CEOIndustries, Inc.

Penetration Test Report

SD Company, D.D.S., P.C.

November 19, 2024

SD Company, D.D.S., P.C.

3907 S Crackerneck Rd.
Independence, MO 64055
United States of America

Tel: 1-816-373-3101
Email: info@companyemail.com
Web: https://www.companywebsite.com

Executive Summary and Overview

CEOIndustries, Inc. ("CEOIndustries") was contracted by SD Company, D.D.S., P.C. ("SD") to conduct a black-box penetration test to determine the company's potential exposure to a targeted attack. SD is a small family dentistry practice. The practice consists of three doctors, three dental hygienists, five dental assistants, and four business administration staff (collectively, "Associates"). SD is committed to ensuring that their website, patient portals, and health records retain their confidentiality, integrity, and availability.

All activities were conducted in a manner that simulated a malicious actor engaged in the beginning stages of reconnaissance to build up an attack against SD with the goals of:

- Assessing the ability of a remote attacker to penetrate SD's defenses simply by searching publicly available information with no internal knowledge of SD's systems or architecture.
- Determining the likelihood of a security breach based on the types and amount of information a passive actor could obtain, including:
    - Confidential and Personally Identifiable Information (PII) such as trade secrets, financial information, or confidential assets
    - Internal infrastructure and vulnerabilities of SD's information systems

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the recommendations outlined in NIST SP 800-115 (http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf).

Summary of Results

Initial passive reconnaissance of the SD network did not result in the discovery of any overt misconfigurations or security issues. An examination of the hosts revealed that the company's domain is hosted in the cloud by WP Engine and Cloudflare and the web server is not physically on-site. Four open ports and running services were discovered, none of which led to a vulnerability that could be exploited.

The active reconnaissance and advanced enumeration phase mainly comprised of web application testing to find an integration point between WordPress and SD's internal systems. Since we gathered information on the third-party companies handling the patient scheduling portal, the billing portal, and the review portal, there were no other avenues to pursue since Denial-of-Service attacks are outside the scope of this penetration test. Further examinations did not reveal any hosting server misconfigurations or poor security, nor any exposed backups or database dumps that might contain internal credentials or other PII.

It is our assessment that the security of SD's website is above average and there are a few minor security modifications we recommend:

1. **Update to the new version of WordPress, v. 6.7.**
2. **Configure SPF and DMARC records to prevent email-based attacks.**
3. **Delete all default or test email addresses, usernames, and the "Test" page on the website.**
4. **Disable CBC-mode ciphers like ECDHE-RSA-AES128-SHA256.**
5. **Strengthen the RSA key to 3072 or 4096 bits for added security.**
6. **Be sure to update all software and hardware promptly and install all patches.**

Attack Narrative

Phase One: Passive Reconnaissance

For the purposes of this assessment, SD Company, D.D.S., P.C., provided minimal information outside of the organizational domain name: www.companywebsite.com. The intent was to closely simulate an adversary who does not possess any internal information.

To gather as much information as possible to identify the potential attack surface, we first examine SD's website: https://www.companywebsite.com. By using both simple and advanced Google searches with operators we were able to gather the necessary basic company information needed to proceed with a more active attack. Specific resources and tools used have been listed in Appendix A – Resources. All data collected as a result of OSINT information gathering can be found in Appendix B – OSINT Data Collected.

Remote System Discovery

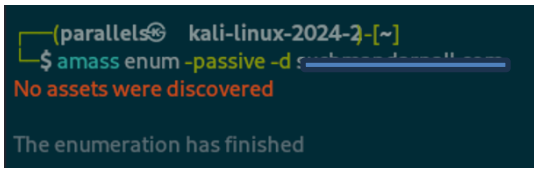
Below, we have provided screenshots or excerpts showing the results of the passive reconnaissance scans performed to create a target profile. We identified the domain IP address, name servers, website host, and various other data points which we then used to perform passive scans. The results of these scans are summarized in the table below with enumeration of specific scans and associated screenshots following.

	Results	Notes
Domain names	https:/	Issued by GoDaddy
IPv4		Owned by Google Cloud --> indicates there is no physical web server at the dentist office physical location
A Records for ns49	IPv4 IPv6	
A Records for ns50	IPv4 IPv6:	
AAAA, CNAME, MX Records	https	
NS Records	ns49.domaincontrol.com and ns50.domaincontrol.com	
SOA Data	Start of Authority: ns49.domaincontrol.com Email: dns@jomax.net Serial: 2020092202	

NSLookup Scan:

DNS Records and Subdomain Discovery:

Analysis of DNS records and output from various DNS and Subdomain enumeration scans indicate that no subdomains were identified. This means that the companywebsite.com domain is directly hosted under the root domain which limits external service exposure. There is evidence of Google services, but further exploration yielded no assets. These results could indicate a simple infrastructure or that the subdomains are hidden behind private DNS zones. DNSKEY queries did not reveal any DNSSEC-related vulnerabilities. Additionally, no significant misconfigurations were evident.



DNS Zone Transfer Attempt Output - Failed:

DNS Zone Transfer attempts failed, indicating that the DNS servers are configured correctly to block unauthorized AXFR requests.

Netcraft Report Indicating Missing SPF and DMARC Records of companywebsite.com:

The Netcraft report shows that the website is not vulnerable to the well-documented SSLv3/Poodle and Heartbleed attacks. Additionally, there are no Web Trackers found. These are good security measures. The report did show a lack of Sender Policy Framework (SPF) or Domain-based Message Authentication, Reporting, and Conformance (DMARC) records which could leave the domain vulnerable to email spoofing or phishing attacks. For example, emails could be forged to appear that they originate from companywebsite.com. This is a critical misconfiguration that should be rectified to protect against email-based attacks.

SSLv3/POODLE

This site does not support the SSL version 3 protocol.

More information about SSL version 3 and the POODLE vulnerability.

Heartbleed

The site did not offer the Heartbeat TLS extension prior to the Heartbleed disclosure, and so was not exploitable.

This test does not exploit the Heartbleed vulnerability but uses information from conventional HTTPS requests. More information about Heartbleed detection.

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see open-spf.org.

Warning: It appears that this host does not have an SPF record.

Setting up an SPF record helps prevent the delivery of forged emails from your domain. Please note that an SPF record will only protect the domain it is added to and not any mail-enabled subdomains. It is recommended to add an SPF record to any subdomain with an MX record.

DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see dmarc.org.

This host does not have a DMARC record. There may be a DMARC record on the site report for [redacted] Check the site report.

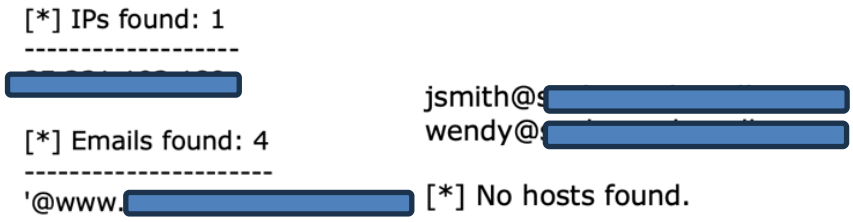
Web Trackers

Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

No known trackers were identified.

Found Email Addresses of companywebsite.com:

The website showed the existence of an email address: info@companyemaildental.com. Email validation was performed using theHarvester to look for additional associated email addresses. Three additional email addresses were found by theHarvester: jsmith@companyemail.com, wendy@companyemail.com, and '@companyemail.com. The HaveIBeenPwned website was also used to determine if there have been any breaches or password leaks related to these email addresses. The results did not indicate a break or leak has occurred. The additional emails found could be used to launch social engineering attacks; however, that is beyond the scope of this penetration test and will not be pursued. It should be noted that if jsmith@companyemail.com and '@companyemail.com are test/default email addresses, they should be deleted if no longer in use.



Attack Narrative

Phase Two: Port and Services Scanning

Ports and Services Discovery

Since no subdomains or overt misconfigurations were found, the next step was to look for open ports, services in use, access to directories and files, and any other potential vulnerabilities. The results of the wafW00f scan indicates the presence of a Web Application Firewall (WAF) or similar security mechanism. The WAF likely filters requests based on user-agent headers, patterns, automated tools, and non-standard requests. To bypass this security, we employed stealth options in our scan commands such as using obfuscated VPN's, routing traffic through TOR and proxy services, randomizing user-agents, reducing the number of threads, slowing the rate of requests, etc.

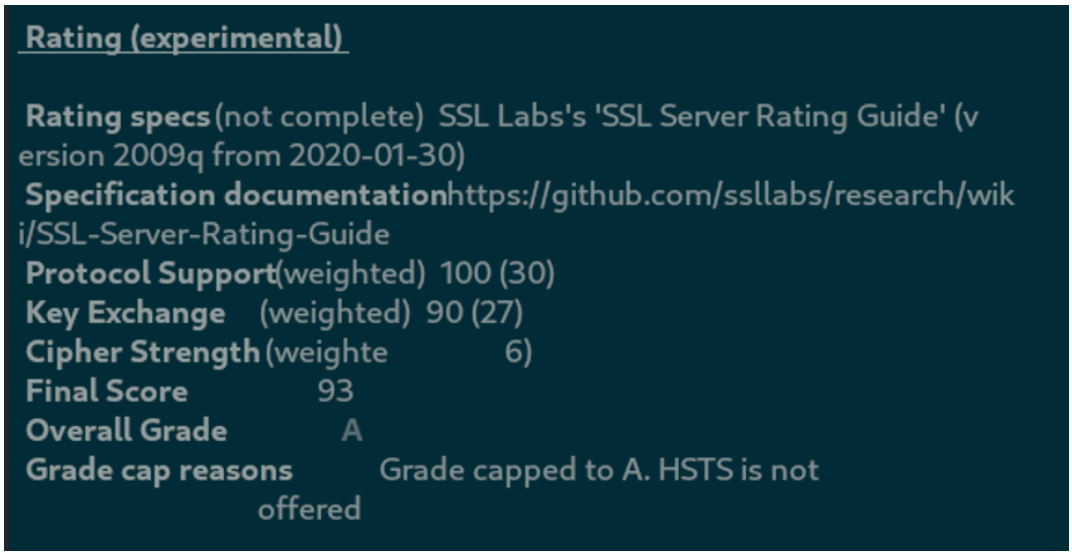
Nmap Scan Results Showing Existence of 4 Open Ports/Running Services:

Based on the Nmap scan results, there are 4 open ports running. Port 53 is the running the DNS server. Port 80 is running the nginx web server. Port 443 is running nginx with SSL. Port 8080 is possibly running an undetermined HTTP proxy, though the actual service could not be identified. Additional Nmap scans that included HTTP scripts indicated that there are no CSRF, DOM-based XSS, or stored XSS vulnerabilities present. Please see the complete Nmap scan results in Appendix C – Scan and Search Results.

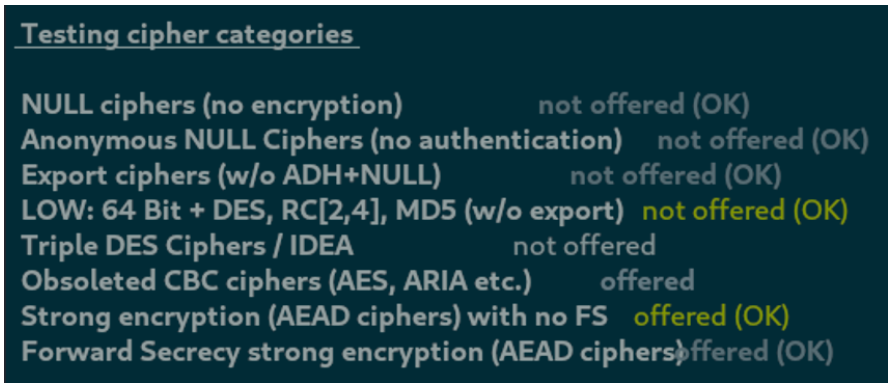
```
┌──(parallels㉿ kali-linux-2024-2)-[~]
└─$ proxychains nmap -sT -Pn --open [redacted] -oA nmap_openports_scan
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/aarch64          gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 01:06 CST
Nmap scan report for 180.103.231.35.bc.googleusercontent.com (35.231.103.180)
Host is up (0.00034s latency).
Not shown: 895 closed tcp ports (conn-refused), 101 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 4.16 seconds
```

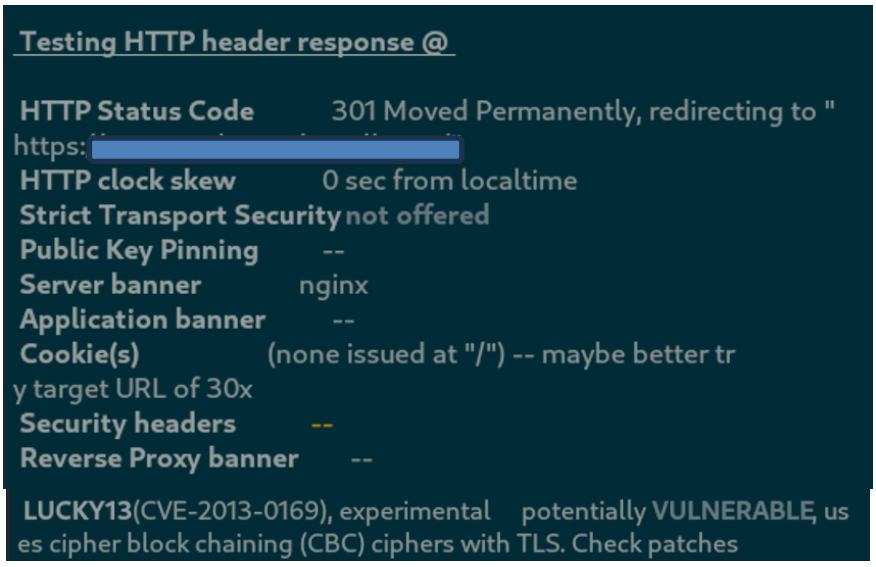
SSL/TLS Scan Results – Security Grade of A:

Several scans were performed to test the SSL/TLS configuration of the domain. They indicate that TLSv1.2 and TLSv1.3 are enabled and legacy/deprecated versions are disabled. This keeps the domain more secure. TLS Fallback to SCSV is supported which confirms that the domain protects against the "POODLE" attack. TLS Compression is disabled, which is a good security practice. The server is not affected by the following known vulnerabilities: Poodle, Heartbleed, Freak, Drown, Robot, Beast, Crime, Sweet32, Logjam. Additionally, the supported cipher suites (with forward secrecy supported), key exchange methods, and SSL Certificates are relatively strong and secure.



Overall, the domain is very secure. There were only a few items that could be updated to increase security even further. The AES128-SHA256 Cipher is not as strong as AES-GCM variants, so this could be disabled for greater security. The key length of the RSA key is 2048 bits which could be strengthened to 3072 or 4096 bits for added security. CBC ciphers are offered, so this could lead to a potential vulnerability known as Lucky13. To protect from this vulnerability, CBC-mode ciphers like ECDHE-RSA-AES128-SHA256 should be disabled.



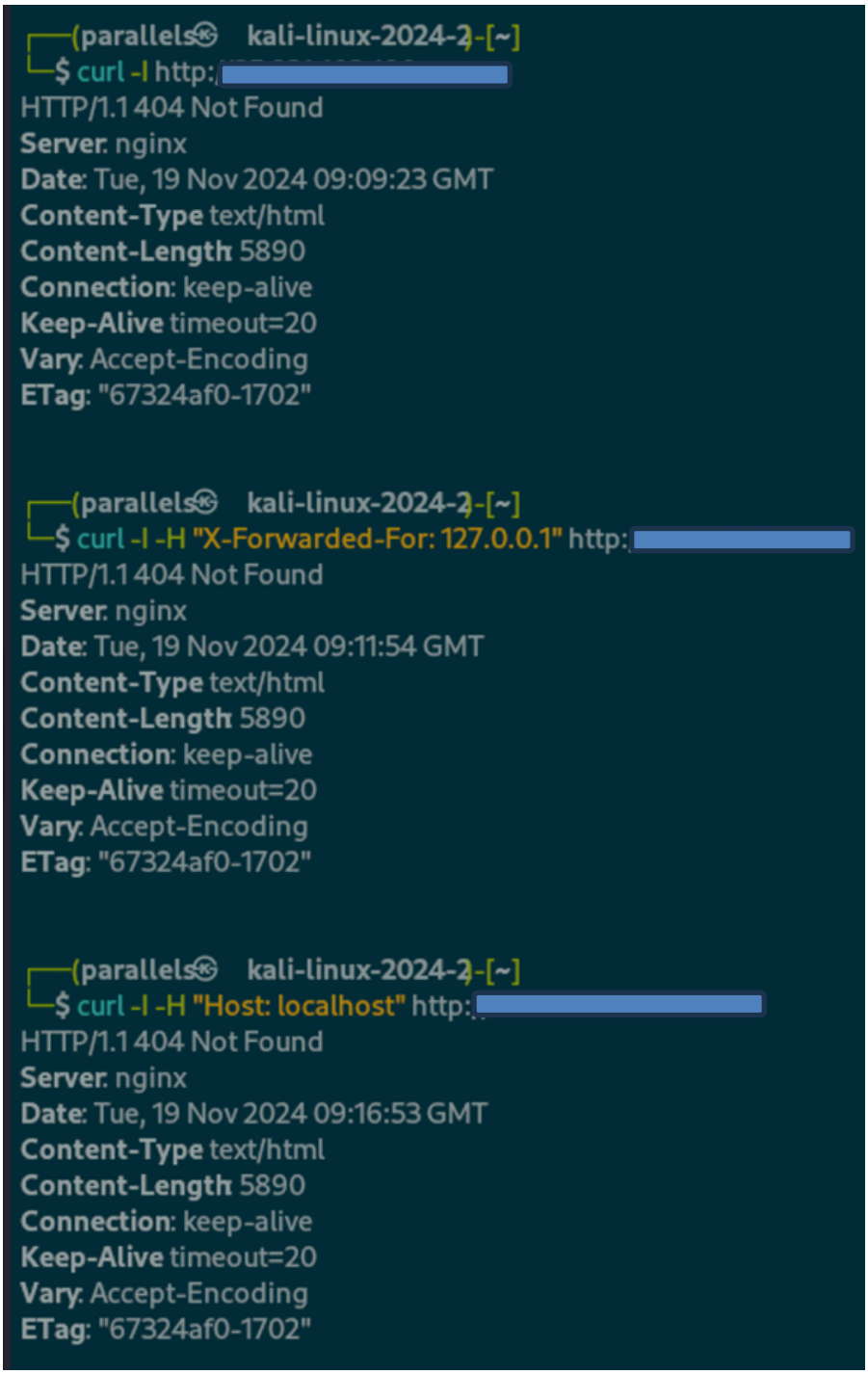


Open Port Services Enumeration:

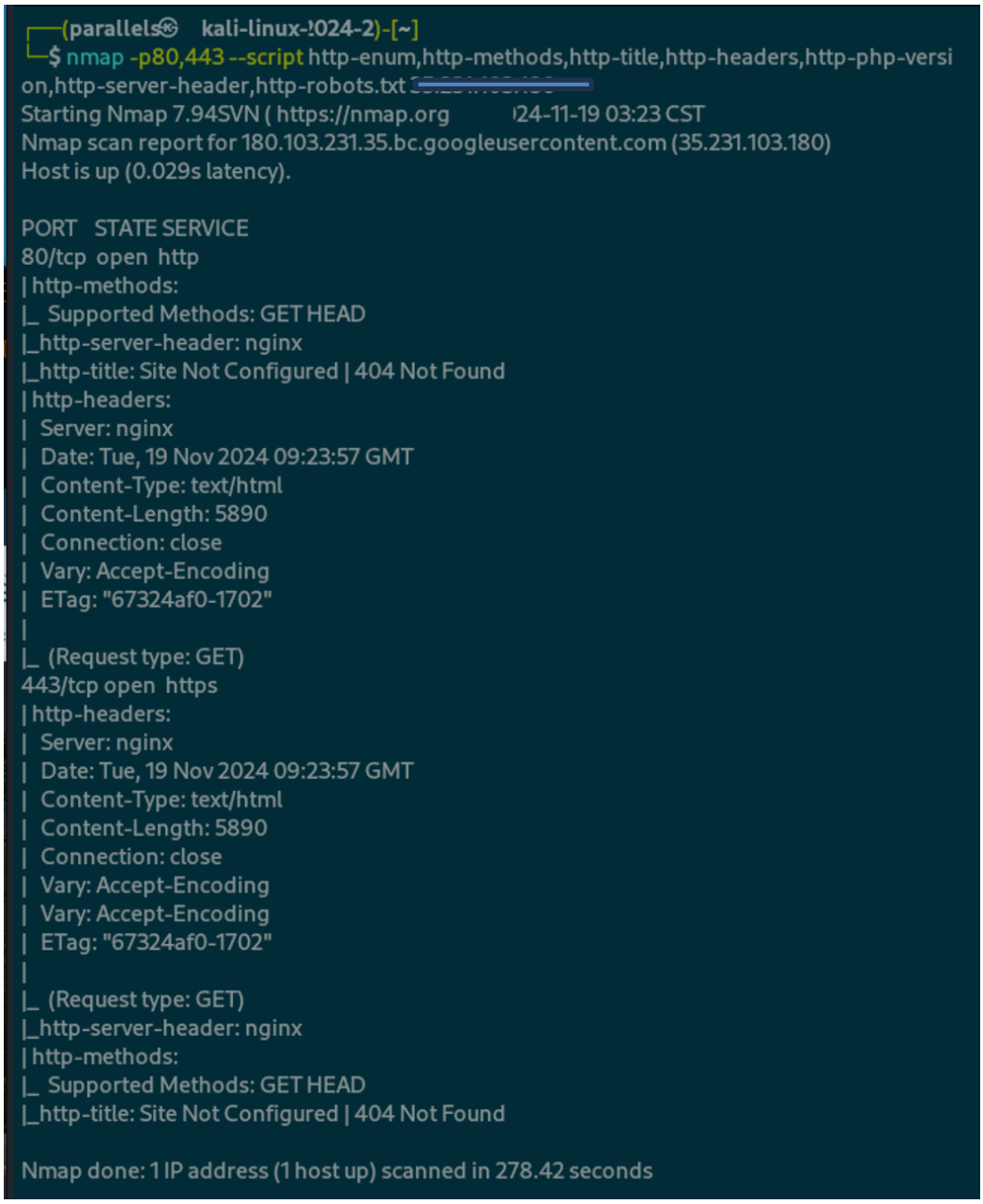
Several scans were performed to find more information about the services running on the open ports of the domain.

- Port 53 → As determined by the results mentioned above regarding DNS vulnerabilities, the scans do not show any existing vulnerabilities.

- Port 80 → Nginx is running on this open port. The server does not seem to process the X-Forwarded-For or Host header in a way that reveals additional information or access.

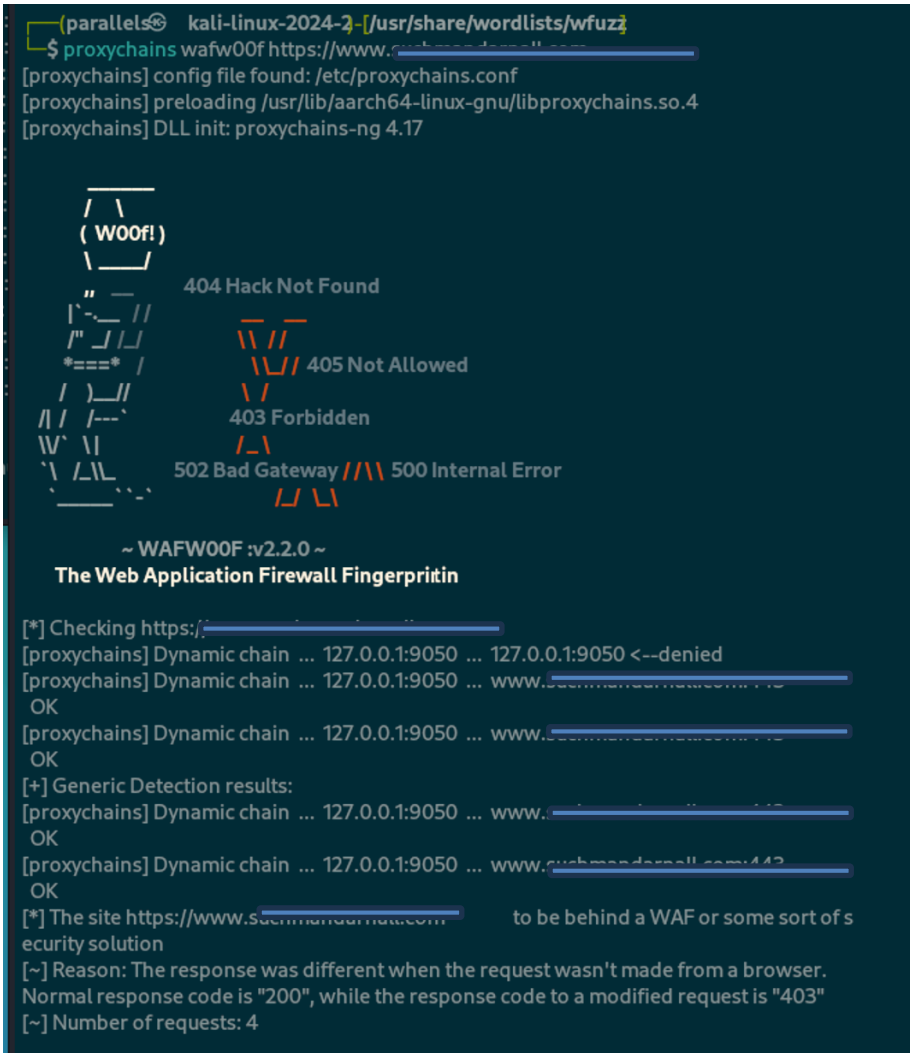


- Port 443 → Nginx web server managed by WP Engine and Cloudflare.



- Port 8080 → The output of scans related to port 8080 were either non-responsive, timed-out, or did not respond as expected for an HTTP-proxy. An aggressive nmap scan on port 8080 indicates that it is connected to a Fortinet FortiGate Firewall 200B model. This firewall is commonly used and the lack of response to HTTP requests indicates the service on this port may not be responding to typical HTTP requests or is highly restricted.

Existence of Web Application Firewall for companywebsite.com:



Existence of Wordpress Defender on companywebsite.com:

The existence of the WordPress security plugin, WP Defender, was found. WP Defender protects the site from excessive unauthorized access attempts and monitoring for malicious activity.

Directory Traversal Attempt Blocked for companywebsite.com:

The server blocked attempts to traverse the directory, indicating that file access controls are implemented properly. During the scan, the server implemented a lockout mechanism due to repeated requests. This indicates a basic intrusion detection system (IDS) and/or rate-limiting mechanism. These are good security measures that should hinder brute-force and automated scans.

Attack Narrative

Phase Three: Active Reconnaissance and Advanced Enumeration

The results of Phase Two did not identify any significant vulnerabilities. The services seem to be properly configured and no immediate misconfigurations, outdated software versions, or exposed sensitive endpoints have been identified. In Phase Three we attempted to find hidden weaknesses using advanced scanning and enumeration techniques.

Website Application Testing

Whatweb Scan Shows Website Security Settings – Good Security:

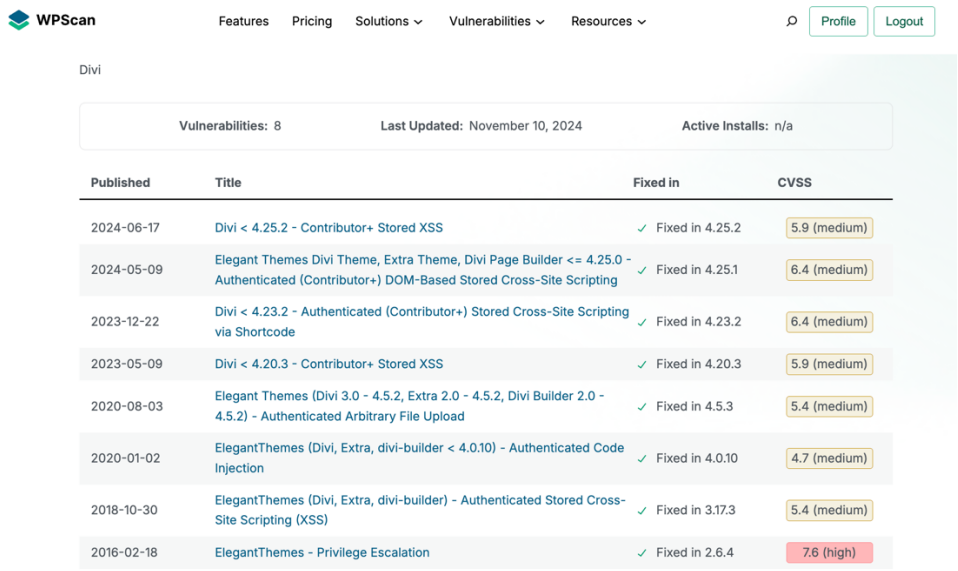
The Whatweb scan results reveal some key observations but do not indicate the existence of any critical vulnerabilities. Please see the comprehensive Whatweb scan results in Appendix C – Search and Scan Results. Information to note:

- The site is powered by WordPress (v6.6.2) and the Divi Child Theme (v.1.0.0) and is hosted on WP Engine (a managed WordPress hosting platform).
- Security Headers are correctly configured such as:
    - Strict-Transport-Security (HSTS) → restricts browsers to HTTPS-only connections
    - X-Frame-Options (sameorigin) → prevents clickjacking
    - X-XSS-Protection → mitigates reflected XSS attacks
    - X-Content-Type-Options (nosniff) → prevent MIME type sniffing
- Matomo is used instead of Google Analytics, which is more privacy-focused and suggests the site owner is aware of privacy and data control.
- The presence of /wp-json/ and /wp-json/wp/v2/pages/7 in headers suggests the WordPress REST API is accessible.

WPScan Results Showing Potential Vulnerabilities:

The WPScan results can be found in full in Appendix C – Search and Scan Results. Several results were found that, upon further investigation, could yield potential vulnerabilities:

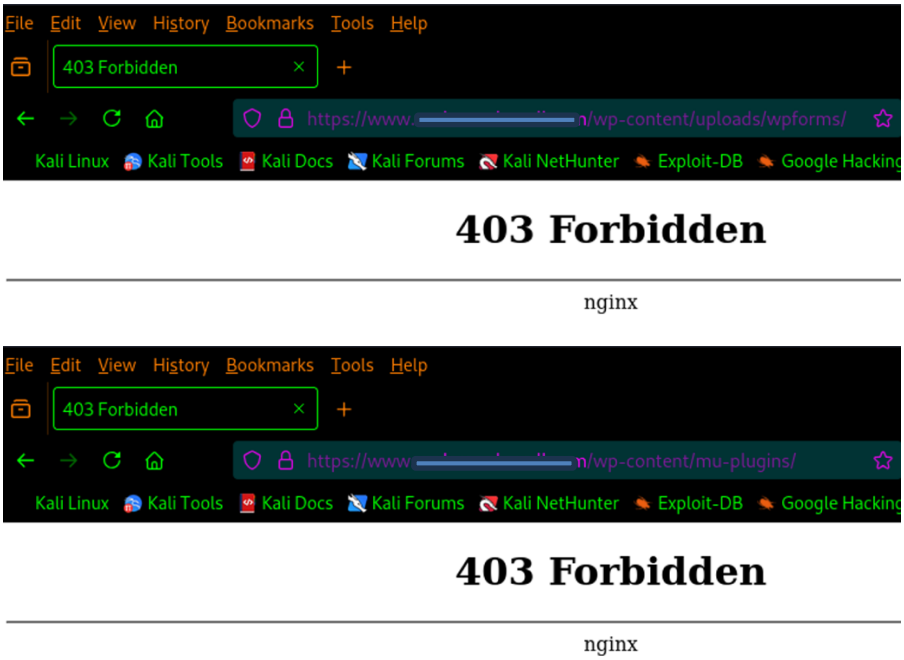
- Outdated WordPress version 6.6.2:
    - There could be known CVE's for outdated WordPress versions.
    - **Further investigation did not yield any known potential vulnerabilities for v6.6.2.**
- Outdated Divi theme version 4.27.1 (latest version is 4.27.3):
    - Unpatched flaws or weaknesses could lead to potential vulnerabilities.
    - **Further investigation did not yield any known potential vulnerabilities for v4.27.1.**

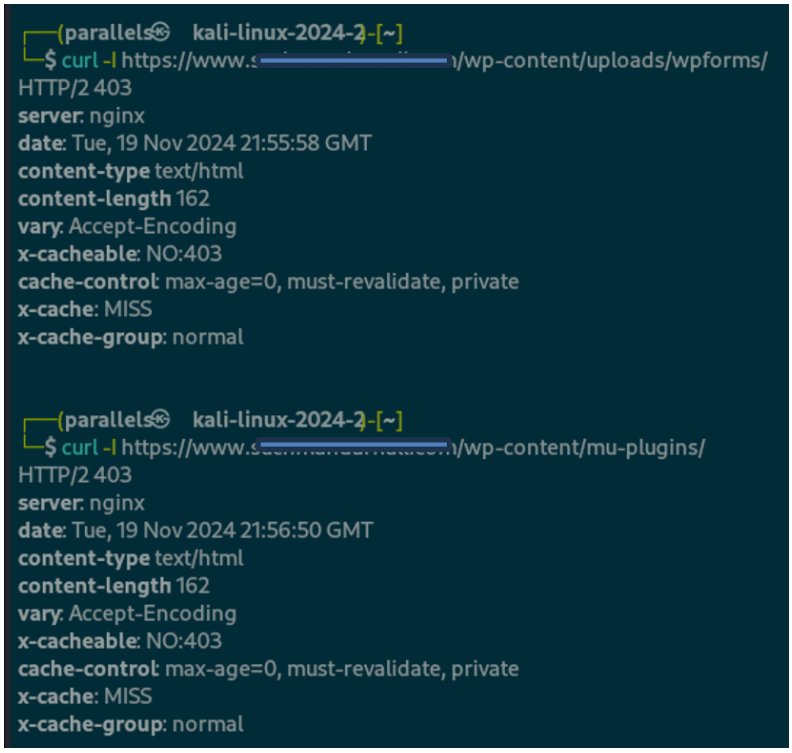


- Exposed Plugins and Sensitive Directories:
    - Unauthorized access could reveal sensitive information:
        - https://www.companywebsite.com/wp-content/uploads/wpforms/

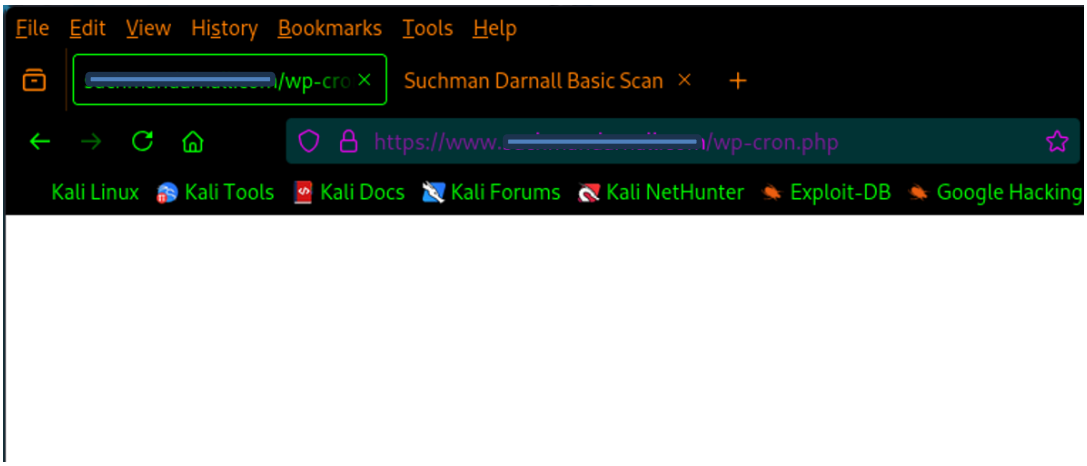
- https://www.companywebsite.com/wp-content/mu-plugins

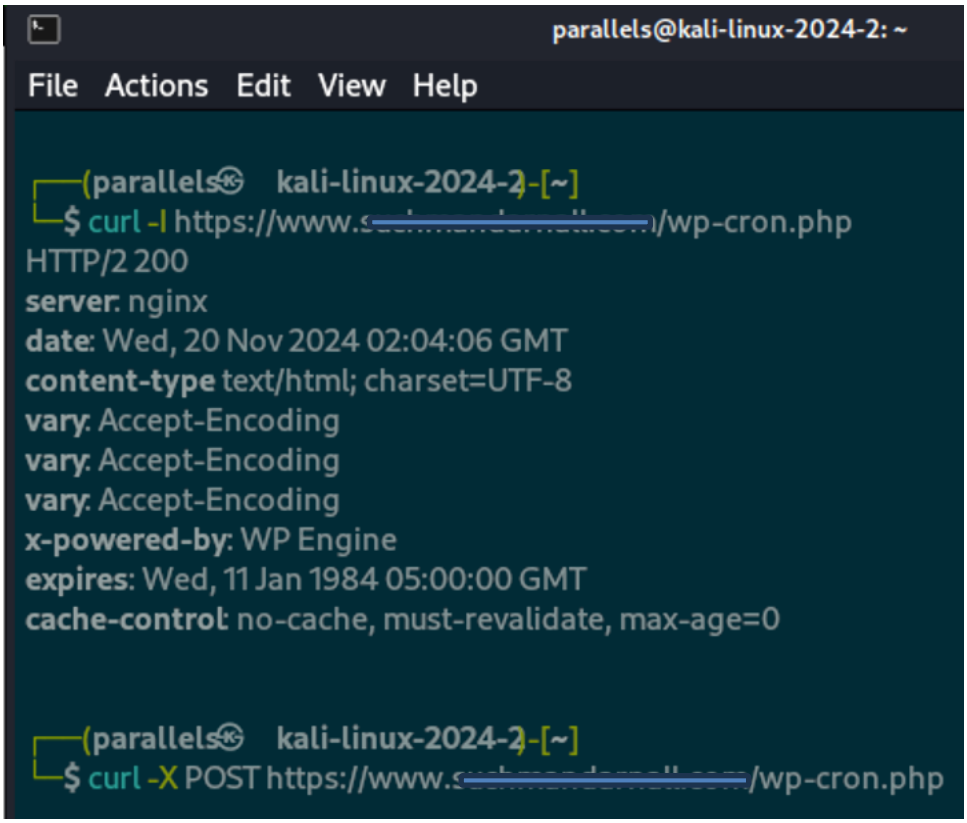
- **Further investigation showed that proper security measures are established to avoid access to these directories and a 403 message is returned:**





- Existence of external WP-Cron:
    - If misconfigured, this could be a potential vulnerability.
    - **Further investigation revealed appropriate behavior and no signs of misconfiguration. No information was provided.**





- XML-RPC Enabled:
    - The presence of xmlrpc.php file could be exploited by brute-force attacks or DDos amplification and pingback attacks. There are Metasploit modules specifically targeting this vulnerability:
        - The xmlrpc.php file is accessible and responds to POST requests, whereas GET requests have a 405 returned. This confirms that it enforces the correct method (POST) for XML-RPC communication.
        - There were a number of other available methods, listed below, that the endpoint supports (system.mulitcall, for instance), that a malicious actor could send batch API requests to in a single HTTP request. They could attempt to brute force logins, bypassing rate-limiting protections.
        - The pingback.ping method is enabled and could be abused to send repeated pingbacks to overwhelm the server in a Denial-of-Service attack.
        - The metaWeblog.newMediaObject method could be used to upload files (including web shell exploits). This could provide a foothold into the network.
    - The issue here is that even if a vulnerability was exploited, unless certain conditions are met, this would lead to gaining access to WP Engine or the web host company and not SD. To obtain access to SD's internal network, one of the following must be true:
        - WordPress integrates with SD internal systems (e.g. appointment scheduling, billing, patient records) → We know that appointment scheduling and billing and patient records are all hosted by third parties. Additionally, there is no evidence of API's or plugins that connect to an internal system. Without access to the server backend – which is outside the scope of this penetration test – I cannot determine whether there is integration and to what extent it may be vulnerable.
        - The hosting server is misconfigured or poorly secured → So far that has not been the case, in fact the web application security has been quite strong.
        - Backups or database dumps are exposed that could contain internal credentials or other PII. → Testing this condition is outside the scope of this penetration test.

Risk Rating

The overall risk identified to SD Company, D.D.S., P.C. as a result of the penetration test is low. No direct path from external attacker to full system compromise was discovered. It is reasonable to believe that a malicious entity would need to perform advanced exploits to be able to successfully execute an attack against SD through targeted attacks.

Appendix A: Resources

Tool/Utility Name	Purpose
Amass	Subdomain Enumeration
Crt.sh	Historical Data
Dig	Domain/IP Lookup
Dirb	Directory and File Enumeration
DNSEnum	Subdomain Enumeration
DNSRecon	Subdomain Enumeration
Enum4Linux	Subdomain Enumeration
ffuf	Directory and File Enumeration
Gobuster	Directory and File Enumeration
Harvest	Username, Email, and Social Media Enumeration
HaveIBeenPawnd	Username, Email, and Social Media Enumeration
HTS	
Hunter.io	Historical Data
IP.teoh.io	Domain/IP Lookup
IP2Location	Historical Data
KnowEm	Username, Email, and Social Media Enumeration
Maltego	Historical Data
Masscan	Service and Port Scanning
Metagoofil	Vulnerability Scanning
Namechk	Username, Email, and Social Media Enumeration
Netcraft	Service and Port Scanning

Nikto	Vulnerability Scanning
Nmap	Service and Port Scanning
NSLookup	Domain/IP Lookup
Open Corporates	Historical Data
OWASP ZAP	Service and Port Scanning
Recon-ng	Historical Data
Retire.js	Vulnerability Scanning
Security Trails	Historical Data
Sherlock	Username, Email, and Social Media Enumeration
Shodan	Historical Data
Site24x7	Historical Data
Social Engineering Toolkit (SET)	OSINT Scanning and Exploitation
SpiderFoot	Historical Data
SQLMap	Vulnerability Scanning
SSL Labs	Vulnerability Scanning
Subfinder	Subdomain Enumeration
Sublist3r	Subdomain Enumeration
Thats Them	Username, Email, and Social Media Enumeration
theHarvester	Username, Email, and Social Media Enumeration
Tree	Subdomain Enumeration
Trufflehog	Subdomain Enumeration
URLScan	Subdomain Enumeration
VirusTotal	Historical Data
Wafw00f	Web Application Firewall Detection

Wappalyzer	Website Technology Identification
WhatCMS	Website Technology Identification
WhatsMyName	Username, Email, and Social Media Enumeration
WhatWeb	Website Technology Identification
Whois ARIN	Domain/IP Lookup
Wig	Vulnerability Scanning
WPScan	CMS Enumeration
ZPhisher	Username, Email, and Social Media Enumeration

Appendix B: OSINT Data Collected - **REDACTED or BLANK**

Incorporation and Business Structure:

Main Company:	**SD Company, D.D.S., P.C.** **Status:** Active and in Good Standing **Founded**: **State of Incorporation**: **Type:** Privately Held **Headquarters Address:** **Number of Employees:** 11-50 **Website Domain:** https://www.companywebsite.com **Phone Number**: **Fax Number**: **General Email**: info@companyemaildental.com
Subsidiaries/Other Associations:	**SD Properties, LLC** **Status:** Active and in Good Standing **State of Incorporation:** **Type:** Privately Held Limited Liability Company **Headquarters Address:**
Executives and Employees:	**- Name → Founder, chief Dentist** **- Name → Founder, chief Dentist** **- Name → Dentist** **- Name → Dental Hygienist** **- Name → Dental Hygienist** **- Name → Dental Hygienist** **- Name → Dental Assistant** **- Name → Dental Assistant** **- Name → Dental Assistant** **- Name → Dental Assistant** **- Name → Dental Assistant** **- Name → Business Administration** **- Name → Business Administration** **- Name → Business Administration** **- Name → Business Administration**
Other Information:	**Public facing sites of interest, such as domains, websites, portals, etc:** They have the following social media accounts: - Facebook

	- Instagram - Linked-In - Pinterest - Twitch - Snapchat - Twitter ("X") - Youtube - Spotify - Github.com

System Architecture:

Domain Names:	https://www.companywebsite.com
IPv4 Address:	**IP Address (Cloudflare DNS server)**

NS Records:	- **ns49.domaincontrol.com**
	  ○ **IPv4: IP Address**
	  ○ **IPv6: IP Address**
	- **ns50.domaincontrol.com**
	  ○ **IPv4: IP Address**
	  ○ **IPv6: IP Address**

SOA Data:	**Start of Authority:** ns49.domaincontrol.com **Email:** dns@jomax.net **Serial:** 2020092202
Site Map:	**About Us: https://www.companywebsite.com/about-us/** **Contact Us: https://www.companywebsite.com/contact-us/** **FAQ & Gallery: https://www.companywebsite.com/faq-gallery/** **Home: https://www.companywebsite.com/** **Our Services: https://www.companywebsite.com/our-services/** **Our Services: https://www.companywebsite.com/our-services-2/** **Patient Center: https://www.companywebsite.com/patient-center/** **Sitemap: https://www.companywebsite.com/sitemap/** **TEST: https://www.companywebsite.com/test/**
Patient Portal – Existing:	**https://app.modento.io/company/sign-up** (redirected to Modento)

Patient Portal – New Patient Help	**https://www.companywebsite.com/patient-center/**
Online Scheduler – Existing:	**https://book.modento.io/company/patient-details** (redirected to Modento)
Online Scheduler – New:	**https://book.modento.io/company/patient-details** (redirected to Modento)
Pay My Bill:	**https://www.paymydentist.net/...** (handled by QuickBill Premium)
Review Page:	**https://reviews.nextadagency.com/company-160745320548396/review-us?dashboard=1** (redirected to NextAdAgency)
Review Page – Contact Form:	**https://reviews.nextadagency.com/company-160745320548396/review-us?dashboard=1** (redirected to NextAdAgency)

Appendix C: Scan and Search Results

REMOVED FOR CONFIDENTIALITY