WhiteHat Dynamic

Web application security for modern and traditional web frameworks and applications

Modern organizations deploy a plethora of web applications, ranging from external-facing corporate websites, customer portals, shopping carts, and login pages to internal-facing HR portals. Web applications are an appealing target for hackers, because they can exploit vulnerabilities in these business-critical applications to gain access to back-end corporate databases.

WhiteHat Dynamic

WhiteHat™ Dynamic is a software-as-a-service (SaaS) dynamic application security testing (DAST) solution that allows your business to quickly deploy a scalable web security program. No matter how many websites you have or how often they change, WhiteHat Dynamic can scale to meet any demand. It provides security and development teams with fast, accurate, and continuous vulnerability assessments of applications in QA and production, applying the same techniques hackers use to find weaknesses, so you can remediate them before the bad guys exploit them.

WhiteHat Dynamic is a cloud-based solution that requires no hardware or scanning software to be installed. It provides

- Unlimited, continuous, and concurrent assessments
- Automatic detection and analysis of code changes in web applications
- Open API integration to security information and event management solutions, bug-tracking systems, and web application firewalls

WhiteHat DAST fits into any environment and is highly scalable, with the ability to assess thousands of websites simultaneously. Furthermore, all vulnerabilities are verified by Synopsys security experts, virtually eliminating all false positives.

Powered by artificial intelligence and machine learning

WhiteHat Dynamic brings together machine learning (ML), artificial intelligence (AI), and expert vulnerability analysis to deliver the most accurate dynamic application security testing results, so you can verify the security of your web applications without slowing down developers with false positives.

Years of valuable data gathered by our highly trained security experts is used to develop our proprietary AI/ML models. This approach provides fast, automated results augmented by expert validation, enabling earlier detection and faster response to cyberattacks.

How WhiteHat Dynamic works

WhiteHat Dynamic combines automated application scanning with the world's largest security

Discovery, fine-tuning, and configuration

Website assessment

Unlimited assessments, vulnerability detection, and verification

Reporting

Results displayed in a portal with customizable reports

WhiteHat Dynamic | Detectable Vulnerabilities

Technical Vulnerabilities

Threat Classification

- Abuse of Functionality
- Application Code Execution
- Application Misconfiguration
- Autocomplete Attribute
- Brute Force
- Buffer Overflow
- Cacheable Sensitive Response
- Clickjacking
- Content Spoofing
- Cross Site Request Forgery
- Cross Site Scripting
- Denial of Service
- Directory Indexing
- Fingerprinting
- Frameable Resource
- HTTP Response Splitting
- Improper Input Handling
- Information Leakage
- Insecure Indexing
- Insu cient Anti-automation
- Insufficient Authorization
- Insu cient Password Policy Implementation
- Insu cient Password Recovery
- Insu cient Process Validation
- Insu cient Session Expiration
- Insu cient Transport Layer Protection
- LDAP Injection
- Mail Command Injection
- Missing Secure Headers
- Non-HttpOnly Session Cookie
- OS Command Injection
- OS Commanding
-