

TUGAS AKHIR

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



AHMAD SULTAN HAKIM

1610651006

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER**

2020

TUGAS AKHIR

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

**Disusun untuk Melengkapi dan Memenuhi Syarat Kelulusan Progam Strata 1
Progam Studi Teknik Informatika Fakultas Teknik
Universitas Muhammadiyah Jember**



AHMAD SULTAN HAKIM

1610651006

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER**

2020

HALAMAN PERSETUJUAN

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

Oleh:

Ahmad Sultan Hakim

1610651006

Telah disetujui bahwa Laporan Tugas Akhir ini untuk diajukan pada Sidang Tugas Akhir sebagai salah satu syarat kelulusan dan mendapatkan gelar Sarjana Komputer (S.Kom)

di

Universitas Muhammadiyah Jember

Disetujui oleh:

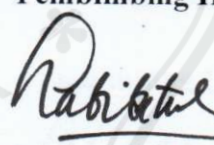
Pembimbing I



Triawan Adi Cahyanto, M.Kom.

NIDN. 0702098804

Pembimbing II



Habibatul Azizah Al Faruq, M.Pd.

NIDN. 0718128901

HALAMAN PENGESAHAN

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

Oleh:

Ahmad Sultan Hakim

1610651006

Telah mempertanggung jawabkan Laporan Tugas Akhirnya pada Sidang Tugas Akhir
tanggal 04 Juli 2020 sebagai salah satu syarat kelulusan dan mendapatkan gelar

Sarjana Komputer (S.Kom)

di

Universitas Muhammadiyah Jember

Disetujui oleh:

Dosen Penguji:

Penguji I



Agung Nilogiri, S.T., M.Kom.

NIDN. 0030037701

Dosen Pembimbing:

Pembimbing I



Triawan Adi Cahyanto, M.Kom.

NIDN. 0702098804


Penguji II



Darvanto, S.Kom., M.Kom.

NIDN. 0707077203

Pembimbing II



Habibatul Azizah Al Faruq, M.Pd.

NIDN. 0718128901

Mengesahkan,

Dekan Fakultas Teknik



Nanang Saiful Rizal, S.T., M.T.
NIDN. 0705047806

Mengetahui,

Ketua Program Studi Teknik Informatika



Triawan Adi Cahyanto, M.Kom.
NIDN. 0702098804

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

NAMA : AHMAD SULTAN HAKIM

NIM : 16 1065 1006

INSTITUSI : Strata-1 Program Studi Teknik Informatika Fakultas Teknik,
Universitas Muhammadiyah Jember.

Menyatakan bahwa Tugas Akhir yang berjudul “**Mekanisme Keamanan dan Evaluasi Situs Terhadap Serangan Cross-Site Scripting (Xss) Berdasarkan Base Metric CVSS V.2**” bukan merupakan Tugas Akhir orang lain baik sebagian maupun keseluruhan kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini dibuat dengan sebenar-benarnya dan apabila pernyataan ini tidak benar penulis bersedia mendapatkan sanksi akademik.

Jember, 04 Juli 2020

Yang Menyatakan,



Ahmad Sultan Hakim

NIM. 16 1065 1006

KATA PENGANTAR

Alhamdulillah segala puji dan syukur atas kehadiran Allah yang senantiasa memberikan rahmat dan nikmat yang sangat luar biasa dalam hidup ini kepada penulis, sehingga bisa menyelesaikan skripsi dengan judul “**MEKANISME KEAMANAN DAN EVALUASI SITUS TERHADAP SERANGAN *CROSS-SITE SCRIPTING (XSS) BERDASARKAN BASE METRIC CVSS V.2***” sebagai syarat untuk menyelesaikan Progam Strata 1 Progam Studi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember.

Atas segala upaya, bimbingan dan arahan dari semua pihak, penulis mengucapkan banyak terima kasih. Dalam kesempatan ini penulis mengucapkan terima kasih sebanyak-banyaknya kepada:

1. Allah SWT atas segala rahmat, nikmat dan hidayah-Nya, terima kasih atas kehendak-Mu telah memberikan kesempatan ini untuk mendapatkan gelar Sarjana Komputer.
2. Kepada orang tua penulis Bapak Suma'i dan Ibu Salama yang selalu mendoakan, memberikan motivasi, dukungan dan memberikan kasih sayang sehingga penulis dapat menyelesaikan tugas akhir ini. Dan tidak lupa juga untuk kakak Defi Juwita Yossianti yang telah memberikan dukungan kepada penulis.
3. Nanang Saiful Rizal, S.T., M.T., selaku Dekan Fakultas Teknik Universitas Muhammadiyah Jember.
4. Bapak Triawan Adi Cahyanto, M.Kom., selaku Ketua Program Studi Teknik Informatika Universitas Muhammadiyah Jember sekaligus menjadi pembimbing 1 yang telah meluangkan waktunya untuk memberi arahan dan membimbing penulis dalam menyelesaikan Tugas Akhir ini.

5. Ibu Habibatul Azizah Al Faruq, M.Pd., selaku dosen pembimbing II yang telah meluangkan waktu untuk memberi arahan dan membimbing penulis dalam menyelesaikan Tugas Akhir ini.
6. Bapak Agung Nilogiri, S.T., M.Kom., selaku dosen penguji 1 dan Bapak Daryanto, S.Kom., M.Kom., selaku dosen penguji II yang telah memberikan saran dan masukan dalam penyelesaian Tugas Akhir ini.
7. Kepada Bapak dan Ibu Dosen Program Studi Teknik Informatika Universitas Muhammadiyah Jember yang telah memberikan ilmunya kepada penulis.
8. Kepada Mas Wahyu laboran yang telah membantu penulis dalam melaksanakan tugas akhir.
9. Kepada Alfian Hadiyatullah yang telah membantu untuk memberikan semangat, dukungan, bantuan, nasihat, saran, dan doa ke penulis untuk menyelesaikan tugas akhir ini.
10. Kepada sahabat yang tergabung dalam HIMAJO (Himpunan Mahasiswa Jomblo) telah membantu untuk memberikan semangat, dukungan, bantuan, nasihat, saran, dan doa ke penulis untuk menyelesaikan tugas akhir ini.
11. Serta kepada teman-teman Program Studi Teknik Informatika yang telah memberikan doa, dukungan, dan bantuannya.

Dan untuk semuanya, semoga Allah menunjukkan kepada kita pada jalan yang telah diridhoi oleh-Nya, diberikan ilmu yang barokah, serta diampuni dosa-dosa kita, dan senantiasa tercurah limpahkan rahmat, taufiq dan hidayah-Nya kepada kita semua.

Aamiin... Yaa Robbal Alamiin...

Jember, 23 Juni 2020

Penulis

MOTTO

“Kuliah bukan penentu kesuksesan seseorang”

(Deddy Corbuzier)

“Bebek berjalan berbondong-bondong, akan tetapi burung elang terbang
sendirian”

(Ir. Soekarno)

“Semakin anda mencintai diri anda, semakin anda berbeda dari orang lain, yang
menjadikan anda unik”

(Walt Disney)

“Dan (ingatlah juga), tatkala Rabbbmu memaklumkan; “Sesungguhnya jika kamu
bersyukur, pasti Kami akan menambah (nikmat) kepadamu, dan jika kamu
mengingkari (nikmat-Ku), maka sesungguhnya azab-Ku sangat pedih”

(QS. Ibrahim: 7)

DAFTAR ISI

HALAMAN JUDUL	i
LEMBAR PERSETUJUAN	ii
LEMBAR PENGESAHAN	iii
ABSTRAK	iv
<i>ABSTRACT</i>	v
KATA PENGANTAR	vi
MOTTO	viii
DAFTAR ISI.....	ix
DAFTAR GAMBAR.....	xii
DAFTAR TABEL	xiv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Tujuan.....	4
1.4 Manfaat.....	4
1.5 Batasan Masalah.....	4
BAB II TINJAUAN PUSTAKA.....	5
2.1 <i>Website</i>	5
2.2 Keamanan Komputer	5
2.2.1 Masalah Keamanan.....	5
2.2.2 Aspek – Aspek Keamanan	6
2.3 Mikrotik.....	7
2.4 <i>Cross-Site Scripting (XSS)</i>	8
2.4.1 Mengetahui <i>Website</i> Dapat Diserang XSS.....	9
2.5 <i>Intrusion Detection System (IDS)</i>	11
2.5.1 Jenis IDS dan Metode IDS	12
2.5.2 Cara Kerja IDS.....	13
2.6 CVSS	14

2.6.1 CVSS V.2	14
2.6.1.1 <i>Base Metric</i>	15
2.7 Penelitian Sebelumnya	19
BAB III METODE PENELITIAN	21
3.1 Tahap Penelitian	21
3.1.1 Tahap Pengumpulan Data	21
3.1.2 Identifikasi Masalah	21
3.2 Alur Penelitian	22
3.3 <i>Software</i> dan <i>Hardware</i>	23
3.3.1 <i>Software</i>	23
3.3.2 <i>Hardware</i>	23
3.4 Situs Penelitian.....	24
3.5 Konfigurasi Mikrotik dan <i>Firewall</i>	24
3.6 Skenario Uji Serangan XSS dari Penerapan	
Mekanisme Keamanan.....	26
3.7 <i>Rules IDS Snort</i>	27
3.8 Evaluasi Situs Terhadap Serangan XSS.....	28
3.8.1 Skenario Pengujian Situs dengan Serangan XSS	28
3.8.2 Menentukan <i>Base Score</i>	29
BAB IV PEMBAHASAN DAN HASIL	34
4.1 Mekanisme Keamanan.....	34
4.1.1 Konfigurasi Mikrotik dan <i>Firewall</i>	34
4.1.1.1 <i>Routing</i> Komputer <i>Server Asli</i>	
dengan Komputer <i>Server Palsu</i>	34
4.1.1.2 Membuat <i>Access Point</i>	40
4.1.1.3 Konfigurasi <i>Firewall</i>	42
4.1.1.4 Hasil Skenario Uji Serangan XSS dari Penerapan	
Mekanisme Keamanan	46
4.1.2 Konfigurasi <i>Ids Snort</i>	49
4.2 Evaluasi Situs	52
4.2.1 Situs Blog	52

4.2.1.1 Skenario Pertama	52
4.2.1.1.1 Penentuan <i>Base Score</i> Skenario Pertama.....	53
4.2.1.2 Skenario Ke-Dua.....	57
4.2.1.2.1 Penentuan <i>Base Score</i> Skenario Ke-Dua	57
4.2.1.3 Skenario Ke-Tiga	61
4.2.1.3.1 Penentuan <i>Base Score</i> Skenario Ke-Tiga	62
4.2.1.4 Skenario Ke-Empat	65
4.2.1.4.1 Penentuan <i>Base Score</i> Skenario Ke-Empat.....	66
4.2.2 Situs Sistem Informasi Akademik	70
4.2.2.1 Skenario Pertama	70
4.2.2.1.1 Penentuan <i>Base Score</i> Skenario Pertama.....	70
4.2.2.2 Skenario Ke-Dua.....	74
4.2.2.2.1 Penentuan <i>Base Score</i> Skenario Ke-Dua	75
4.2.2.3 Skenario Ke-Tiga.....	79
4.2.2.3.1 Penentuan <i>Base Score</i> Skenario Ke-Tiga	79
4.2.2.4 Skenario Ke-Empat	83
4.2.2.4.1 Penentuan <i>Base Score</i> Skenario Ke-Empat.....	84
4.2.3 Validasi	87
BAB V PENUTUP	92
5.1 Kesimpulan.....	92
5.2 Saran	92
DAFTAR PUSTAKA	93

DAFTAR GAMBAR

Gambar 2.1 Contoh halaman <i>website</i>	10
Gambar 2.2 Contoh pemberian <i>script</i>	10
Gambar 2.3 Contoh hasil permintaan <i>script</i>	11
Gambar 2.4 Cara kerja IDS	13
Gambar 3.1 Alur mekanisme keamanan	22
Gambar 3.2 Alur evaluasi situs	23
Gambar 3.3. Topologi jaringan penelitian.....	24
Gambar 3.4 Menu NAT mikrotik.....	25
Gambar 3.5 Konfigurasi <i>action NAT</i>	25
Gambar 3.6 <i>Form</i> pesan situs SIA	26
Gambar 3.7 <i>Form</i> pesan situs blog.....	26
Gambar 3.8 Contoh <i>rule snort</i>	28
Gambar 3.9 Serangan <i>alert</i> pada situs blog.....	29
Gambar 4.1 Ip <i>router A</i> ether 5	35
Gambar 4.5 Ip <i>router B</i> ether 5	35
Gambar 4.2 DHCP <i>server</i> untuk komputer A	35
Gambar 4.3 DHCP <i>server</i> komputer B	36
Gambar 4.4 DNS <i>router A</i>	36
Gambar 4.5 DNS <i>router B</i>	36
Gambar 4.6 Ip yang diperoleh komputer A.....	37
Gambar 4.7 Ip yang diperoleh komputer B	37
Gambar 4.8 Ip <i>router A</i> ether 1	38
Gambar 4.9 Ip <i>router B</i> ether 1	38
Gambar 4.10 <i>Routing router A</i> ether 5 ke <i>router B</i>	38
Gambar 4.11 <i>Routing router B</i> ether 5 ke <i>router A</i>	39
Gambar 4.12 Ping komputer A ke komputer B.....	39
Gambar 4.13 Ping komputer B ke komputer A.....	39
Gambar 4.14 Konfigurasi membuat <i>access point</i>	40
Gambar 4.15 Ip untuk <i>access point</i>	40

Gambar 4.16 DHCP untuk <i>client access point</i>	41
Gambar 4.17 <i>Routing access point</i> ke <i>router A</i>	41
Gambar 4.18 Ping dari <i>client access point</i> ke komputer A dan komputer B	42
Gambar 4.19 Setelan <i>general NAT firewall</i>	42
Gambar 4.20 Setelan <i>action NAT firewall</i>	43
Gambar 4.21 Situs SIA asli sesuai ip asli.....	43
Gambar 4.22 Situs blog asli sesuai ip asli	44
Gambar 4.23 Situs SIA palsu sesuai ip palsu	44
Gambar 4.24 Situs blog palsu sesuai ip palsu	44
Gambar 4.25 Situs SIA palsu namun yang terakses ip situs asli.....	45
Gambar 4.26 Situs blog palsu namun yang terakses ip situs asli	45
Gambar 4.27 Mendaftarkan <i>mac address</i> perangkat yang diijinkan.....	46
Gambar 4.28 Serangan yang tercatat pada <i>database</i> situs blog palsu.....	47
Gambar 4.29 Serangan yang tercatat pada <i>database</i> situs SIA palsu.....	48
Gambar 4.30 <i>Database</i> situs asli tidak terpengaruh serangan.....	49
Gambar 4.31 Pesan peringatan snort.....	51
Gambar 4.32 Laporan hasil snort	51
Gambar 4.33 Hasil serangan skenario pertama	53
Gambar 4.34 <i>Cookie</i> skenario 2 situs blog.....	57
Gambar 4.35 Hasil serangan skenario 3 situs blog.....	61
Gambar 4.36 <i>Cookie</i> skenario 4 situs blog.....	66
Gambar 4.37 Hasil serangan skenario 1 situs SIA	70
Gambar 4.38 <i>Cookie</i> skenario 2 situs SIA	74
Gambar 4.39 Hasil serangan skenario 3 situs SIA	79
Gambar 4.40 <i>Cookie</i> skenario 4 situs SIA	83
Gambar 4.41 Hasil pertama acunetix pada situs blog	88
Gambar 4.42 Hasil kedua acunetix pada situs blog.....	89
Gambar 4.43 Hasil pertama acunetix pada situs SIA.....	90
Gambar 4.44 Hasil kedua acunetix pada situs SIA	91

DAFTAR TABEL

Tabel 2.1. <i>Access vector</i>	15
Tabel 2.2. <i>Access complexity</i>	16
Tabel 2.3. <i>Authentication</i>	16
Tabel 2.4. <i>Confidentiality impact</i>	17
Tabel 2.5. <i>Integrity impact</i>	17
Tabel 2.6. <i>Availability impact</i>	18
Tabel 2.7 Tabel nilai kerentanan	19
Tabel 3.1 Xss payload	26
Tabel 3.2 Skenario pengujian situs blog	28
Tabel 3.3 Skenario pengujian situs SIA	29
Tabel 3.4 Hasil <i>access vector</i> 1	30
Tabel 3.5 Hasil <i>access complexity</i> 1	30
Tabel 3.6 Hasil <i>authentication</i> 1	30
Tabel 3.7 Hasil <i>confidentiality impact</i> 1	31
Tabel 3.8 Hasil <i>integrity impact</i> 1	31
Tabel 3.9 Hasil <i>availability impact</i> 1	32
Tabel 4.1 <i>Rule snort</i> untuk mendeteksi serangan xss.....	49
Tabel 4.2 Skenario 1 situs blog	52
Tabel 4.3 Hasil <i>access vector</i> blog-1.....	53
Tabel 4.4 Hasil <i>access complexity</i> blog-1	54
Tabel 4.5 Hasil <i>authentication</i> blog-1	54
Tabel 4.6 Hasil <i>confidentiality</i> blog-1	55
Tabel 4.7 Hasil <i>integrity</i> blog-1	55
Tabel 4.8 Hasil <i>availability impact</i> blog-1	56
Tabel 4.9 Skenario 2 situs blog	57
Tabel 4.10 Hasil <i>access vector</i> blog-2.....	57
Tabel 4.11 Hasil <i>access complexity</i> blog-2	58
Tabel 4.12 Hasil <i>authentication</i> blog-2	58
Tabel 4.13 Hasil <i>confidentiality</i> blog-2.....	59

Tabel 4.14 Hasil <i>integrity</i> blog-2.....	60
Tabel 4.15 Hasil <i>availability impact</i> blog-2.....	60
Tabel 4.16 Skenario 3 situs blog.....	61
Tabel 4.17 Hasil <i>access vector</i> blog-3.....	62
Tabel 4.18 Hasil <i>access complexity</i> blog-3.....	62
Tabel 4.19 Hasil <i>authentication</i> blog-3.....	63
Tabel 4.20 Hasil <i>confidentiality</i> blog-3.....	63
Tabel 4.21 Hasil <i>integrity</i> blog-3.....	64
Tabel 4.22 Hasil <i>availability impact</i> blog-3.....	64
Tabel 4.23 Skenario 4 situs blog.....	65
Tabel 4.24 Hasil <i>access vector</i> blog-4.....	66
Tabel 4.25 Hasil <i>access complexity</i> blog-4.....	67
Tabel 4.26 Hasil <i>authentication</i> blog-4.....	67
Tabel 4.27 Hasil <i>confidentiality</i> blog-4.....	68
Tabel 4.28 Hasil <i>integrity</i> blog-4.....	68
Tabel 4.29 Hasil <i>availability impact</i> blog-4.....	69
Tabel 4.30 Skenario 1 situs SIA.....	70
Tabel 4.40 Hasil <i>access vector</i> SIA-1.....	71
Tabel 4.41 Hasil <i>access complexity</i> SIA-1.....	71
Tabel 4.42 Hasil <i>authentication</i> SIA-1.....	72
Tabel 4.43 Hasil <i>confidentiality</i> SIA-1.....	72
Tabel 4.44 Hasil <i>integrity</i> SIA-1.....	73
Tabel 4.45 Hasil <i>availability impact</i> SIA-1.....	73
Tabel 4.46 Skenario 2 situs SIA.....	74
Tabel 4.47 Hasil <i>access vector</i> SIA-2.....	75
Tabel 4.48 Hasil <i>access complexity</i> SIA-2.....	75
Tabel 4.49 Hasil <i>authentication</i> SIA-2.....	76
Tabel 4.50 Hasil <i>confidentiality</i> SIA-2.....	76
Tabel 4.51 Hasil <i>integrity</i> SIA-2.....	77
Tabel 4.52 Hasil <i>availability impact</i> SIA-2.....	78
Tabel 4.53 Skenario 3 situs SIA.....	79

Tabel 4.54 Hasil <i>access vector</i> SIA-3	79
Tabel 4.55 Hasil <i>access complexity</i> SIA-3	80
Tabel 4.56 Hasil <i>authentication</i> SIA-3.....	80
Tabel 4.57 Hasil <i>confidentiality</i> SIA-3.....	81
Tabel 4.58 Hasil <i>integrity</i> SIA-3	82
Tabel 4.59 Hasil <i>availability impact</i> SIA-3.....	82
Tabel 4.60 Skenario 4 situs SIA	83
Tabel 4.61 Hasil <i>access vector</i> SIA-4	84
Tabel 4.62 Hasil <i>access complexity</i> SIA-4	84
Tabel 4.63 Hasil <i>authentication</i> blog-4.....	85
Tabel 4.64 Hasil <i>confidentiality</i> blog-4.....	85
Tabel 4.65 Hasil <i>integrity</i> SIA-4	86
Tabel 4.66 Hasil <i>availability impact</i> SIA-4.....	86
Tabel 4.67 Tabel perbandingan pertama hasil manual dengan acunetix situs blog	88
Tabel 4.68 Tabel perbandingan kedua hasil manual dengan acunetix situs blog	89
Tabel 4.69 Tabel perbandingan pertama hasil manual dengan acunetix situs SIA	90
Tabel 4.70 Tabel perbandingan kedua hasil manual dengan acunetix situs SIA	91