HORIZON3

NodeZero® WebApp

Different attack surface. Same outcome: security you can prove.

NodeZero WebApp helps you continuously validate which web application weaknesses attackers can actually exploit into business impact — crawling, authenticating, attacking, and proving consequences the way real attackers operate, so you know exactly what to fix first.

Cybersecurity from the attacker's perspective

Security teams already have scanners, scripts, and manual pentesters, but they need a practical way to continuously test the custom web apps attackers actually target, with attacker-validated proof to trust. NodeZero WebApp closes that gap, navigating custom web apps the way an attacker would: crawling routes, authenticating as a real user, and safely chaining weaknesses.

See what attackers see

NodeZero WebApp provides full visibility into every route, request, and action it takes. Replayable proof shows practitioners and developers exactly what happened and why it matters, turning results into evidence they can verify instead of an abstract findings list. Reports connect exploitable web application weaknesses to business impact and to the broader attack chain across identity and infrastructure — giving you measurable proof of exposure reduction and audit-ready evidence for stakeholders.

Test across:

- → Custom, business-critical web applications
- → Authenticated, role-based workflows and business logic
- → REST, SOAP, and GraphQL APIs
- → Modern single-page applications (SPAs) and hidden routes
- → Hundreds of supported frameworks, libraries, and stacks
- → Production, staging, and internal development environments

Proven Results		
	10,000	Routes crawled by NodeZero WebApp in four hours
	<8%	False positive rate across 500+ vulns surfaced in beta testing
	4	True-positive BOLA/IDOR findings on live hyperscale production web app

Core NodeZero WebApp capabilities

PRODUCTION-SAFE GRADUATED TESTING

Start read-only with GET-only production modes, then safely expand routes, methods, and scope as confidence grows.

AUTHENTICATED & ROLE-AWARE TESTING

Test logged-in workflows and business logic with credential and MFA support (local storage, pause-and-resume), so testing reflects actual usage.

MODERN APP & API DISCOVERY

Headless-browser crawling and route discovery uncover SPAs, hidden functionality, and REST/SOAP/GraphQL APIs that legacy scanners miss.

UNIFIED ATTACK PATH VALIDATION

Web application findings feed into the same NodeZero workflow already used for identity, cloud, and infrastructure risk, connecting app-layer weaknesses to full attack-chain consequence.

BUSINESS LOGIC & ACCESS CONTROL TESTING

Validate broken access control, IDOR, and BOLA issues across multiple roles.

REPLAYABLE PROOF & EVIDENCE

Every finding includes request/response detail, screenshots, and route context so practitioners can verify results and developers can fix faster.

NodeZero WebApp traces the full attack path, from the threat actors and weaknesses attackers exploit to the impacts and business risks they create, turning a single test run into proof of exploitable, business-relevant exposure.

See NodeZero® WebApp *in action.*

horizon3.ai/schedule-demo