WAF Project - Complete Feature Analysis

1. Authentication & User Management

User Authentication System

- **Flask-Login Integration**: Session-based authentication with user roles
- **Password Hashing**: Bcrypt for secure password storage
- **Role-Based Access Control**: Admin and regular user roles
- **Default Admin Account**: Auto-created with credentials (admin/admin123)
- **Session Management**: Secure login/logout functionality

User Management (Admin Only)

- **Add Users**: Create new users with username, email, password, and role
- **Edit Users**: Modify existing user details except passwords
- **Delete Users**: Remove users (except self-deletion protection)
- **Role Assignment**: Admin or regular user privileges

2. IP-Based Security Controls

IP Blacklisting

- **Automatic Blocking**: IPs blocked based on various security violations
- **Manual Blocking**: Admin can manually block specific IPs
- **Persistent Storage**: Blacklist saved to file (`blacklist.txt`)
- **Firewall Integration**: OS-level blocking (iptables/Windows Firewall/macOS pf)
- **Unblocking**: Manual IP unblocking capability

Trusted IP Management

- **Whitelist System**: Trusted IPs bypass most security checks
- **Admin Protection**: Cannot remove own IP from trusted list
- **Automatic Privileges**: Trusted IPs get priority access
- **File-Based Storage**: Persistent trusted IP list (`trusted_ips.txt`)

Rate Limiting

- **Request Rate Control**: 50 requests per 60-second window (configurable)

- **Sliding Window**: Time-based request tracking per IP
- **Concurrent Request Limiting**: Max 10 concurrent requests per IP
- **Automatic Blocking**: Rate limit violators get blacklisted

3. Threat Detection & Analysis

Machine Learning Integration

- **ML Model**: Pre-trained model for malicious payload detection (`waf_model.sav`)
- **Real-time Classification**: Analyzes request parameters and form data
- **Fallback Protection**: Regex patterns when ML model unavailable

Signature-Based Detection

- **SQL Injection**: Pattern matching for SQL injection attempts
- **Cross-Site Scripting (XSS)**: JavaScript injection detection
- **Command Injection**: System command execution attempts
- **Custom Patterns**: Extensible regex-based detection system

VirusTotal Integration

- **IP Reputation Check**: Real-time malicious IP detection
- **API Integration**: VirusTotal API v3 for threat intelligence
- **Caching System**: 24-hour cache to reduce API calls
- **Threat Classification**: Malicious, Suspicious, and Safe categorization

4. Request Analysis & Monitoring

Request Size Controls

- **Content Length Limits**: 10MB maximum payload size
- **Header Size Limits**: Individual header max 8KB, total 100KB
- **Header Count Limits**: Maximum 50 headers per request
- **Protection Against DoS**: Prevents resource exhaustion attacks

Request Timing Analysis

- **Processing Time Monitoring**: Max 30-second processing time
- **Request Timeout**: 45-second total request timeout
- **Slow Request Detection**: Identifies and blocks slow loris attacks

- **Performance Tracking**: Request duration logging

Stream Processing

- **Custom Stream Limiter**: Monitors request data streams
- **Real-time Analysis**: Analyzes requests as they're received
- **Timeout Protection**: Prevents hanging connections
- **Resource Management**: Efficient memory usage

5. Real-time Alerting System

Telegram Integration

- **Instant Alerts**: Real-time security notifications via Telegram
- **Bot Configuration**: Configurable bot token and chat ID
- **Attack Details**: Source IP, ports, attack type, MAC address
- **Automated Notifications**: Sends alerts for all security events

Comprehensive Logging

- **Security Log**: General security events and system status
- **Attack Log**: Detailed attack attempt records
- **Attacker Log**: Blocked IP information with timestamps
- **CSV Format**: Structured data for analysis and reporting

6. Web-Based Management Interface

Dashboard

- **Real-time Statistics**: Active IPs, blacklist size, concurrent requests
- **Quick Actions**: Block/unblock IPs, manage trusted lists
- **Log Viewing**: Real-time log display with filtering
- **System Status**: Overall WAF health monitoring

Management Pages

- **Blacklist Management**: View and modify blocked IPs
- **Trusted IP Management**: Configure whitelist
- **IP Reputation Check**: Manual VirusTotal lookups

- **Settings Configuration**: Runtime parameter modification

Log Management

- **Log Viewing**: Real-time display of all log types
- **Export Functionality**: Download logs as CSV files
- **Log Deletion**: Admin can clear logs when needed
- **Filtering Options**: Search and filter log entries

7. System Integration

Operating System Support

- **Linux**: iptables integration for firewall rules
- **Windows**: Windows Firewall (netsh) integration
- **macOS**: Packet Filter (pf) integration
- **Cross-platform**: Works across different operating systems

Database Integration

- **SQLite Database**: User management and persistent storage
- **Connection Pooling**: Efficient database connections
- **Error Handling**: Robust database error management
- **Data Integrity**: Proper transaction handling

8. Security Features

Request Validation

- **Parameter Analysis**: Checks GET/POST parameters
- **Form Data Validation**: Analyzes form submissions
- **Raw Data Inspection**: Binary data analysis
- **Multi-layer Detection**: Multiple validation techniques

MAC Address Tracking

- **Pseudo MAC Generation**: Creates unique device identifiers
- **Device Tracking**: Associates requests with devices
- **Enhanced Logging**: Device information in security logs
- **Identity Correlation**: Links multiple requests from same device

Session Security

- **Secure Session Keys**: Random session key generation
- **Login Requirements**: Protected routes require authentication
- **Role-based Authorization**: Different access levels
- **Session Timeout**: Automatic logout for security

9. Performance Optimization

Caching Systems

- **VirusTotal Cache**: 24-hour API response caching
- **Memory Management**: Efficient data structure usage
- **Thread Safety**: Thread-safe operations with locks
- **Resource Cleanup**: Proper resource disposal

Concurrent Processing

- **Thread Safety**: Multi-threaded request handling
- **Connection Limits**: Prevents resource exhaustion
- **Request Queuing**: Manages high traffic scenarios
- **Memory Efficiency**: Optimized data structures

10. Configuration Management

Runtime Configuration

- **Dynamic Settings**: Modify settings without restart
- **Configuration Persistence**: Settings saved to files
- **Environment Adaptation**: Adjusts to system capabilities
- **Error Recovery**: Graceful handling of configuration errors

Customizable Parameters

- **Rate Limits**: Adjustable request thresholds
- **Timeout Values**: Configurable timing parameters
- **File Paths**: Customizable log and data file locations
- **API Keys**: External service configuration

11. Error Handling & Recovery

Robust Error Management

- **Exception Handling**: Comprehensive try-catch blocks
- **Graceful Degradation**: Continues operation when components fail
- **Error Logging**: Detailed error information capture
- **Recovery Mechanisms**: Automatic error recovery where possible

System Resilience

- **Failover Protection**: Continues operation without ML model
- **Resource Protection**: Prevents system overload
- **Data Consistency**: Maintains data integrity during errors
- **Service Continuity**: Minimal downtime during issues

12. Compliance & Audit Features

Audit Trail

- **Complete Logging**: All security events recorded
- **Timestamp Tracking**: Precise event timing
- **User Action Logging**: Admin actions tracked
- **Data Export**: Compliance reporting capabilities

Security Standards

- **Input Validation**: Comprehensive input sanitization
- **Output Encoding**: Prevents injection attacks
- **Secure Headers**: HTTP security headers implementation
- **Access Control**: Proper authorization mechanisms

This WAF implementation provides enterprise-grade security features with real-time threat detection, comprehensive logging, and an intuitive management interface suitable for protecting web applications from various cyber threats.