# BAB V

# PENUTUP

## 5.1. KESIMPULAN

Berdasarkan hasil pengujian *Penetration Testing* pada *website* malatours yang telah dilakukan menggunakan metode OWASP Top 10. Berikut beberapa kesimpulannya:

1. Terdapat 14 celah keamanan yang ditemukan OWASP ZAP 2 celah keamanan berada pada tingkat resiko *High,* 3 celah keamanan pada tingkat resiko *Medium*, 6 celah keamanan pada tingkat *Low*, dan 3 celah keamanan pada tingkat *Informational*.
2. Hasil pengujian menunjukan terdapat 5 kategori kerentanan OWASP Top 10 yaitu *Broken Access Control, Cryptographic Failures, Injection, Insecure Design* dan *Identification and Authentication failure*.
3. Terdapat 5 tingkat resiko *Medium* diantaranya *Server Leaks Information via 'X-Powered By' HTTP Response header field, Cross Site Scripting,* Server Leaks Information via 'X-Powered By' *HTTP Response header* field, *Insecure Design* dan *User Enumeration*. Serta 3 tingkat resiko *low* diantaranya *Cookies without SameSite Attribute, Timestamp Disclosure – Unix,* dan *Information Disclosure –Suspicious Comments*Berhasil mengembangkan aplikasi otomatisasi OWASP ZAP untuk memudahkan dalam proses pengujian.
4. Berhasil membuat aplikasi otomatisasi analisis celah keamanan menggunakan OWASP ZAP
5. Berhasil membuat laporan mengenai hasil pengujian

## 5.2. SARAN

Berdasarkan hasil pengujian *Penetration Testing* yang dilakukan terdapat beberapa saran yang dapat digunakan untuk penelitian selanjutnya ataupun sistem pada *website* :

1. Pemilik *website* melakukan penambahan *plugin* keamanan pada *WordPress* seperti *plugin security firewall* untuk sebagai firewall tambahan , *plugin*

*hide WordPress* untuk menyembunyikan data-data tentang CMS *WordPress* dari *tools Scanning* , *plugin* anti XSS (*Cross Site Scripting)*, dan *plugin custom header* untuk mengkustomisasi *response header*.

2. Memberikan sistem kriptografi pada form password serta memberikan sistem captcha pada login field untuk mencegah adanya spam pada sesi login.
3. Melakukan pembaruan secara berkala pada sistem utama CMS *WordPress* seperti mengupdate *plugin,* dan php *version*.
4. Mempekerjakan seseorang yang profesional untuk fokus mengurus keamanan *website* malatours.