

DAFTAR GAMBAR

Gambar 2.1 Logo PT. Global Inovasi Siber Indonesia (CyberArmyID)	6
Gambar 2.2 Misi dari PT. Global Inovasi Siber Indonesia (CyberArmyID)	7
Gambar 2.3 Struktur Organisasi Institusi PT. Global Inovasi Siber Indonesia (CyberArmyID)	8
Gambar 2.4 Alur Pekerjaan yang dilakukan pada tempat magang	10
Gambar 3.1 Contoh pengujian manual pada perangkat lunak fitur login	12
Gambar 3.2 Proses submit kode otentikasi untuk melakukan login	12
Gambar 3.3 Automated Testing menggunakan tools Selenium	13
Gambar 3.4 Automated Testing menggunakan tools Selenium	14
Gambar 3.5 Stress Testing menunjukkan error dengan kode error Connection timed out	14
Gambar 3.6 Detail hasil Stress Testing pada halaman register saat koneksi vpn terputus	15
Gambar 3.7 Penetration Testing pada aplikasi web yang rentan terhadap Cross Site Scripting (XSS)	15
Gambar 3.8 Proses Brute Force Attack berjalan pada BurpSuite	16
Gambar 3.9 Spesifikasi perangkat keras untuk Testing	20
Gambar 3.10 Selenium	21
Gambar 3.11 Apache JMeter	21
Gambar 3.12 Kali Linux OS	21
Gambar 3.13 BurpSuite Proxy	22
Gambar 4.1 Pengujian Manual Testing berdasarkan Test Cases	24
Gambar 4.2 Pengujian Manual Testing berdasarkan Test Cases	25
Gambar 4.3 Pengujian Automated Testing – Tampilan awal Selenium	26
Gambar 4.4 Pengujian Automated Testing – Selenium Testing UI	26
Gambar 4.5 Pengujian Automated Testing - Source Code VSCode menggunakan Python	27
Gambar 4.6 Pengujian Automated Testing - Source Code VSCode menggunakan Python	27
Gambar 4.7 Pengujian Automated Testing - Login menggunakan recovery code	28
Gambar 4.8 Pengujian Automated Testing - Halaman awal setelah melakukan login aplikasi Data Protection	28
Gambar 4.9 Pengujian Penetration Testing – Cross Site Scripting (XSS) Vulnerabilities	29
Gambar 4.10 Pengujian Penetration Testing – Brute Force Attack pada Burpsuite Proxy	29
Gambar 4.11 Pengujian manual dengan invalid blank input	30
Gambar 4.12 Pengujian manual dengan input valid	31
Gambar 4.13 Tampilan aplikasi setelah melakukan registrasi dengan input valid, diarahkan ke halaman 2FA	31
Gambar 4.14 Tampilan awal Selenium	32
Gambar 4.15 Tampilan Tools Selenium	32
Gambar 4.16 Tampilan project automation testing Selenium	33
Gambar 4.17 Tampilan Selenium menambahkan Test Case	33
Gambar 4.18 Tampilan project automation testing Selenium	34

Gambar 4.19 Tampilan project automation testing Selenium	34
Gambar 4.20 Tampilan Visual Studio Code dengan source code untuk melakukan Automated Testing	37
Gambar 4.21 Tampilan Visual Studio Code dengan source code untuk melakukan Automated Testing	37
Gambar 4.22 Penguji menginput 6 digit kode untuk melakukan login ke dalam aplikasi Data Protection	38
Gambar 4.23 Tampilan halaman awal aplikasi Data Protection setelah melakukan login menggunakan recovery code	39
Gambar 4.24 Tampilan UI Apache JMeter	35
Gambar 4.25 Tampilan UI Apache JMeter	35
Gambar 4.26 Tampilan output dari Stress Testing Apache JMeter – View Results Tree	36
Gambar 4.27 Tampilan output dari Stress Testing Apache JMeter – Summary Report	37
Gambar 4.28 Tampilan dari fitur Incident aplikasi Data Protection	38
Gambar 4.29 Tampilan form Task pada fitur Incident aplikasi Data Protection	38
Gambar 4.30 Tampilan dari fitur Incident aplikasi Data Protection	39
Gambar 4.31 Tampilan dari fitur Incident aplikasi Data Protection – Cross Site Scripting (XSS)	39
Gambar 4.32 Tampilan dari fitur Incident aplikasi Data Protection – Cross Site Scripting (XSS)	40