Forum:Hack Forums

Thread: GluePrint | Advanced Recon Fingerprinter | 420+ Technologies | WAF Detection

Vinavil - *January 14, 2026, 10:29 am*

??????????????????????????????????
GLUEPRINT v1.0 RELEASE
Advanced Tech Stack Fingerprinting
??????????????????????????????????

A tool by Vinavil

What Is This Thing?

So you're doing recon on a target and you need to know what's running under the hood. What framework? What libraries? What analytics? What's protecting it? You could click around for hours trying to figure this out manually, or you could let something else do the heavy lifting for you.

GluePrint is a tech stack fingerprinter that actually works. Point it at a URL and it tells you everything the target is running. We're talking servers, frameworks, JavaScript libraries, CSS frameworks, analytics tools, widgets, CDNs, WAFs, the whole nine yards. Over 420 different technologies detected from a single scan.

The difference between this and the garbage tools floating around? Accuracy. No more false positives telling you a site runs WordPress just because it has some random header. The detection patterns are tight and specific. If GluePrint says something is there, it's actually there.

Why Should You Care?

Knowing what a target runs is step zero of any serious engagement. Here's what this intel gets you:
Attack Surface Mapping Every technology has its own set of vulnerabilities. jQuery 1.x? XSS city. Old WordPress? Pick your CVE. Knowing what's there tells you what to look for.

WAF Detection Nothing worse than burning your payloads against a WAF you didn't know existed. GluePrint tells you if Cloudflare, Imperva, ModSecurity, or any of the other usual suspects are sitting in front.

Version Discovery Where possible, it pulls version numbers. Outdated jQuery? Vulnerable Bootstrap? Old Angular with known issues? Now you know exactly what you're dealing with.

Third Party Services Analytics, chat widgets, payment processors, auth providers. All of these expand the attack surface beyond just the main application. GluePrint maps all of it.

What Does It Actually Detect?

Here's the breakdown by category.

? Web Servers
Apache, nginx, IIS, LiteSpeed, Caddy, Gunicorn, Uvicorn, Tomcat, you name it. Server identification is table stakes but you'd be surprised how many tools get this wrong.

? Languages & Frameworks
PHP, Python, Ruby, Node, .NET on the backend. Laravel, Django, Rails, Express, Next.js, Nuxt on the framework side. WordPress, Drupal, Shopify, Magento for CMS and ecommerce. All the major players covered.

? Frontend Stack
React, Vue, Angular, Svelte, Preact, Alpine, HTMX. Plus over 150 JavaScript libraries. jQuery, GSAP, Anime.js, Three.js, Chart.js, Swiper, the list goes on. If it's in the page, GluePrint finds it.

? CSS & Icons
Tailwind, Bootstrap, Bulma, Materialize. Font Awesome, Material Icons, Feather, Heroicons. Design choices tell you a lot about the dev team and what vulnerabilities might exist in their workflow.

? Analytics & Tracking
Google Analytics, Matomo, Hotjar, Mixpanel, Siteimprove, Plausible. Know what data they're collecting and through what services. Sometimes these third parties have their own weaknesses.

? Widgets & Embeds
Spotify, SoundCloud, YouTube, Tidal, Disqus, Calendly, Typeform. ReadSpeaker for accessibility. All those third party integrations that expand the attack surface.

? CDN & WAF
Cloudflare, AWS CloudFront, Fastly, Akamai, Vercel, Netlify. On the protection side, Cloudflare WAF, AWS WAF, ModSecurity, Imperva, Sucuri. Know what's between you and the target.

? SEO & Meta
Open Graph, Twitter Cards, Schema.org, RSS feeds, PWA manifests. Tells you about their marketing stack and sometimes reveals internal tooling.

How Does It Work Under the Hood?

The magic is in the pattern matching. Every technology has fingerprints. Specific headers, cookies, HTML patterns, script references, CSS classes. GluePrint knows what to look for and where to look.

Detection Methods
Header Analysis Server headers, X-Powered-By, custom headers that frameworks leave behind. Quick wins that don't even require parsing HTML.

Cookie Inspection Session cookie names are dead giveaways. Laravel uses laravel_session,

Django uses sessionid, PHP uses PHPSESSID. Each framework has its patterns.

Body Pattern Matching This is where the bulk of detection happens. Script paths, CSS references, inline patterns, meta tags, data attributes. Hundreds of regex patterns tuned for accuracy.

Deep Scanning Optional mode that probes additional paths like /robots.txt, /wp-json/, /api/ to find more evidence. Also pokes the WAF with test payloads to see what blocks you.

Accuracy Over Everything

Here's the thing that makes GluePrint different. Every fingerprint has a minimum match requirement. It doesn't flag WordPress just because it sees one vague pattern. We need specific evidence like wp-content paths, wp-includes references, or the WordPress API header. Same philosophy across all detections.

The confidence scores actually mean something. 95% confidence means we're damn sure. 70% means there's strong evidence but you should verify. No more guessing what a tool's output actually means.

Usage

Dead simple. Python 3.8+, two dependencies, works on anything.

? Installation
Code git clone https://github.com/yourusername/glueprint.git
cd glueprint
pip install -r requirements.txt
? Basic Scan
Code python -m glueprint -u https://target.com
? Deep Scan with Evidence
Code python -m glueprint -u https://target.com --deep --verbose
? JSON Output for Automation
Code python -m glueprint -u https://target.com --json -o report.json
? Custom Headers
Code python -m glueprint -u https://target.com -H "Authorization: Bearer token" -H "X-Custom: value"
The output is clean and organized by category. Color coded confidence scores, evidence trails in verbose mode, and missing security header warnings. Everything you need at a glance.

Use It As a Library Too

Import it into your own scripts and automation.

Code from glueprint import GluePrint

scanner = GluePrint("https://target.com")
result = scanner.scan(deep=True)

```
for tech in result.detections:
    print(f"{tech.name} - {tech.confidence}%")

[h1]Check for specific tech[/h1]
if result.has("WordPress"):
    print("WordPress detected, check for vulns")

[h1]Get by category[/h1]
wafs = result.by_category("waf")
if wafs:
    print(f"Protected by: {wafs[0].name}")

[h1]Export[/h1]
json_data = scanner.to_json()
```

Build it into your recon pipelines, chain it with other tools, automate your workflow. The code is clean and the API is straightforward.

Adding new fingerprints is trivial. Just add patterns to the appropriate file and they're automatically picked up. The architecture is modular by design.

Final Thoughts

Recon is everything. You can't exploit what you don't know exists. GluePrint gives you that knowledge quickly and accurately. 422 technologies, clean output, low false positives, easy to extend.

No bloat, no dependencies nightmare, just what you need to identify what you're dealing with.

If you are lazy enough to not go ahead and download the tool from my github i'll pin the link down here for a small byte fee ?

Biggy_Asian - *January 14, 2026, 10:32 am*

I want to fuck you. Thanks this is really helpful!!!!!! But for real this is sick i am def keeping this safe ;p

Vinavil - *January 14, 2026, 10:38 am*

(Jan 14, 2026 11:32 AM)Biggy_Asian Wrote: [CITE] I want to fuck you. Thanks this is really helpful!!!!!! But for real this is sick i am def keeping this safe ;p

Hey, happy it was useful, Feel free to star the repo if it helps you out?

Saterax - *February 11, 2026, 1:13 pm*

Neat. Appreciated :) Guess I have something to play around with.