BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian yang dilakukan oleh penulis terkait Optimasi dan Implementasi terhadap serangan brute force pada web aplikasi registrasi mahasiswa baru UPN Veteran Jakarta menggunakan penetration testing, kesimpulan yang akan penulis berikan sebagai berikut:

1. Berhasil mengidentifikasi kelemahan keamanan web aplikasi registrasi mahasiswa baru UPN Veteran Jakarta terhadap serangan *brute-force* dengan alat otomatisasi *brute-force* seperti burp suite dapat digunakan untuk menjalankan proses *brute force attack*. Alat ini bekerja dengan mencoba berbagai kombinasi *username* dan *password* secara otomatis hingga menemukan kombinasi yang valid. Dengan menggunakan alat *burp suite*, penulis dapat mengevaluasi apakah aplikasi rentan terhadap serangan brute-force dengan mengidentifikasi tidak adanya proteksi terhadap upaya login yang berlebihan, tidak ada kebijakan *password* yang kuat dan kompleks dan tidak ada mekanisme *CAPTCHA* dan Authentikasi 2 Faktor.
2. Serangan *brute-force* dapat diterapkan secara langsung untuk mengidentifikasi kerentanan pencurian data dalam web aplikasi registrasi mahasiswa baru. Serangan ini berfokus pada pengujian kekuatan kata sandi dan mekanisme login. Diketahui, sistem rentan terhadap *brute-force,* ini membuka peluang bagi penyerang untuk memperoleh akses yang tidak sah, yang kemudian dapat dimanfaatkan untuk melakukan pencurian data. Oleh karena itu, meskipun *brute-force* bukan metode utama untuk mengidentifikasi kerentanan pencurian data, ia dapat menjadi indikator adanya kelemahan yang dapat dieksploitasi lebih lanjut. Tingkat keberhasilan pengambil alihan akun yang tinggi mencapai 389 akun menjadi Kesimpulan bahwa website regmaba upn veteran Jakarta tahun masuk 2024 rentan terhadap pencurian data

mahasiswa baru tahun 2024. Presentase akun yang berhasil diretas berjumlah sekitar 35% dari total mahasiswa SNBP.

3. Efektifitas serangan brute force tergantung pada Tingkat pengetahuan penyerang terkait username dan tanggal lahir. Berdasarkan hasil uji username dapat ditemukan melalui Teknik OSINT dan kemudian menggenerate *username* baru menggunakan kode program.
4. Mengidentifikasi kerentanan pada web aplikasi registrasi ulang mahasiswa baru UPN Veteran Jakarta tahun 2024 dapat dilakukan dengan metode *penetration testing*. Proses ini melibatkan serangkaian langkah, mulai dari perencanaan dan pengumpulan informasi, pemindaian kerentanan, eksploitasi kerentanan, hingga pelaporan.Hasil pemindaian menunjukkan bahwa web aplikasi regmaba menggunakan versi perangkat lunak yang sudah tidak didukung, seperti Apache dan PHP. Versi ini berpotensi memiliki kerentanan keamanan yang tidak diperbaiki oleh vendor, sehingga sangat penting untuk memperbarui ke versi yang didukung. Selain itu, deteksi protokol SSL dan TLS yang usang seperti SSL v2, v3, TLS 1.0, dan TLS 1.1 juga menunjukkan kebutuhan mendesak untuk mengonfigurasi ulang server regmaba agar menggunakan protokol yang lebih aman seperti TLS 1.2 atau 1.3. Dukungan terhadap suite cipher yang rentan seperti RC4 dan SWEET32 juga perlu dinonaktifkan untuk mengurangi risiko serangan.

5.2 Saran

Berdasarkan hasil penelitian ini, berikut ini saran yang penulis berikan untuk pengembangan keamanan di penelitian kedepannya:

1. Untuk mengurangi risiko serangan brute force, implementasikan mekanisme perlindungan seperti rate limiting, captcha, dan lockout setelah beberapa upaya login yang gagal. Batasi metode HTTP yang diizinkan pada server dan nonaktifkan metode yang tidak diperlukan seperti TRACE dan TRACK yang rentan terhadap serangan.
2. Untuk mengurangi Tingkat keberhasilan pengambil alihan akun maka perlu diterapkan Autentikasi 2 Faktor. Dengan adanya autentikasi dua faktor tersebut, nantinya sistem akan melakukan verifikasi tambahan

selain kata sandi, seperti kode yang dikirim ke perangkat lain untuk memastikan bahwa akun tersebut diakses oleh user yang bersangkutan.

3. Lakukan Limit Kesalahan *Password* pada Sistem untuk Mengimplementasikan kebijakan yang membatasi jumlah percobaan gagal dalam login sebelum akun diblokir dan buat sistem password jangan menggunakan tanggal lahir untuk mencegah OSINT.
4. Menerapkan kebijakan keamanan yang komprehensif *seperti Content Security Policy* (CSP dan selalu perbaharui aplikasi yang ada agar tetap update dengan keamanan.