



# YScanner Web Application Scan

YOUNKER

Protect your cloud assets

Built on cloud-based security and compliance platform, YScanner keeps you away from substantial cost, excessive resources, sudden deployment issues. Upon unique methodology, fast deployment, ease of use and maintenance, plus incomparable scalability, it ensures organizations are capable of securing web applications and keeping attackers at bay.



YScanner is a professional scanning suite for web application vulnerability detection, fully supports OWASP Top 10 detections, based on latest browser engine technology and powerful crawlers, excellent detection algorithms, with higher detection rate plus FP rate being effectively suppressed. Being developed and optimized on Linux, it demonstrates the innate high performance and large concurrency, especially is skillfully to dig out hidden storage XSS flaw which listed into second XSS flaw in OWASP Top 10. YScanner has been successfully supplied to market, and stands the test of time, runs effectively and steadily with limited supports, or even maintenance-free.

## Key Features

### Comprehensive discovery

WAS engine enable users to discover and catalogue all applications in their network, especially for those new and unknown ones, that scale from a few to thousands. Furthermore, you also can tag applications with your own pre-defined labels leveraged by reporting and access controlling on scanned data.

### Probe zero-day threats via behavioral analysis

YScanner is adapt to open source software and custom-built applications, approach the topmost level detection rate on critical vulnerabilities. Good at unique behavioral technology, it can quickly and effectively identify and alert 0-days.

### Deep scanning

Dynamic and deep scanning effectively detects all apps on the perimeter of production or ever-changing R&D environment. It sheds a new light to unknown web vulnerabilities, such as SQL injection and XSS, etc., as an enhancement and advantage, authenticated, complicated and progressive scans is fully supported

### Disclose vulnerabilities and misconfigurations

Adhering to professional and distinct observation methodology to sites, customer can be targeted to and focused on vulnerabilities and misconfigurations due to human errors, poor coding, especially hidden faulty hardening policy.