UNIVERSITAS MUHAMMADIYAH MALANG

SKRIPSI

ANALISIS DAN MITIGASI CELAH KEAMANAN WEBSITE SIMPKN INFORMATIKA MENGGUNAKAN METODE OWASP ZED ATTACK PROXY (ZAP)

LATAR BELAKANG

APLIKASI WEB ADALAH SALAH SATU PLATFORM PALING UMUM UNTUK MENYAMPAIKAN INFORMASI DAN LAYANAN MELALUI INTERNET. BAHKAN SAAT INI, APLIKASI WEB BANYAK DIGUNAKAN DALAM LAYANAN PENTING. NAMUN PENGGUNAAN YANG MELUAS INI MEMBUAT APLIKASI WEB MENJADI TARGET POPULER BERBAGAI ANCAMAN DALAM BENTUK SERANGAN CYBER [1]. MESKIPUN SEBAGIAN BESAR TEKNOLOGI TELAH DIKEMBANGKAN UNTUK MELINDUNGI APLIKASI WEB DAN SETIDAKNYA MEMINIMALKAN SERANGAN CYBER, HANYA SEDIKIT YANG TELAH DILAKUKAN UNTUK MEMBANGUN HUBUNGAN ANTARA TEKNOLOGI-TEKNOLOGI INI DAN MEMBERIKAN GAMBARAN MENYELURUH TENTANG PENELITIAN KEAMANAN APLIKASI WEB.

PADA PENELITIAN INI AKAN DILAKUKAN ANALISIS PADA WEBSITE SIMPKN INFORMATIKA YANG NANTINYA ANALISIS TERSEBUT MENAMPILKAN KERENTANAN-KERENTANAN YANG ADA PADA WEBSITE DAN JUGA CARA MENGATASI KERENTANAN PADA WEBSITE. KERENTANAN DAPAT MEMBUAT WEBSITE TERANCAM SEPERTI TERDAPAT PENYERANG ATAU HACKER YANG INGIN UNTUK WEBSITE TERSEBUT DIRUSAK MAKA DARI ITU PENELITIAN DILAKUKAN UNTUK MENGATASI PENYERANGAN DARI HACKER YANG TIDAK BERTANGGUNG JAWAB. HACKER DAPAT MEMBUAT WEBSITE TIDAK BERJALAN NORMAL DENGAN MENCARI CELAH KEAMANAN YANG ADA PADA WEBSITE YANG NANTINYA PENYERANG ATAU HACKER DAPAT MENYUSUPKAN PROGRAM YANG DAPAT MEMANIPULASI SISTEM WEBSITE AGAR TIDAK BERJALAN DENGAN NORMAL.

TUJUAN PENELITIAN

DIPEROLEH TUJUAN DARI PENELITIAN INI SEBAGAI BERIKUT:

A.)MENGETAHUI TINGKAT KEAMANAN PADA WEBSITE SIMPKN INFORMATIKA.

B.)MEREKOMENDASI PERBAIKAN KEAMANAN PADA WEBSITE SIMPKN INFORMATIKA.

METODE PENELITIAN

PADA PENELITIAN INI DIUSULKAN BEBERAPA SKENARIO PENYUSUNAN UNTUK MENDETEKSI, MENGKLASIFIKASIKAN, DAN MEMAHAMI SERANGAN. BERIKUT TAHAPAN YANG DILAKUKAN UNTUK MENYELESAIKAN PENELITIAN DIANTARANYA STUDI YANG TERDIRI DARI PENDAHULUAN DAN OBSERVASI [4], TEKNIK PENGUMPULAN DATA ATAU INFORMASI INI DILAKUKAN DENGAN TUJUAN PENGAMATAN MASALAH APA YANG TERJADI DAN PENDALAMAN PERMASALAHAN YANG TELAH TERJADI PADA WEBSITE SIMPKN INFORMATIKA.

STRUKTUR TAHAPAN YANG DILAKUKAN PENELITIAN INI DENGAN RANCANGAN SEBAGAI BERIKUT:

HASIL PENELITIAN

SCANNING PADA OWASP ZAP (ZED ATTACK PROXY) ADALAH PROSES PENGUJIAN KEAMANAN WEBSITE UNTUK MENGIDENTIFIKASI KERENTANAN KEAMANAN. PROSES SCANNING INI DAPAT MEMBANTU MENGIDENTIFIKASI MASALAH KEAMANAN SEPERTI SQL INJECTION, CROSS-SITE SCRIPTING (XSS), CROSS-SITE REQUEST FORGERY (CSRF), DAN LAINNYA. PADA PROSES SCANNING OWASP ZAP SELESAI NANTINYA AKAN MENYEDIAKAN LAPORAN KERENTANAN KEAMANAN PADA WEBSITE. PADA HASIL SCANNING DAPAT DILIHAT PADA GAMBAR 4.1 TERDAPAT HASIL SEBAGAI BERIKUT KERENTANAN SEDANG SEBANYAK 6 KERENTANAN (29%), KERENTANAN RENDAH SEBANYAK 8 KERENTANAN (38%), DAN KERENTANAN TIDAK BERDAMPAK (INFORMATIF) SEBANYAK 7 KERENTANAN (33%).

KESIMPULAN

PADA PENELITIAN ANALISIS DAN MITIGASI CELAH KEAMANAN WEBSITE SIMPKN INFORMATIKA MENGGUNAKAN METODE OWASP ZED ATTACK PROXY (ZAP) MENDAPATKAN BEBERAPA KERENTANAN PADA WEBSITE SIMPKN YANG DIMANA KERENTANAN-KERENTANAN TERSEBUT DIDAPAT MENGGUNAKAN TOOLS YAITU ZED ATTACK PROXY (ZAP). PADA LAPORAN HASIL YANG DIDAPAT OLEH TOOLS ZED ATTACK PROXY MENDAPATKAN 3 PENGKLASIFIKASIAN KERENTANAN YAITU KERENTANAN SEDANG, KERENTANAN RENDAH, KERENTANAN TIDAK BERDAMPAK (INFORMATIF). PADA HASIL PENGKLASIFIKASIAN TERSEBUT MENDAPATKAN HASIL PRESENTASE SEBAGAI BERIKUT KERENTANAN SEDANG SEBANYAK 6 KERENTANAN (29%), KERENTANAN RENDAH SEBANYAK 8 KERENTANAN (38%), DAN KERENTANAN TIDAK BERDAMPAK (INFORMATIF) SEBANYAK 7 KERENTANAN (33%). KERENTANAN-KERENTANAN TERSEBUT APABILA TIDAK ADA UPAYA PENCEGAHAN DAN PERBAIKAN PADA KERENTANAN WEBSITE SIMPKN INFORMATIKA MAKA KEDEPANNYA KINERJA WEBSITE SIMPKN INFORMATIKA AKAN BERDAMPAK.

PENULIS

NAMA : HELMI INDRA PERDHANA
NIM : 202010370311484
EMAIL : HELMIINDRA22@WEBMAIL.UMM.AC.ID

DOSEN PEMBIMBING 1

NAMA : DIAH RISQIWATI, ST., MT.
NIP. 108.1410.054SPNS.
EMAIL : RIZQIWATI@UMM.AC.ID

DOSEN PEMBIMBING 2

NAMA : ZAMAH SARI, S.T, M.T
NIP. 108.1410.055SPNS.
EMAIL: ZAMAHSARI(@UMM.AC.ID