikut, tahapan pertama adalah untuk mendapatkan *POST Method login*, lalu tahap kedua adalah tahap penginjeksian kueri SQL. Untuk *sniffing attack* tahapan dari serangannya adalah seperti berikut, tahapan pertama adalah *Capturing* paket data, lalu tahapan kedua adalah mendapatkan IP *address,* selanjutnya tahapan ketiga adalah *filtering*, dan tahapan terakhir adalah melakukan proses *sniffing attack* pada paket data.
5. Analisis Hasil Penyerangan, dalam tahap ini penulis akan melakukan analisis terhadap hasil dan mengambil kesimpulan dari hasil penyerangan tersebut.

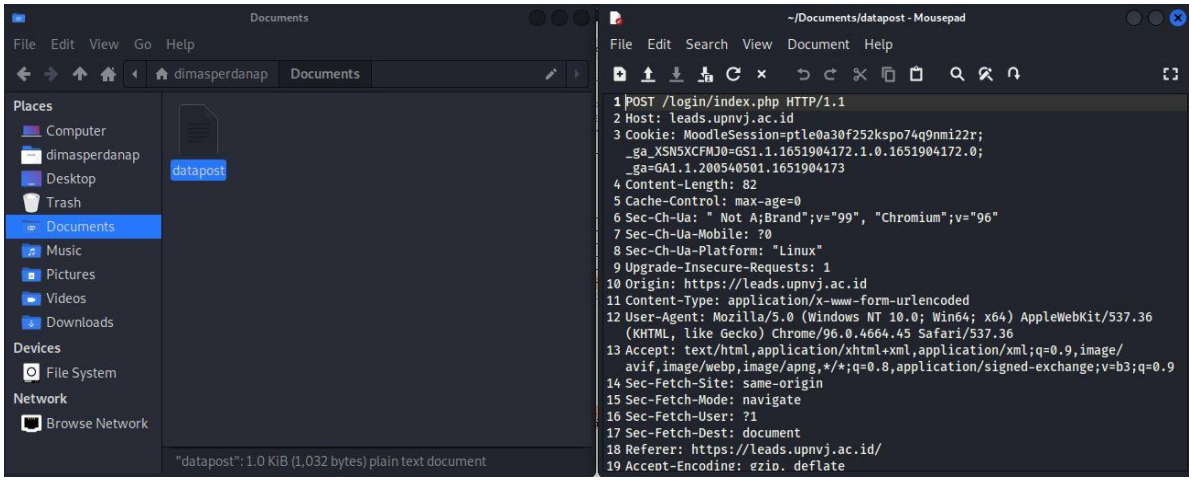
3.1 Serangan SQL *Injection*

SQL *injection* merupakan suatu serangan yang memanfaatkan kerentanan pada suatu lapisan *database* sebuah *website*. Mekanisme dari serangan ini adalah mencoba menginjeksikan perintah-perintah SQL pada *form input* suatu aplikasi sehingga penyerang bisa mengirimkan perintah ke *database website* tersebut, yang pada akhirnya penyerang nanti dapat menguasai *database* pada *website* tersebut. Jika penyerang sudah menguasai *database* maka penyerang bisa mencuri data-data pada *database* yang biasanya bersifat pribadi dan rahasia seperti *username*, *password*, tanggal lahir, dan lain-lain.

Pada penelitian kali ini penulis akan melakukan percobaan serangan SQL *injection* menggunakan *tools* SQLMap dan Burp Suite. Berikut merupakan hasil dari pengujiannya.

A. Mendapatkan POST *Method Login*

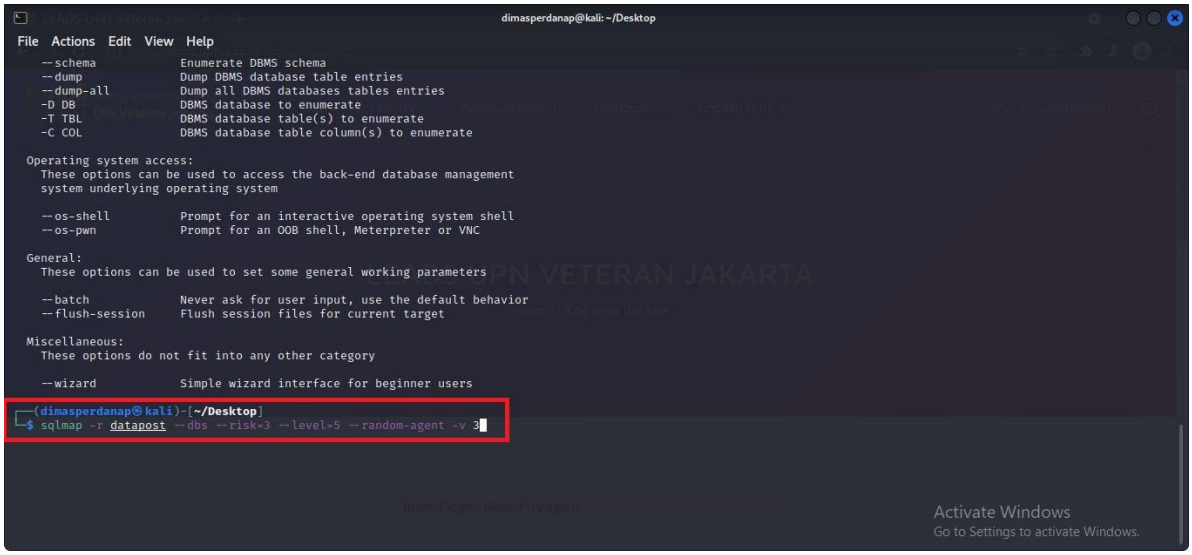
Sebelum melakukan penyerangan kita harus mendapatkan dulu data POST *method login* pada saat kita melakukan penginputan pada *form login website* LEADS UPNVJ. Pengambilan data *POST method login* menggunakan *tools Burp Suite*. Tujuan kita mendapatkan *POST method* tersebut adalah agar nanti *SQLMap* dapat menganalisa *POST method login* yang sudah kita dapatkan tadi lalu selanjutnya *SQLMap* akan mencoba menemukan kerentanan pada *form input website* LEADS UPNVJ dengan cara menginjeksikan perintah-perintah SQL. Berikut adalah hasil dari pengambilan data *POST method login* dengan *tools Burp Suite.*



Gambar. 2 File POST *method login*

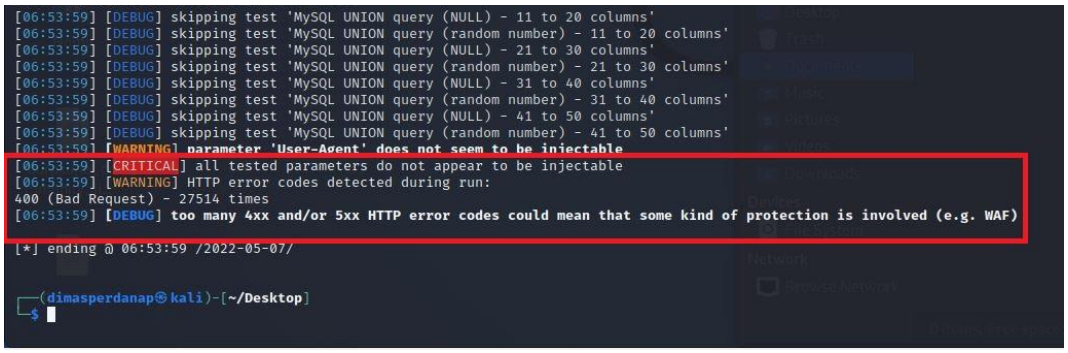
B. Penginjeksian Kueri SQL

Selanjutnya adalah melakukan serangan SQL *injection* menggunakan *tools* SQLMap. Pada tahap ini SQLMap akan melakukan penginjeksian kueri-kueri SQL secara otomatis untuk mencari kerentanan pada layer database dari *website* tersebut. Berikut adalah tampilan dari perintah atau *command* yang digunakan untuk melakukan serangan SQL *injection*.



Gambar. 3 Perintah/*command* yang digunakan pada *tools* SQLMap untuk melakukan serangan SQL *injection*

Setelah melakukan proses penginjeksian kueri SQL maka akan keluar hasil dari serangan yang dilancarkan oleh penyerang. Berikut merupakan hasil dari penyerangan yang sudah dilakukan oleh penyerang.



Gambar. 4 Hasil dari pengujian SQL *injection*

dapat dilihat bahwa SQLMap tidak dapat menemukan kerentanan pada *website* LEADS UPNVJ dan serangan gagal menembus WAF (Web Application Firewall) yang digunakan oleh *website* LEADS UPNVJ.

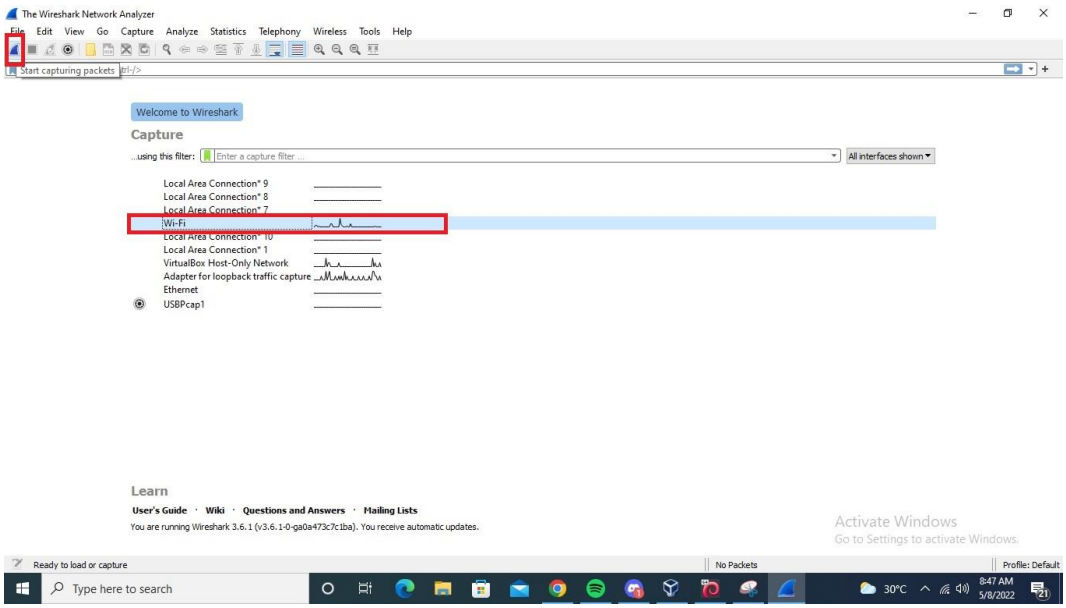
3.2 Serangan S*niffing Attack*

Sniffing attack merupakan suatu skema serangan menggunakan teknik penyadapan aliran paket data melalui jaringan tertentu yang dikirim dari *client* menuju *server* maupun sebaliknya dengan menggunakan bantuan alat *sniffing.* Informasi yang dikirimkan dari client menuju server ataupun sebaliknya bisa berupa informasi yang sensitif dan privat seperti *username, password*, alamat email, dan lain-lain.

Pada penelitian kali ini penulis akan melakukan percobaan serangan *sniffing attack* menggunakan *tools* wireshark. Berikut merupakan hasil dari pengujiannya.

A. Melakukan *Capturing* Paket Data

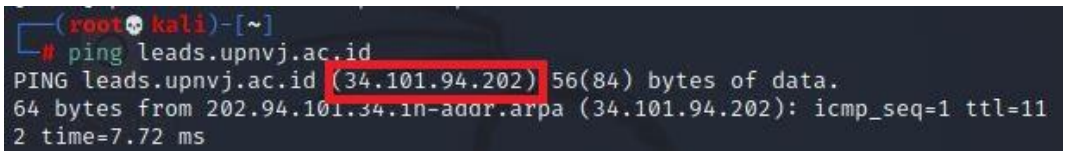
Pertama kita akan menjalankan *tools* Wireshark yang akan membantu kita dalam menyadap aliran paket data yang dikirimkan dari client menuju server maupun sebaliknya, seperti pada gambar berikut.



Gambar. 5 Proses *Capturing* paket data

B. Mendapatkan IP *address*

Selanjutnya adalah mendapatkan alamat IP dari *website* LEADS UPNVJ untuk membantu kita dalam melakukan tahapan selanjutnya yaitu proses *filtering*. Untuk mendapatkan alamat IP address dari website LEADS UPNVJ kita bisa mengetikkan perintah atau *command* pada *terminal* Kali Linux sebagai berikut "ping leads.upnvj.ac.id". Seperti pada gambar berikut.

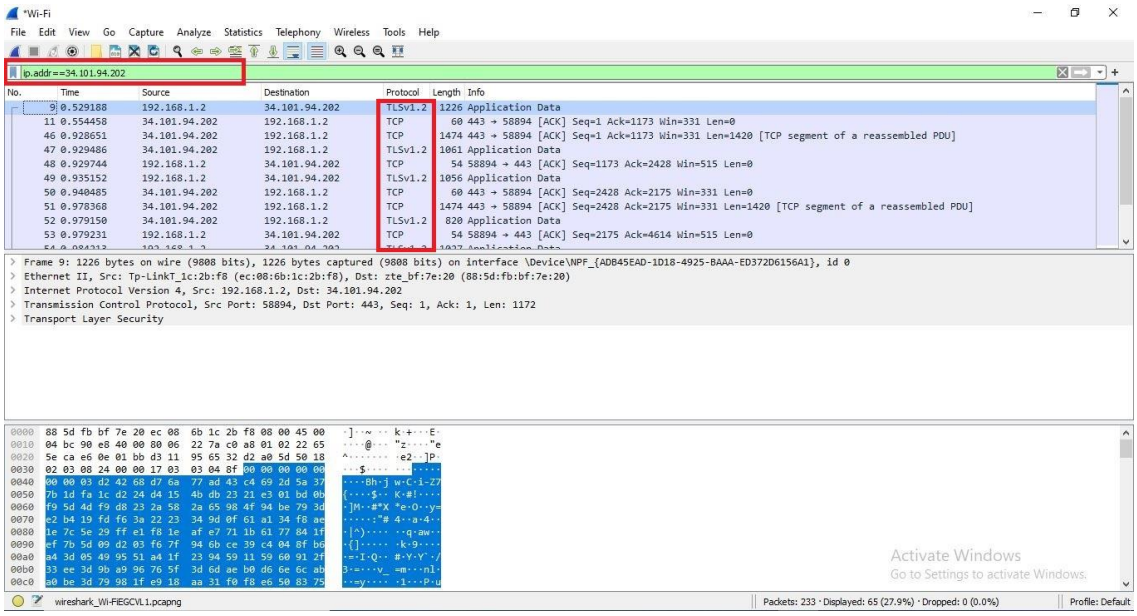


Gambar. 6 Proses mendapatkan alamat IP address website LEADS UPNVJ

Setelah itu maka akan muncul alamat IP dari *website* LEADS UPNVJ yaitu 34.101.94.202.

C. *Filtering*

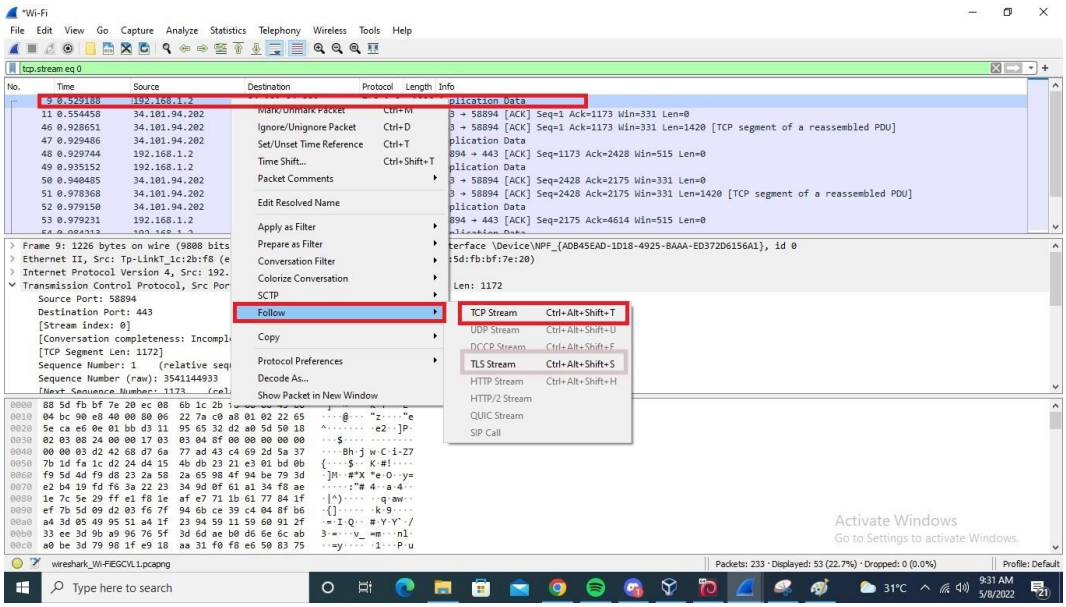
Selanjutnya penulis melakukan proses *filter* yang berfungsi untuk menyaring aliran paket data yang dikirimkan oleh *website* LEADS UPNVJ untuk memudahkan kita dalam menganalisis aliran paket data pada alamat IP yang dituju yaitu alamat IP website LEADS UPNVJ dengan cara menggunakan perintah atau *command* "ip.addr==34.101.94.202".



Gambar. 7 Proses filter paket data dari website LEADS UPNVJ

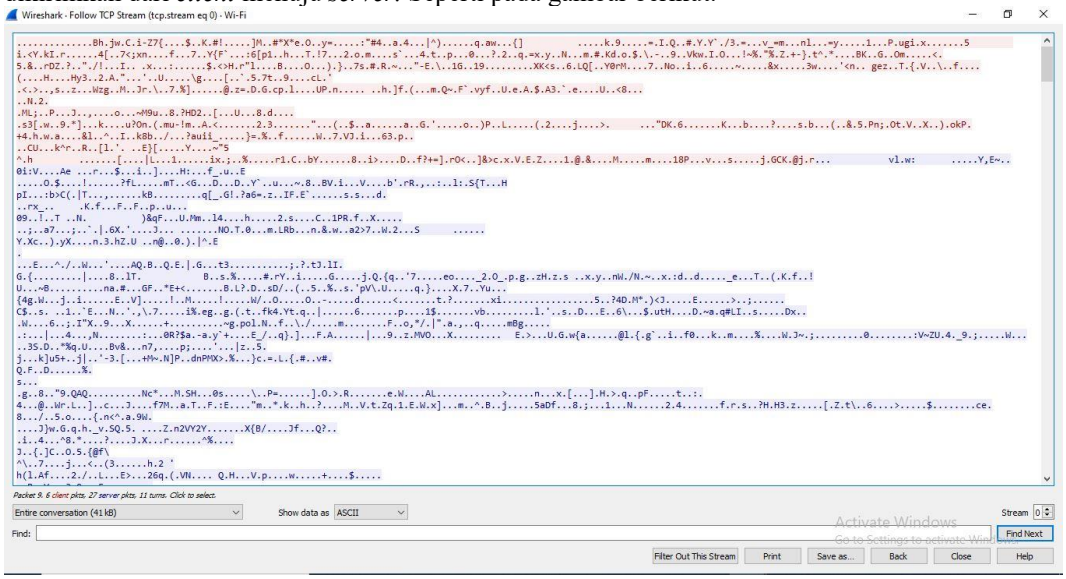
D. Proses *Sniffing Attack*

Selanjutnya penulis akan melakukan proses *sniffing attack* pada aliran paket data yang dikirimkan dari komputer *client* menuju *server* pada saat melakukan *login* pada *website* LEADS UPNVJ yang dimana pada paket data tersebut terdapat informasi mengenai *username* dan *password* yang dikirimkan dari client menuju server. Seperti pada gambar berikut.



Gambar. 8 Proses sniffing attack pada paket data website LEADS UPNVJ

Berikut merupakan hasil dari *sniffing attack* yang dilakukan oleh penyerang kepada isi dari paket data yang dikirimkan dari *client* menuju *server.* Seperti pada gambar berikut.



Gambar. 9 Hasil dari *sniffing attack* pada aliran paket data

Dapat dilihat bahwa pada protokol TCP bahwa isi dari paket data tidak dapat dianalisis oleh penyerang dikarenakan pesan yang dikirimkan sudah dienkripsi oleh protokol TLS. Jadi tools wireshark tidak bisa menyadap aliran paket data yang dikirimkan dari client menuju server website LEADS UPNVJ sehingga informasi yang sensitif seperti username dan password dapat terlindungi dengan baik.

3.3 Hasil Keseluruhan Dari Penyerangan

Berikut merupakan tabel rekap hasil serangan SQL *injection* & *sniffing attack* terhadap *website* LEADS UPNVJ

Tabel. 1 Hasil dari *sniffing attack* pada aliran paket data

No	Jenis Serangan	Tools	Waktu Penyerangan	Hasil Serangan
1	SQL Injection	Burp Suite & SQLMap	6 Jam	*Website LEADS UPNVJ aman dari serangan SQL Injection karena terdapat Web Application Firewall (WAF)*
2	*Sniffing Attack*	Wireshark	15 Menit	Website LEADS UPNVJ aman dari serangan sniffing attack karena terdapat protokol TLS yang mengenkripsi paket data yang dikirim dari client menuju server

4 Kesimpulan dan Saran

4.1 Kesimpulan

Setelah melakukan penelitian dapat ditarik beberapa kesimpulan seperti berikut :

1. Tingkat keamanan pada *Website* LEADS UPNVJ sudah cukup baik dalam menangani serangan SQL *injection* dan *sniffing attack.*
2. Keamanan *Website* LEADS UPNVJ cukup baik menghadapi serangan SQL *injection* karena sudah menggunakan *Web application firewall* (WAF) yang berfungsi melakukan pemantauan, penyaringan, dan

pemblokiran data yang terindikasi berbahaya yang dikirimkan oleh *client* menuju *server* dalam hal SQL *injection* adalah memblokir usaha penginjeksian perintah kueri SQL menuju *database website*.

3. Keamanan *Website* LEADS UPNVJ cukup baik menghadapi serangan *sniffing attack* dikarenakan sudah menggunakan protokol *Transport layer security* (TLS) yang berfungsi untuk melakukan enkripsi pada isi paket data yang dikirimkan oleh *client* menuju *server* maupun sebaliknya sehingga penyerang yang ingin menyadap jalur komunikasi antara *client* dan *server* tidak dapat membaca isi dari paket data yang bersifat sensitif dan rahasia seperti *username*, *password*, nomor telepon, tanggal lahir, dan lain-lain.

4.2 Saran

Berdasarkan kesimpulan diatas, memang *website* LEADS UPNVJ sudah cukup baik dalam menangani serangan SQL *injection* dan *sniffing attack* tetapi untuk tetap menjaga tingkat keamanan yang tinggi, maka saran yang dapat dipertimbangkan untuk kedepannya antara lain :

1. Terus melakukan perpanjangan masa aktif secara berkala pada sertifikat TLS yang digunakan oleh *website* agar terhindar dari hal-hal yang tidak diinginkan.
2. Selalu melakukan *update* terbaru terhadap sistem *Web application firewall* (WAF) agar sistem WAF dapat mengidentifikasi dan menanggulangi ancaman atau serangan yang baru.
3. Terus melakukan *penetration testing* secara berkala untuk memeriksa celah-celah kerentanan pada suatu *website.*
4. Selalu melakukan *update* terbaru dari *browser* yang digunakan oleh pengguna karena pada *update* terbaru biasanya terdapat pembaruan terhadap *bug* atau celah keamanan yang dapat dieksploitasi.

Referensi

[1] Abdulloh, Rohi. (2018). 7 in 1 Pemograman Web untuk Pemula. Jakarta : Elex Media Komputindo.
[2] CSIRT Bappenas. “SQL Injection”. csirt.bappenas.go.id. csirt.bappenas.go.id/ layanan/detail/180a9a4e-7e0a-49f2-ac92-92702ac094f5.
[3] Halvorsen, Hans Petter. 2016. Structured Query Language. Notodden: University College of Southeast Norway.
[4] Pfleeger, Charles P., and Shari Lawrence Pfleeger. 2012. Analyzing computer security: a threat/vulnerability/countermeasure approach. Upper Saddle River, NJ: Prentice Hall.
[5] Tallinn Manual On The International Law Applicable to Cyber Warfare, 2013.
[6] Tim EMS. 2014. Teori dan Praktik PHPMySQL untuk Pemula. Jakarta: Elex Media Komputindo.