PERBANDINGAN KINERJA TOOLS WIRESHARK DAN BURPSUITE UNTUK PENYERANGAN WEBSITE DENGAN METODE SNIFFING

Abdul Aziz Khozindani, Yusuf Muhyidin, M. Agus Sunandar
Program Studi Teknik Informatika S1, Fakultas Teknik, STT Wastukancana Purwakarta
Jalan Cikopak No.53, Mulyamekar, Kec. Babakancikao, Kabupaten Purwakarta, Jawa Barat 41151, Indonesia
Abdulaziz04@wastukancana.ac.id

ABSTRAK

Perkembangan digital seperti *website* berkembang seiring berjalanannya tahun. *Website* menjadi sumber informasi yang besar dan penggunaannya sudah banyak di terapkan di berbagai bidang. Pengamanan sebuah *website* diperlukan sebab semakin banyak terbukanya pengetahuan tentang *hacking* dan *cracking*, didukung dengan *tools* yang bisa digunakan dengan gratis, dimana memudahkan terjadi serangan untuk mencari celah keamanan *website*. Ini mempengaruhi keamanan *website* dimana ancaman siber tampak besar baik dari penjaga data pribadi pengguna dan perentas yang diluar untuk memanfaatkan celah yang ada untuk kepentingan pribadi. Metode penyerangan yang peneliti gunakan adalah dengan metode Pentest, Pentest dapat didefinisikan sebagai kegiatan pengujian keamanan dari sebuah software. Dalam melakukan pengujian keamanan software, ada tahapan uji kerentanan perangkat lunak yang perlu dilakukan. Dengan demikian, uji yang dilakukan bisa terorganisasi dengan baik, dengan dua tools yang digunakan untuk penelitian ini yang dimana penelitian ini berfokus pada perbandingan kinerja setiap tools nya untuk *sniffing attack*. Hasil dari penelitian ini Berdasarkan dari proses penyerangan yang sudah dilakukan, bisa disimpulkan bahwa untuk melakukan *sniffing* lebih disarankan menggunakan *burpsuite* karena dapat membaca pesan request maupun *response* karena aplikasi *burpsuite* telah didukung dengan adanya *CA Certificate* yang bertindak sebagai pihak ketiga yang terpercaya dan memungkinkan dapat menandatangani sertifikat yang digunakan protokol https. Dari penjelasan yang terdapat pada tabel hasil perbandingan yang didapat dari penyerangan *wireshark* dan *burpsuite*, terlihat bahwa tidak ada *tools* yang sempurna.

Kata kunci: *Website, Sniffing Attack, Pentest, Wireshark, Burpsuite*

1. PENDAHULUAN

Kebutuhan manusia pada informasi mendorong kemajuan sarana komunikasi dan informasi yang meningkat di era sekarang ini maka dari itu mobilitas manusia semakin luas dan cepat. Pada saat ini internet sangat berperan dalam kehidupan manusia. Dengan adanya internet, manusia dapat menemukan berbagai informasi dengan mudah. Di internet kita dapat melakukan berbagai hal, mulai dari mencari informasi, berkomunikasi dengan orang lain, transaksi jual beli dan lain sebagainya. Salah satunya dengan menggunakan *website*. *Website* adalah halaman informasi yang disediakan melalui jalur internet sehingga bisa diakses di seluruh dunia selama terkoneksi dengan jaringan internet.

Perkembangan digital seperti *website* berkembang seiring berjalanannya tahun. *Website* menjadi sumber informasi yang besar dan penggunaannya sudah banyak di terapkan di berbagai bidang [1]. Pengamanan sebuah *website* diperlukan sebab semakin banyak terbukanya pengetahuan tentang *hacking* dan *cracking*, didukung dengan *tools* yang bisa digunakan dengan gratis, dimana memudahkan terjadi serangan untuk mencari celah keamanan *website* [2]. Ini mempengaruhi keamanan *website* dimana ancaman siber tampak besar baik dari penjaga data pribadi pengguna dan peretas yang diluar untuk memanfaatkan celah yang ada untuk kepentingan pribadi [3].

Hadirnya *website* sebagai sumber informasi dapat digunakan oleh suatu lembaga pendidikan untuk memberikan informasi yang mudah diakses seperti pada *website* Ponpescireok.org. *Website* Ponpescireok.org menyajikan seputar profile Pondok Pesantren Cireok dan akses membagikan informasi terkini seputar Pondok Pesantren Cireok serta terdapat fitur penerimaan siswa baru. Fitur penerimaan siswa *online* pada *website* Ponpescireok dapat memudahkan bagi calon siswa untuk mendaftarkan sebagai siswa, adanya fitur pendaftaran *online* juga dapat memudahkan bagian administrasi untuk mengolah data-data calon siswa yang akan mendaftar.

Berdasarkan penjabaran diatas, terdapat banyak *tools* untuk melakukan serangan *hacking* dan *cracking* yang dapat mengancam privasi dari penggunanya, ada dua *tools* yang digunakan untuk penelitian ini yang dimana penelitian ini berfokus pada perbandingan kinerja setiap *tools* nya dalam melakukan *sniffing attack*,

2. TINJAUAN PUSTAKA

2.1. *Website*

Merurut Agustiara dalam penelitian nya *website* merupakan sebuah kumpulan halaman pada suatu domain di internet yang dibuat dengan tujuan tertentu dan saling berhubungan serta dapat diakses secara luas melalui halaman depan *(home page)* menggunakan sebuah *browser* menggunakan URL *website* [4].

Sedangkan Menurut [5] *Website* adalah kumpulan halaman yang digunakan untuk menampilkan informasi teks, gambar diam atau gerak, animasi suara, ataupun gabungan dari semuanya, baik yang bersifat statis ataupun dinamis yang membentuk satu rangkaian bangunan yang saling terkait.

2.2. Keamanan Jaringan

Keamanan jaringan didefinisikan sebagai sebuah perlindungan dari sumber daya terhadap upaya penyingkapan, modifikasi, utilisasi, pelarangan dan perusakan oleh *person* yang tidak diijinkan. Bisa juga diartikan sebagai suatu perlindungan yang diusahakan oleh suatu sistem informasi dalam rangka mencapai sasaran hasil yang bisa diterapkan atau memelihara integritas, kerahasiaan dan ketersediaan system informasi sumber daya. Sumber daya informasi meliputi perangkat keras, perangkat lunak, data dan informasi [6].

2.3. Protokol Jaringan

Menurut Hery Protokol adalah aturan-aturan main yang mengatur komunikasi diantara beberapa komputer di dalam sebuah jaringan, aturan itu termasuk didalamnya petunjuk yang berlaku bagi cara-cara atau metode mengakses sebuah jaringan, topologi fisik, tipe-tipe kabel dan kecepatan transfer data [7]

.

2.4. *HTTP* dan *HTTPS*

Hypertext Transfer Protocol (HTTP) merupakan sebuah protokol jaringan aplikasi yang digunakan untuk mendistribusikan informasi antara komputer *server* dengan komputer *client*. *Server* disini yang dimaksud adalah jenis *web server* denan bentuk fisik jaringan computer yang memiliki sekala besar. Sedangkan *client* adalah web browser yang dapat mengakses, menerima dan menampilkan konten melalui browser sedangkan *Hypertext Transfer Protocol Secure (HTTPS)* merupakan pengembangan dari versi *HTTP* sebelumnya. *HTTPS* memiliki tingkat keamanan yang lebih baik dibandingkan dengan *HTTP* sehingga dapat membuat client merasa lebih aman dalam mengakses konten-konten web [8].

2.5. *Wireshark*

Menurut Huzaenia *Wireshark* merupakan aplikasi yang dijadikan *tool* untuk menganalisis paket data jaringan yang sedang berlangsung. *Wireshark* disebut juga sebagai *network packet analyzer* yang berfungsi untuk menampilkan semua informasi pada paket tersebut secara lengkap dan menangkap paket-paket yang dikirimkan maupun diterima [9].

2.6. *Burpsuite*

Burp Suite adalah alat pengujian penetrasi. *Burpsuite* adalah *proxy* penyadap, oleh karena itu, *Burp* ditempatkan di antara server dan klien web sehingga semua permintaan dan tanggapan antara server dan klien web dirutekan dan ditangkap oleh *Burpsuite* [10].

2.7. *Sniffing*

Sniffing Attack, teknik dimana data paket yang mengalir melalui jaringan terdeteksi dan diamati. Administrator jaringan menggunakan alat *sniffing* paket untuk memantau dan memvalidasi lalu lintas jaringan, sementara peretas dapat menggunakan alat serupa untuk tujuan jahat. Dapat disimpulkan bahwa *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 [11].

3. METODE PENELITIAN

3.1. Metode Penelitian

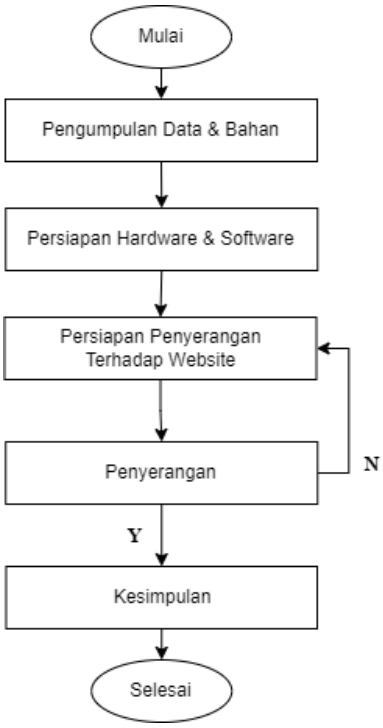
Metode yang digunakan dalam penelitian ini adalah metode deskriptif. Metode penelitian deskriptif adalah salah satu metode penelitan yang banyak digunakan pada penelitian yang bertujuan untuk menjelaskan suatu kejadian. Seperti yang dikemukakan oleh [12] bahwa "Penelitian deskriptif adalah suatu metode dalam meneliti status sekelompok manusia, suatu objek, suatu set kondisi, suatu sistem pemikiran ataupun suatu kelas peristiwa pada masa sekarang".

Pada metode ini menjelaskan bagaimana pengujian sebuah *website*, pengujian ini dilakukan beberapa kali untuk memastikan serangan dengan metode *penetration testing* sampai berhasil mengetahui dan melihat *username* dan *password* korban. Pada saat simulasi penyerangan ini berjalan nantinya penulis akan menganalisa setiap paket data dan juga mengamati setiap perubahan yang terjadi pada *website* yang lewat pada jaringan lokal *wifi*. Paket data yang penulis amati terdapat beberapa komponen, berikut 5 komponen dari paket data:

1. *Time*
   Menjelaskan format waktu *packet* yang tertangkap.
2. *Source*
   Merupakan IP sumber dari suatu *packet* data.
3. *Destination*
   Merupakan IP tujuan kemana suatu *packet* data akan diteruskan.
4. *Protoco*l
   Merupakan jenis *protoco*l apa yang digunakan.
5. *Info*
   Merupakan Info lebih lanjut mengenai suatu *packet*.

3.2. Kerangka Penelitian

Berikut kerangka penelitian yang menjadi gambaran besar mengenai penelitian yang dilakukan dapat dilihat pada Gambar 1.



Gambar 1. Kerangka Penelitian

3.3. Teknik Pengumpulan Data

Teknik pengumpulan data pada penelitian ini sebagai berikut:

3.4.1 Observasi

Teknik pengumpulan data pada penelitian ini dilakukan dengan observasi melalui media internet. Dengan tujuan mencari informasi agar informasi tersebut dapat memenuhi kelengkapan untuk bahan penelitian.

3.4.2 Studi Pustaka

Teknik pengumpulan data studi literatur berupa jurnal, karya ilmiah, dan studi pustaka lainnya digunakan sebagai penunjang keilmuan untuk penelitian ini. Dengan mencari studi kasus yang serupa yang bisa dijadikan sebagai acuan pada penelitian ini.

3.4. Penyerangan

Dalam tahap ini penulis akan mencoba melakukan penyerangan *Sniffing Attack.* Metode penyerangan yang peneliti gunakan adalah dengan metode Pentest, Pentest dapat didefinisikan sebagai kegiatan pengujian keamanan dari sebuah software. Dalam melakukan pengujian keamanan software, ada tahapan uji kerentanan perangkat lunak yang perlu dilakukan. Dengan demikian, uji yang dilakukan bisa terorganisasi dengan baik.

3.5. Penarikan Kesimpulan

Dalam tahap ini penulis akan melakukan analisis hasil dan mengambil kesimpulan dari hasil penyerangan tersebut.

4. HASIL DAN PEMBAHASAN

Analisis ini dilakukan untuk mengetahui bagaimana bentuk dari sebuah penyerangan *packet sniffing* dari beberapa *tools* terhadap *website*, kemudian membandingakan hasil kinerja *tools*. Keamanan dari jaringan *wi-fi* yang terkoneksi ke internet pada umumnya rentan terhadap ancaman.

4.1. *Planning*

Langkah awal yang perlu dilakukan adalah melakukan perencanaan. Perencanaan yang dimaksud mencakup identifikasi hal yang akan dites dan aplikasi yang akan digunakan. Penulis melakukan persiapan untuk analisis kebutuhan pada penelitian ini, berikut beberapa persiapan dan konfigurasi yang dilakukan.

Berikut langkah-langkah penyerangan *sniffing attack* menggunakan *wireshark*:

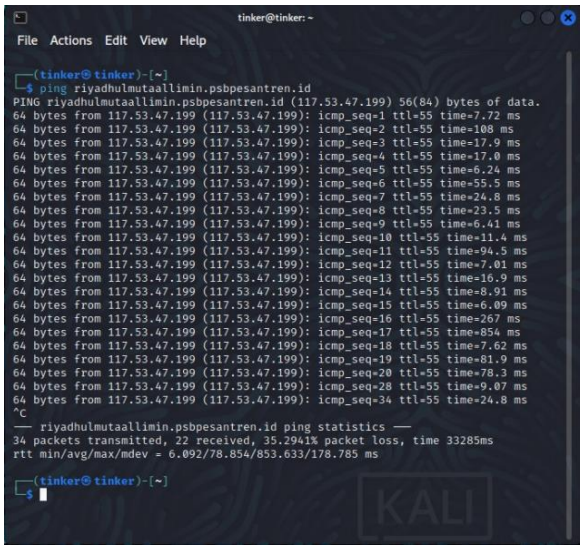
1. Penyerang memastikan target berada didalam satu jaringan yang sama dengan penyerang.
2. Penyerang mencari *website* untuk dijadikan sebagai targer.
3. Selanjutnya penyerang melakukan proses *login* pada sistem *website*.
4. Proses *login* yang dicoba yaitu menggunakan *username* dan *password* yang salah karena penyerang ingin mengetahui tingkat keamanan terhadap *website* tersebut.
5. Penyerang berhasil mengetahui aktivitas dari target dan *software wireshark* dapat merekam beberapa *packet list* yang masuk.

Berikut langkah-langkah penyerangan terhadap target menggunakan *burpsuite* skenario yang dilakukan yaitu:

1. Penyerang menyiapkan beberapa *website*, guna untuk menguji keamanan dari sebuah *website.*
2. Selanjutnya penyerang membuka aplikasi *burpsuite*, pada tahap ini penyerang mengatur *proxy* pada settingan di *browser* guna untuk membuat burpsuite bertindak sebagai *proxy*.
3. Pada *tools burpsuite* penyerang mematikan *intercept is on* menjadi *off* sehingga *website* dapat dibuka pada browser. penyerang akan melakukan serangan untuk mencari kerentanan dari suatu *website*.
4. Penyerang melakukan proses *login* terhadap *website*.
5. Aplikasi *burpsuite* memonitor setiap *request* maupun *respon*se dari *web browser* dengan *server.*
6. Penyerang berhasil menemukan *username* dan *password* target.

4.2. *Informaton Gathering*

Pada tahap ini penulis mencoba mengumpulkan informasi dari target berupa *ip address* dan informasi lainnya yang diperlukan oleh penulis. Tahapan ini bertujuan untuk mengumpulkan informasi sebanyak-banyaknya mengenai *website.* Adapun informasi yang dicari yaitu *Ip addres* dari *website* yang dapat diketahui melalui *ping* pada terminal di *kali linux.*



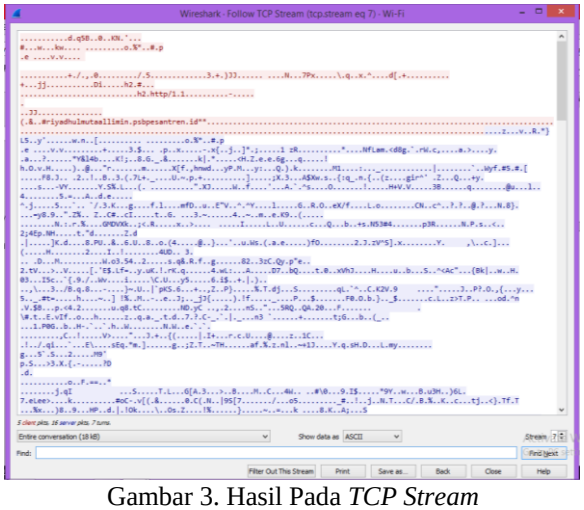
Gambar 2. *Ping website* target

4.3. *Penetraton Attempt*

Tahap ini dilakukan percobaan penyerangan dan ini merupakan fase pengambilan paket data yang dikirimkan melalui jaringan *wifi*, disini proses *sniffing attack* terjadi, informasi yang diperoleh pada fase sebelumnya bisa digunakan sebagai bahan untuk melakukan mengidentifikasi target. Untuk *tools* yang digunakan adalah *wireshark* dan aplikasi *Burpsuite* pada sistem operasi *kali linux*.

4.3.1 Penyerangan Menggunakan *Wireshark*

Dari beberapa *website* yang telah dilakukan simulasi percobaan penyerangan *packet sniffing*. Berkut hasil dari penyerangan *website* menggunakan *tools wireshark.*



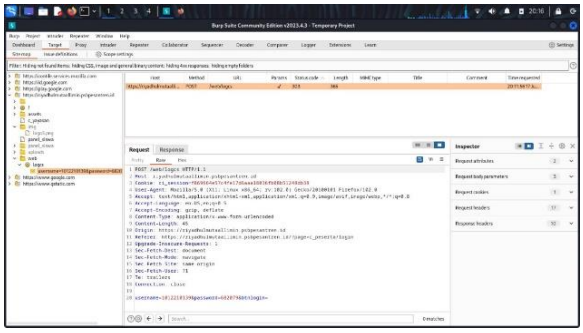
Gambar 3. Hasil Pada *TCP Stream*

Terlihat pada gambar 4.9 dapat disimpulkan bahwa penyerangan *website* dengan keamanan *HTTPS* tidak mudah terbaca oleh t*ools wireshark.* Hasil penyerangan selesai, *tools wireshark* tidak mampu menampilkan *username* dan *password* karna terenkripsi.

Pada hasil *capture packet tools wireshark* dapat membaca data API dari *website* yang terdiri dari hostnya, length atau panjang paket data, tapi terenkripsi oleh *security HTTPS.*

4.3.2 Penyerangan Menggunakan *Burpsuite*

Berikut hasil penyerangan dari *tools burpsuite* dapat menampilkan beberapa *website* yang tertangkap juga dapat menampilkan arsitruktur dari data API-nya sehingga didapatkan hasil token berupa *username* ”1012210139” dan *password* “682079”. Seperti gambar 4.25.



Gambar 4. Tampilan *Site Map*

Pada hasil *site map tools burpsuite* mampu menampilkan pesan *request* dari web *browser*. Tampilan *site map* dapat membaca data APInya yang terdiri dari *hostnya.*

4.4. *Reporting*

Setelah dilakukan penyerangan, maka dibuat informasi untuk mempermudah dalam melihat paket data mana saja yang merupakan informasi sensitif.

4.4.1 Hasil *Capture Packet* Data

Hasil dari *capture packet* menggunakan *wireshark* terdapat beberapa komponen informasi yaitu No, *Time* menjelaskan waktu, *Source* asal *packet* dikirim, *Destination packet* yang dituju, *Protocol* menunjukan *protocol* yang digunakan, *Lenghth* panjang *packet* yang dikirim, info menunjukan informasi *packet.*

Tabel 1. Hasil *Capture Packet* Menggunakan *Wireshark*

No	Time	Source	Destination	Protocol	Lenghth	Info
16576	21.131955	10.159.79.70	117.53.47.199	HTTP	843	POST /web/logcs HTTP/1.1 (application/x-www-form-urlencoded)
16577	21.139997	117.53.47.199	10.159.79.70	TCP	60	80 → 50035 [ACK] Seq=1 Ack=790 Win=30848 Len=0

Hasil dari *capture packet* menggunakan *burp suite* mendapatkan informasi seperti pada **Tabel 2** sebagai berikut.

Tabel 2. Hasil *Capture Packet* Menggunakan *Burpsuite*

Host	Method	Url	Length	IP	Cookies	Time
https://riyadhulmutaallimin.psbpesantren.id	GET	//c_peserta/login	5086	117.53.47.199	ci_session=d2df39fb38ec9cd2d2d32b9cd6f32c53e2d83069	14 : 37 : 33
https://riyadhulmutaallimin.psbpesantren.id	POST	/web/logcs	354	117.53.47.199	-	14 : 37 : 34

4.4.2 Hasil *Capture Packet* Data

Dari pecobaan penyerangan teradap beberapa target penulis menyajikan tabel untuk mendeskripsikan hasil perbandingan kinerja dari dua *tools* yaitu *wireshark* dan *burpsuite*.

Tabel 3. Hasil Penyerangan

No.	Website	Protokol	Sniffing	
			Wireshark	Burpsuite
1.	Pondok Pesantren Riyadhul Muta'allimin cireok	https	Gagal	Berhasil
2.	Kader Pengawas Partisipatif Bawaslu	http	Berhasil	Berhasil
3.	Loker.id	https	Gagal	Berhasil
4.	Shopee.co.id	https	Gagal	Gagal
5.	Journal.ui.ac.id	http	Berhasil	Berhasil

Hasil penyerangan dari kedua *tools* yaitu *wireshark* dan *burpsuite*, pada target pertama *sniffing* menggunakan *wireshark* gagal dikarenakan data yang berhasil diambil ter-enkripsi oleh *Secure Socket Layer (SSL)* sedangkan pada *tools burpsuite* berhasil mengambil data sensitif seperti *username* dan *password.*

Penyerangan target kedua menggunakan *wireshark* dan *burpsuite* berhasil mengambil data sensitif seperti *username* dan *password* tanpa ter-enkripsi karena target kedua mengunakan *protocol http.* pada target ketiga *sniffing* menggunakan *wireshark* gagal dikarenakan data yang berhasil diambil ter-enkripsi oleh *Secure Socket Layer (SSL)* sedangkan pada *tools burpsuite* berhasil mengambil data sensitif seperti *username* dan *password.* Begitupun penjelasan selanjutnya pada Tabel 3.

Pada dasarnya tingkat keamanan dalam mengamankan proses *transmisi packet* data masih aman *HTTPS* dikarenakan adanya proses enkripsi pesan yang diterima oleh tools *wireshark* dan kenapa pada *burpsuite* dapat membaca pesan request maupun *response* karena aplikasi *burpsuite* telah didukung dengan adanya *CA Certificate* yang bertindak sebagai pihak ketiga yang terpercaya yang memungkinkan dapat menandatangani sertifikat yang digunakan protocol *HTTPS*.

5. KESIMPULAN DAN SARAN

Berdasarkan dari proses penyerangan yang sudah dilakukan, bisa disimpulkan bahwa keamanan protokol *http* sedikit rentan dari serangan *sniffing*, lebih aman menggunakan protokol *https*, dari penjelasan yang terdapat pada tabel hasil perbandingan yang didapat dari penyerangan *wireshark* dan *burpsuite*, terlihat bahwa tidak ada *tools* yang sempurna. Dari setiap *tools* mempunyai kelebihan dan kekurangannya, untuk melakukan *sniffing* lebih disarankan menggunakan *burpsuite* karena dapat membaca pesan request maupun *response* karena aplikasi *burpsuite* telah didukung dengan adanya *CA Certificate* yang bertindak sebagai pihak ketiga yang terpercaya dan memungkinkan dapat menandatangani sertifikat yang digunakan protokol https.

DAFTAR PUSTAKA

[1] K. Nisa and M. A. Putra, "Analisis Website Tapanuli Tengah Menggunakan Metode Open Web Application Security Project Zap (Owasp Zap)," *Bulletin of Information Technology (BIT),* p. 308, 2022

[2] N. I. S. Fazriani, B. Cut and Sanusi, "Uji Keamanan Website Terhadap Serangan Path Traversal," *Kandidat : Jurnal Riset dan Inovasi Pendidikan,* pp. 15-20, 2019

[3] M. R. S. Al'Am'yubi, "Analisis Sistem Keamanan Website XYZ Menggunakan Framework OWASP ZAP," *JURNAL ILMU KOMPUTER (JUIK)*, 2023

[4] W. Agustiara, "ANALISIS KEAMANAN PROTOKOL SECURE SOCKET LAYER TERHADAP SERANGAN PACKET SNIFFING PADA WEBSITE PORTAL BERITA HARIAN UMUM KORAN PADANG," *Jurnal Teknik Informatika Kaputama (JTIK)*, 2022

[5] F. Fahira and C. I. Setiawati, "ANALISIS KUALITAS WEBSITE PIKIRAN-RAKYAT.COM SEBAGAI PORTAL BERITA DENGAN MENGGUNAKAN METODE IMPORTANCE PERFORMANCE ANALYSIS," *e-Proceeding of Management*, p. 3498, 2020

[6] P. P. Putra, "Pengembangan Sistem Keamanan Jaringan Menggunakan Rumusan Snort Rule (Hids) untuk Mendeteksi Serangan Nmap," *SATIN - Sains dan Teknologi Informasi, Vol. 2, No. 1, Juni 2016*, 2016

[7] D. Hery, Mikrotik Operating System Jaringan Komputer, Malang, 2015

[8] D. Intern , "Apa Perbedaan HTTP dan HTTPS? Lengkap Beserta Penjelasannya," 2020. [Online]

[9] F. Huzaenia, "Analisis Keamanan Data Pada Website Dengan Wireshark," *JES (Jurnal Elektro Smart)*, 2021

[10] M. A. Al Hilmi, "Pengujian Keamanan Fitur Upload File Pada Sistem Aplikasi Web," *Jurnal Informatika: Jurnal pengembangan IT (JPIT)*, 2022

[11] D. P. Putranto, "Analisis Keamanan Website Leads UPNVJ Terhadap Serangan SQL Injection & Sniffing Attack," *JURNAL INFORMATIK Edisi ke-18, Nomor 3*, 2022

[12] Moh.Nazir, Metode Penelitian, Cetakan Kelima, Jakarta: Ghalia Indonesia, 2003