Secure your API with these 16 Practices  
  
 1. Authentication 🕵️‍♀️ - Verifies the identity of users accessing APIs.  
 2. Authorization 🚦 - Determines permissions of authenticated users.  
 3. Data Redaction 🖍️ - Obscures sensitive data for protection.  
 4. Encryption 🔒 - Encodes data so only authorized parties can decode it.  
 5. Error Handling ❌ - Manages responses when things go wrong, avoiding revealing sensitive info.  
 6. Input Validation & Data Sanitization 🧹 - Checks input data and removes harmful parts.  
 7. Intrusion Detection Systems 👀 - Monitor networks for suspicious activities.  
 8. IP Whitelisting 📝 - Permits API access only from trusted IP addresses.  
 9. Logging and Monitoring 🖥️ - Keeps detailed logs and regularly monitors APIs.  
10. Rate Limiting ⏱️ - Limits user requests to prevent overload.  
11. Secure Dependencies 📦 - Ensures third-party code is free from vulnerabilities.  
12. Security Headers 📋 - Enhances site security against types of attacks like XSS.  
13. Token Expiry ⏳ - Regularly expiring and renewing tokens prevents unauthorized access.  
14. Use of Security Standards and Frameworks 📘 - Guides your API security strategy.  
15. Web Application Firewall 🔥 - Protects your site from HTTP-specific attacks.  
16. API Versioning 🔄 - Maintains different versions of your API for seamless updates.  
  
Follow me here - [Brij kishore Pandey](https://www.linkedin.com/in/ACoAAAKDuMsBugjGZwz0pJy43LJ-6bVwc0gm9xQ)

Activate to view larger image,

