BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan seluruh kegiatan yang telah dilakukan pada BAB IV dengan menggunakan metode VAPT (*Vulnerabilty Assesment and Penetration Testing*) dimulai dari *Reconnaissance* sampai dengan *reporting* dengan menggunakan beberapa teknik terhadap informasi yang didapatkan pada kerentanan *server* atau aplikasi web CV. Kazar Teknologi Indonesia, dapat disimpulkan bahwa:

1. Jenis kerentanan pada sistem *website* perusahaan CV. Kazar Teknologi Indonesia dikategorikan dengan dua jenis kerentanan yaitu berdasarkan aplikasi dan berdasarkan jaringan. Berdasarkan jaringan, kerentanan yang ditemukan Nessus berjumlah 1 *High*, 3 *Medium*, 1 *Low*, dan 37 *Info*, kemudian kerentanan yang ditemukan pada OpenVAS berjumlah *Medium* 9, dan *Low* 1. Selanjutnya, pengujian berdasarkan jaringan yang diujikan yaitu 1 *High*, 11 *Medium*, 1 *Low*, dan 6 *Information*, pengujian dikatakan positif dalam hasil pengujian yaitu terjadi pada protokol SSL/TLS, kemudian pada port HTTP, FTP, IMAP, POP3, dan MySQL. Selanjutnya, kerentanan berdasarkan aplikasi yang ditemukan OWASP ZAP berjumlah 1 *Medium*, 7 *Low*, dan 2 *Info*. Pengujian yang diujikan berdasarkan aplikasi yaitu 1 *Medium*, 5 *Low*, dan 1 *Info*, pengujian dikatakan positif dalam hasil pengujian yaitu tidak adanya CSRF, *cookie* yang bermasalah seperti tidak adanya *HttpOnly* dan tanpa adanya *SameSite Attribute*, terekspos informasi server melalui *X-Powered-By*, dan terjadinya *information disclosure*. Hasil kerentanan pada WPScan bersifat *Information* dan kerentanan tersebut dimanfaatkan oleh penulis untuk membantu keseluruhan pengujian berdasarkan jaringan dan berdasarkan aplikasi. Selain itu, *Severity* dan *Score* didapat berdasarkan dari *database tools* VA yang digunakan sehingga masing-masing VA memiliki penilaiannya masing-masing dalam menentukan *Severity* dan *Score*.

2. Pengujian kerentanan yang dilakukan atau *penetration testing* pada *website* perusahaan CV. Kazar Teknologi Indonesia dengan melakukan analisis jaringan menggunakan Wireshark pada jenis kerentanan jaringan, *bypass password* juga dilakukan pada jenis kerentanan jaringan, *brute force* dilakukan untuk mendapatkan *privilege escalation*, *inspect element* melalui *web browser* dilakukan pada jenis kerentanan aplikasi, dan *port scanning* dengan perintah dari nmap dilakukan pada jenis kerentanan jaringan.
3. Rekomendasi perbaikan untuk celah keamanan yang ditemukan dalam perbaikan keamanan pada sistem perusahaan CV. Kazar Teknologi Indonesia yaitu dengan cara melakukan pembaruan pada *software* dan protokol yang digunakan, melakukan penutupan port yang tidak digunakan dan apabila menggunakan port tersebut gunakan enkripsi dengan kekuatan enkripsi yang kuat. Terakhir, melakukan pelatihan pada seluruh karyawan mengenai *information security awarness* dan pelatihan pada tim IT mengenai pembuatan aplikasi dan jaringan yang *secure*.

5.2 Saran

Dalam penelitian yang telah dilakukan dengan metode VAPT, dibutuhkan pengujian dengan proses yang selalu berkembang mengenai uji kemanan pada server dan aplikasi web. Dibawah ini merupakan saran untuk penelitian selanjutnya:

1. Selain menggunakan *scope blackbox*, dapat menggunakan *scope* yang berbeda seperti *whitebox* atau *greybox* dikarenakan beberapa hasil pemindaian kerentanan yang ditemukan lebih maksimal jika dilakukan dengan satu jaringan yang sama dengan server. Karena dengan satu jaringan yang sama maka mudah mendapatkan informasi pada lalu lintas paket jaringan selama penelitian, contohnya seperti kerentanan *SSL Medium Strength Cipher Suites Supported SWEET 32*, *SSL/TLS: Report Vulnerable Cipher Suites for HTTPS*, dan *SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection*.
2. Penelitian untuk kerentanan dengan hasil pengujian negatif seperti *SSL Medium Strength Cipher Suites Supported SWEET 32, TLS Version 1.0*

Protocol Detection, HSTS Missing From HTTPS Server (RFC 6797), SSL/TLS: Report Vulnerable Cipher Suites for HTTPS, SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection, WebDAV Detection, dan *X-Frame-Options Header Not Set*. Dilakukan eksplorasi lebih dalam pada kerentanan tersebut, dikarenakan pada penelitian ini terkendala pandemi COVID-19 sehingga penelitian dilakukan dari jarak jauh.