Passive Reconnaissance and Threat Modeling Report

Target Website: https://www.geeksforgeeks.org

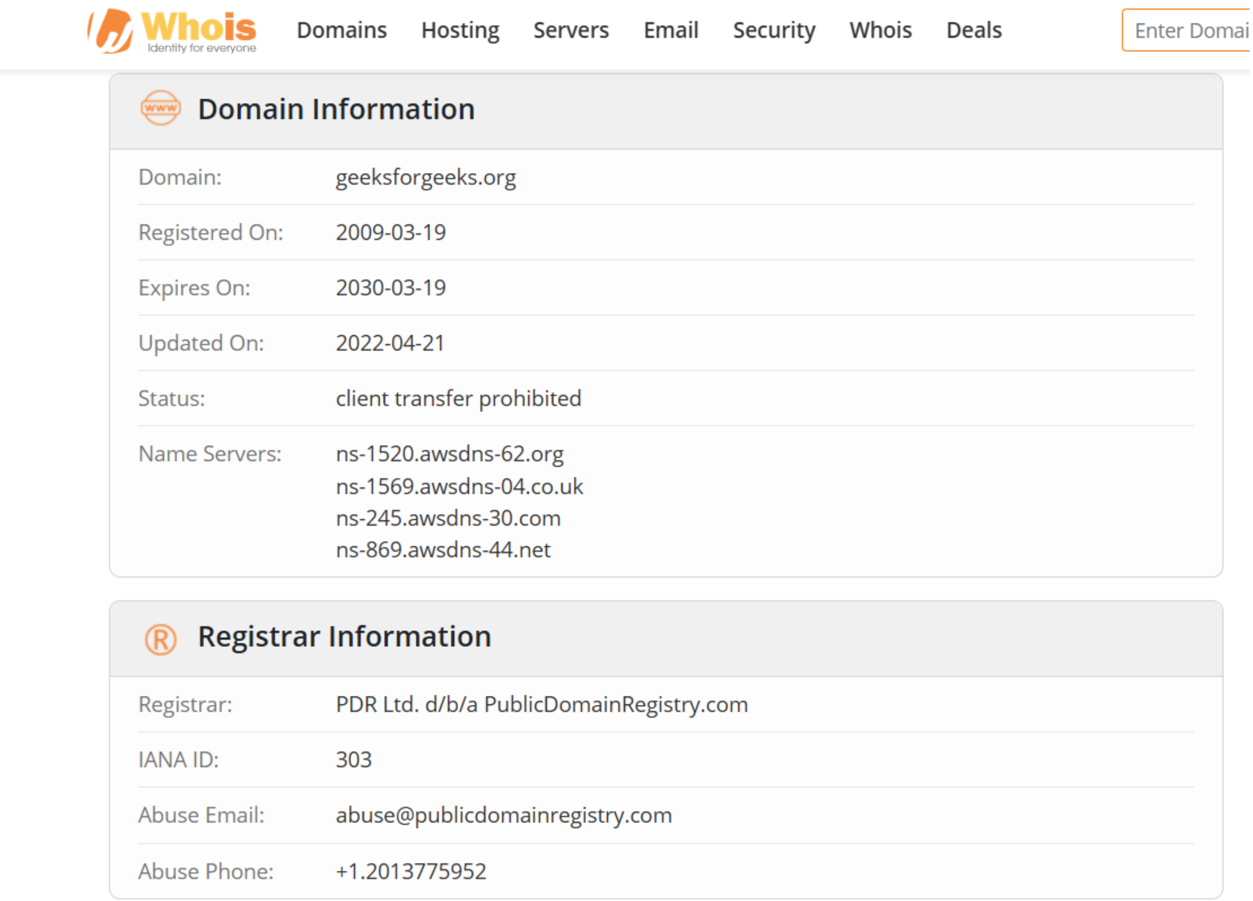
- **Tools Used:** -
  - Whois Lookup (whois.com)
  - MXToolbox (https://mxtoolbox.com)
  - Google Dorking
  - Wappalyzer (browser extension)

---

1. Reconnaissance Findings

Whois Lookup

- **Registrar:** PDR Ltd. d/b/a PublicDomainRegistry.com
- **IANA ID:** 303
- **Abuse Email:** abuse@publicdomainregistry.com
- **Registrant Organization:** Privacy Protect, LLC
- **Location:** Massachusetts, US



Domain Information

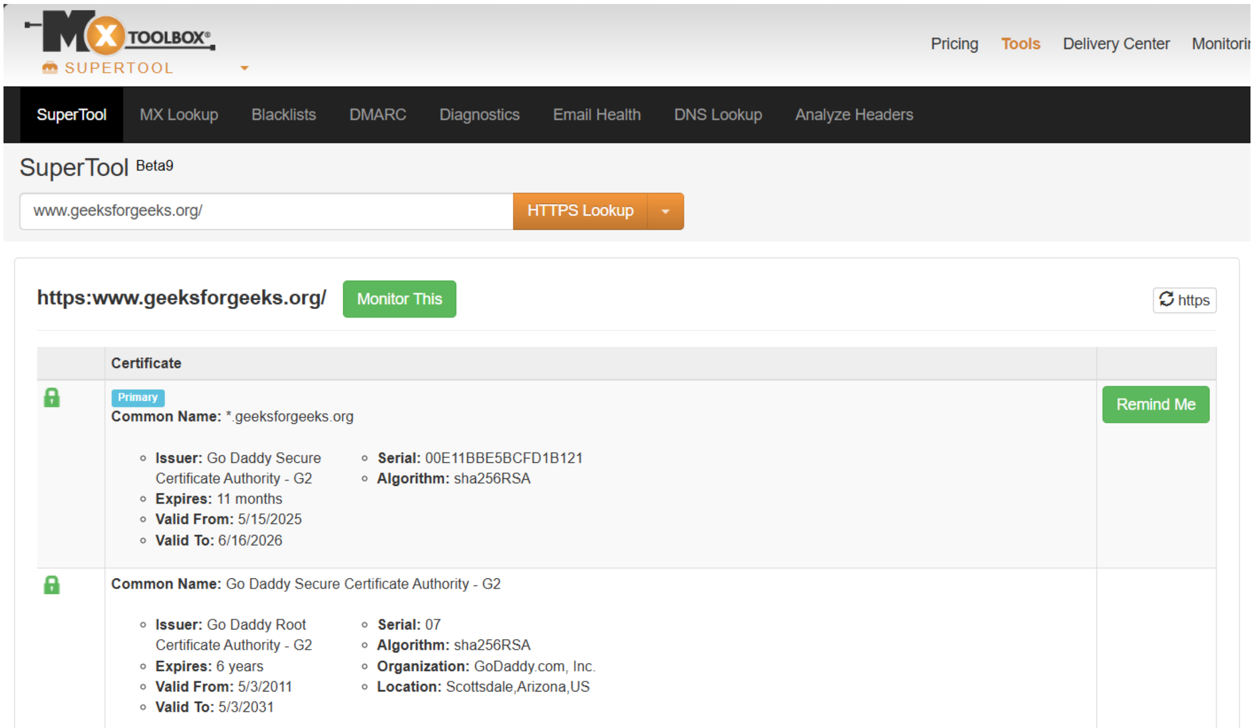
Domain:	geeksforgeeks.org
Registered On:	2009-03-19
Expires On:	2030-03-19
Updated On:	2022-04-21
Status:	client transfer prohibited
Name Servers:	ns-1520.awsdns-62.org ns-1569.awsdns-04.co.uk ns-245.awsdns-30.com ns-869.awsdns-44.net

Registrar Information

Registrar:	PDR Ltd. d/b/a PublicDomainRegistry.com
IANA ID:	303
Abuse Email:	abuse@publicdomainregistry.com
Abuse Phone:	+1.2013775952

MXToolbox – HTTPS Lookup

- **Common Name:** *.geeksforgeeks.org
- **Issuer:** GoDaddy Secure Certificate Authority - G2
- **Algorithm:** sha256RSA
- **Valid From:** 15-May-2025
- **Valid To:** 16-Jun-2026
- **HTTP Status:** 200 OK



SuperTool Beta9

www.geeksforgeeks.org/

https:www.geeksforgeeks.org/

Certificate

Common Name: *.geeksforgeeks.org

- **Issuer:** Go Daddy Secure Certificate Authority - G2
- **Expires:** 11 months
- **Valid From:** 5/15/2025
- **Valid To:** 6/16/2026
- **Serial:** 00E11BBE5BCFD1B121
- **Algorithm:** sha256RSA

Common Name: Go Daddy Secure Certificate Authority - G2

- **Issuer:** Go Daddy Root Certificate Authority - G2
- **Expires:** 6 years
- **Valid From:** 5/3/2011
- **Valid To:** 5/3/2031
- **Serial:** 07
- **Algorithm:** sha256RSA
- **Organization:** GoDaddy.com, Inc.
- **Location:** Scottsdale,Arizona,US

Google Dorking

- **Dorks Used:**
  - `site:geeksforgeeks.org` – Listed all indexed pages
  - `inurl:admin site:geeksforgeeks.org` – Checked for accessible admin directories
  - `intitle:index.of site:geeksforgeeks.org` – Looked for open directories
  - `filetype:pdf site:geeksforgeeks.org` – Identified downloadable resources

Findings: -

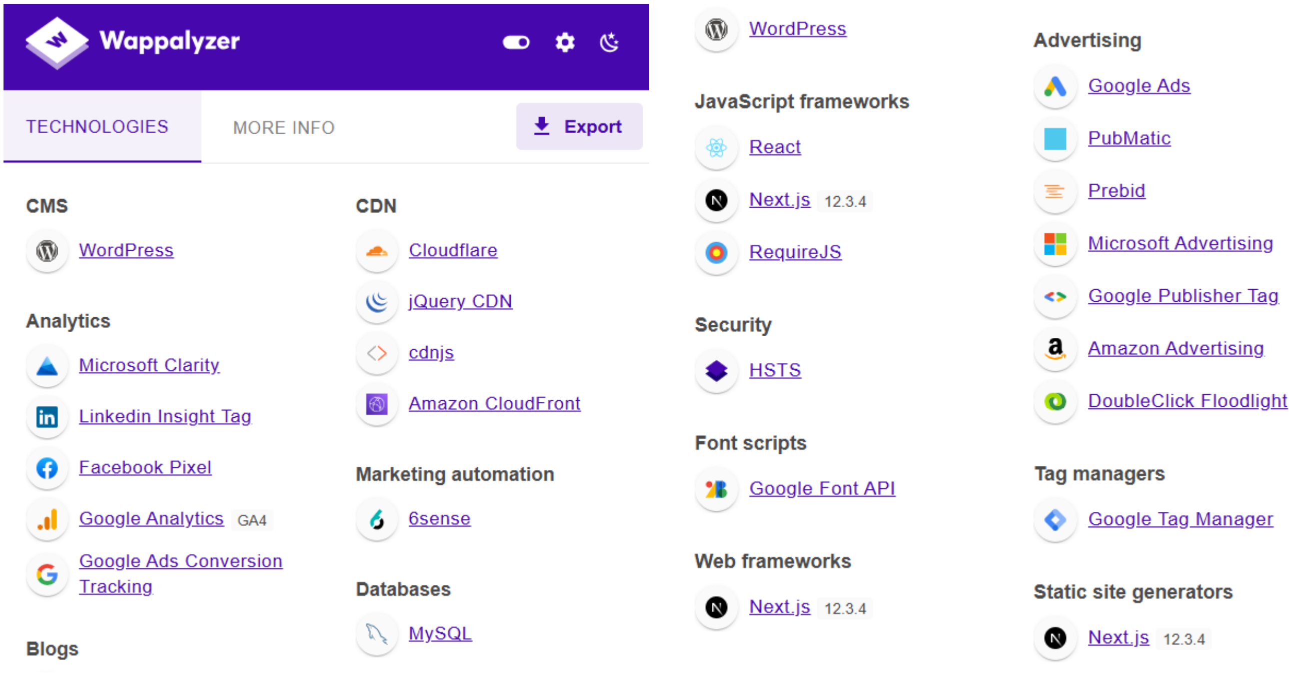
- Indexed internal pages
- Multiple downloadable xls and txt file’s

- No exposed admin or sensitive directories discovered during this scan

Technology Stack (via Wappalyzer)

- **Web Server:** Nginx
- **Programming Languages:** PHP, JavaScript
- **JavaScript Libraries:** jQuery
- **Analytics:** Google Analytics
- **Content Management System:** WordPress (in some sections)
- **CDN/Hosting:** Cloudflare

These technologies provide valuable insight into the structure and potential vulnerabilities of the target website. For instance, the use of JavaScript libraries and CMS platforms may introduce outdated components if not regularly patched.



CMS
- WordPress

Analytics
- Microsoft Clarity
- Linkedin Insight Tag
- Facebook Pixel
- Google Analytics GA4
- Google Ads Conversion Tracking

Blogs

CDN
- Cloudflare
- jQuery CDN
- cdnjs
- Amazon CloudFront

Marketing automation
- 6sense

Databases
- MySQL

- WordPress

JavaScript frameworks
- React
- Next.js 12.3.4
- RequireJS

Security
- HSTS

Font scripts
- Google Font API

Web frameworks
- Next.js 12.3.4

Advertising
- Google Ads
- PubMatic
- Prebid
- Microsoft Advertising
- Google Publisher Tag
- Amazon Advertising
- DoubleClick Floodlight

Tag managers
- Google Tag Manager

Static site generators
- Next.js 12.3.4

---

2. Threat Modeling

Identified Exposed Assets

- SSL/TLS certificate metadata
- Domain registrar information
- Indexed files and pages
- Downloadable public documents (e.g., .pdf files)

- Technology stack and plugins/libraries in use

Potential Attackers

- Cybercriminals
- Competitors
- Script kiddies

Possible Attack Techniques

- Directory brute forcing
- Exploitation of outdated plugins (if identified via Wappalyzer)
- Information harvesting via OSINT tools and social engineering

3. Threat Model Table

Actor	Asset	Threat
Script Kiddie	Indexed documents	Download and extract sensitive data
Cybercriminal	Whois/Certificate info	Use domain metadata for phishing or spoofing
Competitor	Tech stack via Wappalyzer	Identify weaknesses for competitive intelligence
Phisher	SSL Metadata	Create fake clone for credential harvesting

4. Short Summary

During the passive reconnaissance phase, various tools were used to gather publicly available data on geeksforgeeks.org. The Whois lookup revealed registrar and contact details, protected by Privacy Protect LLC. SSL certificate information showed the use of GoDaddy Secure CA with valid HTTPS implementation. Google dorking confirmed the presence of indexed documents and downloadable files but revealed no major exposed directories.

Technology stack analysis via Wappalyzer uncovered the use of Nginx, PHP, JavaScript (with jQuery), Cloudflare, and WordPress, among others. These components can be potential targets if outdated or misconfigured. This insight further enriches the threat modeling process by exposing additional attack surfaces.

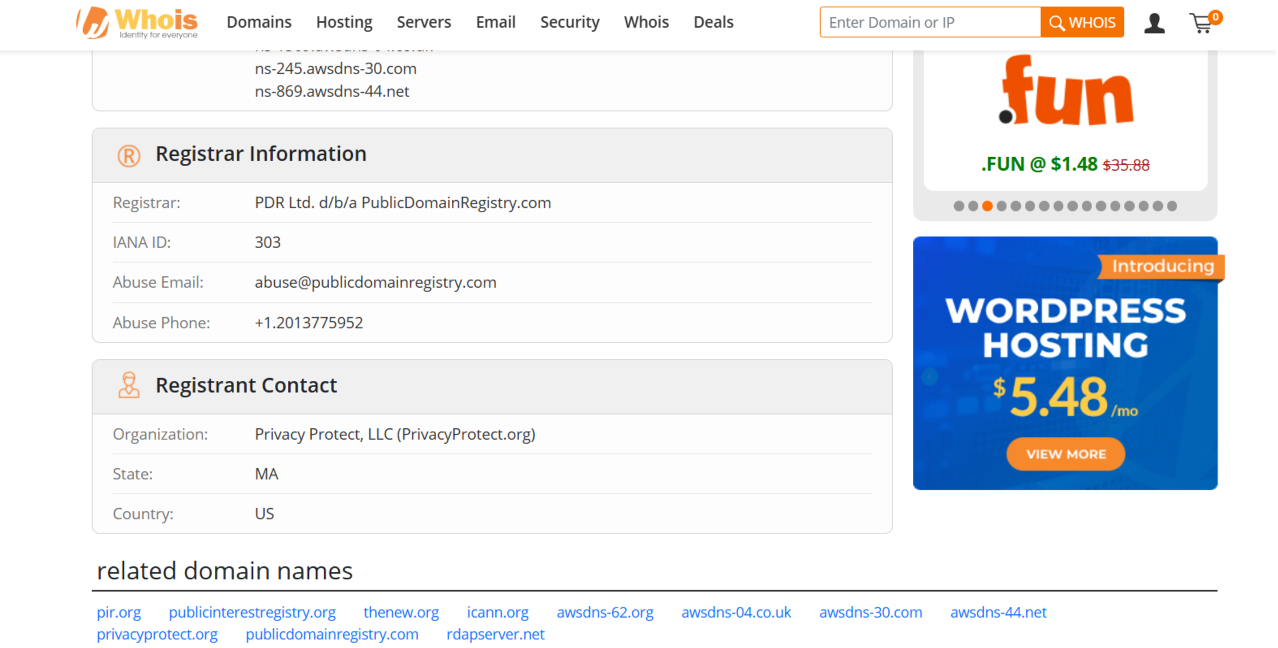
From a threat modeling perspective, potential risks include attackers exploiting indexed files, certificate metadata, and technical stack information. While no immediate vulnerabilities were discovered, the presence of metadata and accessible PDFs suggests a need for improved access control and obfuscation strategies. Overall, the domain displays strong security hygiene but should continue monitoring for potential passive threats.

5. Bug and Vulnerability Analysis

1. **Outdated or Unpatched Libraries (e.g., jQuery)**
   - Solution: Implement a continuous update mechanism for frontend libraries to mitigate XSS and DOM-based attacks.
2. **Exposed WHOIS and Certificate Metadata**
   - Solution: Utilize domain privacy services and registrar-level security like domain locking to reduce exposure to phishing and impersonation.
3. **Indexed Downloadable Files (e.g., PDFs)**
   - Solution: Restrict access to sensitive documents using authentication and configure robots.txt to prevent indexing by search engines.
4. **Use of WordPress in Subsections**
   - Solution: Update CMS components regularly and minimize plugin usage to reduce vulnerability to CMS-specific exploits.
5. **Public Exposure of Site Structure through Google Indexing**
   - Solution: Deploy restrictive rules in robots.txt and .htaccess to control crawler access and limit unintended content exposure.

Attached Screenshots

1. Whois Lookup –



ns-245.awsdns-30.com
ns-869.awsdns-44.net

Registrar Information

Registrar:	PDR Ltd. d/b/a PublicDomainRegistry.com
IANA ID:	303
Abuse Email:	abuse@publicdomainregistry.com
Abuse Phone:	+1.2013775952

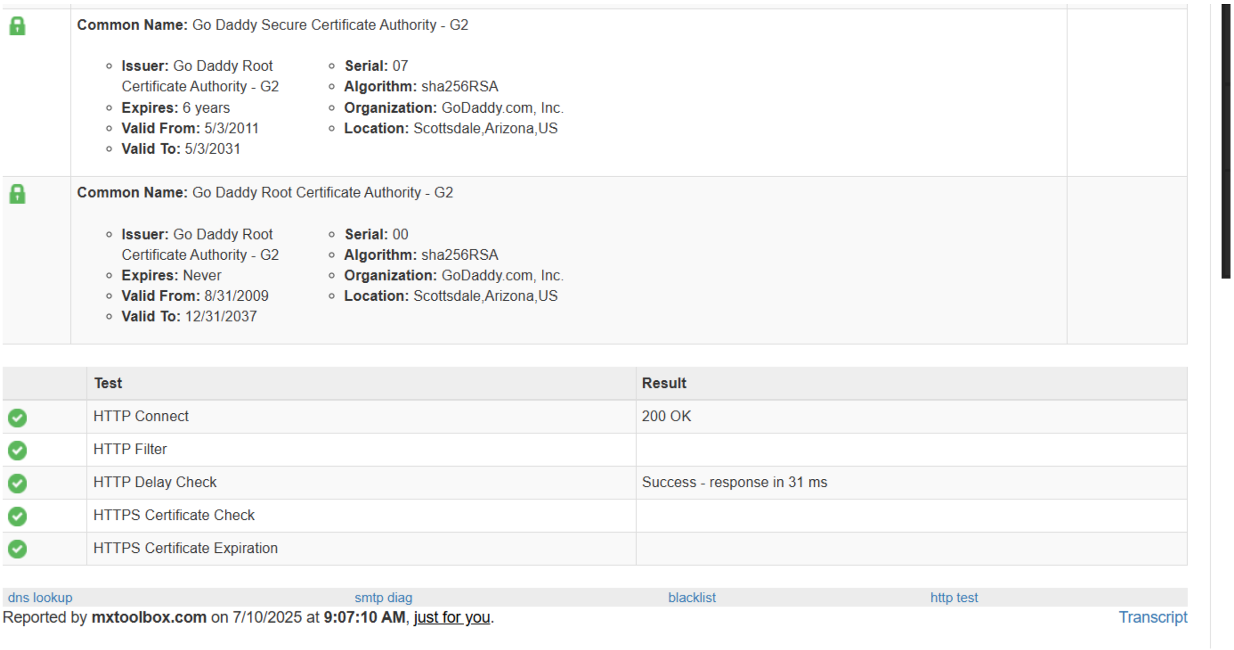
Registrant Contact

Organization:	Privacy Protect, LLC (PrivacyProtect.org)
State:	MA
Country:	US

related domain names

pir.org publicinterestregistry.org thenew.org icann.org awsdns-62.org awsdns-04.co.uk awsdns-30.com awsdns-44.net privacyprotect.org publicdomainregistry.com rdapserver.net

2. MXToolbox HTTPS Lookup –



Common Name: Go Daddy Secure Certificate Authority - G2

- **Issuer:** Go Daddy Root Certificate Authority - G2
- **Expires:** 6 years
- **Valid From:** 5/3/2011
- **Valid To:** 5/3/2031
- **Serial:** 07
- **Algorithm:** sha256RSA
- **Organization:** GoDaddy.com, Inc.
- **Location:** Scottsdale,Arizona,US

Common Name: Go Daddy Root Certificate Authority - G2

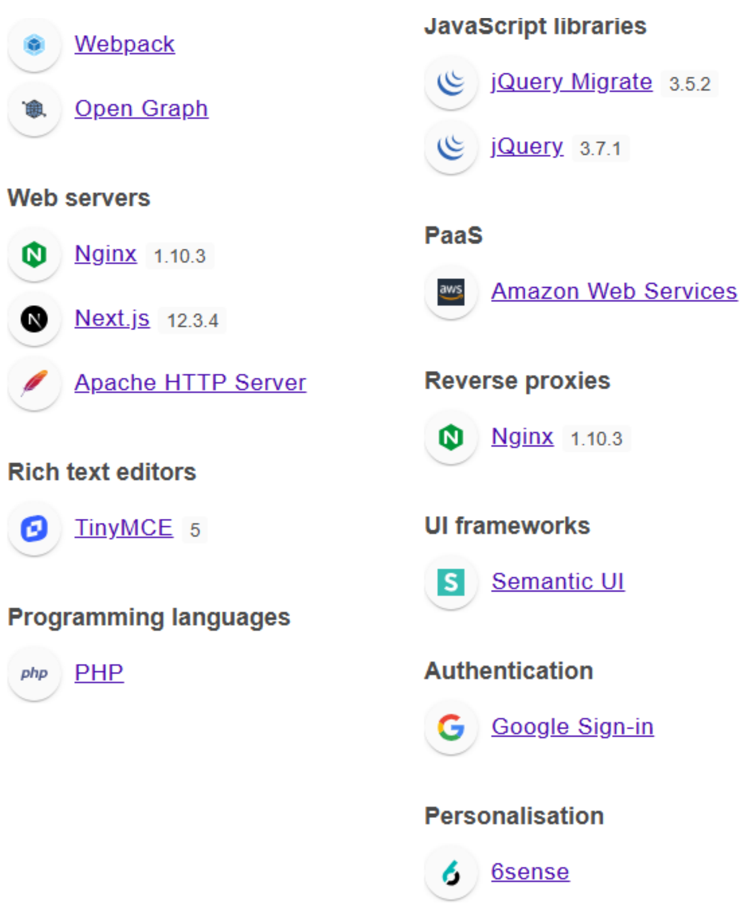
- **Issuer:** Go Daddy Root Certificate Authority - G2
- **Expires:** Never
- **Valid From:** 8/31/2009
- **Valid To:** 12/31/2037
- **Serial:** 00
- **Algorithm:** sha256RSA
- **Organization:** GoDaddy.com, Inc.
- **Location:** Scottsdale,Arizona,US

	Test	Result
✓	HTTP Connect	200 OK
✓	HTTP Filter	
✓	HTTP Delay Check	Success - response in 31 ms
✓	HTTPS Certificate Check	
✓	HTTPS Certificate Expiration	

dns lookup smtp diag blacklist http test

Reported by **mxtoolbox.com** on 7/10/2025 at **9:07:10 AM**, just for you. Transcript

3. Wappalyzer Results –



Webpack

Open Graph

Web servers

Nginx 1.10.3

Next.js 12.3.4

Apache HTTP Server

Rich text editors

TinyMCE 5

Programming languages

PHP

JavaScript libraries

jQuery Migrate 3.5.2

jQuery 3.7.1

PaaS

Amazon Web Services

Reverse proxies

Nginx 1.10.3

UI frameworks

Semantic UI

Authentication

Google Sign-in

Personalisation

6sense