

LIST OF FIGURES

Figure I.1. Number of Users Internet in Indonesia (APJII, 2020)	1
Figure II.1. Website is a collection of webpage.....	5
Figure II.2. Different types of penetration testing techniques	9
Figure III.1 Stages of Problem Solving.....	13
Figure IV.1 Testing Scenario	19
Figure IV.2 Attack Topology	20
Figure V.1 First Search Engine Discovery	27
Figure V.2 Second Search Engine Discovery	27
Figure V.3 Fingerprint Web Server (netcraft).....	28
Figure V.4 Fingerprint Web Server (demascara.me).....	28
Figure V.5. Meta Tag XYZ Website.....	29
Figure V.6 Analyzing robots.txt.....	29
Figure V.7. Reverse IP Domain Check.....	30
Figure V.8 Analysis using nmap	30
Figure V.9 Webpage comments and Metadata for Information Leakage	31
Figure V.10 Identify Application Entry Points (GET).....	32
Figure V.11 Identify Application Entry Points (POST).....	32
Figure V.12 Map Execution Path Through Application	32
Figure V.13 Fingerprint Web Application Framework.....	33
Figure V.14 Fingerprint Web Application.....	33
Figure V.15 Map Application Architecture	34
Figure V.16 Testing for Reflected Cross-Site Scripting (Owasp ZAP).....	34
Figure V.17 First Step Testing XSS Reflected Using Burp Suite.....	35
Figure V.18 Second Step XSS Reflected Test Using Burp Suite	35
Figure V.19 Result XSS Reflected Using Burp Suite.....	36
Figure V.20 Testing for Stored Cross-Site Scripting.....	36
Figure V.21 HTTP Verb Tampering (OPTION).....	37
Figure V.22 HTTP Verb Tampering (GET)	37
Figure V.23 HTTP Verb Tampering (POST)	38

Figure V.24 HTTP Verb Tampering (HEAD)	38
Figure V.25 HTTP Verb Tampering (PUT).....	39
Figure V.26 HTTP Verb Tampering (DELETE)	39
Figure V.27 HTTP Verb Tampering (TRACE)	40
Figure V.28 First step for testing HTTP Parameter Pollution	41
Figure V.29 Second Step for testing HTTP Parameter Pollution	41
Figure V.30 Testing HTTP Parameter Pollution.....	42
Figure V.31 Testing for SQL Injection Using OWASP ZAP	43
Figure V.32 Testing for SQL Injection Using SQLMap.....	43
Figure V.33 LDAP Injection Payload.....	44
Figure V.34 LDAP Injection Result.....	44
Figure V.35 XML Injection Using OWASP ZAP	45
Figure V.36 SSI Injection Using OWASP ZAP	45
Figure V.37 XPATH Injection Input Code	46
Figure V.38 XPATH Injection Result.....	46
Figure V.39 Code Injection Using First Code Injection.	47
Figure V.40 First Code Injection Result	48
Figure V.41 Code Injection Using Second Code Injection.....	48
Figure V.42 Second Code Injection Result.....	49
Figure V.43 Command Injection using OWASP ZAP	49
Figure V.44 Buffer Overflow testing using OWASP ZAP	50
Figure V.45 First step of testing Incubated Vulnerabilities	51
Figure V.46 Result after submitting data from registration.	51
Figure V.47 Second step of testing Incubated Vulnerabilities.....	52
Figure V.48 Result after clicking the login button.....	52
Figure V.49 First step for testing HTTP Splitting/Smuggling.....	53
Figure V.50 Second Step for HTTP Splitting and Smuggling.....	54
Figure V.51. Inputting the code result to the browser.....	54
Figure V.52 Result for HTTP Splitting and Smuggling.	55
Figure V.53 DOM Based Scripting.....	56
Figure V.54 Input Code for JavaScript Execution.	56
Figure V.55 Result Javascript Execution	57

Figure V.56 HTML Injection Result using Burp Suite.....	58
Figure V.57 First Step for Client Side URL Redirect Testing.....	59
Figure V.58 Second Step for Client Side URL Redirect	59
Figure V.59 Result for Client Side URL Redirect	60
Figure V.60 CSS Injection Result.....	60
Figure V.61 Client Side Resource Manipulation	61
Figure V.62 Cross Origin Resource Sharing.....	62
Figure V.63 Testing for Cross-Site Flashing	62
Figure V.64 First Step Testing for Clickjacking.....	63
Figure V.65 Clickjacking Result.....	63
Figure V.66 Testing Websocket Result	64
Figure V.67 Testing Web Message Application	65
Figure V.68 Result for Local Storage Testing	65