XECbuild

We build.
We test.
We secure.

Web development + offensive security

WEB DEVELOPMENT | WEB APPLICATIONS | VAPT | API SECURITY | HARDENING

SERVICES OVERVIEW

One team that builds it and attacks it.

xecbuild.com
Connect@xecbuild.com
@xecbuild xecbuild

01 DEVELOPMENT

Websites that look good. Web apps that actually work.

We build fast, responsive and maintainable digital products, with security considered from the first commit rather than bolted on before launch.

Static / business website

7-12 DAYS

A mobile-responsive site for a business that needs to be found and contacted: enquiry form, WhatsApp and call buttons, Google Maps and Google Business setup, SSL and on-page SEO.

RESPONSIVE DESIGN · ENQUIRY FORM · MAPS & BUSINESS · SSL · ON-PAGE SEO

Custom web app - low complexity

3-4 WEEKS

Logins, dashboards, database-backed forms, an admin panel, basic reporting and the integrations around them - payment links, email, exports.

AUTH & ROLES · DASHBOARD · ADMIN PANEL · REPORTING · INTEGRATIONS

Custom web app - high complexity

5-8 WEEKS · PHASED

Multi-role systems, custom workflows, e-commerce and booking, payment gateways, inventory, APIs and the business systems they have to talk to. Delivered in phases you can review as they land.

MULTI-ROLE · WORKFLOWS · PAYMENTS · INVENTORY · PUBLIC API · PHASED DELIVERY

ANY STACK

Next.js, Django, Rails, Laravel, Go, Spring. We work in what your team already runs rather than migrating you onto ours.

YOU OWN IT

Source, hosting and documentation are handed over at the end. No lock-in and nothing you need us to unlock.

Ongoing care is available on every build: hosting and domain handling, security and framework updates, daily backups, uptime monitoring, small content changes, bug fixes, priority support and one annual security check.

02 SECURITY

VAPT that goes beyond a scanner report.

We test web applications, APIs and external infrastructure manually, verify every finding by hand and show how it can actually be exploited.

HOW SCOPE WORKS

We scope first, then fix the price.

A short call establishes the footprint, the environments and what you need evidence for. You get a fixed price, fixed dates, a named tester and rules of engagement in writing before anything is touched. Nothing is billed by the hour and nothing is added at the end.

What we cover

Web applications
Injection, access control, session handling, client-side trust and file handling across the full authenticated surface.

APIs
REST and GraphQL. Object-level authorization, mass assignment, resolver logic and undocumented routes.

Authentication
Registration, login, MFA, password reset, token lifetime and revocation, federated flows.

Authorization
Role boundaries, tenant isolation, privilege escalation paths and inherited permissions.

Business logic
Pricing, quotas, workflow state, refunds and any process where the order of operations carries value.

Cloud configuration
IAM policy, storage exposure, secret management, network boundaries and metadata access.

Source review
Optional. Targeted review of the code behind high-risk flows to confirm root cause and reduce guesswork.

Larger infrastructure. Multiple applications, internal networks, cloud, Active Directory or compliance-mapped reporting are scoped on a call and quoted against that scope.

Ongoing security. Regular testing for teams that ship frequently, so each release is checked rather than each year.

03 HOW AN ENGAGEMENT RUNS

Five stages.
No surprises in any of them.

01

Scope definition and rules of engagement

The exact footprint and the legal boundaries, agreed in writing before anything is touched.

02

Reconnaissance and identification

Active and passive discovery of the target's attack surface, using AI-assisted intelligence and our own tooling.

03

Deep manual and AI-assisted testing

Automation covers the surface area. Hands-on testing goes after business logic, authorization and real attack paths.

04

Exploitation and risk validation

Impact proved with working proofs of concept, tenant isolation verified and false positives removed before anything is reported.

05

Reporting and remediation

Technical evidence, reproduction steps and stack-specific fixes, walked through with your engineers. One retest is included.

What lands at the end

Executive summary
Two pages for leadership. Risk posture, themes and what to prioritise.

Technical report
Every finding with severity, affected assets and reproduction steps.

Proof of concept
Working requests or scripts, so your team can reproduce the issue.

Risk ratings
CVSS v3.1 plus a business-context rating we agree with you.

Screenshots
Annotated evidence captured at the point of exploitation.

Remediation guidance
Specific fixes for your stack, with code and architectural guidance.

04 WHY XECBUILD

Built by developers. Tested like attackers.

Security is not an add-on for us. It is part of how we approach the product.

01

One team. One accountability.

No developer-versus-auditor blame game. The people building understand the findings.

02

Manual + AI-assisted testing.

Automation covers surface area. Human testing targets logic, authorization and real attack paths.

03

Reports developers can use.

Clear reproduction steps, impact and remediation, not a pile of scanner output.

04

You own everything.

Source code, hosting and documentation are handed over. No lock-in.

05

Ready after launch.

Support, fixes and retests when your product changes.

06

Fixed pricing after scope.

We scope first, then give you a fixed price. No surprise costs at the end.

RECOGNISED BY

Our testers hold hall-of-fame and disclosure acknowledgements from organisations that run their own security programmes.

APPLE · NASA · ERICSSON · BAYER · ZEPTO · NCIIPC · FLUID TOPICS · WEBHIZZY

XECbuild

LET'S TALK

Have a project?
Have an attack surface?

Twenty minutes on a call. Tell us what you need and what is in scope, and we come back with a fixed, itemised quote.

Connect@xecbuild.com

xecbuild.com/contact

/company/xecbuild

@xecbuild