Prosiding Seminar Nasional Riset Information Science (SENARIS)
ISSN: 2686-0260
September 2019
Hal:994-1001

Penetration Testing Untuk Deteksi *Vulnerability* Sistem Informasi Kampus

Sahren[1], Ruri Ashari Dalimuthe[2], Muhammad Amin[3]
STMIK Royal Kisaran
sahren.one@gmail.com[1],ruriashari1986@gmail.com[2],stmikroyal13@gmail.com[3]

Abstract -*Security is an effort that can be done to protect the information contained in it which refers to confidentiality. Information systems that are centrally prone to various types of attacks such as DoS, SQL Injections, Cross Site Scripting (XSS), Clickjacking, CSRF / Cross-site request forgery and so on. This will be a polemic for the information service owner and manager. The method to be carried out in this study is to do penetration testing to audit the security of the campus information system webserver. This activity aims to identify and exploit vulnerabilities in the web server. In this study, several tools will be used as a tool, including WHOIS, NMAP and Acunetix Web Vulnerability Scanner. Tests carried out are to look for vulnerabilities on the web server while the level of vulnerability that will be detected in this test sawill be inter alia higt risk, Medium risk and low risk. The aim is to find out the weaknesses in the web server so that in the future it can avoid DoS attacks, CSRF / Cross-site request forgery, Cross Site Scripting (XSS) and clickjacking. The results of this test are expected to be an input for the management of campus information systems for the future can be made improvements to existing weaknesses.*

Keywords*: Penetration Testing, Vulnerability, CSRF, Clickjacking, Acunetix*

Abstrak*-Keamanan merupakan upaya yang dapat dilakukan guna melindungi informasi yang terdapat didalamnya yang mana mengacu kepada kerahasiaan. Sistem informasi yang secara terpusat sangat rawan terhadap berbagai macam serangan seperti DoS, SQL Injectiion, Cross Site Scripting (XSS), Clickjacking, CSRF/ Cross-site request forgery dan lain sebagainya. Hal ini akan menjadi sebauh polemik bagi pemilik dan pengelola layanan sebuah informasi. Metode yang akan dilakukan pada penelitian ini adalah dengan melakukan penetration testing untuk mengaudit keamanan webserver sistem informasi kampus. Kegiatan ini bertujuan untuk mengidentifikasi dan eksploitasi kerentanan pada webserver. Pada penelitian ini akan digunakan beberapa tools sebagai alat bantu antara lain WHOIS, NMAP dan Acunetix Web Vulnerabilty Scanner. Pengujian yang dilakukan adalah untuk mencari vulnerability pada web server adapun tingkatan vulnerability yang akan dideteksi dalam pengujian ini nantinya antar lain higt risk, Medium risk dan low risk. Tujuannya adalah untuk mengetahui kelemahan pada webserver supaya kedepannya dapat menghindari dari serangan DoS, CSRF/ Cross-site request forgery, Cross Site Scripting (XSS) maupun clickjacking. Hasil dari pengujian ini diharapkan dapat sebagai bahan masukan kepada pihak pengelola sistem informasi kampus untuk kedepannya dapat dilakukan perbaikan terhadap kelemahan yang ada.*

Kata kunci*: Penetration Testing, Vulnerability, CSRF, Clickjacking, Acunetix*

1. PENDAHULUAN

Sistem informasi yang secara terpusat sangat rawan terhadap berbagai macam serangan seperti *DoS*, *SQL Injectiion*, *Cross Site Scripting (XSS)*, *Clickjacking*, *CSRF/ Cross-site request forgery* dan lain sebagainya. Seorang penyerang akan

ISSN: 2686-0260
September 2019
Hal:994-1001

menyerang sistem kemanan jaringan dengan tujuan untuk mengalahkan layanan keamanan pada fasilitas jaringan tersebut. Dengan mempertimbangkan fakta bahwa jaringan *public* pada awalnya dirancang untuk keterbukaan tanpa mempertimbangkan keamanan, jelas membuka peluang akan terjadi kejahatan [2]. *Hacker* dengan kemampuan tinggi dapat melakukan *remote* setelah mendapat celah dengan melakukan serangan *SQL Injection*. Dimana hacker dapat mengirimkan *script* dengan mengunakan *script* khusus ke *website* tertentu dengan cara melakukan teknik rekayasa sistem. Serangan *Cross Site Scripting (XSS)* adalah jenis injeksi dengan mengirimkan kode-kode script berbahaya. Umumnya dalam bentuk *script* ke sisi *browser* pada pengguna akhir yang berbeda [8]. Selain bentuk serangan tersebut terdapat bentuk serangan lainnya yang cukup populer pada masa sekarang ini yaitu *clikjacking*. *Clickjacking* adalah sebuah ancaman yang muncul di *web*. Serangan ini merupakan salah satu contoh trik pengambilan data, dengan modus penipuan, serangan ini berpotensi mengirimkan perintah yang tidak sah atau mengungkapkan informasi rahasia sementara korban berinteraksi pada halaman *web* yang tampaknya tidak berbahaya [5]. Celah ini muncul biasanya dikarenakan *X-Frame Header Option* yang tidak di set pada *web server*. Untuk dapat mengurangi kerugian yang diakibatkan oleh para *hacker*, maka langkah awal yang harus dikembangkan adalah melakukan evaluasi terhadap keamanan *server* yang ada. Hal ini bertujuan untuk mengurangi resiko terjadinya penyalahgunaan terhadap sumber daya yang ada pada suatu perguruan tinggi atau pun kampus. Sebagian besar orang di suatu instansi akan merasa bingung dan kesulitan saat diminta untuk melakukan evaluasi atau audit keamanan *server* yang ada. Hal ini dikarenakan memang banyak orang yang merasa awam untuk melakukan evaluasi *server*. Istilah *Penetration testing* atau yang lebih dikenal dengan *penetrasi* adalah serangkaian kegiatan yang dilakukan untuk mengidentifikasi dan mengeksploitasi kerentanan yang ada [7]. Oleh karena adanya permasalahan tersebut maka kebutuhan yang penting saat ini adalah membantu meminimalisir dan mengantisipasi *server* yang ada dari kejahatan *hacking.*

Beberapa penelitian terdahulu telah banyak dilakukan berkaitan dengan *penetration testing*. [7] melakukan penelitian untuk menganalisa perbandingan *Penetration Testing Tool* untuk menguji suatu aplikasi *web*. [1] melakukan penelitian untuk menganalisa kelemahan *port* pada pengguna *public WiFi.* [3] melakukan penelitian untuk menganalisa keamanan suatu website dengan metode *scanning* serta menerapkan peritungan *security* matriks dan menggunakan formula *base score* untuk mengukur tingkat kerentanan jaringan apakah *low medium* atau *high*. Tujuan pada penelitian ini adalah menggunakan metode *penetration testing* untuk mencari kelemahan *(vulnerability*) yang ada pada sistem informasi kampus untuk kemudian akan dijadikan sebagai bahan evaluasi oleh pihak terkait.

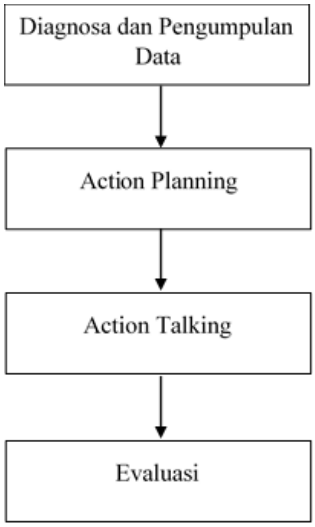
2. METODOLOGI PENELITIAN

Metodologi penelitian ini dilakukan secara sistematik yang bisa digunakan sebagai pedoman atau acuan untuk peneliti ketika melaksanakan penelitian agar hasil yang dicapai tidak menyimpang dan tujuan yang diinginkan bisa terlaksana dengan baik, benar dan sesuai terhadap apa yang telah ditentukan sebelumnya.

2.1 Kerangka Kerja Penelitian *(Frame Work)*

ISSN: 2686-0260
September 2019
Hal:994-1001

Kerangka kerja penelitian merupakan langkah-langkah yang harus dilakukan dalam penelitian hingga mencapai suatu kesimpulan. Adapun alur penelitian yang penulis gunakan terlihat pada gambar berikut ini:



Gambar 1. Kerangka Penelitian

Berdasarkan kerangka kerja pada gambar 1 maka dapat diuraikan langkah kerja sebagai berikut :

1. Diagnosa dan Pengumpulan Data

Pengumpulan data merupakan hal yang sangat penting dalam sebuah penelitian. Dalam penelitian ini pengumpulan data penulis lakukan melalui :

a. Jurnal–jurnal yang penulis jadikan sebagai referensi adalah jurnal yang berkaitan dengan sistem pembuatan informasi online dalam pembuatan laporan yang berhubungan dengan judul yang penulis tulis.
b. Buku yang berrhubungan dengan penelitian yang dilakukan. Buku yang penulis gunakan sebagai referensi adalah buku yang berkaitan dengan judul penulis tulis.

2. *Action Planing*

Tahap kedua adalah membuat rencana tindakan *(Action Planning*) tahapan ini peneliti melakukan pemahaman pokok masalah yang ada dan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada. Peneliti akan mulai menyusun rencana pengujian yang akan dilakukan pada sistem informasi.

3. *Action Talking*

Tahap ketiga adalah melakukan tindakan *(Action Taking)* mengimplementasikan rencana tindakan yang telah disusun. Pada langkah ini peneliti mulai melakukan tahapan-tahapan investigasi guna mendapatkan informasi kelemahan.

4. Evaluasi

Tahap keempat adalah melakukan evaluasi *(Evaluating*) setelah tahapan *Action Taking* dilaksanakan peneliti mulai melakukan evaluasi pada hasil dari implementasi sebelumnya dan mulai menyimpulkan hasil dari langkah sebelumnya. Hasil dari evaluasi ini adalah berupa daftar celah kemanan dari

ISSN: 2686-0260
September 2019
Hal:994-1001

sistem informasi yang telah diketemukan pada proses sebelumnya, hasil temuan ini akan memberikan sebuah kesimpulan mengenai tingkat keamanan dari *web server* itu sendiri.

2.2 Pengertian Keamanan jaringan

Keamanan jaringan adalah sebuah upaya untuk melakukan kendali terhadap akses sumberdaya jaringan, akses jaringan dikontrol supaya hanya bisa diakses oleh siapa saja yang berhak dan menghalangi dari yang tidak berhak [6]. Menurut Garfinkel, yang merupakan pakar dalam bidang *security*. Kemanan komputer terdiri dari empat aspek yaitu, *privacy, integrity, authentication* dan *availability.*

a. Privacy atau *confidentiality.*

Privacy atau kerahasiaan informasi. Inti dari aspek ini adalah bagaimana menjaga kerahasiaan dari informasi agar tidak dapat dilihat atau diakses oleh orang yang tidak memiliki hak sama sekali [6].

b. Integrity

Aspek *integrity* atau biasa juga disebut sebagai integritas mencakup keutuhan atau orisinalitas informasi [6]. maksud dari aspek ini adalah bagaimana infomasi agar tetap utuh. Sebuah informasi tidak boleh diubah, baik ditambah maupun dikurangi informasi tersebut kecuali atas izin dari pihak yang memiliki kewenangan.

c. Authentication

Aspek authentication, mensyaratkan ketika pengiriman suatu informasi bisa untuk diidentifikasi dengan baik dan benar serta memberikan jaminan bahwa indentitas yang diperoleh adalah benar atau tidak palsu.

d. Availability

Aspek yang ke 4 ini berkaitan dengan ketersediaan informasi. Sesuatu yang dibutuhkan oleh pengguna layanan teknologi informasi haruslah dapat dipenuhi sehingga tingkat ketersediaan informasi dapat.

Berkaitan dengan aspek *security* di atas, seorang pakar *security* yang bernama W. Stallings. Juga mengemukakan pendapatnya yakni ada beberapa kemungkinan serangan yang terjadi terhadap keamanan suatu sistem informasi, yaitu *interuption, interception, modification* dan *fabrication*. Tiga serangan yaitu *interuption, modification* dan *fabrication* ini digolongkan kedalam serangn aktif. Sedangkan *interception* bisa kita golongkan kedalam bentuk serangan pasif. Dalam jenis serangan ini penyerang akan mengirim suatu aliran data ke salah satu atau kedua kelompok yang terlibat komunikasi dan akan menotong aliran data [4].

2.3 *Penetration Testing*

Berdasarkan definisi dalam modul CEH, *Penetration Testing* merupakan metode evaluasi keamanan sistem komputer atau jaringan dengan mensimulasikan serangan dari sumber yang berbahaya dan merupakan bagian dari *security* audit. Simulasi serangan yang dilakukan dibuat seperti kasus yang bisa dibuat oleh *black hat hacker, cracker,* dan sebagainya. Tujuannya adalah menentukan dan mengetahui macam – macam serangan yang mungkin dilakukan pada sistem beserta akibat yang bisa terjadi karena kelemahan sistem.

ISSN: 2686-0260
September 2019
Hal:994-1001

Dalam melakukan *penetration testing*, diperlukan analisa intensif untuk setiap kerentanan yang diakibatkan oleh kelemahan sistem. Nantinya setelah seluruh analisa selesai dilakukan, akan didokumentasikan dan diberikan kepada pemilik beserta solusi dan dampak yang dapat diakibatkan dari celah keamanan yang ada.

Hal – hal yang perlu diuji dalam *penetration testing* ada banyak, hal ini dibutuhkan untuk mengidentifikasi ancaman – ancaman utama seperti kegagalan komunikasi, *e-commerce*, dan kehilangan informasi rahasia. Selain itu ketika berhadapan dengan infrastruktur publik, seperti situs, *gateway e-mail*, akses jarak jauh, DNS, kata sandi, FTP, IIS, dan *server* situs, pengujian dilakukan pada semua perangkat keras dan lunak di sebuah sistem keamanan jaringan. Adapun faktor – faktor pendukung seperti tujuan, batasan, dan penyesuaian prosedur yang diperlukan untuk membuat *penetration testing* lebih maksimal. Selain hal tersebut diperlukan orang yang profesional untuk melakukannya serta pertimbangan biaya yang sesuai dengan kebutuhan. Pada akhirnya diperlukan juga dokumentasi yang jelas serta penjelasan mengenai potensi resiko dan hasil penemuan dari hasil analisa dan uji coba kepada klien atau pihak pengelola layanan.

3. HASIL DAN PEMBAHASAN

Pada bab ini penulis akan memaparkan dan menganalisa beberapa celah ataupun kelemahan dari sistem informasi kampus dari beberapa tahap pengujian yang dilakukan antara lain *information gatering* dan *vulnerability scanning*.

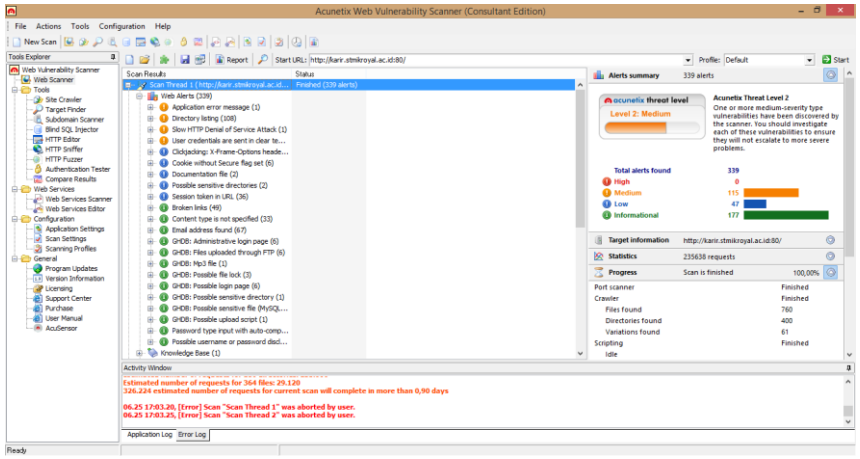
3.1. *Information Gatering*

Dengan memanfaatkan situs bantuan seperti *Domain Tools*, informasi mengenai sejarah sebuah domain akan tercantum dan dilampirkan dalam format *Whois*, dimana informasi seperti tanggal pembuatan domain, nama pemilik domain dan informasi sederhana seperti jenis *server* yang digunakan, lokasi dan alamat *IP Address* akan terlampir didalamnya.

3.2. *Vulnerability Scanning*

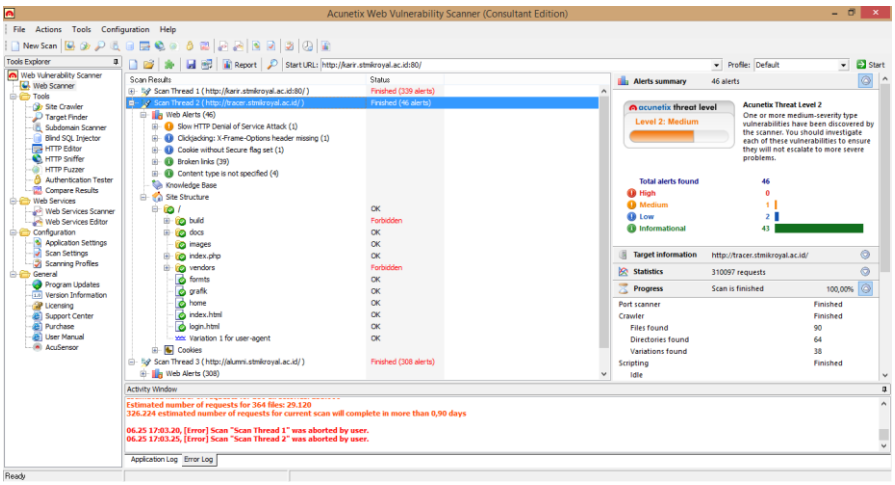
Di dalam mendeteksi kerentanan pada penelitian ini menggunakan *Acunetix* untuk mengetahui celah keamanan yang ada di aplikasi berbasis *website*. Dimana pengembangan aplikasi *website* pada sistem inforamasi kampus yang sudah dibagun menggunakan PHP dan *Wordpress* sebagai *platform web aplication development*. Pada gambar 2 merupakan tampilan hasil scanning menggunakan *tools acunetix web vulnerability scanner.*

ISSN: 2686-0260
September 2019
Hal:994-1001



Gambar 2. Hasil Scaning dengan *Tools Acunetix Web Vulnerability Scanner* Pada Domain 1

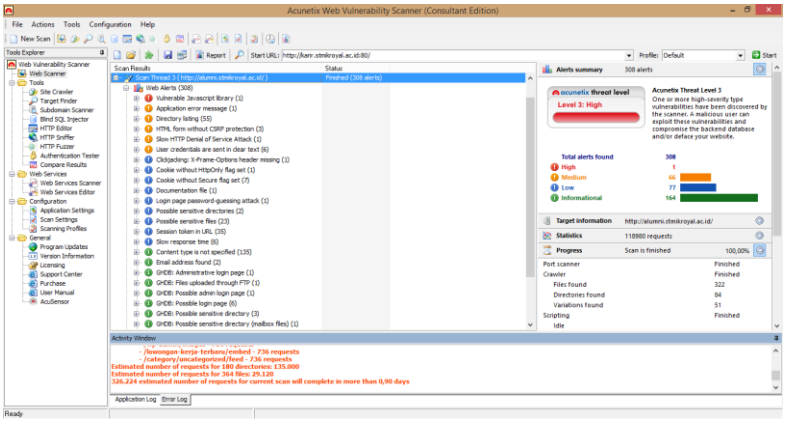
Pada gambar 2 merupakan hasil *scanning* dilakukan pada Domain 1. Berdasarkan *scanning* yang dilakukan pada domain 1 untuk level kerentanan adalah medium dan *web allert* 339 diantara kemungkinan bentuk serangan yang akan terjadi berdasarkan hasil penetrasi dengan metode *web scanning* antara lain *Denial of Service Attack* (Level Medium) dan *Clickjacking (Level Low)*. Selanjutnya pada Gambar 3 akan menampilkan hasil scanning pada domain yang kedua dari sistem informasi kampus yang di testing.



Gambar 3. Hasil Scaning dengan Tools Acunetix Web Vulnerability Scanner Pada Domain 2

Pada gambar 3 merupakan hasil yang didapat dari tahapan *web scanning* dengan *tools Acunetix* pada Domain 2. Dimana pada *penetration testing* pada domain yang kedua ini untuk tingkat kerentanan yang diperoleh adalah medium dengan *web allert* sebanyak 46, serta kemungkinan serangan yang dapat terjadi diantaranya adalah *Denial of Service* (level Medium) dan *Clickjacking* (level *Low*). Selanjutnya pada gambar 4 dapat dilihat hasil temuan kelemahan pada pada domain lainnya.

ISSN: 2686-0260
September 2019
Hal:994-1001



Gambar 4. Hasil *Scaning* dengan *Tools Acunetix Web Vulnerability Scanner* Pada Domain 3

Pada gambar 4 telah didapatkan hasil dari vulnerability scanning terhadap aplikasi web pada domain 3, dimana pada domain ke 3 ini untuk level kerentanan adalah high dengan web allert 308 dengan temuan celah kemanan antara lain *Vulnerabel Javascript liblary* (*Level High*), CSRF/*Cross-site request forgery* (Level Medium), Dos (level Medium) dan *Clickjacking (level Low).* Berikut pada Tabel 1 akan ditunjukkan daftar keseluruhan celah kerentanan pada sistem informasi kampus.

Tabel 1. Celah Keamanan Yang Ditemukan

Domain	**Kerentanan**
Domain Pertama (Level *Threat* Medium)	*Application Error Message* *Directory Listing* *Slow HTTP Denial of Service Attack* *User Credentials are Sent in Clear Text* *Clickjacking X Frame Option Header Missing* *Cookie Without Secure Flag Set*
Domain Kedua (Level *Threat* Medium)	*Slow HTTP Denial of Service Attack* *Clickjacking X Frame Option Header Missing* *Cookie Without Secure Flag Set*
Domain Ketiga (Level *Threat High*)	*Vulnerable Javascript Library* *Application Error Message* *Directory Listing* *HTML Form Without CSRF Protection* *Slow HTTP Denial of Service Attack* *User Credentials are Sent in Clear Text* *Clickjacking X Frame Option Header Missing* *Cookie Without Secure Flag Set* *Login Page Password Guessing Attack* *Slow Response Time*

4. KESIMPULAN

ISSN: 2686-0260
September 2019
Hal:994-1001

Tidak ada sistem yang benar-benar aman dan sempurna di dunia *cyber*. Sebagai seorang *web programmer* maupun *server* administrator hanya bisa mengupayakan untuk mengamankan *web server* dengan semaksimal mungkin dan mengurangi risiko-risiko terjadinya celah kerentanan yang bisa dimasuki oleh *hacker.* Berdasarkan hasil pengujian dengan melakukan *penetration testing* terhadap 3 domain yang berbeda, terdapat dua domain yang threat levelnya medium dan satu domain yang threat levelnya adalah high. Pada pengujian ini juga telah di temukan beberapa celah kelemaahan atau kerentanan pada sistem informasi kampus yang bisa saja nantinya digunakan untuk memanipulasi file lokal, mengganggu kenerja dari server itu sendiri dengan teknik DoS , melakukan *clickjacking* serta melakukan CSRF/*Cross-site request forgery.* Hasil temuan ini akan peneliti jadikan sebagai bahan masukan kepada pihak pengelola sistem informasi kampus untuk segera melakukan perbaikan terhadap kelemahan *(Vulnerability)* tersebut.

Proses *penetration testing* yang peneliti gunakan masih sangat memungkinkan untuk dilakukan kembali secara lebih mendalam dan menggunakan metode yang berbeda maupun tools bantu yang lainnya supaya dapat memperoleh hasil pengujian keamanan yang lebih detal lagi.

DAFTAR PUSTAKA

[1] Babys, J. Y, "Analisis Vulnerable Port Pada Client Pengguna Publik Wifi" *Simetris: Jurnal Teknik Mesin, Elektro Dan Ilmu Komputer.*, *9*(1), 261–268, https://doi.org/10.24176/simet.v9i1.2073, 2018.

[2] Bogdanoski M, Shuminoski T dan Risteski A, "Analysis of The SYN Flood DoS Attack" I.J Computer Network and Information Security., No 8, Hal 1-11, DOI: 10.5815/ijenis.2013.08.01, 2013.

[3] Maharani, M. Z., Andrian, H. R., Juli, S., & Ismail, I, "Analisis Keamanan Website Menggunakan Metode Scanning Dan Perhitungan Security Metriks" *E-Proceeding of Applied Science.*, *3*(3), 1775–1782, 2017.

[4] Prabhakar, Shruthi, "Network Security in Digitalization Attacks and Defence" International Journal of Research in Comoputer Application and Robotics., Vol 5, Issue 5, Hal 46-52., 2017.

[5] Shahriar, H., Devendran, V. K., & Haddad, H, "*ProClick: A Framework for Testing Clickjacking Attacks in Web Applications"* 144–151. https://doi.org/10.1145/2523514.2523538, November 2013

[6] Syariful Ikhwan, & Elfitri, I, "Analisa Delay yang Terjadi Pada Penerapan Dimilitarized Zone (DMZ) Terhadap Server Universitas Andalas" *Nasional Teknik Elektro* Jaringan., 118–124, 2014.

[7] Tarigan, B. V., Kusyanti, A., & Yahya, W, "Analisis Perbandingan *Penetration Testing Tool* Untuk Aplikasi Web" *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer (J-PTIIK) Universitas Brawijaya.*, *1*(3), 206–214, 2017.

[8] W, Ynanri., Riadi, Imam., & Yudhana Anton, "Analisis Deteksi Vulnerability Pada Webserver Open Jurnal System Menggunakan OWASP Scanner" JURTI., Vol.2 No. 1, Juni 2018.