MEKANISME KEAMANAN DAN EVALUASI SITUS TERHADAP SERANGAN *CROSS-SITE SCRIPTING* (XSS) BERDASARKAN *BASE METRIC* CVSS V.2

Ahmad Sultan Hakim[1], Triawan Adi Cahyanto[2], Habibatul Azizah[3].
Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Jember
Email = hakimsultan73@gmail.com

ABSTRAK

Situs adalah sebuah layanan di suatu domain internet yang terdiri dari 1 atau lebih halaman yang dapat diakses oleh orang di dunia maya. Situs bisa rentan terhadap serangan – serangan yang terjadi pada sistem keamanannya, masalah keamanan ini sering tidak mendapat perhatian bahkan terabaikan. Penelitian ini membuat mekanisme keamanan pada situs blog dan SIA MAN 1 Jember. Ketika client mengakses situs asli dibuatlah mekanisme keaanan dengan cara mengarahkan ke situs tiruan. Uji coba mekanisme keamanan dilakukan dengan cara mencari berapakah total serangan yang lolos pada situs asli, dengan melakukan serangan xss sebanyak 16 kali pada situs tiruan. Penelitian ini juga mengevaluasi tingkat kelemahan situs terhadap serangan xss berdasarkan perhitungan metrik keamanan bertipe CVSS versi 2 dengan kategori kelompok base metric. Evaluasi ini untuk mencari berapakah level kerentanan situs terhadap serangan xss berdasarakan skenario uji yang diberlakukan. Metode untuk mekanisme keamanan menggunakan mikrotik dengan mengkonfigurasi firewall sedangkan dalam evaluasi situs menggunakan perhitungan CVSS v.2 dengan kategori kelompok base metric. Hasil pengujian mekanisme keamanan dapat menahan serangan xss sejumlah 16 kali serangan dan tidak mempengaruhi kinerja situs asli. Hasil evaluasi situs didapatkan untuk situs blog level tertinggi adalah medium dengan nilai base score 4,758. Sedangkan situs SIA MAN 1 Jember level tertinggi adalah high dengan nilai base score 7,042.

Kata Kunci: Situs, Mekanisme Keamanan, *Cross Site Scripting, Firewall, CVSS, Base Metric*.

ABSTRACT

Site is a service on an internet domain consisting of 1 or more pages that can be accessed by people in cyberspace. The site can be vulnerable to attacks that occur on its security system, this security problem often does not get attention even ignored. This research made a security mechanism on the blog site and SIA MAN 1 Jember. When the client accesses the original site, a security mechanism is created by directing it to the artificial site. The security mechanism testing is carried out by finding out how many total attacks have passed on the original site, by carrying out xss attacks 16 times on artificial sites. This study also evaluates the weakness level of the site against xss attacks based on the security metrics calculation of type CVSS version 2 with the base metric group category. This evaluation is to find out what is the level of site vulnerability to xss attacks based on the test scenario that is applied. The method for security mechanisms uses a proxy by configuring a firewall while in site evaluation it uses the CVSS v.2 calculation with the base metric group category. The testing security mechanism results can withstand xss attacks 16 times and do not affect the performance of the original site. Site evaluation results obtained for the highest level blog site is medium with a base score of 4.758. While SIA MAN 1 Jember site's highest level is high with a base score of 7.042.

Keywords: *Site, Security Mechanism, Cross Site Scripting, Firewall, CVSS, Base Metric*.

1. Pendahuluan

Pada era sekarang internet sudah bukan menjadi hal baru atau asing, dari anak kecil sampai orang tua pun sudah mengetahui, *website* atau situs yang merupakan salah satu bagian dari internet juga telah menjadi bagian bagi manusia, karena *website* dapat menyediakan sebuah informasi yang dapat dijangkau dengan mudah bagi yang memiliki akses layanan internet.

Website adalah sebuah layanan di suatu domain internet yang terdiri dari 1 atau lebih halaman untuk tujuan tertentu yang dapat diakses oleh orang di dunia maya (Waryanto, 2018). Namun sebuah *website* bisa juga rentan terhadap serangan – serangan yang terjadi pada sistem keamanan yang ada pada sebuah *website*, jikalau *website* tidak mempunyai sistem keamanan atau sistem keamanan yang dimiliki *website* itu lemah maka ancaman dapat terjadi sewaktu waktu. Masalah keamanan ini sering tidak mendapat perhatian dari pengelola sistem informasi bahkan kadang terabaikan dan bahkan berada di urutan kedua atau urutan terakhir dari daftar hal hal yang dianggap penting (Ariyus, 2009).

Celah yang terdapat pada sistem disebut dengan vulnerability yaitu suatu celah pada sistem yang menyebabkan terjadinya orang lain yang masuk dengan mengexploitasi sistem tersebut. Maka dari itu perlu adanya sistem sebagai peringatan dini ketika situs yang dimiliki diserang oleh peretas.

Masalah yang terdapat pada penelitian ini yaitu bagaimana membuat mekanisme keamanan system *serve*r sehingga penanganan berada di awal bukan lagi di belakang menunggu system rusak atau dieksploitasi, maka di sini peneliti akan membuat sebuah mekanisme keamanan dimana apabila seseorang mengaskses situs asli yang akan diserang namun oleh *serve*r asli akan diarahkan pada situs palsu namun berisi hal yang sama.

Cross-site *script*ing atau disebut xss, salah satu teknik serangan pada *website* ini yaitu xss merupakan serangan yang dilakukan pada *website* yang tidak perlu melakukan sebuah validasi dan sanitasi (Syaifuddin, Diah dan Hanugra. 2018), peretas dapat memanfaatkan hal itu dengan memasukan sebuah kode atau *script* yang dikirimkan pada *serve*r, salah satu *script* tersebut bila bekerja dapat mem-bypass akun serta keamanan.

Intrusion Detection System (IDS), Menurut Onno Purbo(2010), IDS adalah usaha untuk mengidentifikasi adanya peretas yang memasuki sistem tanpa adanya hak akses atau totrisasi (misal cracker) atau seorang pengguna yang legal namun sumberdaya sistemnya di salah gunakan. IDS dalam penelitian ini akan digunakan sebagai pendeteksi serangan xss.

Selain itu untuk penelitian ini juga mengevaluasi tingkat kelemahan situs terhadap serangan xss dengan mengukur seberapa besar dampak serangan xss pada *website* dengan perhitungan metrik keamanan yang merupakan pengukuran kuantitatif untuk menilai tingkat kelemahan suatu situs dan untuk membuat keputusan tentang berbagai aspek keamanan. Perhitungan yang dipakai yaitu berdasarkan perhitungan metrik keamanan bertipe CVSS (Common Vulnerability Scoring System) versi 2 dengan kelompok base metric. Base metric ini hasilnya dapat menunjukkan base score, base score inilah yang menjadi acuan tingkat dampak serangan dari kelemahan sebuah situs apakah *low*, *medium*, bahkan *high* dengan rentang nilai 0-10. Penentuan base score tentunya terdapat perhitungan di dalamnya, perhitungan tersebut ditentukan dari beberapa variabel penentu tingkat vulnerability, untuk itu penelitian kali juga akan meneliti bagaimana nilai base score tersebut dihasilkan untuk menentukan seberapa besar kerentanan situs terhadap serangan xss.

Situs yang digunakan pada penelitian ini adalah situs berjenis blog dan situs sistem informasi akademik MAN 1 Jember, dua situs yang memiliki karakteristik berbeda sehingga diharapkan dapat

memunculkan hasil dan dampak yang berbeda. Pada situs blog hanya menampilkan sebuah informasi berupa artikel dan fitur komentar dan siapapun dapat mengaksesnya, pada situs sistem informasi akademik menampilkan sebuah informasi akademik berupa nilai siswa, jadwal siswa, profil siswa dll, dan untuk mengaksesnya harus mempunyai hak akses seperti guru atau siswa maka apabila seseorang yang tidak berhak mengakses namun dapat masuk sebagai *admin* yang diakibatkan adalah dapat merubah semua isi tabel pada *database*.

2. Tinjauan Pustaka

2.1 *Website*

Website adalah sebuah layanan di suatu domain internet yang terdiri dari 1 atau lebih halaman untuk tujuan tertentu yang dapat diakses oleh orang di dunia maya (Waryanto, 2018). World Wide Web (WWW) adalah suatu program yang ditemukan oleh Sir Timothy Jhon Tim Berners-Lee pada tahun 1991 (Hidayatullah dan Khairul, 2017). Awalnya Berners-Lee hanya ingin bagaimana menemukan suatu cara untuk memudahkan menyusun arsip – arsip risetnya. Maka dari itu Berners-Lee mengembangkan suatu sistem untuk keperluan pribadinya. Sistem yang dikembangkan adalah software yang bernama Enquire. Dengan sistem tersebut Berners-Lee berhasil menciptakan jaringan yang dapat menautkan arsip – arsip riset sehingga memudahkan dirinya ketika ingin mencari sebuah informasi yang diinginkan. Sehingga hal inilah yang menjadi dasar atau awal terbentuknya *website* yang sekarang sudah berkembang pesat.

2.2 Masalah Keamanan

Masalah kemanan menjadi aspek yang paling penting dari sebuah sistem multimedia, masalah keamanan sering dianggap sepele dan kurangnya perhatian dari perancang sistem multimedia (Ariyus, 2009).

Sangat fatal apabila sistem informasi yang didalamnya terdapat rahasia tercuri. untuk itu keamanan dari sistem informasi ini harus dijaga dan diperhatikan betul untuk mencegah terjadinya kejahatan komputer.

2.3 Mikrotik

Mikrotik adalah perangkat yang digunakan untuk *router network* dengan sitem operasi linux base, untuk menggunakannya biasanya bisa melalui aplikasi bernama winbox.

. Mikrotik didesain khusus untuk memudahkan pengguna dalam berbagai keperluan jaringan komputer seperti rancang bangun sistem jaringan dari skala kecil hingga kompleks, fitur mikrotik juga dibilang banyak sehingga tambah mempermudah penggunanya. Fiturnya meliputi Ipsec, caching DNS client, routing static, *firewall* dan NAT, web proxy, UpnP, SNMP, MNDP, monitoring atau accounting, tools dan masih banyak fitur lainnya.

2.4 *Cross-Site Scripting* (XSS)

Cross-Site *Script*ing (XSS) merupakan kejahatan keamanan *website* dengan memanfaatkan celah keamanan pada form *input website*(Fogie, Grossman, Hansen, Rager, DAN Petkov. 2007). Ketika penyerang menemukan sebuah celah xss pada sebuah *website* , penyerang akan memanfaatkan hal tersebut dengan memasukan sebuah *script* salah satunya untuk menjebak korban yang apabila korban masuk pada jebakan tersebut maka *website* dapat diambil alih kendali.

Serangan xss terbagi dalam 2 kategori, diantaranya:

1. *Persistent*

Serangan ini biasanya disebut dengan *stored* xss, biasanya ditemukan pada halaman situs dimana client di ijinkan memasukan *script* contohnya pada halaman kotak pencarian (Wang dkk. 2007, 2011, Van-Acker dkk. 2012).

2. *Non-persistent*

Serangan XSS ini biasanya disebut *reflected* XSS, serangan dimana penyerang dapat memasukan *script* yang dapat

disimpan pada *database* sebuah situs, di mana *script* yang dimasukkan dikembalikan ke *serve*r aplikasi web korban contohnya tampilan kesalahan pesan yang dapat ditampilkan pada browser client lain (Avancini and Ceccato 2011, Athanasopoulos dkk. 2010).

2.5 IDS

Menurut Onno Purbo(2010), IDS adalah usaha untuk mengidentifikasi adanya peretas yang memasuki sistem tanpa adanya hak akses atau totrisasi (misal cracker) atau seorang user yang legal namun sumberdaya sistemnya disalah gunakan. IDS adalah aplikasi atau program yang mampu mendeteksi adanya gangguan maupun serangan pada sistem jaringan. Pada saat ini ada beberapa IDS yang umum digunakan pada jaringan, salah satunya adalah snort.

2.6 *CVSS V.2*

Common vulnerability scoring system atau disingkat CVSS merupakan bentuk perhitungan untuk mengkomunikasikan karakteristik dan dampak kerentanan TI. CVSS terdiri dari 3 kelompok: Base metric, temporal metric dan environmental metric. Setiap kelompok menghasilkan skor numerik mulai dari 0 hingga 10. Kelompok base metric mewakili kualitas intrinsik kerentanan. Kelompok temporal metric mencerminkan karakteristik kerentanan yang berubah seiring waktu. kelompok environmental metric mewakili karakteristik kerentanan yang unik untuk lingkungan pengguna mana pun.

2.7 *Base Metric*

Base metric merupakan salah satu kelompok metrik dalam CVSS. Terdapat 6 parameter untuk menentukan peringkat atau nilai kerentanan dan hasil akhir dari base metric adalah base score. *Access vector*, *access complexity*, dan *authentication* menangkap bagaimana kerentanan diakses dan apakah diperlukan kondisi tambahan untuk mengeksploitasinya. *confidentiality impact*, *integrity impact*, dan *availability impact* merupakan nilai dampak yang diakibatkan dari sebuah vulnerability terhadap sistem. Hasil akhir dari metrik base akan menghasilkan base score serta nilai tingkat kerentanan terhadap kelemahan sistem, parameter dan deskripsi disesuaikan sesuai sumber pada jurnal “A *Complete* Guide to the Common Vulnerability Scoring System Version 2.0”.

Berikut nilai setiap kategori untuk menentukan nilai setiap parameternya:

1. *Access vector*

Metrik ini menggambarkan bagaimana kerentanan dieksploitasi dengan melihat akses jaringan yang dipakai. Dalam hal ini ada 3 kategori dalam menentukan nilai *access vector* sesuai panduan cvss v.2 yaitu *local*, *adjacent network* dan *network*. Apabila akses penyerang adalah *local* maka nilainya 0,395 jika *adjacent network* nilainya 0,646 jika *network* maka nilainya 1.

2. *Access complexity*

Metrik ini mengukur kompleksitas serangan yang dibutuhkan untuk mengeksploitasi kerentanan saat penyerang mendapatkan akses ke sistem target. Terdapat 3 kategori dalam menentukan nilai *access complexity* sesuai panduan cvss v.2 yaitu *low*, *medium* dan *high*. Apabila penyerang tidak menggunakan hak akses khusus maka dikategorikan *low* dengan nilai 0,35, apabila menggunakan hak akses agak khusus maka dikategorikan *medium* dengan nilai 0,61, apabila menggunakan hak akses khusus seperti penyerang harus mampu masuk sebagai *admin* terlebih dahulu maka dikategorikan *high* dengan nilai 0,71.

3. *Authentication*

Metrik ini mengukur berapa kali penyerang membutuhkan autentikasi untuk dapat mengeksploitasi sistem target. Dalam menentukan nilai autentikasi terdapat 3 kategori yaitu *none* jika penyerang masuk tanpa autentikasi dan nilainya 0,45, *single* jika penyerang masuk dengan 1 kali autentikasi dan nilainya 0,56, *multiple* jika penyerang mengharuskan 2 bahkan lebih autentikasi untuk masuk ke sistem target dan nilainya 0,704.

4. *Confidentiality impact*

Metrik ini mengukur dampak dari kerahasiaan saat penyerang berhasil mengeksploitasi. Terdapat 3 kategori dalam menentukan nilai dampak kerahasiaan yaitu *complete* jika banyak bahkan semua kerahasiaan terungkap dan nilainya 0,660, *partial* jika hanya sebagian kerahasiaan terungkap dan nilainya 0,275, *none* jika tidak ada kerahasiaan yang terungkap dan nilainya 0.

5. *Integrity impact*

Metrik ini mengukur dampak dari integritas, integritas mengacu pada sebuah kebenaran dan kepercayaan informasi yang sesuai dan terjamin. Terdapat 3 kategori dalam menentukan dampak integritas yaitu *complete* jika penyerang mampu merubah banyak hingga semua informasi yang ada dalam sistem dan nilainya 0,660, *partial* jika penyerang hanya sebagian dapat memodifikasi informasi dalam sistem dan nilainya 0,275, *none* jika penyerang tidak dapat memodifikasi informasi yang ada dalam sistem dan nilainya 0.

6. *Availability impact*

Serangan yang memakai bandwitch jaringan, siklus prosesor, serta ruang disk untuk mempengaruhi ketersediaan sebuah sistem. Terdapat 3 kategori dalam menentukan available *impact* yaitu *complete* jika penyerang mampu membuat sistem kehilangan sumber daya sehingga tidak dapat diakses dan nilainya 0,660, *partial* jika penyerang hanya membuat sistem mengalami penurunan kinerja sistem dan nilainya 0,275, *none* jika penyerang tidak mampu membuat sistem mengalami gangguan apapun dan nilainya 0.

2.7.1 *Base score*

Maka setelah nilai parameter ditentukan rumus, untuk menghitung nilai *base metric* sebagai berikut:

Base Score =(0,6**Impact*+0,4* *Exploitability*-1,5)**f(Impact)*

Impact = 10,41* (1 - (1 - *ConfImpact)* * *(1 - IntegImpact)* * *(1 – AvailImpact))*

Exploitability = 20**AccessComplexity* * *Authentication * AccessVector*

f(Impact) = 0 *if Impact*=0; 1,176 *otherwise*

Sumber: https://www.first.org/cvss/v2/guide

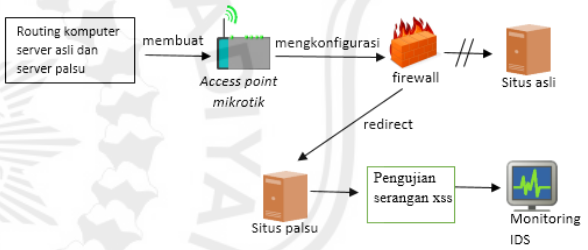
Berikut nilai tingkat kerentanan bila diukur menggunakan cvss v.2:

Tabel 2.7 Tabel nilai kerentanan

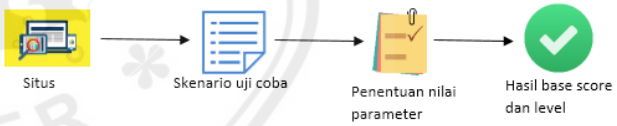
Level	*Basescore range*
Low	0 – 3,9
Medium	4 – 6,9
High	7 – 10

Sumber: https://nvd.nist.gov/vuln-metrics/cvss

3. Metode Penelitian



Gambar 3.1 Alur mekanisme kemanan



Gambar 3.2 Alur evaluasi situs

Alur pertama yaitu melakukan mekanisme keamanan situs. dengan menyiapkan sebuah situs yang dapat dieksploitasi oleh serangan xss, terdapat dua situs uji coba dalam penelitian ini yaitu situs blog dan situ sistem informasi akademik (SIA), mempersiapkan komputer untuk situs *server* asli dan komputer untuk situs palsu, melakukan konfigurasi mikrotik untuk menghubungkan komputer *server* situs asli dengan komputer *server* situs palsu dan membuat access point, konfigurasi firewal yang terdapat pada mikrotik agar saat client mengakses situs asli akan diarahkan ke situs palsu namun memiliki isi yang sama, penyerang

akan melakukan exploitasi dengan serangan berupa xss sebanyak 16 serangan dengan parameter berbeda, memasangkan software IDS pada *server* palsu untuk memberi sebuah peringatan sekaligus memastikan bahwa penyerang berada di situs palsu

Tabel 3.1 contoh *script* serangan xss skenario uji mekanisme keamanan

No	*Script*
1	<*script*>alert('XSS')</*script*>
2	<img src=x onerror=alert(String.fromCharCode(88,83,83));>
3	MOVE HERE
...	
16	<meter value=2 min=0 max=10 onmouseover=alert(1)>2 out of 10</meter>

Alur kedua yaitu melakukan evaluasi situs terhadap serangan xss, evaluasi disesuaikan dengan sknario uji yakni dengan 4 skenario uji pada masing – masing situs, dan dari skenario uji tersebut ditentukan parameter agar dapat menghitung serta menghasilkan base score. Berikut tabel skenario pada masing – masing situs:

Tabel 3.2 skenario uji untuk evaluasi

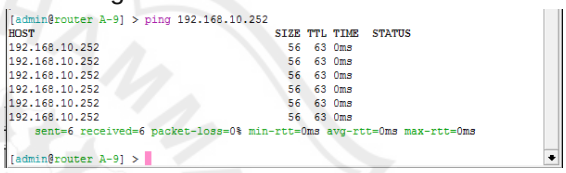
No.	Topologi jaringan	Tipe serangan xss
1.	Jaringan antar kabel	Serangan berupa *alert*
2.	Jaringan antar kabel	Serangan *bypass cookie*
3	Jaringan dengan koneksi *wifi* yang sama	Serangan berupa *alert*
4	Jaringan dengan koneksi *wifi* yang sama	Serangan *bypass cookie*

4. Hasil

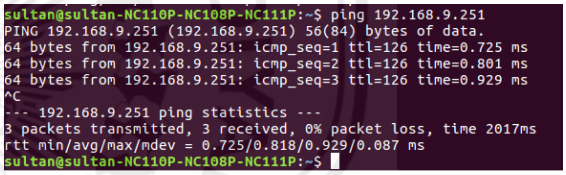
4.1 Mekanisme Keamanan

4.1.1 Hasil Routing

Routing dilakukan dengan menggunakan 2 buah *router* yakni *router* A dan *router* B serta menggunakan 2 komputer yakni komputer A sebagai *server* situs asli dan komputer B sebagai *server* situs palsu. Setelah dikonfigurasi serta melakukan routing maka hasilnya komputer A dan komputer B saling terhubung.



Gambar 4.1 Ping komputer A ke komputer B

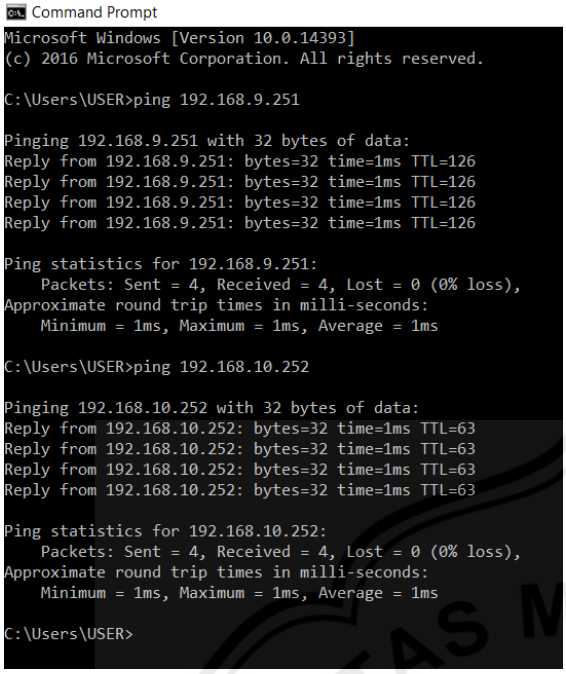


Gambar 4.2 Ping komputer B ke komputer A

4.1.2 Hasil Membuat *Access Point*

Acces point dalam jaringan komputer berguna untuk membuat sebuah layanan jaringan nirkabel dengan istilah *wirelless area network* (WAN), pada penelitian kali ini access point digunakan sebagai akses client agar dapat mengakses situs penelitian. Dalam konfigurasinya access point akan di aktifkan pada *router* B dengan menghidupkan wirelles.

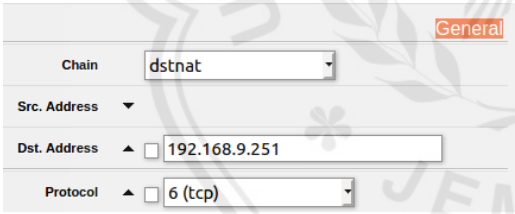
pada *router* A harus melakukan routing pada access point agar client access point dapat terhubung pada semua *router* serta komputer *server* situs. Berikut hasil apabila konfigurasi access point berhasil:



Gambar 4.3 hasil client dapat ping ke semua komputer

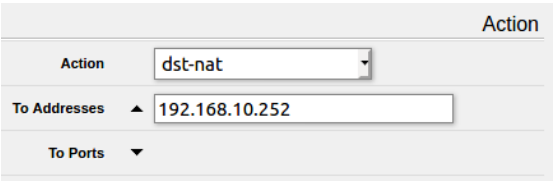
4.1.3 Hasil Konfigurasi *Firewall*

Pada saat client mengakses situs yang berapa pada ip komputer A akan diarahkan pada ip komputer B perlu dilakukan konfigurasi *firewall* pada mikrotik. Konfigurasi dilakukan pada menu NAT yang ada pada *firewall router* B, Berikut gambar konfigurasinya



Gambar 4.4 setelan *general* NAT *firewall*

Pada *general* NAT, chain yang digunakan adalah dstnat dengan Dst. Address berisikan alamat ip komputer A dan protocol yang dipakai adalah tcp karena aplikasinya digunakan dalam http serta https.



Gambar 4.5 Setelan *action* NAT *firewall*

Pada *action* NAT, *action* yang digunakan adalah dst-nat dengan tujuan alamat ip komputer B. Maka dengan konfigurasi seperti ini sebagai pengatur client saat mengakses situs asli dengan ip komputer A akan diarahkan pada situs palsu, apabila client ingin mengeksploitasi situs maka yang dieksploitasi adalah situs palsu sehingga situs asli tetap aman.

4.1.4 Hasil Skenario Uji Serangan XSS Pada Mekanisme Keamanan

Pada situs palsu serangan xss sebanyak 16 parameter serangan berhasil dimasukan dan situs palsu mengalami gangguan, disaat situs palsu mengalami gangguan maka konfigurasi firewal di nonaktifkan hasilnya situs asli yang terjadi adalah tidak mengalami gangguan.

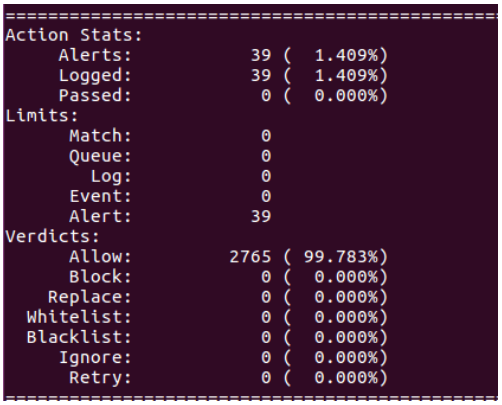
4.1.5 Hasil IDS Snort

Snort tidak memiliki rule bawaan untuk mendeteksi serangan xss, untuk dapat mendeteksi serangan xss maka diberikan rule yang dapat mengandung *script* berbahaya sesuai isi dari payload xss.

Tabel 4.1 Contoh r*ule* snort untuk mendeteksi serangan xss.

RULES
alert tcp any any -> $HOME_NET 80 (msg:"XSS attempt: XSS detected (*script*) "; f*low*:to_*server*, established; content: "*script*"; classtype:attempted-*admin*;sid:10000004; rev:004;)

Dengan snort menampilkan pesan peringatan menandakan *rule* yang terpasang berhasil memberi peringatan adanya serangan xss berdasarkan parameter yang sudah ditentukan. Berikut laporan hasil peringatan snort:



Gambar 4.31 laporan hasil snort

4.2 Evaluasi Situs

4.2.1 Situs Blog

Situs blog pada penelitian ini memang dibuat sebagai bahan uji coba serangan xss, dalam skenario serangan pada situs ini dilakukan pada form *input* pesan yang ada pada halaman *guestbook* dengan jenis serangan non-*persistent* atau reflected xss.

4.2.1.1 Hasil Skenario Pertama

Hasil yang diperoleh dari skenario pertama dengan topologi jaringan antar kabel dan serangan berupa *alert*:
Access vector = local
Access complexity = low
Authentication =none
confidentiality impact = none
integrity impact = partial
availability impact = partial

base score = 3,578
level = low

4.2.1.2 Hasil Skenario Ke-dua

Hasil yang diperoleh dari skenario kedua dengan topologi jaringan antar kabel dan serangan berupa *bypass cookie*:
Access vector = local
Access complexity = low
Authentication = none
confidentiality impact = partial
integrity impact =none
availability impact = none

base score = 2,113
level = low

4.2.1.3 Hasil Skenario Ke-tiga

Hasil yang diperoleh dari skenario ketiga dengan topologi jaringan *wifi* yang sama dan serangan berupa alert:
Access vector = adjacent network
Access complexity = low
Authentication = none
confidentiality impact = none
integrity impact = partial
availability impact = partial

base score = 4,758
level = medium

4.2.1.4 Hasil Skenario Ke-empat

Hasil yang diperoleh dari skenario keempat dengan topologi jaringan *wifi* yang sama dan serangan berupa *bypass cookie*:
Access vector = adjacent networl
Access complexity = low
Authentication = none
confidentiality impact = partial
integrity impact = none
availability impact = none

base score = 3,294
level = low

4.2.2 Situs SIA

4.2.2.1 Hasil Skenario Pertama

Hasil yang diperoleh dari skenario pertama dengan topologi jaringan antar kabel dan serangan berupa *alert*:
Access vector = low
Access complexity = medium
Authentication = single
confidentiality impact = none
integrity impact = partiall
availability impact = partial

base score = 2,989
level = low

4.2.2.2 Hasil Skenario Ke-dua

Hasil yang diperoleh dari skenario kedua dengan topologi jaringan antar kabel dan serangan berupa *bypass cookie*:
Access vector = low
Access complexity = medium

Authentication = single
confidentiality impact = complete
integrity impact =complete
availability impact = partial

base score = 6,235
level = medium

4.2.2.3 Hasil Skenario Ke-tiga

Hasil yang diperoleh dari skenario ketiga dengan topologi jaringan *wifi* yang sama dan serangan berupa alert:
Access vector = adjacent network
Access complexity = medium
Authentication = single
confidentiality impact = network
integrity impact = partial
availability impact = partial

base score = 3,797
level = Low

4.2.2.4 Hasil Skenario Ke-empat

Hasil yang diperoleh dari skenario keempat dengan topologi jaringan *wifi* yang sama dan serangan berupa bypass cookie:
Access vector = adjacent network
Access complexity = medium
Authentication = single
confidentiality impact = complete
integrity impact =complete
availability impact = partia

base score = 7,042
level = high

5. Kesimpulan dan Saran

5.1 Kesimpulan

1. Penggunaan firewal dapat dijadikan solusi untuk mengelabuhi client pada saat mengakses situs asli ke situs palsu.
2. Hasil dari mekanisme keamanan yang sudah diterapkan dapat menahan serangan xss sejumlah 16 serangan dengan parameter berbeda, sedangkan serangkaian serangan dari situs palsu tidak mempengaruhi kinerja situs yang asli..
3. Level kerentanan pada situs blog terendah *low* dengan nilai base score 2,113 dan tertinggi *medium* dengan nilai base score 4,758.
4. Level kerentanan pada situs sia man 1 jember terendah *low* dengan nilai base score 2,989 dan tertinggi *high* dengan nilai base score 7,042.
5. Dengan ini cvss v.2 dan kelompok metrik base metric dapat dijadikan reverensi untuk menghitung serta menentukan level kerentanan situs terhadap serangan xss.

5.2 Saran

1. Dari serangkaian mekanisme keamanan dapat dikembangkan kembali untuk penelitian lebih lanjut dalam mekanisme keamanan vulnerability yang lain.
2. Dalam membuat situs perlu diperhatikan dalam membuat form *input*, disarankan untuk menggunakan source code yang dapat meng-encode semua tag html dan special karakter.
3. Untuk penelitian lebih lanjut mengenai cvss dapat dilakukan penelitian lain dengan vulnerability yang lain dan dengan membandingkan cvss versi lain serta kelompok metrik yang lain.

6. Daftar Pustaka

Hidayatullah, dan jauhari khairul. 2017. Pemograman WEB Edisi Revisi. Bandung:INFORMATIKA

Ariyus, Renati(ed). 2009. Keamanan Multimedia. Yogyakarta: ANDI Darmawan,Deden Hendra, dan Nita(ed). 2016. Desain dan Pemograman *Website*. Bandung:PT Remaja Rosdakarya Offset

Robby. 2013. “Analisis Web Vulnerability pada Portal Pemerintahan Kota Palembang Menggunakan Acunetix Vulnerability”. Universitas Bina Darma. Palembang, Indonesia.

Moazzam. 2013. “Security Metric Based *Network* Risk Assessment”. Georgia Institute of Technology. Atlanta, Georgia, Amerika Serikat.

Zattu Mia. 2017. “Analisis Keamanan *Website* Menggunakan Metode Scanning Dan Perhitungan Security Metrik”. Universitas Telkom. Bandung, Indonesia.

Mell, Scarfone, dan Romanosky. 2007. A *Complete* Guide to the Common Vulnerability Scoring System, di

https://www.first.org/cvss/v2/guide (diakses pada 25 Maret 2020).

Alamsyah. 2011. “Implementasi Keamanan Instrusion Detection System (IDS) Dan Instrusion Prevention System (IPS) Menggunakan Clearos”. Teknik Elektro, Universitas Tadulako. Palu.

Fogie, Grossman, Hansen, Rager, and Petkov. 2007. XSS Attacks: Cross Site *Script*ing Exploits and Defense

Mulya, Beta Wahyu Retna dan Tarigan. 2018. “Pemeringkatan Risiko Keamanan Sistem Jaringan Komputer Politeknik Kota Malang Menggunakan Cvss dan Fmea”. POLITEKNIK. Malang. Indonesia.

Jayantha, Dharma, dan Firdaus. 2007. “Analisis Tingkat Kemanan Terhadap Cross-Site *Script*ing Pada Aplikasi Web Berbasis Ajax Dibandingkan Dengan Aplikasi Web Konvensional”. Universitas Telkom. Indonesia.

Syarifudin Irwan. “Pentesting dan Analisis Keamanan Web Paud Dikmas”. Jurusan Teknik Informatika dan Komputer. Politeknik Negeri Jakarta. Depok, Indonesia.

PT.Citraweb Solusi Teknologi. Penggunaan Custom Chain pada *Firewall* MikroTik di http://mikrotik.co.id/artikel_lihat.php?id=146 (diakses pada 25 Maret 2020).

PT.Citraweb Solusi Teknologi. Fitur *Router*OS di http://mikrotik.co.id/artikel_lihat.php?id=1 (diakses pada 25 Maret 2020).