API SECURITY: THE INVISIBLE ATTACK SURFACE

How to Secure REST, GraphQL, and gRPC APIs

Executive Summary

APIs have become the primary attack surface for modern applications. With 83% of web traffic now API-based and mobile apps driving digital transformation, API security vulnerabilities pose existential risks to organizations. This whitepaper examines the OWASP API Security Top 10, analyzes real-world breaches, and provides actionable guidance for securing APIs across REST, GraphQL, SOAP, and gRPC protocols.

The API Security Crisis

APIs are fundamentally different from traditional web applications. While web apps present a visual interface that can be tested through browsers, APIs operate invisibly in the background, making vulnerabilities harder to detect. Key challenges include:

- **Broken Object-Level Authorization (BOLA):** 52% of APIs allow unauthorized access to other users' data
- **Broken Authentication:** 41% have authentication bypass vulnerabilities
- **Excessive Data Exposure:** 38% leak sensitive data in responses
- **Lack of Resources & Rate Limiting:** 45% vulnerable to DoS attacks
- **Mass Assignment:** 29% allow parameter manipulation attacks

CASE STUDY: INDIAN ARMY CYBER GROUP

How VIGIL Protects Critical Defense Infrastructure

Background

The Indian Army operates 100+ public-facing websites providing information to soldiers, veterans, and civilians. These sites face constant cyber threats from nation-state actors, hacktivist groups, and opportunistic attackers seeking to deface government property or gather intelligence. Prior to VIGIL deployment, the Army relied on manual security assessments and commercial scanners that failed to detect sophisticated attacks in real-time.

Challenge

The Army required a security platform that could:

- Detect defacement attacks within minutes, not hours
- Provide continuous vulnerability scanning across all sites
- Deploy on-premise for classified networks (air-gapped)
- Operate reliably under sustained nation-state attacks
- Generate automated compliance reports for audits

Solution

In April 2023, the Indian Army deployed VIGIL across their entire web infrastructure. The deployment included:

- AI-powered visual defacement detection scanning every minute
- Comprehensive vulnerability scanning with 50,000+ payloads
- Supply chain security monitoring for third-party scripts
- On-premise deployment for sensitive networks
- Integration with Army SOC for instant alerting

Results

18+ Months. 100+ Websites. Zero Breaches.

Threat Detection:

- Multiple sophisticated attack attempts blocked
- Average defacement detection time: 43 seconds
- Zero successful defacements in 18+ months
- Nation-state APT campaigns detected and mitigated

Operational Excellence:

- 99.9% platform uptime
- 75% reduction in security team workload
- Automated compliance reporting saving 200+ hours/quarter

"VIGIL has proven itself as an exceptional security platform under the most demanding operational conditions. The AI-powered threat detection is truly best-in-class, and the platform's reliability has been outstanding."

- Senior Security Officer, Indian Army Cyber Group

USER GUIDE: WEBSITE SECURITY MODULE

Complete Guide to Website Scanning and Vulnerability Management

Getting Started

The VIGIL Website Security Module provides comprehensive vulnerability scanning, defacement detection, and security monitoring for your web applications. This guide will walk you through setup, configuration, and daily operations.

Adding Your First Website

1. Log into VIGIL dashboard at https://cyber-shieldpro.com
2. Navigate to Assets > Websites > Add New
3. Enter website URL (e.g., https://example.com)
4. Verify ownership by adding DNS TXT record or uploading verification file
5. Click 'Start Scanning' to begin initial assessment

Configuring Scan Settings

Scan Types:

- **Unauthenticated Scan:** Tests public-facing surfaces (default)
- **Authenticated Scan:** Tests behind login (70% more coverage)
- **API Scan:** Tests REST/GraphQL/SOAP/gRPC APIs
- **Defacement Monitoring:** Real-time visual monitoring (1-min intervals)

Schedule Options:

- Continuous: 24/7 monitoring with daily scans
- Weekly: Every Sunday at 2 AM
- Monthly: First Sunday of month
- Custom: Define your own schedule

Understanding Scan Results

Vulnerability Severity Levels

CRITICAL (CVSS 9.0-10.0): Remote code execution, SQL injection, authentication bypass

HIGH (CVSS 7.0-8.9): XSS, CSRF, privilege escalation, sensitive data exposure

MEDIUM (CVSS 4.0-6.9): Information disclosure, weak encryption, security misconfiguration

LOW (CVSS 0.1-3.9): Best practice violations, minor information leakage

Remediation Workflow

6. **Review Findings:** Click on vulnerability to see details, affected URLs, proof of concept
7. **Get AI Guidance:** Click 'AI Copilot' for code-level remediation instructions
8. **Create Ticket:** Click 'Create Jira/ServiceNow Ticket' to assign to developer
9. **Apply Fix:** Implement remediation in your code/configuration
10. **Re-scan:** Click 'Verify Fix' to confirm vulnerability resolved
11. **Close Finding:** Mark as resolved after successful re-scan

Advanced Features

Authenticated Scanning

Authenticated scanning tests areas behind login, providing 70% more coverage than unauthenticated scans. Configure authentication:

- **Form-based:** Provide username/password, VIGIL logs in automatically
- **OAuth 2.0:** Provide client ID/secret, VIGIL handles token refresh
- **JWT:** Provide long-lived token or token generation endpoint
- **SAML:** Configure SAML assertion for SSO-protected apps

AI Visual Defacement Detection

VIGIL's AI monitors your website every minute, detecting defacements in <60 seconds:

- **Content Integrity:** Detects unauthorized text changes
- **SSL/TLS Monitoring:** Alerts on certificate expiry or changes
- **Visual Analysis:** AI compares screenshots to detect visual defacements
- **Instant Alerting:** Slack/email/PagerDuty notifications within 60 seconds

Supply Chain Security

VIGIL scans all JavaScript libraries loaded by your website:

- 15,000+ libraries checked against Snyk, npm audit, retire.js
- Detects vulnerable versions (jQuery, Bootstrap, Lodash, etc.)
- Identifies outdated libraries with known CVEs
- Alerts on new vulnerabilities in your dependencies

Compliance Reporting

VIGIL generates audit-ready compliance reports for major standards:

PCI-DSS Reports

- Quarterly ASV scan reports
- Evidence for all 12 requirements
- QSA-friendly format

CERT-In Reports

- Automated 6-hour incident reports
- Evidence collection (logs, screenshots, timeline)
- Government-approved format

Best Practices

- **Enable continuous scanning** for production websites
- **Configure authenticated scanning** for 70% more coverage
- **Enable defacement monitoring** for public-facing sites
- **Integrate with ticketing** (Jira/ServiceNow) for workflow automation
- **Configure SOC alerts** for critical findings
- **Review AI Copilot guidance** for faster remediation
- **Re-scan after fixes** to verify remediation

Support and Resources

Email Support: support@aaizeltech.com

Documentation: https://docs.cyber-shieldpro.com

24/7 Chat Support: Available in dashboard

VIGIL TECHNICAL SPECIFICATIONS

Architecture, Security, and Deployment Options

System Architecture

VIGIL is built on a modern, cloud-native architecture designed for scalability, reliability, and security:

Core Components

- **Scanning Engine:** Distributed scanner with 50,000+ vulnerability payloads
- **AI Defacement Detection:** Machine learning models with 98% accuracy
- **API Gateway:** RESTful API with OAuth 2.0 authentication
- **Data Pipeline:** Real-time processing with Apache Kafka
- **Database:** PostgreSQL with TimescaleDB for time-series data
- **Cache Layer:** Redis for high-performance caching
- **Web Interface:** React-based SPA with real-time updates

Security Certifications

- **SOC 2 Type II:** In progress (expected Q2 2025)
- **ISO 27001:** Information Security Management
- **ISO 27017:** Cloud Security
- **PCI-DSS:** Service Provider Level 1 (planned)

Deployment Options

SaaS (Multi-Tenant Cloud)

- Fastest deployment (< 1 hour)
- Automatic updates and new features
- 99.9% SLA with financial penalties
- Data centers in Delhi and Mumbai

Private Cloud (Dedicated Instance)

- Dedicated infrastructure for your organization
- Data isolation and custom security controls
- Custom SLA options
- Deployment in your preferred cloud/region

On-Premise (Air-Gapped)

- Full control over infrastructure
- No external data transfer
- Suitable for classified/sensitive networks
- Battle-proven by Indian Army

Integrations

SIEM

- Splunk, QRadar, ArcSight, Elastic SIEM

Ticketing

- Jira, ServiceNow, PagerDuty, Zendesk

DevOps

- GitHub Actions, GitLab CI/CD, Jenkins, CircleCI

Communication

- Slack, Microsoft Teams, Email, SMS, Webhook

Performance & Scalability

- **Scan Performance:** Up to 1,000 websites scanned concurrently
- **API Throughput:** 10,000+ requests/second
- **Data Retention:** 2 years (configurable)
- **Alert Latency:** <60 seconds for critical findings