

**ANALISIS TINGKAT KEAMANAN WEB SIPS.BAWASLU.GO.ID
MENGUNAKAN OWASP ZAP DAN ACUNETIX**

SKRIPSI

**Disusun untuk memenuhi sebagai persyaratan
mencapai derajat sarjana**



Disusun oleh :

Chandra Surya

1900018101

PROGRAM STUDI S1 INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS AHMAD DAHLAN

YOGYAKARTA

2023

**LEMBAR PERSETUJUAN PEMBIMBING
SKRIPSI**

ANALISIS TINGKAT KEAMANAN WEB SIPS.BAWASLU.GO.ID

MENGGUNAKAN APLIKASI OWASP ZAP DAN ACUNETIX

Dipersiapkan dan disusun oleh:

Chandra Surya Negarawan

1900018101

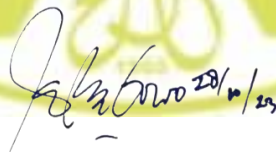
PROGRAM STUDI S1 INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS AHMAD DAHLAN

Telah disetujui oleh:

Pembimbing



Eko Aribowo 28/1/23

Eko Aribowo, S.T., M.Kom.

NIP : 197002062005011001

**LEMBAR PERSETUJUAN PENGUJI
SKRIPSI**

**ANALISIS TINGKAT KEAMANAN WEB SIPS.BAWASLU.GO.ID
MENGUNAKAN APLIKASI OWASP ZAP DAN ACUNETIX**

Dipersiapkan dan disusun oleh:

Chandra Surya Negarawan
1900018101

Telah dipertahankan di depan Dewan Penguji pada Tanggal 29 September 2023 dan dinyatakan telah memenuhi syarat

Susunan Dewan Penguji

Ketua : Eko Aribowo, S.T., M.Kom.

Penguji 1 : Ir. Nuril Anwar, S.T., M.Kom.

Penguji 2 : Nur Rochmah Dyah Puji Astuti, S.T., M.Kom.

Yogyakarta, 29 September 2023
Dekan Fakultas Teknologi Industri
Universitas Ahmad Dahlan



Ir. Sunardi, S.T., M.T., Ph.D.

NIPM. 197405212000021110862028

LEMBAR PERNYATAAN KEASLIAN SURAT PERNYATAAN

Yang Bertanda Tangan Dibawah Ini:

Nama : Chandra Surya Negarawan

Nim : 1900018101

Prodi : Informatika

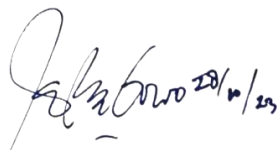
Judul Ta/Skripsi : ANALISIS TINGKAT KEAMANAN WEB SIPS.BAWASLU.GO.ID MENGGUNAKAN
APLIKASI OWASP ZAP DAN ACUNETIX

Dengan ini saya menyatakan bahwa Laporan Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar Ahli Madya/Kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 23 September 2023

Mengetahui,

Dosen Pembimbing



Eko Aribowo, S.T., M.Kom.

NIP. 197002062005011001

Yang menyatakan,



Chandra Surya Negarawan

NIM. 1900018101

LEMBAR PERNYATAAN TIDAK PLAGIAT

Saya yang bertanda tangan dibawah ini:

Nama : Chandra Surya Negarawan

NIM : 1900018101

Email : chandra1900018101@webmail.uad.ac.id

Program Studi : S1 Informatika

Fakultas : Teknologi Industri

Judul Skripsi : ANALISIS TINGKAT KEAMANAN WEB SIPS.BAWASLU.GO.ID MENGGUNAKAN

APLIKASI OWASP ZAP DAN ACUNETIX

Dengan ini menyatakan bahwa:

1. Hasil karya yang saya serahkan ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar kesarjanaan baik di Universitas Ahmad Dahlan maupun di institusi pendidikan lainnya.
2. Hasil karya saya ini bukan saduran/terjemahan melainkan merupakan gagasan, rumusan, dan hasil pelaksanaan penelitian/implementasi saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing akademik dan narasumber penelitian.
3. Hasil karya saya ini merupakan hasil revisi terakhir setelah diujikan yang telah diketahui dan disetujui oleh pembimbing.
4. Dalam karya saya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali yang digunakan sebagai acuan dalam naskah dengan menyebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

Pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari terbukti ada penyimpangan dan ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya saya ini, serta sanksi lain yang sesuai dengan ketentuan yang berlaku di Universitas Ahmad Dahlan.

Yang menyatakan,

Mahasiswa



Chandra Surya Negarawan

NIM. 1900018101

LEMBAR PERNYATAAN PERSETUJUAN AKSES

Saya yang bertanda tangan dibawah ini:

Nama : Chandra Surya Negarawan

NIM : 1900018101

Email : chandra1900018101@webmail.uad.ac.id

Program Studi : S1 Informatika

Fakultas : Teknologi Industri

Judul Skripsi : ANALISIS TINGKAT KEAMANAN WEB SIPS.BAWASLU.GO.ID MENGGUNAKAN

APLIKASI OWASP ZAP DAN ACUNETIX

Dengan ini Saya menyerahkan hak sepenuhnya kepada Perpustakaan Universitas Ahmad Dahlan untuk menyimpan, mengatur akses serta melakukan pengelolaan terhadap karya saya ini dengan mengacu pada ketentuan akses tesis elektronik sebagai berikut (beri tanda pada kotak):



Saya (~~tidak mengizinkan~~ **mengizinkan**)* karya tersebut diunggah ke dalam aplikasi

Repository Perpustakaan Universitas Ahmad Dahlan.

Demikian pernyataan ini saya buat dengan sebenarnya.

Yogyakarta, 23 September 2023

Mengetahui,

Dosen Pembimbing



Eko Aribowo, S.T., M.Kom.

NIP. 197002062005011001

Yang menyatakan,



Chandra Surya Negarawan

NIM. 1900018101

KATA PENGANTAR

Bismillahirrahmanirrahim

Assalamualaikum Warahmatullahi Wabarakatuh

Puji syukur penulis panjatkan atas kehadiran Allah SWT atas limpahan berkah dan rahmatNya sehingga pada kesempatan ini penulis dapat menyelesaikan skripsi ini dengan baik. Tak lupa pula sholawat beriring salam penulis haturkan kepada Nabi Muhammad SAW, beserta keluarga, sahabat dan pengikutnya hingga akhir zaman. Skripsi yang berjudul “Analisis Tingkat Keamanan Web Sips.Bawaslu.Go.Id Menggunakan Aplikasi Owasp Zap Dan Acunetix” disusun guna memenuhi persyaratan menyelesaikan derajat Sarjana Komputer di Program Studi Informatika Fakultas Teknologi Industri Universitas Ahmad Dahlan Yogyakarta.

Penulisan skripsi ini tidak lepas dari bantuan dan bimbingan dari berbagai pihak. Oleh karena itu, dalam kesempatan ini, dengan segala kerendahan hati penulis ingin memberikan ucapan terima kasih kepada :

1. Bapak Dr. Muchlas Arkanuddin, M.T. selaku Rektor Universitas Ahmad Dahlan Yogyakarta.
2. Bapak Ir. Sunardi, S.T., M.T., Ph.D. selaku Dekan Fakultas Teknologi industri UniversitasAhmad Dahlan Yogyakarta.
3. Bapak Dr. Murinto, S.Si., M.Kom. sebagai Kepala Prodi Informatika di Universitas Ahmad Dahlan.
4. Bapak Eko Aribowo, S.T., M.Kom. selaku Dosen pembimbing yang telah memberikan bimbingan dan berbagai macam masukan kepada saya dalam menyelesaikan skripsi ini.
5. Bapak Faisal Fajri Rahani S.Si., M.Cs. selaku Dosen pembimbing akademik yang telah memberikan bimbingan selama masa kuliah.
6. Kedua orang tua saya Bapak Dr. Abdullah Iskandar, S.H., M.H. dan Ariyati Pitter yang selalu memberikan doa, nasehat, inspirasi dan semangat untuk semua yang saya lakukan
7. Teman-teman yang selalu memberikan support.

Penulis menyadari bahwa dalam pembuatan skripsi ini masih banyak terdapat banyak kekurangan, oleh karena itu penulis mengharapkan saran dan kritik yang sifatnya membangun agar dapat digunakan demi perbaikan nantinya. Semoga skripsi ini dapat memberikan banyak manfaat bagi para pembaca.

Yogyakarta, 29 September 2023

Penulis

A handwritten signature in black ink, consisting of stylized initials 'CSN', positioned above a horizontal line.

Chandra Surya Negarawan

1900018101

DAFTAR ISI

LEMBAR PERSETUJUAN PEMBIMBING	iii
LEMBAR PERNYATAAN KEASLIAN.....	v
LEMBAR PERNYATAAN TIDAK PLAGIAT.....	vi
LEMBAR PERNYATAAN PERSETUJUAN AKSES	vii
KATA PENGANTAR.....	viii
DAFTAR ISI	x
DAFTAR GAMBAR	xii
DAFTAR TABEL.....	xiv
ABSTRAK	xv
BAB I PENDAHULUAN	16
1.1 Latar Belakang	16
1.2 Batasan Masalah.....	18
1.3 Rumusan Masalah	18
1.4 Tujuan.....	19
1.5 Manfaat Penelitian	19
BAB II TINJAUAN PUSTAKA	20
2.1 Penelitian Terdahulu	20
2.2 Landasan Teori.....	27
2.2.1 Website	27
2.2.2 Information Gathering.....	27
2.2.3 Vulnerability Assessment	28
2.2.4 Penetration Testing	28
2.2.5 OWASP ZAP.....	31
2.2.6 Acunetix.....	31
BAB III METODOLOGI PENELITIAN.....	33
3.2 Objek Penelitian	33
3.3 Metode Pengumpulan Data	37
3.4 Analisis Kebutuhan	38
3.5 Tahapan Penelitian	39
BAB IV HASIL DAN PEMBAHASAN	43
4.1 Hasil	43
4.2 Pembahasan	88
4.2.1 Rekomendasi Perbaikan	94

BAB V KESIMPULAN DAN SARAN	103
5.1 Kesimpulan	103
5.2 Saran.....	105
DAFTAR PUSTAKA	106
LAMPIRAN	108

DAFTAR GAMBAR

Gambar 2. 1 Alur Baku Penetration Testing.....	28
Gambar 2. 2 OWASP ZAP	31
Gambar 2. 3 Acunetix.....	32
Gambar 3.1 Tampilan Beranda website sips.bawaslu.go.id	34
Gambar 3. 2 Tampilan tentang SIPS.....	34
Gambar 3.3 tampilan permohonan.....	35
Gambar 3.4 Tampilan halaman daftar	35
Gambar 3.5 Tampilan Login	36
Gambar 3. 7 Proses Alur Penelitian.....	39
Gambar 4. 1 Tools MALTEGO	45
Gambar 4.2 Investigate MALTEGO.....	45
Gambar 4.3 Proses Information gathering MALTEGO	46
Gambar 4.4 Terminal open OWASP ZAP.....	47
Gambar 4.5 Tampilan utama OWASP ZAP	48
Gambar 4.6 Hasil scanning OWASP ZAP.....	48
Gambar 4.7 Tampilan login Acunetix	49
Gambar 4.8 Tampilan dashboard acunetix	50
Gambar 4.9 Tampilan add target	50
Gambar 4.10 Tampilan target information	51
Gambar 4.11 Tampilan choose scanning	52
Gambar 4.12 Tampilan proses scanning acunetix.....	53
Gambar 4.13 Hasil scanning OWASP ZAP	54
Gambar 4.14 Hasil scan Acunetix.....	60
Gambar 4.15 Alert Cross Site Scripting	61
Gambar 4.16 Parameter Directory Traversal	65
Gambar 4.17 Path Traversal.....	69
Gambar 4.18 URL Target	70
Gambar 4.19 Integrity constarint violation.....	70
Gambar 4.20 Website sips.bawaslu.go.id	71
Gambar 4.21 Icon Sensepostjack	72
Gambar 4.22 icon Sensepostjack	72

Gambar 4.23 Captured Senspostjack	73
Gambar 4.24 Tools Burpsuite.....	74
Gambar 4.25 Intercept Burpsuite	75
Gambar 4.26 Request Intercept.....	76
Gambar 4.27 Parameter AntarPeserta%2Search%5nomor%5D.....	76
Gambar 4.28 Request Cross Site Scripting	77
Gambar 4.29 Request Cross Site Scripting	78
Gambar 4.30 Parameter TLS 1.0 Enabled	79
Gambar 4.31 Tampilan Metasploit	80
Gambar 4.32 Tampilan “scanner/ssl/openssl_heartbleed”	80
Gambar 4.33 Tampilan IP address dan port ke “scanner/ssl/openssl_heartbleed”	81
Gambar 4. 34 Tampilan syntax “set verbose true”	81
Gambar 4.35 Hasil“scanner/ssl/openssl_heartbleed”	82
Gambar 4.36 Tools Burp-Suite	83
Gambar 4.37 tampilan website berdasarkan vurnerability affects	83
Gambar 4.38 Tampilan intercept	84
Gambar 4.39 Tampilan send to repeater	84
Gambar 4.40 Tampilan request script directory traversal	85
Gambar 4.41 Response Script	86
Gambar 4.42 Iframe Script	87
Gambar 4.43 Clickjacking POC	87
Gambar 4.44 source code prevent path traversal	98
Gambar 4.45 hasil sslscan	99
Gambar 4.46 middleware.....	100
Gambar 4.47 file FrameGuard.php	100
Gambar 4.48 \$middleware pada app/Http/Kernel.php.....	101
Gambar 4.49 syntax cache control.....	102
Gambar 4.50 cache control pada file route	102

DAFTAR TABEL

Tabel 2 1 Penelitian terdahulu atau form telaah jurnal.....	23
Tabel 3.1 Hasil Pengujian OWASP ZAP	40
Tabel 3.2 Tabel Hasil Anlisis Acunetix	41
Tabel 3.3 Analisis OWASP ZAP	41
Tabel 3.4 Analisis Acunetix.....	41
Tabel 3.5 Rekomendasi Perbaikan OWASP ZAP.....	42
Tabel 3.6 Rekomendasi Perbaikan Acunetix	42
Tabel 4.1 Hasil Scanning OWASP ZAP	54
Tabel 4.2 hasil Scan Acunetix	60
Tabel 4.3 Analisis OWASP ZAP	88
Tabel 4.4 Analisis Acunetix.....	92
Tabel 4.5 Rekomendasi Perbaikan OWASP ZAP.....	94
Tabel 4.6 Rekomendasi Perbaikan Acunetix	96

ANALISIS TINGKAT KEAMANAN WEB SIPS.BAWASLU.GO.ID

MENGGUNAKAN APLIKASI OWASP ZAP DAN ACUNETIX

Chandra Surya Negarawan

1900018101

Jurusan Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan, Yogyakarta,
Jl. Ringroad Selatan, Kragilan, Tamanan, Kec. Banguntapan, Kab. Bantul, Yogyakarta 55191

Email : chandra1900018101@webmail.uad.ac.id

ABSTRAK

Keamanan adalah hal yang penting dan harus diperhatikan dalam mengelola atau membuat sebuah web. Dengan yang semakin canggih, banyak instansi pendidikan di Indonesia menggunakan website menjadi media informasi yang bisa memudahkan seseorang dalam mencari tahu informasi yang berada dalam institusi tersebut. Website tidak hanya berguna untuk media informasi, tetapi website juga dapat membantu sebuah instansi untuk mengerjakan suatu pekerjaan yang dilakukan secara manual menjadi terkomputerisasi. Oleh karena itu dibutuhkan suatu cara untuk menjaga keamanan website suatu instansi, salah satu contohnya adalah dengan melakukan *penetration testing*.

Penelitian kali ini menggunakan metode *Penetration testing* sebagai solusi yang bersifat legal dan resmi yang berfungsi untuk mengeksploitasi suatu sistem dengan maksud untuk menemukan kerentanan pada web dan pengujian penetrasi juga berfungsi untuk meningkatkan keamanan sistem. Pengujian penetrasi ini berobjek pada web yang merupakan website pada sebuah instansi yaitu BAWASLU RI

Hasil dari penelitian ini menampilkan beberapa kerentanan-kerentanan pada website SIPS BAWASLU RI, setiap bagiannya akan ditampilkan level risk, mulai dari high, medium, dan low. Penelitian ini menggunakan tools OSWASP ZAP, tools kedua akan menggunakan Acunetix, dalam proses information gathering menggunakan tools MALTEGO, tools MALTEGO akan menampilkan informasi dari web tersebut. Hasil dari analisis website sips.bawaslu.go.id ditemukan beberapa bagian yang level risknya *high, medium, low, dan informational*. Setelah mendapatkan hasil vulnerability scanning, selanjutnya adalah melakukan pengujian attacking dengan menggunakan tools attacking seperti, *Metasploit dan Burpsuite*. Pada pengujian attacking beberapa kerentanan dapat dibuktikan. Nantinya hasil pengujian *attacking* akan dimasukkan pada tahapan analisis. Apabila pengujian tersebut telah dijabarkan dalam tahapan analisis selanjutnya adalah memberikan rekomendasi perbaikan.

Kata kunci : Acunetix, Keamanan website, MELTAGO, OWASP ZAP, Penetration Testing