BAB I

PENDAHULUAN

1.1 Latar Belakang

Zaman sekarang ini penggunaan internet sangat penting bagi umat manusia, internet sangat berguna bagi kelangsungan kehidupan manusia dalam kehidupan sehari-hari, internet sangat membantu manusia dari segala sektor maupun segala aspek kehidupan, baik dari sektor industri, transportasi, dan komunikasi. Menurut data dari kominfo total pengguna internet Di tahun 2022 ini, mencapai angka 4,9 Miliar pengguna internet dunia , untuk Indonesia sendiri tersdapat 204 juta pengguna internet.berdasarkan data total lalu lintas dan konsumsi data sebesar 64,2 *Zettabyte* pada tahun 2020 dan diprediksi akan bertambah 3 kali lipat sebesar181 Zettabyte pada tahun selanjutnya[1].

Banyak tidak diketahui bahwa banyak sisi kelemahan dari internet itu sendiri, sebagai contoh adalah aplikasi web, aplikasi web sangat rentan dari serangan *hacker*, terkadang mereka tidak memproteksi web mereka dari berbagai serangan, mulai dari serangan malware, phising, DOS (*Denial Of Service*), Eksploitasi, dll. Sehingga sampai detik ini tidak ada *website* yang aman dari berbagai serangan. Salah satu cara untuk memproteksi suatu web yaitu dengan mengananalisis tingkat keamanan web itu sendiri. Setelah melakukan analisis, kita dapat melakukan metode pengamanan dari website tersebut[2].

Terkait dengan penelitian ini objek yang digunakan adalah aplikasi website sips.bawaslu.go.id. Aplikasi sips.bawaslu.go.id merupakan website Sistem Informasi Penyelesaian Sengketa pemilihan dan pemilu yang terdiri dari sub sistem informasi meliputi Permohonan Sengketa baik langsung maupun online, verifikasi formil dan materiil, registrasi , musyawarah/ajudikasi, putusan dan tindaklanjut putusan., website sips.bawaslu.go.id memiliki manfaat Mendigitalisasi proses permohonan sengketa, sampai

dengan putusanan. Fitur SIPS antara lain permohonan online, data register permohonan, data putusan, grafik serta lainnya yang berkaitan dengan proses permohonan sengketa Bawaslu, baik data sengketa pemilihan maupun pemilu. Berdasarkan hasil chat dengan admin sips.bawaslu.go.id, didapatkan informasi mengenai website sips.bawaslu.go.id bahwasannya beberapa waktu yang lalu website sips.bawaslu.go.id mendapat serangan, oleh karena itu web yang menjadi objek penelitian sangat direkomendasikan agar menerapkan analisis keamanan terhadap aplikasi, yang bertujuan untuk meminimalisir terjadinya gangguan pada kinerja aplikasi berbasis web sehingga harus adanya evaluasi terhadap keamanan sistem aplikasi. Dengan adanya Analisis Keamanan Aplikasi Web sips.bawaslu.go.id dengan tujuan menemukan keretanan dan menguji pada aplikasi sehingga pemilik aplikasi web tersebut dapat memperbaiki dan meningkatkan keamanan dari sebuah aplikasi[3]

Pada peneltian kali ini tahapan pertama yang dilakukan adalah Vulnerability scanning dengan menggunakan tools OWASP ZAP dan Acunetix untuk mendeteksi kerentanan seperti injeksi SQL dan XSS, private IP *disclosure, application error disclosure*, hasil vulnerability scanning dari OWASP ZAP dan Acunetix akan menjadi acuan dalam tahapan attacking. Tahapan attacking menjadi pembuktian terhadap hasil vulnerability scanning. Tools yang digunakan dalam tahapan attacking berdasarkan dengan kebutuhan hasil vulnerabitly scanning. Setelah melakukan attacking tahapan selanjutnya adalah dengan melakukan analisis terhadapa kerentanan tersebut, setelah melakukan analisis langkah selanjutnya adalah melakukan rekomendasi perbaikan terhadap system.

,

1.2 Batasan Masalah

Berdasarkan masalah masalah yang telah diindentifikasi, maka disampaikan beberapa batasan sebagai berikut :

1. Target analisis aplikasi web, yaitu sips.bawaslu.go.id,
2. Di dalam penelitian ini objek *domain* yang di analisis adalah , https://sipsbawaslu.go.id
3. Aplikasi yang digunakan adalah *OWASP ZAP* versi *kali linux* dan *software Acunetix web vulnerability.*
4. Dalam proses attacking, tools yang digunakan berdasarkan hasil proses vulnerability scanning.
5. Di dalam aplikasi OWASP ZAP metode yang digunakan adalah *Automated Scan* , dengan menggunakan media *scan firefox*.

1.3 Rumusan Masalah

Setelah diindentifkasi dan dibatasi masalah diatas dapat dirumuskan masalah sebagai berikut:

1. Bagaimana melakukan pengujian dalam menemukan celah keamanan aplikasi sips.bawaslu.go.id sebagai langkah awal dalam memproteksi tingkat keamanan web sips.bawaslu.go.id ?
2. Bagaiamana menerapkan *tools Acunetix* dan *tools* OWASP ZAP dalam menganalisis tingkat keamanan website sips.bawaslu.go.id ?
3. Bagaimana menerapkan *tools attacking* sebagai pembuktian hasil *vulnerability scanning*?

1.4 Tujuan

Tujuan Penelitian ini untuk menganalisis keamanan aplikasi web sips.bawaslu.go.id menggunakan aplikasi OWASP ZAP dan Acunetix, yang merupakan langkah awal dalam memproteksi tingkat keamanan kerentanan web sips.bawaslu.go.id dari berbagai serangan dari pihak yang tidak bertanggung jawab.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah agar kedepan web sips.bawaslu.go.id bisa meningkatkan tingkat keamanan webnya lebih baik lagi, untuk menghindari tindakan tindakan yang jahat daripihak yang tidak bertanggung jawab, dan dari hasil penelitian kali ini diharapkan menjadi landasan bagi website instansi divisi Penyelesaian Sengketa Badan Pengawas Pemilu Republik Indonesia agar lebih memperhatikan tingkat keamanan webnya, untuk menghindari dari berbagai serangan yang dapat merusak web atau bahkan mencuri data dari web tersebut.