# Advanced Threat Detection Rules for Acunetix / Vulnweb

## 1. Introduction

Acunetix is a web vulnerability scanner that identifies SQL injection, XSS, CSRF, RCE, LFI, RFI, SSRF, and other security flaws. This document presents advanced threat detection rules to enhance security monitoring and response mechanisms.

## 2. Fundamentals of Threat Detection

To create effective threat detection rules, we rely on:  
- Behavioral Analysis: Identifying anomalies in HTTP requests and responses.  
- Signature-Based Detection: Using known exploit patterns.  
- Heuristic Analysis: Detecting unknown threats through behavior.  
- Correlation Rules: Mapping attack patterns across multiple logs.

## 3. Rule Book Design for Advanced Threat Detection

Detection rules should be applied to:  
- Acunetix Scanner Logs  
- Web Application Logs (Apache/Nginx)  
- WAF Logs (ModSecurity, Cloudflare)  
- SIEM Rules (Splunk, ELK, Wazuh, Azure Sentinel)

## 3.1 Detecting Automated Vulnerability Scanning

Indicators:  
- High frequency of requests from a single IP.  
- Requests targeting known vulnerable paths.  
- Requests containing exploit payloads.

## 3.2 SQL Injection Detection

Indicators:  
- Use of SQL syntax (SELECT, UNION, DROP TABLE).  
- Error messages in HTTP responses.  
- Multiple failed login attempts with SQL payloads.

## 3.3 Cross-Site Scripting (XSS) Detection

Indicators:  
- Presence of <script> tags or onerror=alert(1).  
- Encoded payloads in requests.

## 3.4 Local File Inclusion (LFI) & Remote File Inclusion (RFI) Detection

Indicators:  
- Requests with ../ for directory traversal.  
- Requests with file://, http://, or ftp:// in parameters.

## 3.5 Credential Stuffing & Brute Force Attack Detection

Indicators:  
- Multiple failed login attempts within seconds.  
- Requests from different geolocations using the same credentials.

## 4. Testing & Validation

Once rules are created, testing is essential:  
- Simulate attacks using Acunetix, OWASP ZAP, and manual payloads.  
- Monitor SIEM alerts and adjust rule thresholds.  
- Reduce false positives by refining detection patterns.

## 5. Threat Intelligence & Rule Maintenance

To improve detection capabilities:  
- Integrate external threat feeds (AlienVault OTX, AbuseIPDB).  
- Update detection rules weekly based on new CVEs.  
- Use machine learning-based anomaly detection to enhance accuracy.

## 6. Conclusion

These advanced threat detection rules provide real-time protection against vulnerability scanners and exploits. The rules have been validated using real-world attack simulations, ensuring effective monitoring and mitigation.