PRODUCT BROCHURE

ZScanner

Find the weaknesses in your own applications, on your own machines, before somebody else does.

A desktop web application vulnerability scanner for Windows, macOS and Linux. Nothing you scan and nothing you find leaves your network.

ZHOST Consulting Private Limited
zscanner.bithost.in | sales@bithost.in | 2026

THE CASE FOR CHECKING

Your provider secures their platform. You are still responsible for what you built on it.

Every serious cloud and SaaS provider publishes a shared responsibility model, and they are right to. They secure the data centre, the hypervisor, the managed database engine and the platform they operate. What they do not secure, and never claim to, is the application you wrote on top of it: your access control logic, your API parameters, your session handling, your third party integrations, your file uploads, your admin panel that was meant to be internal.

So a provider saying "our platform is secure" and your application being secure are two different statements. Both can be true at once. Only one of them is your responsibility, and it is the one nobody else is testing.

This is verification, not suspicion

You take backups from a system that reports every backup as successful, and you still restore one occasionally to prove it works. You are not accusing the backup software of lying. You are confirming an assumption you would rather not discover was wrong at the worst possible moment. Testing your own application sits in exactly the same category of ordinary professional care.

What changed recently

Two things made independent checking more useful than it used to be. Applications now assemble far more third party pieces than they once did, so the surface that belongs to you has grown even when your own codebase has not. And a growing share of code is now written with AI assistance, which means code arrives faster than anyone can read it line by line. Neither of those is a reason to panic. Both are reasons to look, rather than assume.

The honest position is simple. Nobody can tell you your application is safe, including us. What a scanner can tell you is what it found, how it found it, and how to reproduce it. That is a fact you can act on, rather than an assurance you have to accept.

THE PRODUCT

A scanner that runs on your machine, not in somebody else’s cloud

ZScanner is a desktop application. You install it on Windows, macOS or Linux, point it at an application you are authorised to test, and it works from there. The scan engine runs locally and binds only to your own machine. Attack traffic originates from your network. Findings and reports are written to your disk.

Why that matters in practice

- **You can test what is not on the public internet.** Staging environments, applications behind a VPN, internal tools and admin systems are all reachable, because if your machine can reach it, the scanner can test it. A cloud scanner cannot, without you exposing the application or installing an agent inside your network.
- **Your findings stay yours.** A completed scan report is a precise description of how to compromise your application. ZScanner keeps it on the machine that produced it.
- **It works offline.** Licences are cryptographically signed and verified on the machine, so a scan does not need connectivity. That makes the scanner usable in air gapped and restricted environments.
- **Nothing is metered.** Scans, domains and applications are unlimited for the term of the licence, so the cost of looking does not rise every time you add a service.

What we receive

After a scan the application sends a hash of your licence key, the scan timestamps, the target domain and the count of findings by severity. That is the complete list. It does not send report content, vulnerability details, request or response bodies, or page data. Reports reach our servers only if you deliberately use the report vault feature.

HOW IT WORKS

What happens during a scan

STAGE	WHAT HAPPENS
1. Scope	You give the target and confirm you are authorised to test it. Policy rules can block an out of scope host before anything is sent.
2. Authenticate	You record a login sequence once. The scanner replays it, keeps the session alive during the crawl and signs in again if the session drops.
3. Map	The crawler discovers pages, forms, parameters and API endpoints. An OpenAPI file can be imported to compare what is documented against what is actually exposed.
4. Test	Nineteen modules probe the surface that was found, covering injection, access control, transport, configuration and exposure.
5. Judge	Each finding gets a confidence score and a business weighted risk score, then a priority and a remediation window.
6. Report	HTML and PDF reports, mapped to the frameworks you are audited against, in five languages.

What a scanner can and cannot tell you

Being straight about this matters more than a longer feature list. An automated scanner is very good at finding the classes of problem it knows how to look for, and at proving them with a request you can replay. It will find injection points, broken access control on paths it can reach, weak transport settings, exposed files and configuration mistakes.

It will not reason about the intent of your business rules the way a human tester does, and it cannot test a screen it was never able to reach. That is why authenticated scanning and scope configuration matter so much, and why the honest use of this tool is as a regular, repeatable baseline rather than a replacement for a penetration test before a major release.

A clean scan is a fact about the scan

If ZScanner reports nothing, that means these nineteen modules found nothing on the surface they were able to reach. It is a useful and reassuring result. It is not a certificate that your application is secure, and we will not print one. Any vendor who offers you that is selling a feeling rather than a finding.

COVERAGE

Nineteen modules, one licence

Every plan includes all of it. There is no higher tier that unlocks the tests that matter.

AREA	WHAT IS TESTED
Injection	SQL injection using error based, boolean blind and time blind techniques. OS command injection. Server side template injection. XML external entities. CRLF injection.
Cross site scripting	Reflected and DOM based cross site scripting.
Access control	Authorisation flaws and business logic abuse, including workflow and state handling that behaves differently than intended.
APIs	REST and GraphQL endpoints tested as first class targets, plus drift between an imported OpenAPI specification and the endpoints actually observed.
Server side requests	Server side request forgery and open redirect chains.
File handling	Local file inclusion and path traversal.
Transport	TLS configuration, cipher selection and certificate problems.
Browser controls	Security headers, cross origin resource sharing policy, cross site request forgery defences and cookie flags.
Exposure	Backup files, exposed secrets, directory listings and files that were never meant to be reachable.
Reconnaissance	Technology fingerprinting, subdomain discovery and detection of any web application firewall in front of the target.
Anti automation	Gaps in rate limiting and bot defences.
Passive analysis	Findings derived from traffic already captured, sending no additional requests to the target.

Signal, not noise

A scanner that reports everything it suspects is a scanner nobody reads twice. Every ZScanner finding carries a confidence score, and every finding ships with a sanitised request you can replay to see the behaviour yourself. Dismissing a finding requires a reason, an owner and an expiry date, and it comes back for review when that date passes, so a suppression cannot quietly become permanent.

WHERE IT FITS

Six points in the life of an application

Most teams start at one of these and add the others once the first one pays off.

1 **Choosing a vendor or platform**

Procurement, IT leadership

Before you commit, test the trial tenant you have been given, within whatever the provider's terms permit. A short scan turns a sales conversation about security into a specific conversation about findings, and gives you informed questions instead of a questionnaire nobody reads.

2 **While the application is being built**

Developers, engineering leads

Run a scan against staging at the end of a sprint. Findings can be pushed straight into Jira, GitHub, GitLab or Azure Boards as tickets, so the work lands in the same backlog as everything else rather than in a document somebody has to transcribe.

3 **Before a release goes out**

Release managers, DevOps

Define what is unacceptable and let a policy decide. Environment specific gates evaluate the scan and return a pass or fail, so the release conversation is about an agreed rule rather than about who feels comfortable.

4 **Once it is live**

Security teams, platform owners

Schedule regular scans with blackout windows so testing avoids your busy hours. Continuous subdomain discovery keeps an inventory of what is exposed, tagged by environment and criticality, which is usually where forgotten hosts surface.

5 **When an audit is coming**

Compliance, risk, finance

Findings are mapped to OWASP Top 10 (2021), OWASP API Security Top 10 (2023) and PCI DSS 4.0, with coverage shown per framework. The report is the evidence, produced from your own testing rather than assembled by hand the week before.

6 **After you ship the fix**

Developers, QA

Every finding carries a replayable proof. Re issue it and the finding is marked reproduced or candidate fixed. Verifying a patch takes one action instead of a full rescan, and closes the linked ticket automatically when the fix holds.

WHO USES IT

Industries, and the specific reason each one needs its own testing

The common thread is that something about these environments makes an external cloud scanner awkward, insufficient, or simply not permitted.

SECTOR	THE SITUATION	WHAT CHANGES
Software and SaaS	You are the provider making the assurance. Customers ask you the security questions.	Test your own product continuously and answer from findings rather than from intent.
Financial services	Card data brings PCI DSS into scope. Regulators expect evidence of testing, not statements.	PCI DSS 4.0 mapping with per requirement coverage, produced from your own scans.
Healthcare	Patient data cannot be handed to a third party scanner as part of a test.	Nothing leaves the operator machine, so testing does not create a new disclosure.
Government and defence	Systems are frequently isolated, and sending traffic through an external service is not an option.	Runs fully offline with locally verified licensing.
Retail and ecommerce	Checkout and payment paths are the highest value target you operate.	Authenticated testing of the logged in journey, not only the public catalogue.
Education	Many small applications, limited budget, few dedicated security staff.	Unlimited targets on one licence, so scanning the tenth application costs nothing extra.
Agencies and consultancies	You are answerable for applications you built for other people.	One licence covers every client engagement you are authorised to test.
Manufacturing and logistics	Operational dashboards and supplier portals sit on internal networks.	Reaches anything the operator machine can reach, VPN included.

A note on scope and permission

Only scan systems you own or have written authorisation to test. Active scanning sends genuine attack traffic, which can trigger alerts, fill logs and in some configurations change application state. ZScanner includes scope validation so an out of scope host can be blocked before a scan starts, and we recommend using it. If your provider’s terms restrict testing, ask them first. Most reputable providers have a documented process for exactly this request.

OUTPUT AND COMMERCIALS

What you get, and what it costs

Reports

Every scan produces a standalone HTML report and a PDF, available in English, French, Spanish, Portuguese and German. Findings are ordered by a risk score weighted for exploitability, data sensitivity, internet exposure and asset criticality, then given a priority and a remediation window, so the first page tells you what to fix first rather than listing everything alphabetically.

Licensing

Priced by duration, never by target. Every plan includes unlimited scans, unlimited targets and all nineteen modules on Windows, macOS and Linux.

Starter	Pro	Business	Enterprise
$193	**$482**	**$843**	**$1,446**
INR 15,999	INR 39,999	INR 69,999	INR 1,19,999
1 month	3 months	6 months	12 months

Prices shown in US dollars and Indian rupees. Payment is handled by Razorpay and supports UPI, Indian cards, net banking and international cards. Your licence key arrives by email as soon as the payment is captured.

Try it before you decide

ZScanner runs a limited scan without a licence, so you can point it at an application you own and see the output for yourself before any money changes hands. Download it from zscanner.bithost.in/download.

Talk to us

Sales and licensing: sales@bithost.in
Technical support: support@bithost.in
Product: zscanner.bithost.in
Company: ZHOST Consulting Private Limited, powered by Bithost, www.bithost.in