

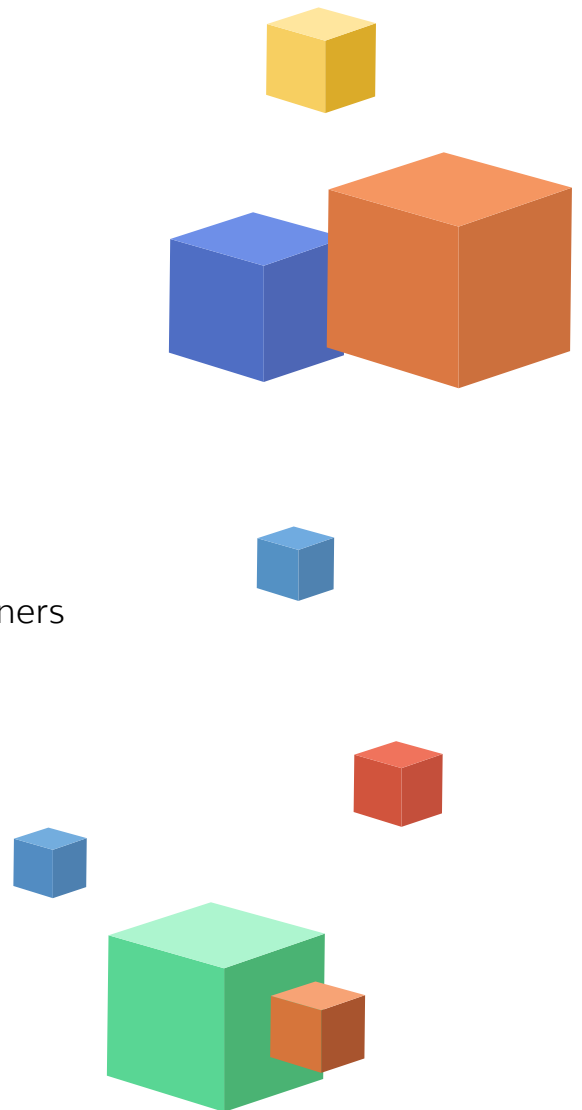


WHITEPAPER

The best free and open source tools for cyber risk assessment and mitigation

Table of Contents

- Summary
- Introduction
- Detect
 - Application Scanners
 - Network and Infrastructure Scanners
- Prioritize
- Remedy
- Automate
- Conclusion



Summary

It is difficult to fully fathom the impact of a hacker gaining access to your data and exploiting it for personal gain or just leaking it to the world. A successful cyberattack is every business executive's worst nightmare. In addition to the considerable direct costs, the loss of consumer confidence and damage to reputation can cripple a company or even cause its downfall. That's why it's critical for those in charge of IT security to stay on top of

software and hardware vulnerabilities, and for application and web developers to make sure that their code is airtight. This paper discusses some of the free and open source tools and data sources that security, IT operations, and DevOps personnel can use to help keep their computers, networks, and code fully patched, up to date, and protected from the ever-growing list of security vulnerabilities.



Introduction

Let's start with the end-game: The goal of vulnerability management is remediation. Success is not measured by how many vulnerabilities you detect but rather how well you fix the ones that expose your company to the greatest cybersecurity risk. The path to vulnerability remediation, however, winds its way through important tasks and processes, such as detection and prioritization. And for a vulnerability remediation program to be effective, especially at scale, its workflows must be as automated and as efficient as possible.


The front end of every vulnerability remediation program is scanning. You can't fix what you can't find. So, the first set of free tools we review are two classes of scanners: Those that scan applications throughout their lifecycle and those that scan networks and infrastructures.

But then what do you do with all those detected vulnerabilities? There will always be too many to remediate them all. More importantly many

vulnerabilities might not even need to be remediated based on risk or potential impact to the business, with every business having its own risk profile. This is where prioritization kicks in, and we'll describe some of the leading vulnerability repositories and databases that can help identify the high-priority vulnerabilities you need to focus on.

Still, the journey isn't over. Now, you have to find the best fixes, solutions, and remedies for each of those high-priority vulnerabilities. Here, we'll introduce you to a new, unique and free library from Vulcan Cyber®: [Remedy Cloud](#).

Last but not least, we describe some free and open-source tools that promote automation and collaboration so that remedies can be applied consistently across your organization. This paper will help you get fix done, at the speed of business.



Detect

Vulnerability scanners monitor network-based assets (firewalls, routers, servers) or applications for known weaknesses due to misconfigurations or flawed code. In this section, we review the most popular, and free, vulnerability scanners available to developers and IT operators today.

APPLICATION SCANNERS

Vulnerabilities are all too often the vector through which hackers gain access to your networks and data. It is important, therefore, that code is scanned for vulnerabilities long before it goes into production.

Static Application Security Testing (SAST)

enforces coding guidelines and standards without executing code (white box testing). SAST scanners compare the code to libraries of known vulnerabilities and report on weak spots that need to be hardened. Some of the best free SAST tools are:

- [Bandit](#) is managed by the Python Code Quality Authority and specifically analyzes Python code.
- [NodeJsScan](#) is Docker-ready and easily integrated with CI/CD pipelines via a CLI or Python API. It scans for common security vulnerabilities such as remote code injection, open redirect, XSS, and more.
- [SonarQube](#) supports 25+ languages (both modern and legacy) and has a library of thousands of automated Static Code Analysis rules.

Dynamic Application Security Testing (DAST)

means running the application to perform functional testing to detect vulnerabilities, such as remote procedure calls, Session Initiation Protocol (SIP), and so on. This black box testing is extremely important because some security vulnerabilities only show up when the program is executed. The most popular free DAST tools are:

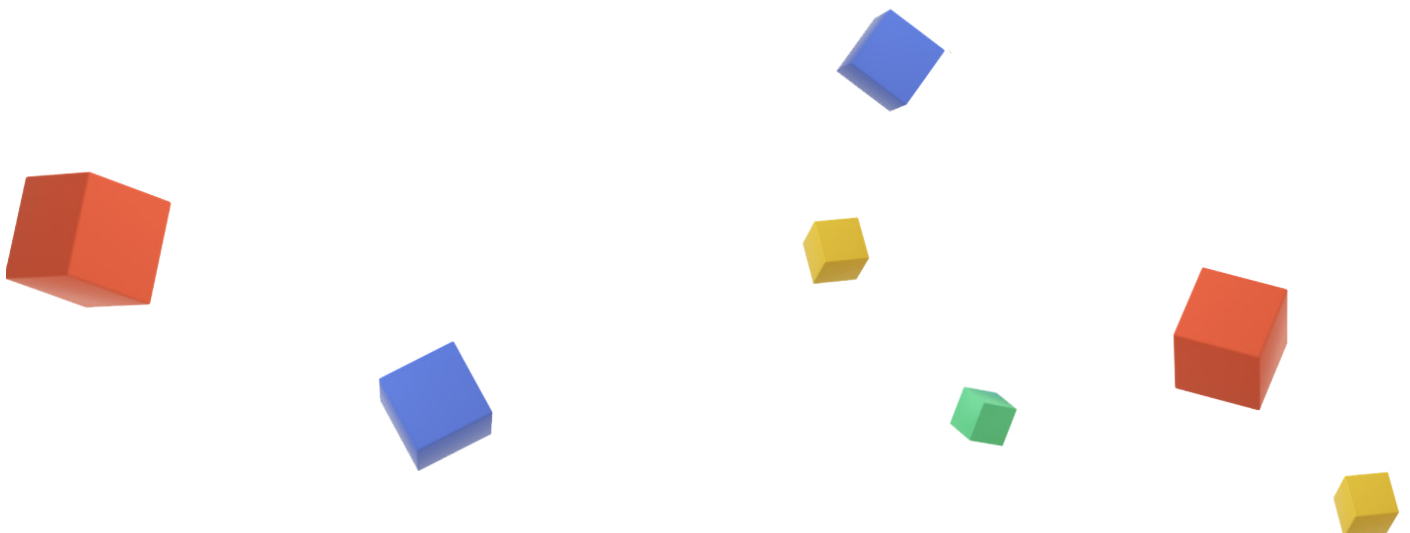
- [Archery](#) provides a color-coded dashboard view of the security status of applications running within an environment. Developers and pentesters can use it to catch and patch security vulnerabilities before the application is released to the public.
- [Arachni](#) is a full-featured, platform-agnostic program that can be deployed easily for both small and global-scale projects. The Arachni scanner offers "[extensive crawl coverage](#)" and "[near-perfect](#)" [vulnerability detection scores](#).
- [OWASP ZAP](#) (ZED Attack Proxy) passes website traffic through a proxy server, where built-in automated tests (or user-customized tests) are run to detect web application vulnerabilities. It supports all major OSes as well as Docker.

In this era of modern distributed application architectures that rely heavily on open-source code, it is also important that developers use **dependency scanners** to check for vulnerabilities in third-party code. Here are three free dependency scanners that you can use with confidence:

- [OWASP Dependency-Check](#) detects known vulnerabilities or vulnerable components within a project's dependent libraries.
- [Snyk](#) can detect vulnerabilities during coding (integrated IDE check) as well as monitor projects directly from the repository (native Git scanning). It can also set up a CI/CD security gate that prevents vulnerabilities from passing through the Build process.
- [WhiteSource Bolt for GitHub](#) continuously scans private and public repositories to detect vulnerabilities in open-source components. It also provides fixes.

Last but not least, there are **Runtime Application Self-Protection (RASP) tools** that use the application itself to continuously monitor its runtime behavior in order to identify and mitigate vulnerabilities without human intervention. Here are two free RASP tools:

- [Sqreen](#) covers all of the OWASP Top 10 security vulnerabilities, such as SQL injection, XSS, and SSRF, with a very low rate of false positives. Sqreen offers a free version limited to one production app.
- [Wapiti](#) audits web applications by crawling their web pages and injecting payloads to see if a script or form is vulnerable.



NETWORK AND INFRASTRUCTURE SCANNERS

Network and infrastructure scanners identify vulnerabilities in networks and network-attached devices such as communications equipment, servers, and edge devices. They scan for security vulnerabilities like unprotected network ingress and egress ports, unknown devices, account abuse, security misconfigurations, missing software updates, and more.



The leading free infrastructure vulnerability scanner is [OpenVAS](#), an open-source tool that includes over 50,000 vulnerability tests—and growing. It is secured with SSL and comprises a number of different modules that, together, deliver a comprehensive vulnerability analysis of your network infrastructure. OpenVAS' main drawbacks are that it can only be run in Linux, plus it has a steep learning curve.

The main alternatives to OpenVAS, all of which offer at least some form of free license, are:

- [Wireshark](#) is an open-source network protocol analyzer whose rich feature set includes deep inspection of hundreds of protocols, live capture of packets with offline analysis, and advanced display filtering.
- [Nmap](#) (“Network Mapper”) is an open-source tool used for network discovery and security auditing. It was first released in 1997 and runs on all major OSes; although it was designed to scan large networks, it also works well against single hosts.
- [Qualys Community Edition](#) automatically discovers IT assets and scans infrastructure and applications against their comprehensive vulnerability knowledge base
- [Burp Suite Community Edition](#) is a set of basic manual tools for auditing web security by intercepting and editing all requests and responses between the browser and the target application. The user gains granular control over rules and has access to free extensions from the user community.
- [W3af](#) is a mature but well-maintained open-source web application and audit tool that is typically used for application security/testing, pentesting, vulnerability scanning, and web application analysis.
- [Vuls](#) is an agentless open-source vulnerability scanner for Linux/FreeBSD based on multiple vulnerability databases such as NVD, JVN, and OVAL. It can run anywhere, supports both remote and local as well as fast and deep scans, and can also scan vulnerabilities of non-OS packages.

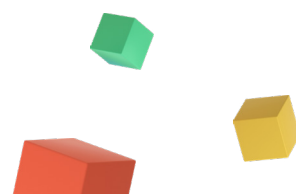


Prioritize

Vulnerability scanners check your code, applications, and infrastructure for known security vulnerabilities in a wide range of public repositories and databases that are maintained by governments and organizations around the world. These public sources also rank the vulnerabilities according to their technical severity; most scanners use this ranking to prioritize their list of detected vulnerabilities.

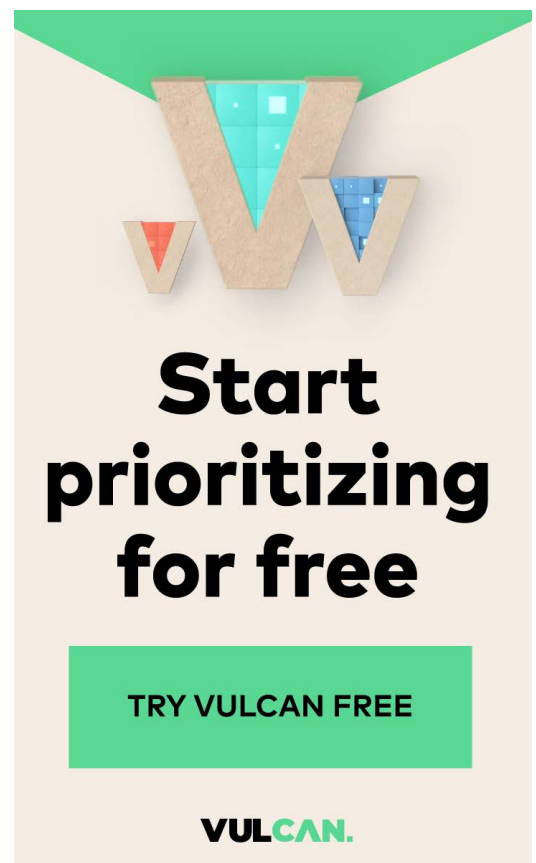
[Daniel Miessler](#), an Information Security Professional, provides [a list](#) of vulnerability repositories and databases, including the US government's NVD, among others. Here's our own short list.

- [Vulcan Free](#), by Vulcan Cyber, is the only risk-based vulnerability assessment and prioritization service available to security teams, at no cost. Vulcan Free was created based on the belief that vulnerability prioritization is critical, but it should never be the end game. The goal should be getting vulnerabilities fixed. The vulnerability management industry has long had plenty of free scanners to choose from, now the next step in a risk-based vulnerability management process has a free service for prioritizing all of the discovered vulnerabilities. The combination of free scanners plus a free prioritization service allows cyber security teams to focus their limited time, resources and budget on getting fix done.
- [CVE Details](#) is a definitive list of Common Vulnerabilities and Exposures (CVEs) curated from other websites and databases into a single list. You can search for specific CVEs, view the top 50 vulnerabilities, read reports, and view informative graphs and charts that make the data easily understandable in today's fast-moving world of cyber vulnerabilities.
- [WPScan Vulnerability Database](#) is incredibly important, as in 2019, approximately [37%](#) of the world's websites ran on WordPress. An online browsable database of all security vulnerabilities found in the WordPress core, themes, and plugins, the WPScan Vulnerability Database is the go-to authority for WordPress website developers.
- [CERT-EU](#) (Computer Emergency Response Team for the EU organizations) is a network of small teams of computer security experts in both the public and private sector in various EU member states. CERT-EU maintains a comprehensive and well-documented list of computer security vulnerabilities, including vulnerabilities found in products, general vulnerabilities, cybersecurity threats and incidents, and hacking techniques.



- [Zero Day Initiative](#) is a project that helps to protect users around the world from Zero-Day attacks by financially rewarding white-hat hackers who find security vulnerabilities in software. Although ZDI is run by Trend Micro (a security software provider), security vulnerabilities are not released to the public until the vendors have had a chance to provide security responses for their customers.
- [Vulners](#) is a free infrastructure-scanning tool for Linux. However, the Vulners project also maintains an impressive public database of security vulnerabilities. Calling itself “Google for Hackers,” the database is fully searchable and includes tens of links to security blogs and articles by independent security consultants, general software vendors, and security software companies.

- [Rubysec](#) maintains the Ruby Advisory Database as a community-based repository of security vulnerabilities that affect [Ruby](#) libraries and Virtual Machines. Ruby is an extremely popular and versatile programming language, so it is important to keep the Ruby community informed of all security vulnerabilities associated with it.



Remedy

Remember, the end-game of vulnerability remediation is not detecting or prioritizing vulnerabilities but fixing them. This is where the rubber meets the road. The public databases and repositories described above often include vendor recommendations on how to fix a vulnerability—most typically a link to a vendor patch that plugs the security gap. Many scanners leverage that information to provide remediation tips for the vulnerabilities detected. But depending on your process, either the IT team or the security team has to manually research, enrich and validate those tips in order to determine the optimal fix for their business and infrastructure context.

Remediation intelligence is a core feature of the Vulcan Cyber remediation orchestration platform. At the heart of remediation intelligence is a knowledge base curated by the Vulcan Cyber research team to deliver the best fixes for any given vulnerability. And for Vulcan Cyber, a fix doesn't necessarily always mean a patch. Sometimes it is just as effective—but less risky and more efficient—to fix a vulnerability with a configuration script, workaround, compensating control, or mitigating action. We are proud to announce

that this extensive knowledge base is now available to the infosec and IT communities as a freely available resource. Get access to [Vulcan Remedy Cloud](#) here.

For Vulcan users, remediation intelligence goes beyond the knowledge base to automatically generate the fixes and deployment scripts, and apply automated remediation workflows at scale. However, [Remedy Cloud](#), in and of itself, can help organizations achieve a more-mature vulnerability remediation program.

**It's time to own
your risk.**

REQUEST A DEMO

VULCAN.

Automate

Open-source tools can be used to automate various aspects of your vulnerability remediation activities, from ticketing to automated configuration changes.

Commercial tools like Jira and Slack are great for automatically generating a service ticket to remediate a vulnerability and then keeping the relevant teams in the loop as the ticket is processed. Here are three free open-source alternatives to these tools:

- [Redmine](#) is a flexible cross-platform and cross-database project management application released under the GNU General Public License.
- [OpenProject](#) is an open-source project management application that's powerful and easy to use; its free Community Edition offers a wide range of features and plugins.
- [Rocket.Chat](#) is an open-source and highly customizable team chat and collaboration application with a large community of contributors. It has a free self-managed version.

Here are some free open-source tools that you can use to automate patch deployment:

- [Windows Server Update Services \(WSUS\)](#) from Microsoft fully manages the distribution of Microsoft updates to network-attached endpoints.
- [Comodo ONE Windows Patch Management](#) deploys third-party and Windows updates or patches and serves as an endpoint vulnerability discovery tool. It is fully compatible with WSUS and SCCM and supports the creation and automated deployment of update policies.
- [Opsi](#) is an open-source client management system for the automated deployment and

configuration of OSES and software on Windows and Linux computers.

- [Patch Manager Plus Free Edition](#) is a fully functional version of ManageEngine's automated patch deployment solution for Windows, macOS, and Linux endpoints. It can be used for up to 20 computers and five servers.

As an alternative to the leading platforms of Chef, Puppet, SaltStack, and Ansible, all of which are well known open-source configuration automation tools, the following open-source tools can also be used to automate configuration changes at scale:

- [Foreman](#) is a complete lifecycle management tool for physical and virtual servers, giving you a configuration management solution with external node classifiers for Puppet and Salt, support for parameterized classes, and hierarchical parameter storage.
- [Windows PowerShell DSC](#) (Desired State Configuration) is a declarative platform from Microsoft for managing IT and development infrastructure with configuration as code.
- [CFEngine](#) delivers a lightweight but powerful configuration management solution where IT infrastructure is codified into policy to ensure consistent and compliant system behavior. CFEngine Enterprise can be used for free for up to 25 hosts.



Conclusion

You can use these (and other) free open-source tools to roll your own vulnerability management and remediation stack. For a hands-on example, check out our [webinar](#) where we demonstrate how to use three open-source tools to build a vulnerability prioritization engine.

However, there is always a hidden cost to “free” and it isn’t easy to create an enterprise-grade solution on your own that is flexible, supports cross-team collaboration, delivers remediation intelligence, and unlocks the power of automation. The Vulcan Cyber

remediation orchestration platform integrates easily with all your teams’ existing tools and platforms, including vulnerability assessment, collaboration, deployment, and more.

It packages all of this into a slick, clean interface that delivers: contextual risk-based prioritization; the right fix for each vulnerability; high levels of workflow automation; end-to-end, single-source-of-truth visibility into the remediation process; and single-pane monitoring of remediation campaigns.

