Recce Report for blog.offgridtech.xyz

Tool: WHOIS

- Command Used: whois offgridtech.xyz
- Purpose: WHOIS is used to query information about the domain registration, including the registrar, domain status, and registration dates.
- Key Findings:
    - Registrar: GoDaddy, LLC.
    - Domain Status: Various statuses including clientTransferProhibited, indicating restrictions on domain transfer.
    - Registrant: Registered under Domains By Proxy, LLC, suggesting privacy protection is enabled.
    - Name Servers: Utilizes AWS DNS (AWSDNS), indicating hosting on AWS infrastructure.

Tool: SSLyze

- Command Used: sslyze offgridtech.xyz
- Purpose: SSLyze is a tool to analyze the SSL/TLS configuration of a web server for security vulnerabilities and compliance.
- Key Findings:
    - SSL/TLS Support: Supports TLS 1.2 and TLS 1.3 with various cipher suites, indicating strong encryption protocols.
    - Certificate Details: The certificate is valid from January 9, 2024, to February 6, 2025, issued by Amazon RSA.
    - SSL/TLS Compliance: The certificate life span exceeds the recommended 366 days.

Tool: Nmap

- Command Used: nmap -sV blog.offgridtech.xyz
- Purpose: Nmap is a network scanning tool used to discover hosts and services on a computer network.
- Key Findings:
    - Open Ports: Ports 80 (HTTP) and 443 (HTTPS) are open.
    - Web Server Identification: AWS Elastic Load Balancer and Apache 2.4.52 running on Ubuntu detected.
    - Redirection: HTTP requests are being redirected to HTTPS.

- Reverse DNS Record: ec2-52-60-131-26.ca-central-1.compute.amazonaws.com, indicating an AWS EC2 instance.

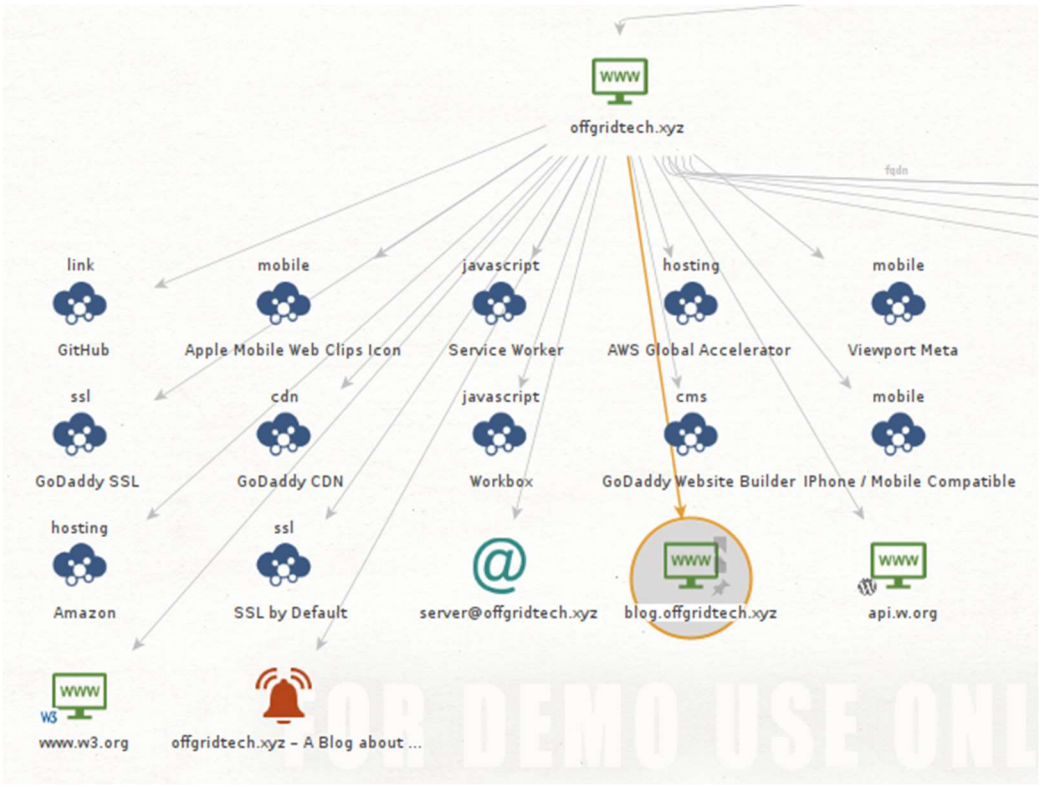
Tool: WhatWeb

- Command Used: whatweb -v blog.offgridtech.xyz
- Purpose: WhatWeb identifies website technologies, including content management systems, server software, and other technologies.
- Key Findings:
    - Server Header: AWS Elastic Load Balancer (awselb/2.0).
    - Content Management System: Running WordPress 6.4.2.
    - Technologies Identified: Apache 2.4.52, HTML5, Ubuntu Linux, jQuery 3.7.1.
    - Security Headers**:** Presence of uncommon headers including Link for WordPress REST API.

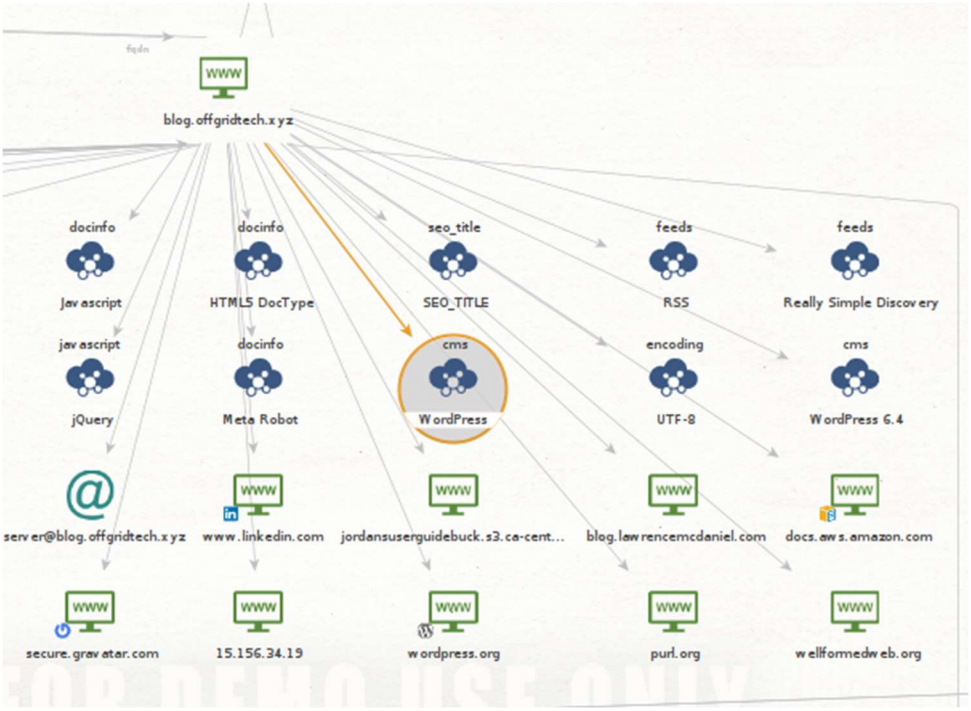
Tool: Maltego

Maltego Footprinting Summary for offgridtech.xyz

- Core Entities: The domain offgridtech.xyz, along with its associated blog subdomain and three key IPv4 addresses (52.60.131.26, 35.182.136.138, 3.97.175.11), forms the central network structure.
- Technological Profile: Analysis identified 22 different technologies via BuiltWith, including AWS Global Accelerator, GoDaddy CDN and SSL, HTML5, WordPress 6.4, and jQuery.
- DNS Infrastructure: Identified primary DNS names and records, with significant links to ns-2004.awsdns-58.co.uk and other AWS DNS servers, highlighting the use of AWS services.
- WHOIS Data: Registrant information is protected by Domains By Proxy, LLC, indicating a privacy-focused domain registration. The domain is registered with GoDaddy and shows standard client and server statuses.
- Web Presence: The analysis shows a well-connected web infrastructure, with offgridtech.xyz having the highest number of both incoming and outgoing links, reflecting its central role in the network.
- Subdomain Analysis: blog.offgridtech.xyz is prominent in the network, suggesting it as a key component of the site's online presence.



Screenshot of Maltego Footprint on “offgridtech.xyz”



Maltego Footprint of “blog.offgridtech.xyz”

Chrome Dev Tools Findings on https://blog.offgridtech.xyz

Request Details

- **Request URL: https://blog.offgridtech.xyz/**
    - Indicates the URL of the requested resource.
- **Request Method: GET**
    - A GET request is used to retrieve data from the server. This is typical for fetching a webpage.
- **Status Code: 200 OK**
    - This is a standard response for successful HTTP requests. It means the request was successfully processed and the content is being sent back.

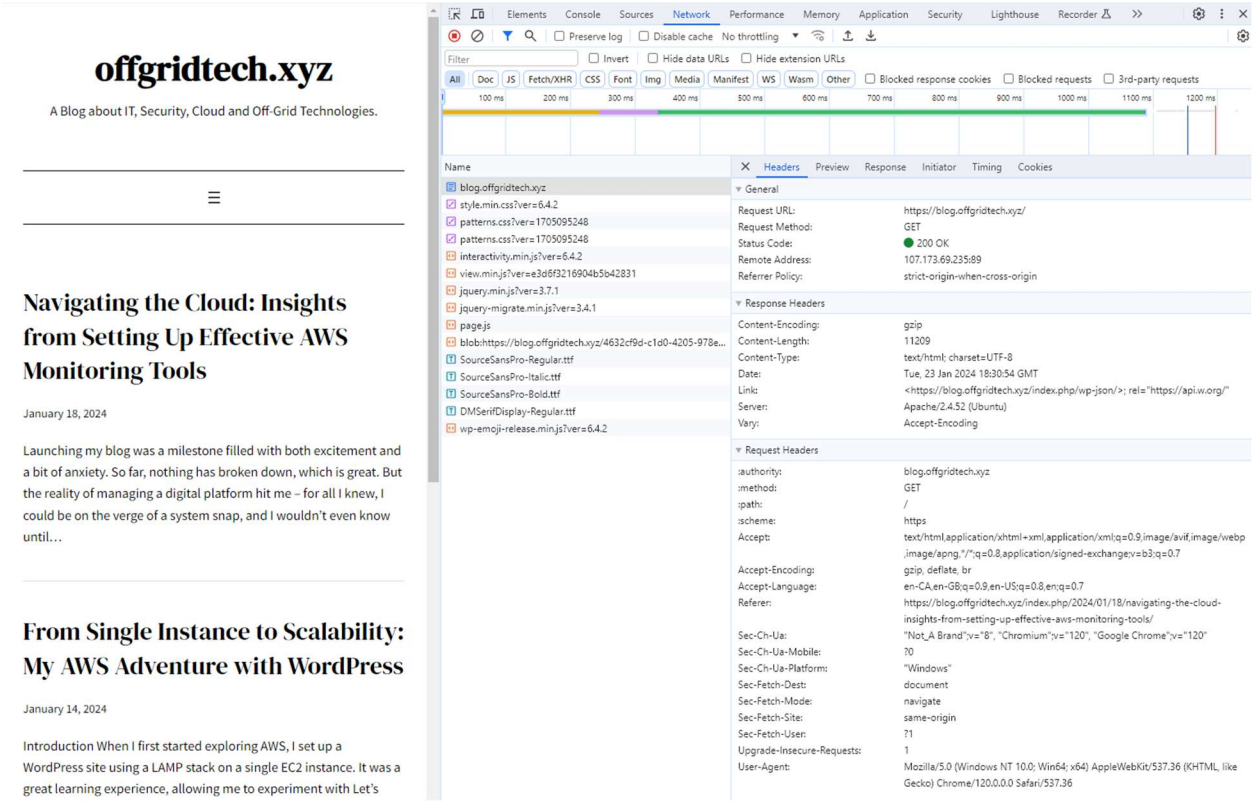
Response Details

- **Remote Address: 107.173.69.235:89**
    - This is the IP address and port number of the server handling your request.
- **Content-Encoding: gzip**
    - Indicates that the content is compressed using gzip, which is a method to speed up the loading of the website.
- **Content-Length: 11209**
    - The size of the response body, in bytes. It gives an idea of the page size.
- **Content-Type: text/html; charset=UTF-8**
    - Indicates that the server is sending an HTML document with UTF-8 character encoding.
- **Date: Tue, 23 Jan 2024 18:30:54 GMT**
    - The date and time when the response was sent.
- **Link: <https://blog.offgridtech.xyz/index.php/wp-json/>; rel="https://api.w.org/"**
    - Points to the WordPress REST API endpoint. This is typical for WordPress sites.
- **Server: Apache/2.4.52 (Ubuntu)**
    - Identifies the web server software and its version, along with the operating system. This can be useful for understanding the server environment and potential vulnerabilities.

Request Headers

- :authority, :method, :path, :scheme
    - These are part of the HTTP/2 protocol and represent various components of the request.

- **Accept, Accept-Encoding, Accept-Language**
    - Indicates the types of content the client can process, the encoding formats accepted, and the preferred language.
- **Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site, Sec-Fetch-User**
    - Part of the Fetch Metadata Request Headers which provide information about the context of the request, enhancing security.
- **User-Agent**
    - Identifies the browser and operating system of the user. Useful for analytics and potential browser-specific optimizations or issues.



Summary and Analysis

- The target blog.offgridtech.xyz exhibits a robust online presence with key services hosted on AWS, as indicated by DNS and server information.
- The use of AWS Elastic Load Balancer and Apache on Ubuntu for web hosting implies a focus on scalability and security.
- The domain's WHOIS information suggests privacy-conscious administration, limiting exposure of registrant details.

- SSL/TLS configuration reflects a strong security posture with modern encryption standards, although there's room for improvement in aligning with best practices regarding certificate lifespans.
- The recce process did not reveal any immediate critical vulnerabilities. However, it highlighted the importance of regular monitoring and updates, especially given the site's use of popular platforms like WordPress.

Well-Configured Aspects

1. **SSL/TLS Configuration**:
    - The use of TLS 1.2 and TLS 1.3 indicates strong, modern encryption protocols are in place.
    - The server supports a range of secure cipher suites with Forward Secrecy, enhancing the confidentiality and integrity of data transmission.
2. **Domain Registration and Privacy**:
    - The domain is registered through GoDaddy with privacy protection (Domains By Proxy), which helps in masking the real registrant details, reducing the risk of targeted attacks or social engineering.
3. **Web Server and Load Balancer**:
    - The use of AWS Elastic Load Balancer (ELB) implies a scalable and secure front-end handling traffic, providing benefits like DDoS protection.
    - The Apache server is running a recent version (2.4.52), suggesting that the server is reasonably up-to-date.
4. **Content Management System (CMS)**:
    - WordPress is updated to version 6.4.2, which is a positive sign of keeping the CMS updated against known vulnerabilities.
5. **Redirection and Content Delivery**:
    - HTTP requests are correctly redirected to HTTPS, ensuring encrypted communication.
    - The presence of a **Link** header for WordPress REST API indicates a modern implementation of content delivery.

Potential Actionable Insights

1. **Domain and Server Information:**
    - Use WHOIS data to explore potential domain-related vulnerabilities and understand the privacy measures in place.
    - The Apache/2.4.52 server on Ubuntu might have specific vulnerabilities; look for exploits targeting this configuration.
2. **SSL/TLS Configuration:**
    - Investigate any potential weaknesses in the SSL/TLS setup, especially considering the extended certificate lifespan.
    - Examine cipher suite preferences for older, less secure options that could be exploited.
3. **CMS and Web Application Analysis:**
    - WordPress version 6.4.2 should be checked for any known vulnerabilities, particularly in plugins or themes.
    - The WordPress REST API endpoint could be a target for unauthorized access or data exfiltration attempts.
4. **Network Infrastructure:**
    - The visibility of AWS infrastructure details could be leveraged for AWS-specific attack vectors.
    - Open ports (80 and 443) confirmed via Nmap scan indicate potential points of entry; further exploration of these ports may reveal vulnerabilities.
5. **HTTP Headers and Web Traffic:**
    - Analyze the response headers and content types for potential security misconfigurations or clues for further exploitation.
    - The presence of gzip compression suggests exploring compression-based security exploits.
    - Investigate the server's response behavior, MIME types, and any other anomalies that could be exploited.
6. **WordPress API and Content Delivery:**
    - Examine the Link header pointing to the WordPress API for any security misconfigurations or weak points.
    - Check if the server's redirection from HTTP to HTTPS is properly configured and secure.