# DAFTAR ISI

ABSTRAK ........................................................................................ ii

*ABSTRACT* ........................................................................................ iii

LEMBAR PENGESAHAN ........................................................................ iv

LEMBAR PERNYATAAN ORISINALITAS .................................................... i

Kata pengantar .................................................................................. ii

Daftar Isi ......................................................................................... iii

Daftar Gambar ................................................................................. viii

Daftar Tabel ..................................................................................... x

Daftar lampiran ................................................................................. xi

Daftar Istilah ..................................................................................... xii

Bab I Pendahuluan ............................................................................ 1

I.1 Latar Belakang ................................................................................ 1

I.2 Perumusan Masalah ........................................................................ 3

I.3 Tujuan Penelitian ............................................................................ 3

I.4 Batasan Penelitian ........................................................................... 3

I.5 Manfaat Penelitian ........................................................................... 4

Bab II Tinjauan Pustaka ...................................................................... 5

II.1 Penelitian Terdahulu ....................................................................... 5

II.2 *Cyber Crime* ................................................................................. 6

II.3 Keamanan Informasi ....................................................................... 7

II.4 Kerentanan *Website* ....................................................................... 8

II.5 Damn Vulnerable Web App (DVWA) ................................................. 10

II.6 *Walkthrough* ................................................................................ 11

II.7 *Threat Modelling* .......................................................................... 11

II.8 *Activity Diagram* .......................................................................... 11

II.9 *Data Flow Diagram* ........................................ 12
II.10 Web Application Firewall ........................................ 12
II.11 OctopusWAF ........................................ 12
II.12 Kali Linux ........................................ 12
II.13 *Penetration Testing* ........................................ 13
II.14 *Vulnerability* ........................................ 13
II.15 *Threat* ........................................ 13
II.16 *Control* ........................................ 13
II.17 CWE ........................................ 13
II.18 CVE ........................................ 14
II.19 CVSS ........................................ 14
II.20 CVSS v2 Calculator ........................................ 14
II.21 CVSS Score ........................................ 14
II.22 *Attack Trees* ........................................ 15
II.23 Arachni ........................................ 15
II.24 Information Systems Security Assessment Framework (ISSAF) ..... 15
........................................ 16
Bab III Metodologi Penelitian ........................................ 17
III.1 Sistematika Penyelesaian Masalah ........................................ 17
III.2 Pengumpulan Data ........................................ 19
III.3 Pengolahan Data atau Proses Pengembangan Produk / Artifak ........... 19
III.3.1 Tahap Awal ........................................ 19
III.3.2 Tahap Hipotesis ........................................ 19
III.3.3 Tahap Eksperimen ........................................ 19
III.3.4 Tahap Analisis ........................................ 20
III.3.5 Tahap Akhir ........................................ 20

III.4 Metode Evaluasi ........ 20

III.5 Alasan Pemilihan Metode ........ 20

III.6 Jadwal Kegiatan ........ 21

Bab IV Perancangan sistem dan skenario pengujian ........ 22

IV.1 *Information Gathering* ........ 22

IV.1.1 Spesifikasi Perangkat Keras ........ 22

IV.1.2 Spesifikasi Perangkat Lunak ........ 23

IV.1.3 Platform Eskperimen ........ 25

IV.2 *Network Mapping* ........ 26

IV.2.1 Daftar IP *Address* ........ 26

IV.2.2 Gambaran Mekanisme Topologi ........ 26

IV.2.3 Gambaran Mekanisme TCP/IP ........ 28

IV.3 *Vulnerability Identification* ........ 29

IV.3.1 Skenario Pengujian *Vulnerability Scanning* Menggunakan Arachni 29

IV.4 *Penetration* ........ 30

IV.4.1 Skenario Pengujian Serangan Berdasarkan *Activity Diagram* ........ 31

IV.4.2 Skenario Pengujian Berdasarkan *Data Flow Diagram* ........ 31

Bab V Analisis ........ 33

V.1 Analisis Pemilihan Metode ISSAF Berdasarkan Literatur ........ 33

V.2 Analisis Pemilihan OctopusWAF Berdasarkan Literatur ........ 34

V.3 Analisis Literatur *Vulnerability* pada DVWA ........ 36

V.4 Analisis *Vulnerability* berdasarkan Data Sampling ........ 37

V.5 Analisis serangan Berdasarkan CWE ........ 38

V.6 Analisis Serangan Berdasarkan CVE ........ 40

V.7 Perancangan *Activity Diagram* ........ 41

V.7.1 Hasil perancangan *Activity Diagram* SQL Injection ..................... 42

V.7.2 Hasil perancangan *Activity Diagram Blind* SQL .......................... 44

V.7.3 Hasil perancangan *Activity Diagram Brute Force Attack* ............. 46

V.7.4 Hasil perancangan *Activity Diagram Command Injection* ........... 48

V.7.5 Hasil perancangan *Activity Diagram Clickjacking* ....................... 50

V.7.6 Hasil perancangan *Activity Diagram XSS* (Reflected) .................. 52

V.7.7 Hasil perancangan *Activity Diagram* SQL *Injection* Menggunakan *Web Application Firewall* .......................................................................... 53

V.7.8 Hasil perancangan *Activity Diagram Blind* SQL Menggunakan *Web Application Firewall* ...................................................................... 56

V.7.9 Hasil perancangan *Activity Diagram Brute Force Attack* Menggunakan *Web Application Firewall* ................................................... 58

V.7.10 Hasil perancangan *Activity Diagram Command Injection* Menggunakan *Web Application Firewall* ................................................... 61

V.7.11 Hasil perancangan *Activity Diagram Clickjacking* Menggunakan *Web Application Firewall* .......................................................................... 64

V.7.12 Hasil perancangan *Activity Diagram XSS* (*Reflected*) Menggunakan *Web Application Firewall* .......................................................................... 66

V.8 Perancangan *Data Flow Diagram* ....................................................... 70

V.8.1 Hasil *Data Flow Diagram Walkthrough* SQL *Injection* ............... 70

V.8.2 Hasil *Data Flow Diagram Walkthrough Blind SQL* ..................... 72

V.8.3 Hasil *Data Flow Diagram Walkthrough Brute Force Attack* ....... 74

V.8.4 Hasil *Data Flow Diagram Walkthrough Command Injection* ...... 75

V.8.5 Hasil *Data Flow Diagram Walkthrough Clickjacking* ................. 76

V.8.6 Hasil *Data Flow Diagram Walkthrough XSS* (*Reflected*) ............. 77

V.8.7 Hasil *Data Flow Diagram Walkthrough* SQL *Injection* Menggunakan *Web Application Firewall* ................................................... 79

V.8.8 Hasil *Data Flow Diagram Walkthrough Blind SQL* Menggunakan *Web Application Firewall* ........ 80

V.8.9 Hasil *Data Flow Diagram Walkthrough Brute Force Attack* Menggunakan *Web Application Firewall* ........ 82

V.8.10 Hasil *Data Flow Diagram Walkthrough Command Injection* Menggunakan *Web Application Firewall* ........ 84

V.8.11 Hasil *Data Flow Diagram Walkthrough Clickjacking* Menggunakan *Web Application Firewall* ........ 86

V.8.12 Hasil *Data Flow Diagram Walkthrough XSS* (*Reflected*) Menggunakan *Web Application Firewall* ........ 87

V.9 Analisis Perhitungan *Vulnerability* Dengan CVSS Calculator v2 ........ 90

V.9.1 Analisis Efektivitas Secara Kuantitatif Berdasarkan *Vulnerability* dan *Threat* ........ 98

V.9.2 Analisis Hasil Serangan Secara Kualitatif Berdasarkan *Vulnerability* dan *Threat* ........ 101

Bab VI Kesimpulan dan saran ........ 103

VI.1 Kesimpulan ........ 103

VI.2 Saran ........ 103

Daftar Pustaka ........ 104

Lampiran ........ 106