BAB 5

PENUTUP

5.1 Kesimpulan

Berdasarkan pengujian menggunakan OWASP *ZAP* menunjukkan bahwa *website server local* yang berdomain mail.umkt.sch.id memiliki 9 kerentanan yaitu, *Absence of Anti-CSRF Tokens, Content Security Policy (CSP) Header Not Set, Cookie No HttpOnly Flag, Cookie without SameSite Attribute, Server Leaks Version Information via "Server" HTTP Response Header Field, X-Content-Type-Options Header Missing, GET for POST, Modern Web Application, User Agent Fuzzer* dan berdasarkan pengujian penetrasi dengan menggunakan *tools Acunetix* dengan ketentuan OWASP *TOP* 10 2017 terdeteksi memiliki 5 kategori kerentanan *yaitu (A2) Broken Authentication, (A3) Sensitive Data Exposure, (A5) Broken Access Control, (A6) Security Misconfiguration* dan *(A9) Using Components with Known Vulnerabilities.*

5.2 Saran

Berdasarkan kesimpulan di atas maka saran dari penilitian ini adalah perlu dilakukan penelitian dengan menggunakan *metode Information System Security Assessment Framework* (ISSAF) agar dapat diketahui kerentanan apa saja secara mendalam pada web server.