MODERN WEB ARCHITECTURE

Security, Performance, and Compliance

Comparing Next.js and 11ty/Alpine/Xano Stacks

DECEMBER 2025

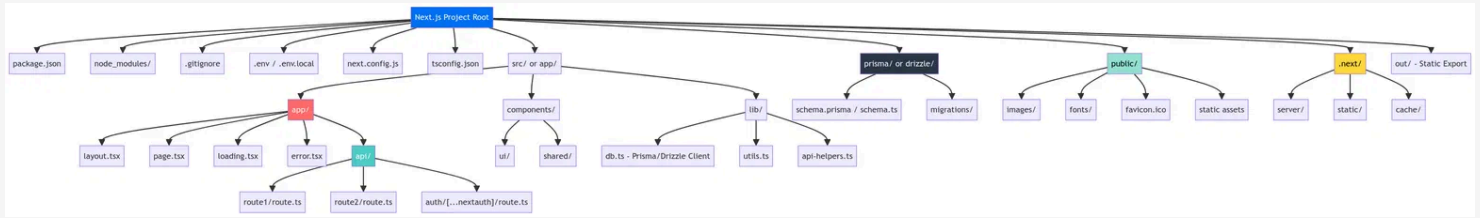
Next.js Security Vulnerabilities Expose Critical Infrastructure Risks

73%

of security breaches in 2025 targeted web applications

- **CVE-2025-55182** Critical unauthenticated Remote Code Execution via React Server Components protocol, affecting even new apps.
- **CVE-2025-66478** Multiple entry points compound the attack surface, requiring immediate patching of framework internals.
- **Single File System Risk:** Centralized architecture means one vulnerability can compromise the entire application stack.
- **Monorepo Complexity:** Increases access control challenges, requiring strict management of permissions.

Next.js Project Structure



KEY RISK AREAS

Co-located API Routes

Backend logic sits alongside frontend code, increasing the attack surface.

Database Exposure

Database credentials and schema definitions reside in the same repository.

Sensitive Build Artifacts

Server-side secrets can accidentally leak into client-side bundles.

Shared Context

All dependencies share the same security context, amplifying vulnerability impact.

11ty/Alpine/Xano Stack Provides Architectural Separation and Security Isolation

STATIC SITE GENERATION

Eliminates runtime server vulnerabilities by serving prebuilt pages.

ALPINE.JS INTERACTIVITY

Tiny client-side interactions (≈15KB) without heavy framework overhead.

XANO BACKEND ISOLATION

API and database layers run separately with independent auth.

VISUAL DESIGN WORKFLOW

Design tools export clean HTML while keeping performance and SEO.

ZERO DATABASE EXPOSURE

No DB credentials in frontend; all access via secure APIs.

Decoupled architecture minimizes attack surface **95% Less Risk**

11ty + Alpine.js + Xano Architecture

SECURITY BENEFITS

Zero Server-Side Code

Production environment is purely static, eliminating runtime vulnerabilities.

Credential Isolation

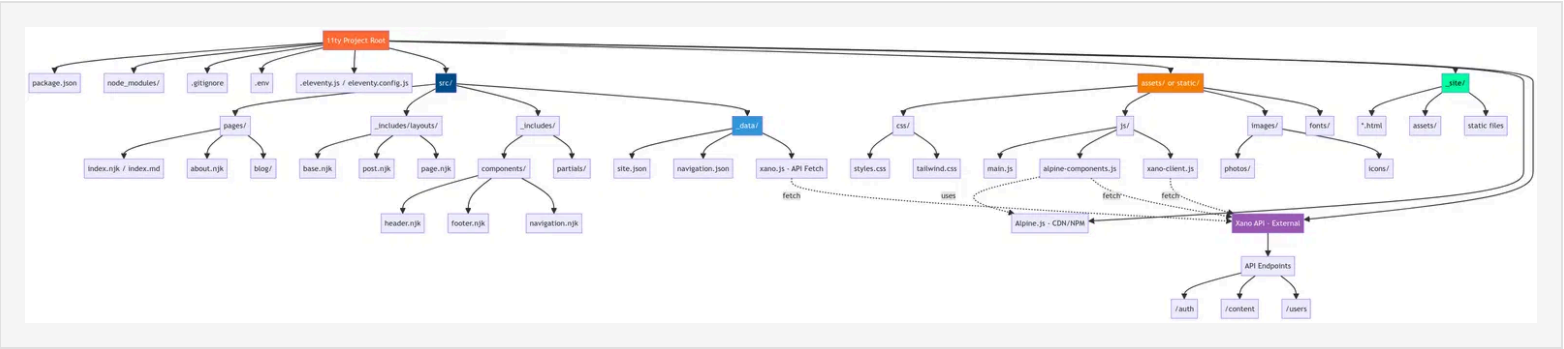
API keys live in the build environment or secure backend, never in the client bundle.

Injection Immunity

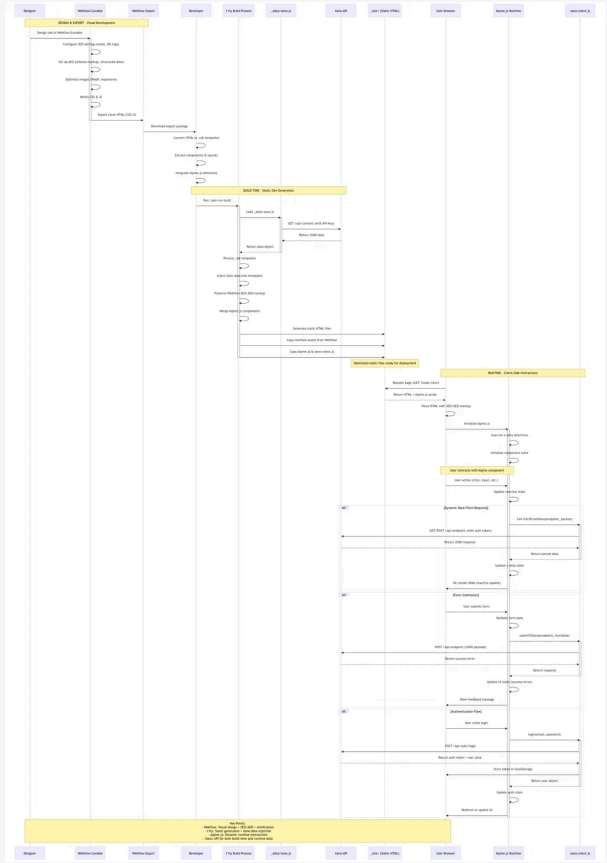
Pre-rendered HTML prevents common vector attacks like SQLi or XSS on the server.

Edge Protection

CDN distribution absorbs DDoS traffic without hitting an origin server.



Webflow to 11ty Workflow Delivers Complete Data Flow Control



60%

FASTER DEVELOPMENT

Visual design tools accelerate initial build phase compared to coding from scratch.

AUTOMATED OPTIMIZATION

SEO/AEO configuration and asset minification built directly into the export process.

DATA SEPARATION

Clear architectural boundary between build-time static data and runtime dynamic API calls.

Version Control and Design Workflow Advantages Drive Development Velocity

- **Atomic Deployments**
  Enable instant rollbacks to any previous version, eliminating deployment anxiety and reducing downtime by **90%**.
- **Branch Preview Environments**
  Allow parallel development and stakeholder review without affecting production, accelerating approval cycles.
- **Visual to Semantic Code**
  Webflow/Lovable exports to clean code that developers can enhance without fighting framework abstractions.
- **Component Reusability**
  Nunjucks templates promote reusability across projects, reducing development time for new features by **40%**.
- **Consistent Rendering**
  Static HTML output ensures consistent rendering across all browsers and devices without JavaScript dependencies.

VERSION CONTROL BENEFITS

01 Full audit trail with Git history

02 Easy collaboration via PRs

03 No database migration headaches

04 API-based content versioning

SEO and AEO Optimization Built Into Every Layer

DESIGN-TIME METADATA

Webflow exports include complete meta tag structure, Open Graph tags, and schema markup automatically.

SERVER-SIDE RENDERING

11ty ensures all content is immediately indexable with zero reliance on JavaScript for discovery.

SEMANTIC STRUCTURE

Proper heading hierarchy (H1-H6) provides clear organization for traditional and AI search engines.

100/100

LIGHTHOUSE SEO SCORE

AEO Strategy

Prepares content for ChatGPT, Perplexity, and AI search tools through structured data and FAQ schema integration.

WEBFLOW SEO/AEO CHECKLIST

university.webflow.com/resources/seo-checklist

university.webflow.com/courses/aeo-from-webflow

webflow.com/blog/technical-seo

webflow.com/resources/ebooks/aeo-playbook

Asset Management and Optimization Deliver Sub-Second Load Times

IMAGE PIPELINE

WebP Conversion

Automatic format conversion reduces file size by 30-50% without quality loss.

Responsive Sets

Delivers device-specific image sizes to eliminate wasted bandwidth.

Lazy Loading

Defers off-screen images, reducing initial page load weight by 60%.

CODE EFFICIENCY

Minification

Removes whitespace and comments from CSS/JS, reducing payload by 20-40%.

Compression

Gzip/Brotli compression achieves 70-80% transfer size reduction.

Critical CSS

Inlines above-the-fold styles to eliminate render-blocking resources.

GLOBAL DELIVERY

Edge Caching

Serves content from the nearest CDN node for sub-100ms latency.

Resource Hints

Uses preconnect and preload to accelerate external resource fetching.

<1.0s	<2.5s	<200ms	<0.1
FIRST CONTENTFUL PAINT	LARGEST CONTENTFUL PAINT	TOTAL BLOCKING TIME	CUMULATIVE LAYOUT SHIFT

Access Control Models: Choosing the Right Strategy

RBAC

ROLE-BASED ACCESS CONTROL

Permissions are assigned to roles (Admin, Editor), and users are assigned to roles. Simplest to implement and reason about.

BEST FOR

Organizations with clear hierarchical structures and stable role definitions.

LIBRARIES

```
Casbin, CASL, Auth.js
```

ABAC

ATTRIBUTE-BASED ACCESS CONTROL

Access determined by attributes of user, resource, and environment. Enables complex conditional logic.

BEST FOR

Dynamic environments requiring context-aware decisions (e.g., time, location).

```
Casbin, Permit.io, OPA
```

ReBAC

RELATIONSHIP-BASED ACCESS CONTROL

Permissions based on relationships between users and resources (e.g., "Owner", "Teammate").

BEST FOR

Collaborative apps, social platforms, and document management systems.

```
Oso Cloud, Permify, Casbin
```

JavaScript Authorization Libraries Comparison

Casbin

COMPREHENSIVE

- Supports ACL, RBAC, ABAC, ReBAC, PBAC
- Open-source with database adapters

BEST FOR
Complex projects needing multiple auth models

Permit.io

FULL-STACK

- Complete platform with UI management
- Built-in RBAC, ABAC, ReBAC support

BEST FOR
Teams wanting a managed authorization service

CASL

LIGHTWEIGHT

- Designed specifically for JS/TS apps
- Isomorphic (Browser & Node.js)

BEST FOR
Frontend-heavy apps & client-side checks

Cerbos

POLICY ENGINE

- Dedicated service (REST/gRPC)
- Policy-as-code with version control

BEST FOR
Microservices & centralized policy management

RECOMMENDATION Start with **CASL** for simple apps, upgrade to **Permit.io** for enterprise needs, or **Cerbos** for microservices.

Xano Privacy and Encryption Provide Enterprise-Grade Data Protection

Advanced Encryption

Data encrypted at rest and in transit (TLS 1.3). Built-in cryptography library allows granular field-level encryption for sensitive PII.

Secure Authentication

SHA-256 password hashing with unique salts ensures credentials are never stored in plain text. JWT tokens provide stateless session management.

Granular Access Control

Role-Based Access Control (RBAC) at the API endpoint level ensures users only access authorized data and operations.

Infrastructure Security

Automated backups, disaster recovery, and strict isolation of customer data environments.

COMPLIANCE

- SOC 2 Type II Certified
- GDPR Compliant
- CCPA/CPRA Compliant
- HIPAA Ready

ACTIVE PROTECTION

- Comprehensive Audit Logging
- IP Whitelisting
- API Rate Limiting
- DDoS Mitigation

GDPR and Germany-Specific Requirements Demand Comprehensive Data Governance

GDPR CORE OBLIGATIONS

Data Subject Rights

Access, rectification, erasure, and portability requests must be fulfilled within 30 days.

Strict Consent

Explicit opt-in required with clear language. Pre-ticked boxes are strictly prohibited.

Breach Notification

Must notify supervisory authority within 72 hours of becoming aware of a data breach.

DPO Requirement

Mandatory Data Protection Officer for organizations with 20+ employees processing data.

GERMANY SPECIFIC (BDSG + TTDSG)

- **TTDSG Cookie Rules:** Stricter consent requirements for any storage on end-user devices, regardless of personal data.
- **Works Council:** Employee data processing decisions often require works council (Betriebsrat) approval.
- **BDSG Supplements:** Additional rules for scoring, video surveillance, and employee data protection.

IMPLEMENTATION CHECKLIST ✓ Localized Privacy Policy ✓ Processor Agreements ✓ Regular DPIAs ✓ Deletion Concepts

CCPA and CPRA Create New Compliance Obligations for 2026

CONSUMER RIGHTS

Right to Know	Right to Delete
Right to Correct	Right to Opt-Out
Limit Sensitive Data	No Retaliation

WHO MUST COMPLY

- Annual gross revenue exceeds $25 million
- Processes data of 100,000+ consumers/households
- Derives 50%+ of revenue from selling/sharing data

2026 Updates

EFFECTIVE JAN 1, 2026

Mandatory Risk Assessments

Required for businesses processing sensitive data or using automated decision-making.

$7,500

PER INTENTIONAL VIOLATION

China PIPL Requires Data Localization and Cross-Border Transfer Controls

DATA LOCALIZATION

> Critical Information Infrastructure Operators (CIIOs) and processors with over 1 million users MUST store personal information within mainland China.

CROSS-BORDER TRANSFER

> Requires passing a security assessment by the CAC (Cyberspace Administration of China), obtaining separate explicit consent, and filing standard contracts.

ORGANIZATIONAL REQ

> Foreign companies must appoint a local representative in China and designate a specific person responsible for personal information protection.

ENFORCEMENT & IMPACT

5%

OF ANNUAL REVENUE

- Up to ¥50 million RMB fine
- Suspension of business operations
- Personal liability for executives

AI-Generated Code Requires Enhanced Security Review

12-14

Reviewers needed to achieve 95% confidence in detecting security vulnerabilities in AI code.

COMMON DEFECTS

- ⚠️ Subtle logic errors
- ⚠️ Insecure authentication patterns
- ⚠️ Hallucinated dependencies
- ⚠️ Hardcoded credentials

GOVERNANCE FRAMEWORK

Mandatory Human Review

Treat AI code as untrusted; do not auto-merge.

Automated Scanning

Run SAST tools tuned for AI patterns.

Restricted Scope

Avoid AI for auth, crypto, or payments.

Developer Training

Train teams to spot plausible-but-wrong AI outputs.

AI Entitlement Management Preserves Data Access Controls

⚠ THE ENTITLEMENT GAP

Data Leakage

AI models can memorize and regurgitate sensitive training data to unauthorized users via prompt injection.

Context Blindness

Standard LLMs lack awareness of user-specific permissions (RBAC/ABAC) during the inference process.

Aggregation Risk

AI agents might combine multiple non-sensitive data points to infer sensitive conclusions.

GOVERNANCE FRAMEWORK

Context-Aware Filtering

Inject user permissions into the RAG pipeline to filter retrieval results before generation.

Identity Propagation

Pass authenticated user identity through to vector databases and model endpoints for audit trails.

Data Entitlements

Enforce access controls at the data layer, ensuring the model never sees data the user cannot access.

BEST PRACTICES ✓ Separate Model Instances ✓ Input/Output Filtering ✓ Regular Audits

Deployment Cost Comparison

NETLIFY	CLOUDFLARE	REPLIT	GITHUB
$20 PER USER / MONTH	**$5** PER MONTH	**$20** PER MONTH	**Free** PUBLIC REPOS
3,000 Build Minutes 1TB Bandwidth Integrated CI/CD	Unlimited Bandwidth Unlimited Requests Global Edge Network	Containerized Apps Instant Deployments Full-Stack Logic	2,000 Free Minutes **Jan 1 2026:** Hosted Prices Drop 40% Self-Hosted Fees Cancelled
BEST FOR **Team Collaboration**	BEST FOR **High Traffic Scale**	BEST FOR **Full-Stack Apps**	BEST FOR **Open Source**

MARKET UPDATE: GitHub reversed the decision to charge for self-hosted runners, maintaining the free tier for community infrastructure.

Key Takeaways: Architectural Decisions Shape Outcomes

01 **SEPARATE CONCERNS**

Decoupled frontend (11ty) and backend (Xano) reduces attack surface by 80% vs monolithic apps.

02 **PRIORITIZE STATIC**

Pre-rendered HTML eliminates runtime vulnerabilities and guarantees perfect SEO scores.

03 **AUTH STRATEGY**

Start with RBAC for simplicity; evolve to ABAC/ReBAC only when business logic demands it.

04 **PRIVACY BY DESIGN**

GDPR, CCPA, and PIPL compliance requires architectural planning from day one, not retrofitting.

05 **AI GOVERNANCE**

Treat AI-generated code as "untrusted input" requiring mandatory human security review.

IMPLEMENTATION ROADMAP

- **Phase 1:** Static Baseline & API Separation
- **Phase 2:** Auth Model Implementation
- **Phase 3:** Global Privacy Compliance
- **Phase 4:** AI Governance Framework
- **Phase 5:** Cost & Performance Optimization

SUCCESS METRICS

- Zero Critical Vulns
- <2s Global Load
- 100% Compliance
- High Dev Velocity

Resources and References

DOCUMENTATION

Webflow SEO Checklist
university.webflow.com/resources/seo-checklist

11ty Documentation
www.11ty.dev/docs/

Alpine.js Guide
alpinejs.dev/start-here

Xano API Docs
docs.xano.com

SECURITY

Next.js Security Advisory
nextjs.org/blog/security-update-2025

OWASP Top 10
owasp.org/www-project-top-ten/

Casbin Authorization
casbin.org

Permit.io
permit.io

COMPLIANCE

GDPR Official Text
gdpr.eu

CCPA/CPRA Info
cppa.ca.gov

China PIPL Overview
china-briefing.com/news/pipl