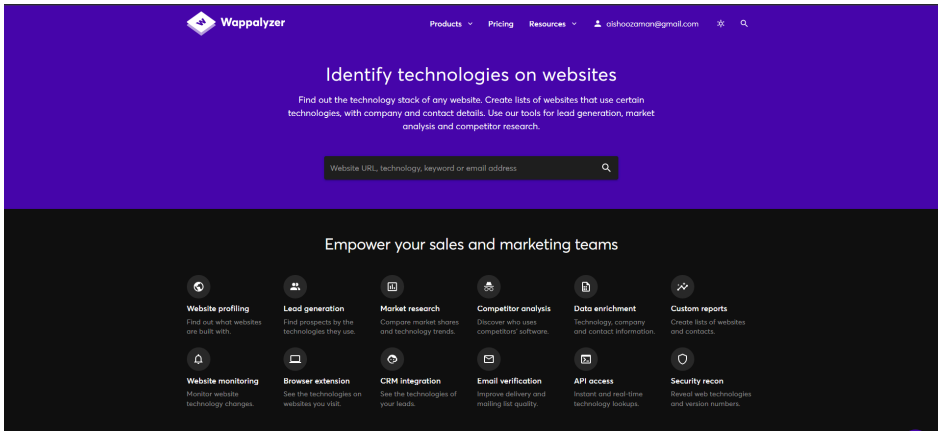
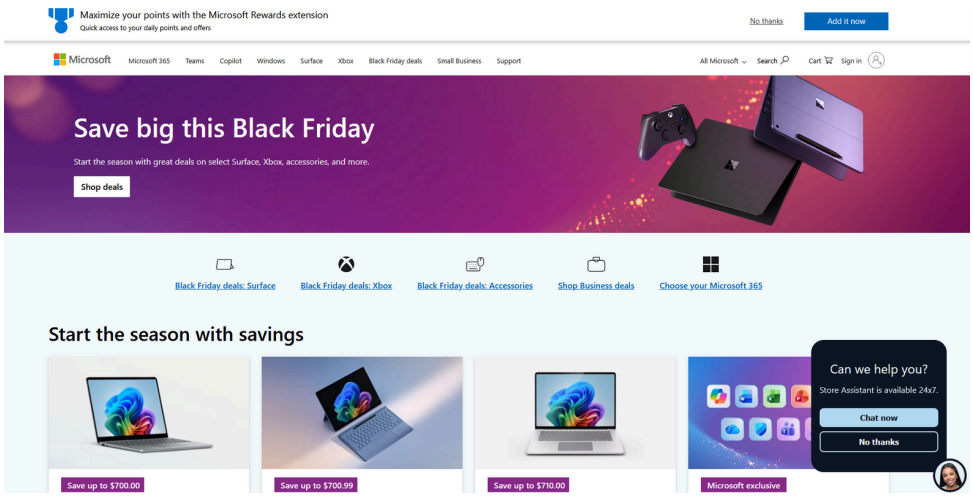
Identify Website Tech

Identifying what technologies a website is built with is an essential step in web reconnaissance, penetration testing, competitive research, and general web analysis. The goal is to understand what frameworks, CMS, analytics tools, plugins, server details, and programming languages are used.

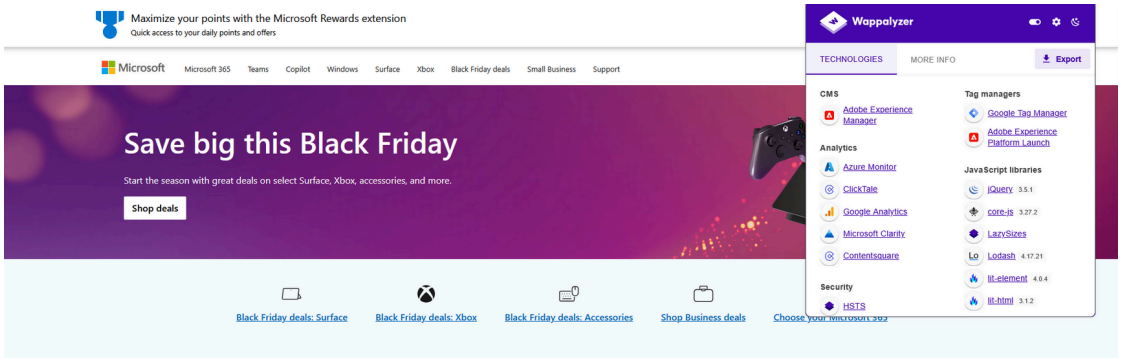
1. Browser Extensions for Technology Detection

1.1 Wappalyzer





Wappalyzer is a browser extension that automatically analyzes websites and identifies:



➔ CMS platforms (Adobe Experience Manager)

➔ Analytics tools (Google Analytics, Microsoft Clarity, Azure Monitor)

➔ JavaScript libraries (jQuery, Lodash, lit-element, core-js)

➔ Tag managers (Google Tag Manager, Adobe Launch)

➔ Security features (HSTS headers)

➔ Frameworks / Web servers

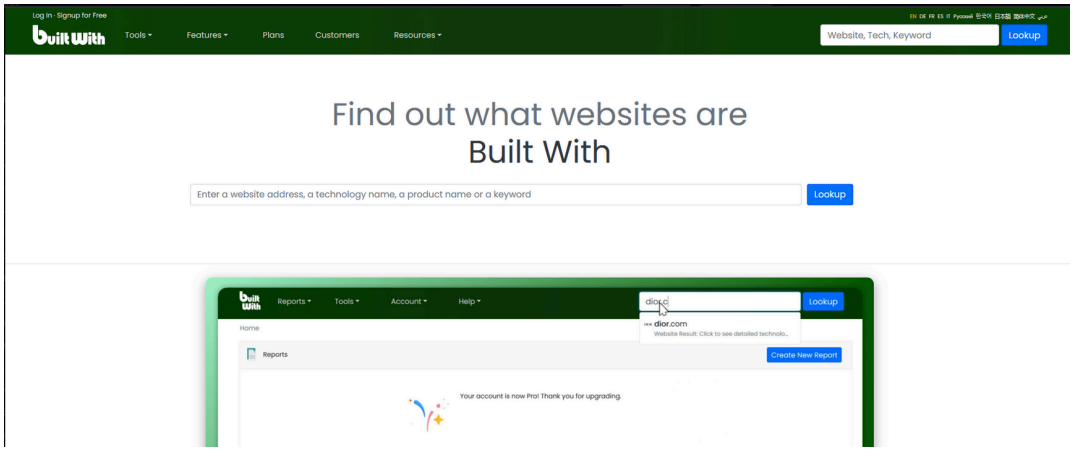
Why this is useful

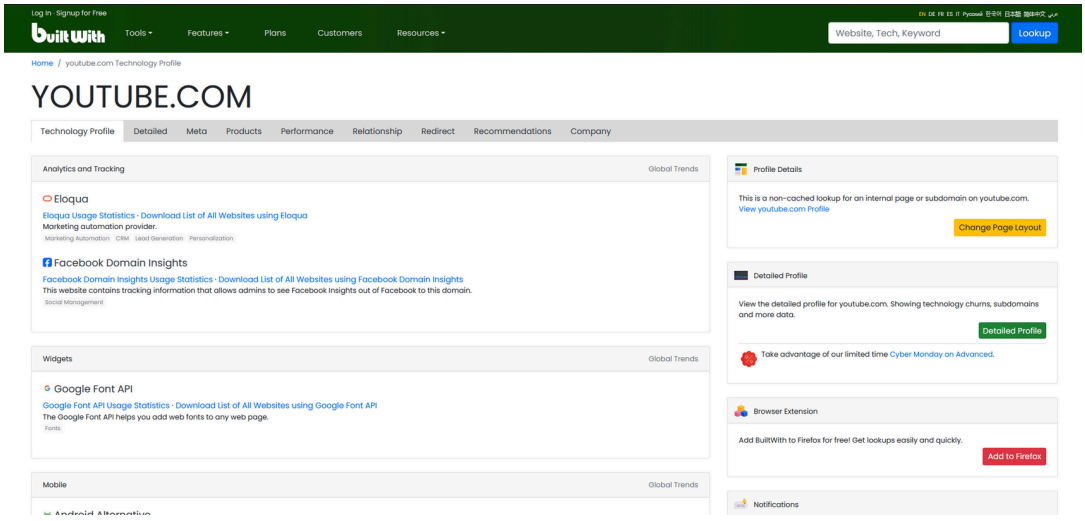
- Helps attackers understand potential vulnerabilities in used components.
- Helps analysts understand architectural structures.
- Saves time vs manual enumeration.

1.2 BuiltWith

BuiltWith performs a deeper server-side scan than browser extensions and is useful for:

- Full technology profiles
- Historical technology changes
- Traffic analytics
- E-commerce platform detection
- Hosting providers
- Email services

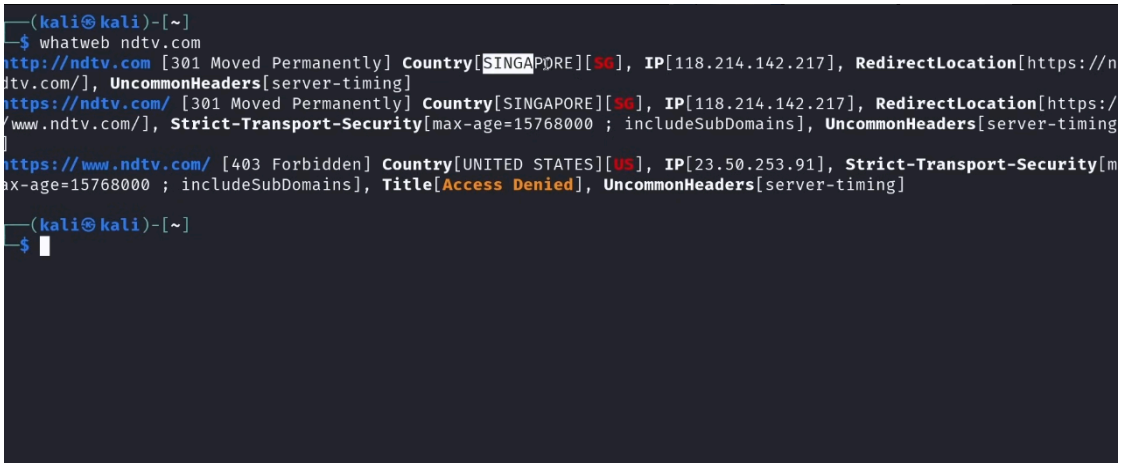




2. Command-Line Tools for Technology Detection

WhatWeb is a CLI tool used mainly in Linux/Kali for web reconnaissance. It identifies:

- Server type
- Country/Hosting origin
- IP addresses
- Redirect chains
- Security headers (Strict-Transport-Security)
- Response status (403 Forbidden, 301 Moved Permanently)



whatweb ndtv.com

http://ndtv.com Country: Singapore (SG)

IP: 118.214.142.217

Redirects to https://www.ndtv.com

Final Status: 403 Forbidden

Country: United States (US)

IP: 23.50.253.91

Security: Strict-Transport-Security enabled

MORE:

General Methodology for Technology Enumeration

Step 1 – Use Browser Tools

- Wappalyzer or BuiltWith extension
- Quick detection of frameworks/analytics/CMS

Step 2 – Use Online Scanners

- BuiltWith website
- Netcraft
- DNSdumpster

Step 3 – Use Terminal-Based Tools

- `whatweb`
- `wafw00f` (for firewall detection)
- `curl -I <website>` (to analyze headers manually)

Step 4 – Manually Inspect the Website

- Check page source (`Ctrl + U`)
- Look at response headers in Developer Tools
- Identify JS/CSS files that reveal frameworks