Tool: AbuseIPDB

Tool Name

AbuseIPDB

Description

AbuseIPDB (Abuse Internet Protocol Database) is a collaborative cybersecurity platform that collects and shares reports on malicious IP addresses from users, organizations, and automated systems around the world. It serves as a global threat intelligence service, helping security analysts, system administrators, and developers identify, report, and respond to abusive or suspicious IP activities such as: Spam sending, DDoS attacks, Hacking attempts, Phishing or malware delivery etc.

What Is This Tool About ?

AbuseIPDB is a specialty search engine and IP reputation service that helps identify malicious IP addresses by collecting abuse reports from around the world. It acts like a central intelligence hub for detecting cyber threats coming from suspicious or harmful IP addresses

Key Characteristics / Features

•Global IP reputation checking
• Free and paid API access
• Community-driven reports
• CSV and JSON export options
• Confidence score
• Categories of abuse classification
• Blacklist support
• Geolocation and ASN info
• Public reporting UI
• Bulk IP checking
• Abuse type breakdown
• RESTful API for integration
• Custom alerts and watchlists

Types / Modules Available

- IP Lookup
- API Access
- Bulk IP Analysis
- Abuse Report Submission
- Watchlist & Alerts
- Dashboard Analytics

How Will This Tool Help?

1. Detects Suspicious or Malicious IPs Instantly

– Helps identify whether an IP is associated with hacking, spam, scanning, or DDoS activity by checking its abuse history and score.

2. Improves Incident Response Speed

– During attacks or investigations, analysts can quickly verify IPs and take action (e.g., block, escalate, or ignore).

3. Supports Proactive Blocking and Threat Prevention

– Organizations can use the data to block dangerous IPs before they cause harm, based on their abuse confidence score.

4. Integrates with Security Systems (API Access)

– Easily integrates with firewalls, SIEM tools, or custom scripts to automate IP checking, blacklisting, and alerts.

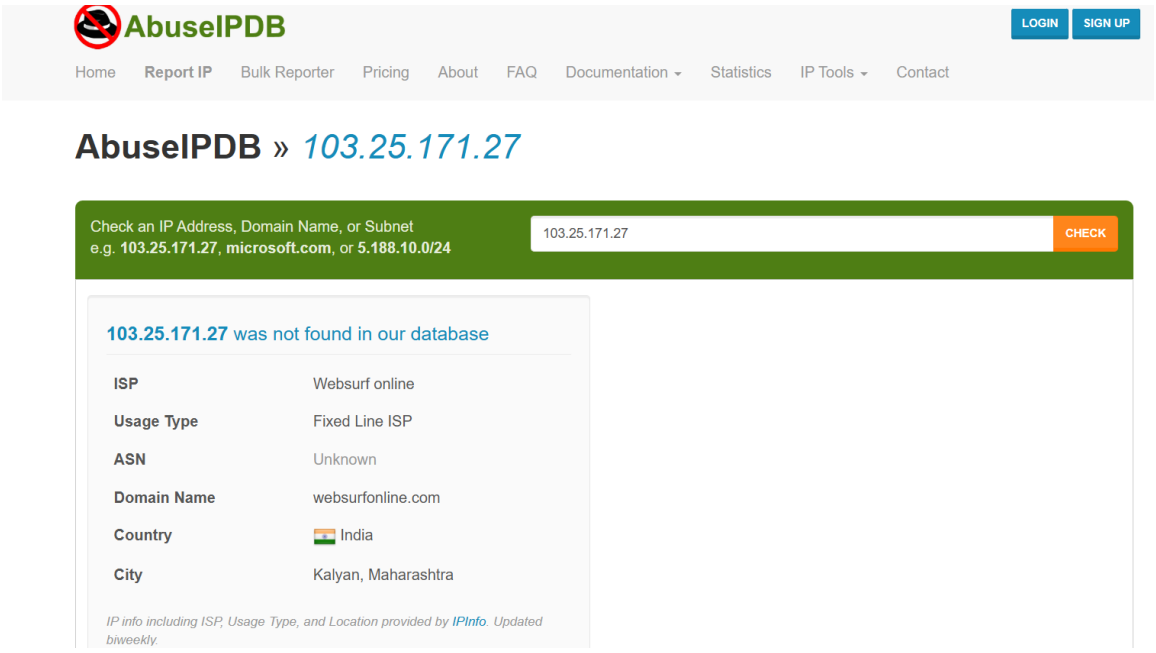
5. Enhances Threat Intelligence Capabilities

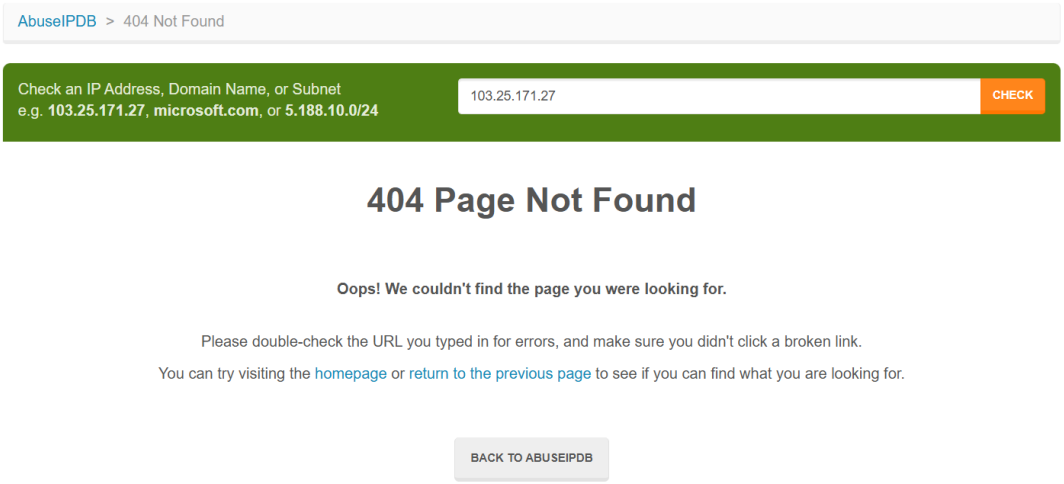
– Offers context (abuse category, frequency, source, location) that helps analysts understand the nature and behaviour of attackers.

Proof of Concept (PoC) Images

1. Homepage Interface
URL: https://www.abuseipdb.com

No Abuse Detected

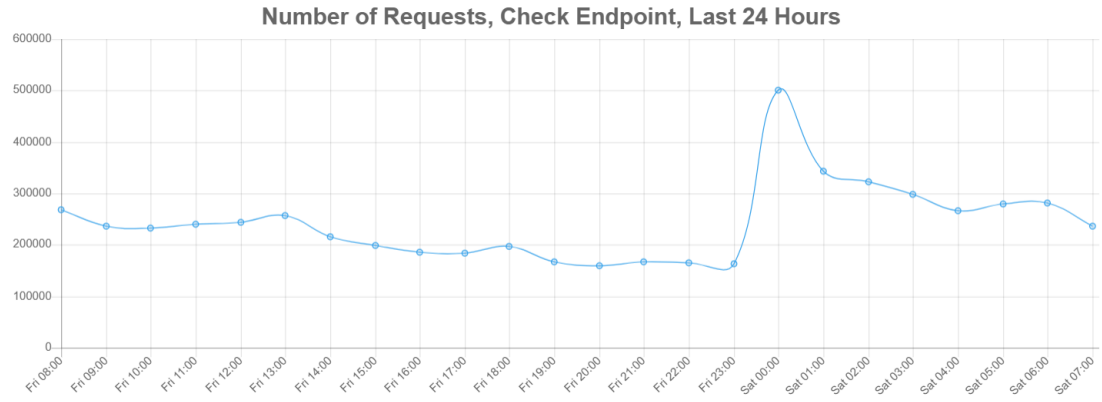




2) Abuse Trends or Statistics Page

https://www.abuseipdb.com/statistics

○ blacklist ○ bulk-report ◉ check ○ check-block ○ clear-address ○ report ○ reports



Most Widely Reported IP Addresses (Last 24 Hours)

1. **179.43.189.98** (2394 reports from 502 distinct users)
2. **195.178.110.160** (2220 reports from 445 distinct users)
3. **185.93.89.24** (2813 reports from 430 distinct users)
4. **195.178.110.125** (1370 reports from 413 distinct users)
5. **195.178.110.108** (1517 reports from 407 distinct users)
6. **116.110.79.137** (645 reports from 370 distinct users)
7. **193.32.162.157** (585 reports from 350 distinct users)
8. **195.178.110.211** (621 reports from 349 distinct users)
9. **116.110.79.123** (405 reports from 307 distinct users)
10. **176.65.149.226** (516 reports from 280 distinct users)

Summary

1. A global, community-driven IP abuse database.
2. Helps identify malicious IPs based on real user reports.
3. Assigns a confidence score (0–100) to rate IP risk.
4. Detects abuse types like spam, DDoS, brute-force, etc.
5. Offers RESTful API for integration and automation.
6. Supports bulk IP lookups for faster analysis.
7. Provides geolocation and ASN info for each IP.
8. Logs historical abuse data with timestamps.
9. Categories abuse reports for easier investigation.
10. Export results in JSON or CSV formats.
11. Integrates with firewalls, SIEMs, and scripts.
12. Enables custom alerts and IP watchlists.
13. Displays abuse trends with analytics and graphs.
14. Easy-to-use web interface and developer-friendly.
15. Free and paid tiers available based on usage needs.

Time to Use / Best Case Scenarios

• During live incident response
• While analyzing firewall logs
• Before allowing inbound IPs
• During SIEM rule development

When to Use During Investigation

• IP threat correlation
• Phishing detection
• Brute-force or scan tracking
• Suspicious login source analysis

Best Person to Use This Tool & Required Skills

Best Users : SOC Analysts, Threat Intelligence Analysts, Incident Responders, Network/System Administrators SIEM/Firewall Engineers, Cybersecurity Students/Interns.
Required Skills:

- Basic Networking Knowledge
- Log Analysis Skills
- Report Documentation
- Threat Intelligence Understanding
- SIEM/Firewall Familiarity
- API Usage & Automation

Flaws / Suggestions to Improve

• Limited API usage on free tier
• Some false reports
• No real-time attack feed
• Could add AI scoring

Good About the Tool

• Accurate scoring
• Community support
• Free access
• Integrates easily
• Simple UI

Tool: BeVigil

Tool Name
BeVigil

Description

BeVigil is the world's first mobile security search engine focused on analysing Android applications (APKs) for potential vulnerabilities, privacy violations, and malicious behaviours. It allows users—especially cybersecurity analysts, researchers, and app developers—to examine mobile applications for security flaws before installation or deployment.

BeVigil works by scanning APK files and identifying hardcoded secrets, dangerous permissions, outdated SDKs, and malware indicators. It assigns each app a security score (0–100) and aligns its results with the OWASP Mobile Top 10 risks, making it a trusted resource in mobile app security assessments.

The platform supports manual APK uploads, automatic crawling of public APK repositories, and offers RESTful API access for automation. It's especially helpful during app store reviews, third-party app vetting, DevSecOps pipelines, and mobile malware investigations.

What Is This Tool About ?
BeVigil is a mobile application security search engine designed to help users identify security and privacy risks in Android apps before installation or distribution. It acts like a "Shodan for mobile apps", scanning and indexing Android APKs for:

- Hardcoded secrets like API keys, tokens, and passwords
- Use of insecure or outdated SDKs and libraries
- Dangerous permissions that may lead to privacy violations

BeVigil is widely used by cybersecurity analysts, penetration testers, DevSecOps teams, and Android developers to assess app security posture and reduce the attack surface in mobile environments. It also provides a security score (0–100) that helps measure an app's overall safety.

Key Characteristics / Features
• APK scanning
• Hardcoded key detection
• Vulnerability scoring
• SDK/Tracker identification

• OWASP Mobile Top 10 alignment
• SSL/HTTPS flaw detection
• Play Store & APKMirror support
• API Access
• MITM detection
• CVE mapping

Types / Modules Available

• APK Analyzer
• Security Scorecard
• Hardcoded Secret Detection
• Tracker & SDK Summary
• Behavior Monitoring
• API Access

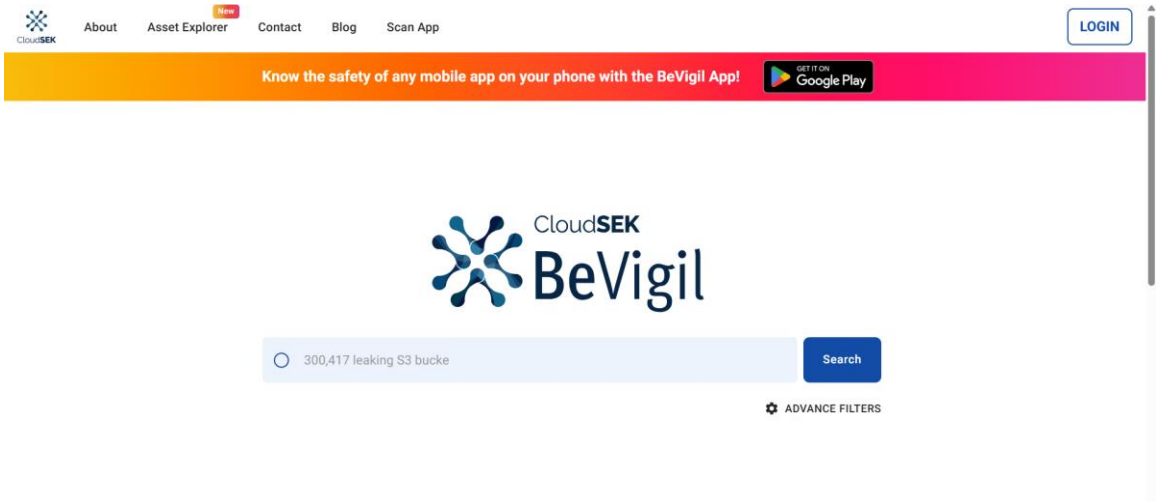
How Will This Tool Help?

- Detects Security Flaws in Android Apps Before Use: BeVigil scans APKs to identify vulnerabilities, insecure permissions, and exposed secrets, helping prevent exploitation before the app is installed or published.

- Protects User Privacy & Data: It flags apps that request unnecessary or dangerous permissions (like camera, SMS, or storage access), helping you avoid apps that could steal user data or spy.
- Assists in Mobile Malware Analysis: Security researchers and incident responders can analyze malicious APKs, uncover hardcoded payloads, and detect stealthy trackers or backdoors.

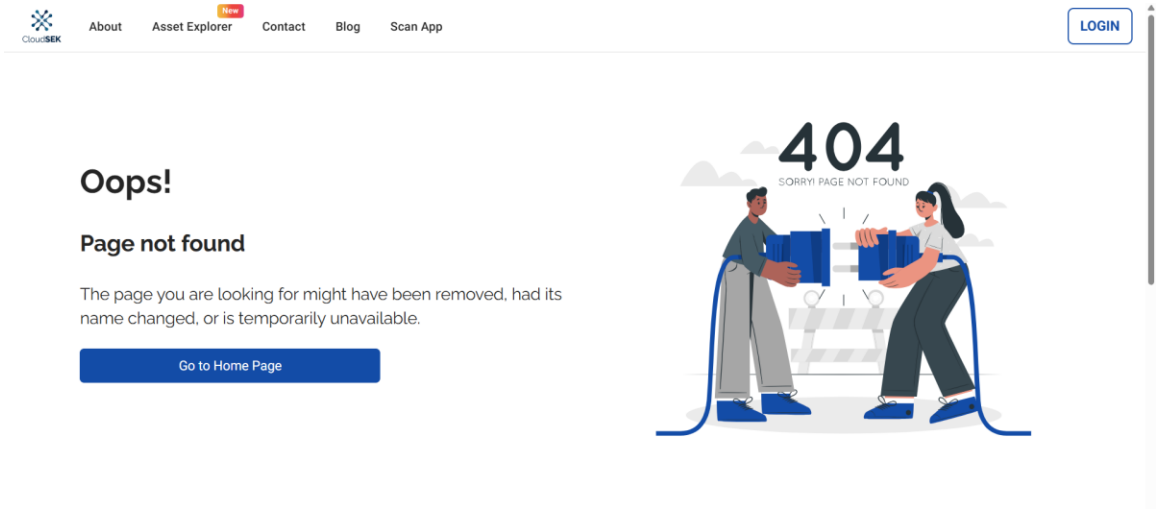
Proof of Concept (PoC) Images

url : https://bevigil.com



Limitations or Flaws in Tool

https://bevigil.com/en/upload



Summary

1. World's first mobile app security search engine.
2. Specializes in scanning Android APKs for vulnerabilities.
3. Assigns a security score (0–100) to each app.
4. Detects hardcoded secrets like API keys and passwords.
5. Flags apps with risky or overreaching permissions.
6. Identifies known trackers and analytics SDKs.

7. Checks for outdated or vulnerable libraries (CVEs).
8. Maps findings to OWASP Mobile Top 10 risks.
9. Offers API access for DevSecOps and automation.
10. Allows uploading and scanning of custom APKs.
11. Compares versions of the same app over time.
12. Provides source metadata like certificates and package names.
13. Helps in app store vetting and threat detection.
14. Useful for malware analysis and secure development.
15. Free to use with optional enterprise integrations.

Time to Use / Best Case Scenarios

- App security review
- Before APK installation
- Malware investigation
- Pre-publishing audits

When to Use During Investigation

- Phishing apps
- Data leaks via apps
- Malicious APK detection
- Internal app threat checks

Best Person to Use This Tool & Required Skills

- Best Users: Mobile Security Analysts, Android Developers, Penetration Testers, Malware Researchers etc.
- Required Skills:
  - Knowledge of Android App Structure (APK, Manifest, etc.)
    – Understand how apps are built and packaged in Android format.
  - API Integration & Automation (Optional)
    – Ability to use REST APIs for automated scanning and app monitoring during development.
  - Understanding of Mobile App Permissions & Security Risks
    – Recognize how permissions affect privacy and what makes them dangerous.

Flaws / Suggestions to Improve

- Android-only
- No iOS support
- No real-time scan

- Could improve behavior analysis

Good About the Tool

- Simple interface
- Free usage
- Shows hidden risks
- Great for researchers