

## BAB V

### KESIMPULAN DAN SARAN

#### 5.1 KESIMPULAN

1. Penelitian ini mengidentifikasi dan mengeksploitasi berbagai celah keamanan dalam sistem informasi, seperti; Cross-Site Scripting (XSS), NoSQL *Injection* – Remote Code Execution (RCE), SQL *Injection*, Hidden API Functionality Exposure, XML RPC User Enumeration, Mass Assignment, Path Traversal, JSON Hijacking, Command *Injection* – Remote Code Execution (RCE), dan Insecure Direct Object Reference (IDOR).
2. Open-appsec terbukti mampu mendeteksi dan mencegah berbagai jenis serangan yang disebutkan di atas dengan efektivitas yang tinggi. Penggunaan open-appsec pada DVWS-Node memberikan lapisan perlindungan tambahan yang signifikan, meningkatkan kemampuan deteksi terhadap ancaman dan mitigasi terhadap kerentanan yang ada. Pengujian ini menunjukkan bahwa open-appsec dapat mendeteksi dan mencegah serangan Cross-Site Scripting (XSS), NoSQL *Injection*, SQL *Injection*, dan berbagai jenis serangan lainnya, yang mengindikasikan bahwa penggunaan WAF ini dapat meningkatkan keamanan aplikasi web secara keseluruhan.

#### 5.2 SARAN

1. Perlu dilakukan pengujian lebih lanjut dengan berbagai jenis serangan lain untuk memverifikasi efektivitas WAF Open-appsec dalam kondisi yang lebih bervariasi.
2. Implementasi WAF sebaiknya dikombinasikan dengan metode keamanan lainnya untuk meningkatkan lapisan perlindungan.
3. Penelitian lebih lanjut mengenai optimalisasi perancangan WAF Open-appsec agar dapat digunakan secara maksimal di lingkungan industri.
4. Penelitian lebih lanjut menggunakan metode eksploitasi yang otomatis.