AI for OWASP Top 10 Detection

AI-Powered Web Application Security with MITRE ATT&CK Mapping and WAF Rules

Detect OWASP Top 10 Vulnerabilities with Natural Language AI

Analyze web application attacks instantly. Get OWASP categorization, MITRE ATT&CK mapping, and automated WAF rules without writing complex queries.

Sample AI Prompt

```
"Analyze all web application security events from the past
7 days. Correlate injection attempts, authentication
failures, and access control violations. Map to OWASP Top
10 and MITRE ATT&CK. Include WAF rules and firewall
blocks."
```

From a single prompt, the AI analyzes web attacks and delivers:

What You Get

OWASP Mapping	MITRE ATT&CK	WAF Rules
Firewall Blocks	Priority Matrix	Compliance Impact

OWASP Top 10 Detection

OWASP ID	Category	Events	Status
A03:2021	Injection (SQLi, XSS)	100+	Critical
A07:2021	Auth Failures	100+	High
A01:2021	Broken Access Control	70+	High
A05:2021	Security Misconfig	50+	Medium

MITRE ATT&CK Mapping

Technique	Name	Evidence
T1190	Exploit Public-Facing App	100+ SQLi attempts
T1110.001	Password Guessing	12,453 failures
T1059	Command Interpreter	Command injection
T1078	Valid Accounts	Privilege escalation

AI-Generated Attack Sources

Source IP	Attack Type	Action
89.81.210.247	SQL Injection	Detected
220.227.62.168	Command Injection	Blocked
178.217.190.104	SQL Injection	Blocked
144.125.187.18	Brute Force	Blocked

AI-Generated WAF Rules

```
# ModSecurity - Block SQL Injection
SecRule ARGS "@detectSQLi" \
  "id:1001,phase:2,block,log,\
  msg:'SQL Injection Detected',\
  tag:'OWASP_TOP_10/A03'"

# Block Command Injection
SecRule ARGS "@rx (?i:(bash|sh|cmd))" \
  "id:1005,phase:2,block"
```

Firewall Block Commands

```
# Cisco ASA - Block attackers
access-list BLOCK deny ip host 89.81.210.247 any
access-list BLOCK deny ip host 220.227.62.168 any

# iptables - Linux
iptables -I INPUT -s 89.81.210.247 -j DROP
```

Compliance Impact

Framework	Status	Finding
PCI DSS 6.5.1	Fail	40% SQLi success
GDPR Art. 32	Risk	Data breach potential
HIPAA §164.312	Partial	Access control gaps

Key Capabilities

OWASP Mapping

Auto-categorize attacks to A01-A10

WAF Rule Generation

ModSecurity, AWS WAF, Cloudflare rules

Trend Analysis

Compare attack patterns over time

Log Sources

LogZilla accepts logs from **any syslog-compatible source**. App Store integrations include:

WAF: ModSecurity, AWS WAF, Cloudflare

Web: Apache, Nginx, IIS, HAProxy

Firewalls: Palo Alto, Fortigate, Cisco

IDS/IPS: Zeek, Snort, Suricata

Load Balancers: F5, Citrix, AWS ALB

API: Kong, AWS API GW, Azure APIM

Contact: sales@logzilla.net | www.logzilla.net