

# Understanding Subdomains

## Results

### Subdomain Scan Results

The Subdomain Scan provides a comprehensive overview of the subdomains associated with the scanned domain. Monitoring subdomains is crucial as they often host various services and applications that can be potential targets for attackers if not properly secured. The scan results start with an overview of all discovered subdomains, highlighting key information such as IP addresses, open ports, HTTP status codes, content length, and more. Clicking on a specific subdomain takes you to its detailed analysis page.

#### Overview of Subdomains:

This section lists all subdomains discovered during the scan. Each entry provides essential information to quickly assess the subdomain's characteristics:

1. **SUBDOMAIN:**

The name of the subdomain found under the main domain, such as `planner.demodata.com`. Subdomains typically serve different functions within an organization, such as hosting web applications, APIs, or administrative portals.

2. **IP ADDRESS:**

The IP address associated with the subdomain, indicating where it is hosted. While the IP is not shown here for security reasons, it helps identify the server's location and assess potential security measures in place.

3. **OPEN PORTS:**

The list of open ports on the subdomain, such as `80/www-http` and `443/https`. Open ports indicate which services are accessible and may need further scrutiny to ensure they are securely configured.

4. **HTTP STATUS:**

The HTTP response code returned when the subdomain is accessed. A status code of `200` indicates a successful response, meaning the subdomain is live and serving content.

5. **CONTENT LENGTH:**

The size of the response content, providing insight into the volume of data the subdomain returns. Large content length may indicate a complex page or application.

6. **PAGE TITLE:**

The title of the web page served by the subdomain, giving a brief idea of its purpose. For

example, "Simple Planner v10.65.4" suggests a planning application.

## 7. **SCREENSHOT:**

A visual capture of the subdomain's homepage, useful for quickly identifying the nature of the content and potential risks, such as impersonation or phishing.

# Subdomain Detail Page:

Clicking on a specific subdomain, such as `planner.demodata.com`, takes you to a detailed analysis page that provides an in-depth view of the subdomain's configuration and security posture.

## Overview of `planner.demodata.com`

### 1. **Subdomain Information:**

- **Full URL:** The complete URL for accessing the subdomain, e.g., `https://planner.demodata.com`.
- **Page Title:** A brief description of the web page, indicating the subdomain's function.
- **Content Length:** Size of the content returned by the subdomain.
- **HTTP Response Code:** Indicates the HTTP status, such as `200` for a successful request.

### 2. **IP Addresses:**

Lists the associated IP address(es) hosting this subdomain. The IP address information is crucial for tracking hosting providers and understanding the subdomain's network setup.

### 3. **Ports:**

Displays open ports on the subdomain, revealing the services running, such as HTTP (`80`) or HTTPS (`443`). Open ports must be secured to prevent unauthorized access.

### 4. **Services:**

Identifies the software and technologies in use on the subdomain, such as `nginx/1.25.3`. Knowing the services helps in assessing the security posture and checking for known vulnerabilities.

### 5. **Vulnerabilities Discovered:**

The number of vulnerabilities found on the subdomain. Each vulnerability is listed with its severity level and the URL where it was discovered, aiding in prioritizing security efforts.

An example of a critical vulnerability that may be discovered is:

- **CVE-2021-44228 - Apache Log4j Vulnerability:**

A critical vulnerability in Apache Log4j identified by CVE-2021-44228 has been publicly disclosed, potentially allowing for remote code execution in impacted Elasticsearch 5 installations. This severe flaw can be exploited by attackers to execute arbitrary code, leading to full system compromise. Immediate remediation is necessary, such as updating Log4j to the latest patched version.

### 6. **Missing Security Headers Grade:**

A grade indicating the presence or absence of critical security headers. A low grade, such as "F," means essential security headers are missing, increasing the risk of attacks like cross-site scripting (XSS) or clickjacking.

## 7. Suffixes Discovered:

Lists any URL suffixes found during the scan. These suffixes can point to accessible directories or files that may expose sensitive information.

## 8. SSL Grade:

Assesses the quality of the SSL/TLS configuration for the subdomain. A "N/A" or low grade indicates potential issues with encryption, putting data transmission at risk.

# Subdomain Vulnerabilities:

Provides a detailed overview of the vulnerabilities detected on the subdomain. Each vulnerability is listed with its severity and the URL where it was found. For instance, in addition to informational findings like technology detection, a critical vulnerability like the Apache Log4j exploit (CVE-2021-44228) indicates an urgent need for remediation to prevent remote code execution attacks.

# Header Overview:

Displays a list of missing security headers that could improve the subdomain's security posture. Headers such as `Content-Security-Policy` or `X-Frame-Options` are crucial for protecting against attacks like XSS and clickjacking.

# Suffixes Found:

Lists any suffixes (e.g., `example.com/admin`) discovered during the scan, which can expose additional entry points to the subdomain.

# SSL/TLS Information:

Provides details about the SSL/TLS configuration of the subdomain, ensuring secure data transmission. No data indicates that an SSL scan is needed to evaluate the security of encrypted connections.

# Response Information:

Shows the HTTP response headers returned by the subdomain, including information about the server, cookies, and security configurations. This helps in understanding how the server is configured and identifying potential security gaps.

# Example Analysis:

- **Subdomain:** `planner.demodata.com`
  - **Open Ports:** 80, 443 (indicating HTTP and HTTPS services)
  - **Services:** Nginx/1.25.3
  - **Vulnerabilities:** 10 discovered, including critical vulnerabilities like the Apache Log4j (CVE-2021-44228) exploit that allows for remote code execution.

- **SSL Grade:** N/A
- **Analysis:** This subdomain runs a web application accessible over HTTP and HTTPS. It has multiple vulnerabilities, including a critical issue with Apache Log4j, which allows for remote code execution and must be addressed immediately. Other issues, such as missing security headers, further result in a low security grade. Urgent action is recommended, including patching Log4j, updating server software, and implementing necessary security headers to secure this subdomain.

By regularly monitoring subdomains and addressing detected vulnerabilities, including critical ones like the Apache Log4j exploit, you can strengthen your organization's security posture, protect sensitive information, and prevent potential exploitation by attackers.

---

Revision #2

Created 16 September 2024 11:59:44 by Raphael

Updated 16 September 2024 12:31:33 by Raphael