CyStack

DATA SHEET

Vulnerability Assessment Powered by CyStack Web Security

Automatically scan and monitor security vulnerabilities in your system

Security Challenges

Vulnerability assessment (VA) is an important part of an organization's cybersecurity program because it helps organizations identify and prioritize vulnerabilities in their systems and networks. Identifying and addressing vulnerabilities can help organizations reduce the risk of a cyber-attack and protect against potential threats.

However, performing a vulnerability assessment is not an easy thing for every business because of:

- Lack of expertise: VA requires specialized knowledge and skills in security, networking, and software development. Non-security companies may not have the necessary expertise in-house to conduct a thorough and effective vulnerability assessment.
- Limited resources: VA can be a time-consuming and resource-intensive process, especially for larger organizations with complex systems and networks. Non-security companies may not have the resources or personnel dedicated to conducting a comprehensive vulnerability assessment.
- The complexity of systems and networks: VA involves examining the systems and networks of an organization for vulnerabilities. These systems and networks may be complex, making it difficult to identify and assess all potential vulnerabilities.
- Constant changes: Systems and networks are constantly evolving, and new vulnerabilities are being discovered all the time. This means that VA is an ongoing process that requires continuous monitoring and updating. Non-security companies may not have the resources or expertise to keep up with these constant changes

Customer Benefits

- Save time with automated tasks
- Identify known, surface-level security issues and misconfigurations
- Establish a security baseline
- Focus remediation with prioritized vulnerabilities
- Validate company patching/hardening program

How CyStack Helps

CyStack Web Security (CWS) is a Security vulnerability scanning and monitoring tool for web applications developed by CyStack. It's built to simplify and automate the Vulnerability Assessment by focusing to:

- Identify vulnerabilities: CWS helps automatically scan vulnerabilities in the web applications and hosts that their owners may not have been aware of.
- Prioritize vulnerabilities: CWS helps organizations prioritize vulnerabilities based on their severity and potential impact. CVSS Score is an important tool supporting us in this task. This can help organizations prioritize their efforts to address the most critical vulnerabilities first.
- Monitor for new vulnerabilities: CWS scans and detects vulnerabilities continuously to alert them when new risks are discovered. This can help organizations stay up-to-date and proactively address new vulnerabilities as they are identified.
- Track progress: CWS helps organizations track their progress in addressing vulnerabilities over time. This can help organizations ensure that they are making progress in mitigating the risk of a cyber attack.

Targets can be

- Domains
- IP range
- CIDR
- URL

Deep Scan

Security vulnerabilities are the leading cause of web applications being attacked by cybercriminals. CWS helps detect and address critical security vulnerabilities in web applications for a secure end-user experience and your system.

Intelligence Gathering

Intelligence Gathering is an essential part of CWS which refers to the process of collecting information about a target tech stack, network, and infrastructure. By combining our unique crawler and automated reconnaissance technologies, CWS can collect full information related to the target to prepare for the vulnerability analysis stage.

Fuzzing

Fuzzing is a technique used to discover vulnerabilities in software by inputting large amounts of random data, or "fuzz", into the software in an attempt to cause it to crash or otherwise behave unexpectedly. CWS has implemented this technology to discover 0-day and unknown vulnerabilities in the target.

Vulnerability Database

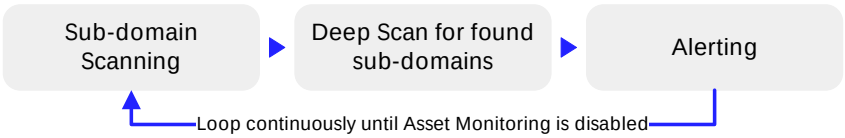
Besides the Fuzzing, our team builds and maintains a vuln database for well-known and published vulnerabilities. We do that by continuously collecting new CVE IDs, 1-day vulnerabilities, and exploited in-the-wild flaws from multi-trusted sources; then we write the PoC code for them and add them to the CWS. Our vuln database is updated at https://web.cystack.net/vulnerability/.

Authenticated Testing

Most web applications have both public and private areas. The public areas can be accessed by anyone, while the private areas are only accessible to users with an account like Dashboard or Admin page. When testing a web application with an authenticated account, it is more likely to find vulnerabilities and access restricted areas of the site compared to testing without authentication. CWS offers two options for scanning behind login: Headers modification (Cookies and auth token) and Basic authentication.

Asset Monitoring

Asset Monitoring helps improve the security of your system by continuously discovering sub-domains, and IP addresses in the same private network and alerting you to any exposed files, vulnerabilities, or misconfigurations. This helps you keep your system secure and prevent potential security breaches.



DevSecOps

Be a part of CI/CD

CWS fully supports API calls, so the vulnerability scan is set to start when a new Git commit is created by request to our API. The result will be responded to in minutes to help developers know the flaws and fix them before officially merging or deploying the application.

By integrating vulnerability scanning into the development and deployment process, organizations can ensure that their applications are secure and compliant with industry standards and best practices.

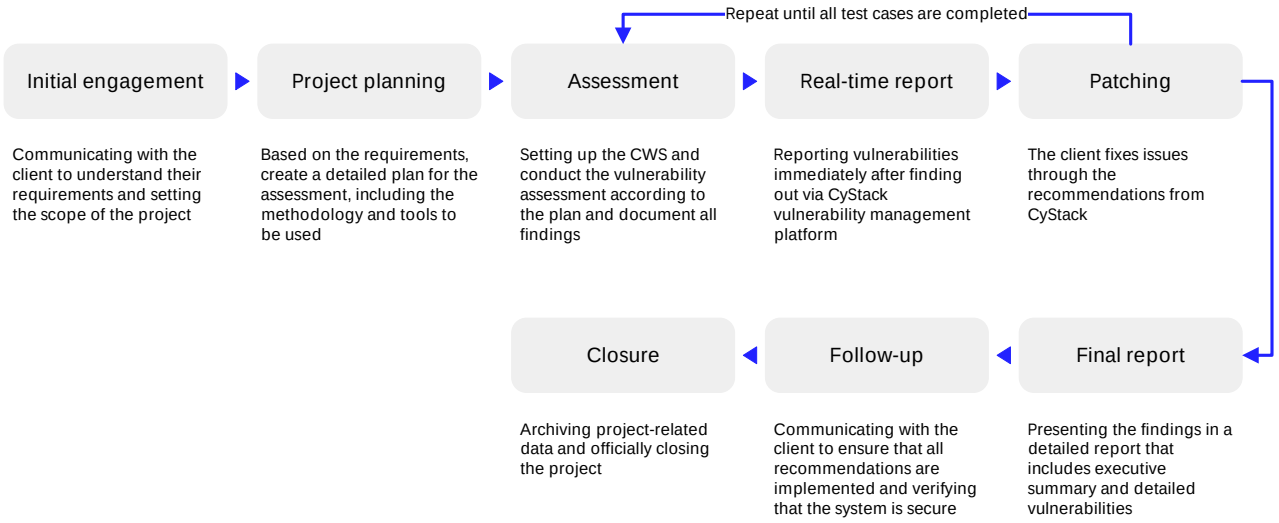
Seamlessly integrate CWS with your favourite tools

- **Slack**: Receive updates about the scan status, report exporting status as well as updates on vulnerability findings based on your settings and preferences.
- **Jira**: Create an issue and assign it to the responsible engineer when a new vulnerability is found.

Key Features

- Scan sub-domains and addresses in private networks
- Discover vulnerability by using fuzzing and our own vulnerability database
- Monitor and alert new issues continuously and automatically
- Manage, track, prioritize and remediate the findings in a unique platform
- Can integrate the scan with CI/CD and productivity tools

Flow To Work With Clients



About CyStack

CyStack is an innovative company in the field of cybersecurity in Vietnam. We are a pioneer in building next gen security products for businesses and individuals. Our solutions focus on data protection, cyber attack prevention, and security risk management.

For more information, please call **(+84) 247 109 9656** or send an email to **contact@cystack.net** to speak to CyStack security specialist.
cystack.net