# STATE OF WEB SECURITY 2024: INDIA REPORT

*Analysis of 10,000+ Indian Websites and Emerging Threat Trends*

## Executive Summary

This whitepaper analyzes the security posture of 10,000+ Indian websites across banking, healthcare, e-commerce, and government sectors. Our findings reveal that 78% of Indian websites have at least one high or critical severity vulnerability, with API security emerging as the fastest-growing threat vector. The average time to detect a defacement attack is 18.7 hours, resulting in significant brand damage and revenue loss.

**Key Findings:**

- 78% of Indian websites have high/critical vulnerabilities
- API vulnerabilities increased 157% year-over-year
- Supply chain attacks rose 312% (vulnerable JavaScript libraries)
- Average defacement detection time: 18.7 hours
- Banking sector most targeted with 2,847 attacks per month
- PCI-DSS compliance rate: only 23% of e-commerce sites

## Methodology

This report is based on security assessments of 10,247 Indian websites conducted between January 2023 and December 2024 using VIGIL's comprehensive vulnerability scanning platform. The dataset includes:

- 2,341 banking and financial services websites
- 1,856 healthcare provider websites
- 3,124 e-commerce platforms
- 1,789 government websites
- 1,137 educational institutions

Each website was scanned using 50,000+ vulnerability payloads covering OWASP Top 10, API security, supply chain vulnerabilities, and configuration issues. Authenticated scanning was performed where possible to achieve maximum coverage.

## Vulnerability Landscape

### Overall Security Posture

78% of websites have at least one high or critical severity vulnerability

Average 6.3 high/critical vulnerabilities per website

Median time to remediate critical vulnerability: 47 days

### Top 10 Vulnerabilities Found:

- **1. Broken Access Control (43% of websites)** - Authorization bypass, IDOR, privilege escalation
- **2. Cryptographic Failures (38%)** - Weak TLS, exposed sensitive data, inadequate encryption
- **3. Injection (34%)** - SQL injection, XSS, command injection
- **4. Insecure Design (31%)** - Missing security controls, business logic flaws
- **5. Security Misconfiguration (29%)** - Default credentials, unnecessary features, verbose errors
- **6. Vulnerable Components (27%)** - Outdated libraries, known CVEs
- **7. Authentication Failures (23%)** - Weak passwords, missing MFA, session issues
- **8. Software/Data Integrity Failures (19%)** - Insecure CI/CD, unverified updates
- **9. Logging/Monitoring Failures (17%)** - Insufficient logging, no alerting
- **10. SSRF (12%)** - Server-Side Request Forgery attacks

## API Security Crisis

API vulnerabilities emerged as the fastest-growing threat vector in 2024, with a 157% increase compared to 2023. This aligns with the rapid adoption of mobile apps and microservices architecture.

**API Vulnerability Trends:**

- **Broken Object Level Authorization (BOLA):** Found in 52% of APIs
- **Broken Authentication:** 41% of APIs have auth bypass vulnerabilities
- **Excessive Data Exposure:** 38% of APIs leak sensitive data in responses
- **Mass Assignment:** 29% vulnerable to parameter manipulation
- **Security Misconfiguration:** 34% use default or weak API keys

**Industry Impact:**

- **Banking:** Mobile banking APIs most targeted - 67% have critical vulnerabilities
- **Healthcare:** 43% of patient portals leak PHI through API responses
- **E-commerce:** 56% of payment APIs vulnerable to authorization bypass

## Supply Chain Security

Supply chain attacks targeting third-party JavaScript libraries increased 312% in 2024. The average Indian website loads 37 third-party scripts, each representing a potential attack vector.

**Most Commonly Vulnerable Libraries:**

- **jQuery (versions <3.5.0):** Found on 62% of websites
- **Bootstrap (versions <4.3.1):** Found on 48% of websites
- **Lodash (versions <4.17.21):** Found on 34% of websites
- **Moment.js (all versions):** Deprecated, found on 29% of websites
- **Angular.js (versions <1.8.0):** Found on 23% of websites

**Real-World Impact:**

British Airways breach (2018): Compromised Magecart script - £183M fine

Ticketmaster breach (2018): Third-party chatbot script - $1.7M fine

Event-stream attack (2018): Malicious NPM package - 8M downloads affected

## Defacement Attack Trends

Website defacements remain a significant threat, particularly for government and e-commerce sites. Our data shows that traditional monitoring approaches detect defacements far too late.

**Detection Time Analysis:**

- Traditional monitoring (24-hour checks): Average 18.7 hours to detect
- Content monitoring (hourly checks): Average 3.2 hours to detect
- VIGIL AI visual monitoring (1-minute checks): Average 0.8 minutes to detect

**Cost of Defacement:**

- E-commerce: ₹2-5 lakhs revenue loss per hour
- Banking: ₹8-12 lakhs brand damage per hour
- Government: National security implications, public trust erosion
- 60% of customers permanently abandon brand after seeing defacement

## Compliance Landscape

**PCI-DSS Compliance (E-commerce/Banking):**

- Only 23% of e-commerce sites fully compliant
- Average audit preparation time: 6-8 months
- Common gaps: Quarterly ASV scans (67%), vulnerability management (52%)

**HIPAA Compliance (Healthcare):**

- 43% of patient portals have PHI exposure vulnerabilities
- 38% lack proper access controls
- 29% have insufficient audit logging

**CERT-In Compliance (Government/All Sectors):**

- 6-hour incident reporting requirement
- 78% of organizations struggle with timely reporting
- Manual processes take 8-12 hours on average

## Recommendations

**For Organizations:**

- **Implement continuous security monitoring** rather than annual assessments
- **Prioritize API security testing** for mobile apps and microservices
- **Deploy real-time defacement detection** with <5 minute response time
- **Automate compliance reporting** for PCI-DSS, HIPAA, CERT-In
- **Scan all JavaScript dependencies** for supply chain vulnerabilities

**For Security Leaders:**

- **Shift from reactive to proactive security** with continuous monitoring
- **Invest in automation** to reduce MTTR by 70%+
- **Consolidate security tools** to reduce costs and complexity
- **Build security into DevOps pipelines** for shift-left approach

## Conclusion

The web security landscape in India is at a critical juncture. With 78% of websites containing high/critical vulnerabilities and API attacks increasing 157% year-over-year, organizations must modernize their security approaches. Traditional point-in-time assessments are no longer sufficient - continuous monitoring, automated compliance, and AI-powered threat detection are essential for protecting digital assets and customer data.

Organizations that adopt comprehensive security platforms like VIGIL can reduce their attack surface by 70%, accelerate compliance by 80%, and prevent costly breaches that damage brand reputation and customer trust.

### About VIGIL

VIGIL is India's most comprehensive web security and compliance platform, trusted by the Indian Army and leading enterprises. For more information, visit cyber-shieldpro.com