Penetration Testing Report

Interstellar

SECURITY

https://interstellarsecurity.com

Report Prepared for:

Matt M.
CEO of Automattic

Report Prepared by:

Dean Sheldon
Senior Security Consultant
Interstellar Security
dsheldon@interstellarsecurity.com

Testing Completed by Interstellar Security

Table of Contents:

Introduction:

This penetration test was conducted by Interstellar Security.

Purpose:

Interstellar Security was asked to perform a detailed Black Box security examination on https://wordpress.org/ to see what information could be found from the outside. This Penetration testing effort took place on _____ and concluded on _____. Some preliminary findings were provided under separate cover, and this report is being presented to show the full results of our testing efforts and to make recommendations where appropriate.

Scope:

The scope of this examination is merely passive. No penetration test will be conducted. We will do recon on https://wordpress.org/ and find out anything we can. Information being searched for includes, but is not limited to, domain information, IP ranges, web server gaging, phone numbers, addresses, email addresses, outside information relating to the domain.

Project Outline:

The penetration testing work done in serval steps:

- Gathering information about the company, company employees, company contacts.
- Scanning technologies used by this company (Server information, Web Framework used, Architecture … etc).
- Mapping the network and performing DNS enumeration to get all subdomains. (Using tools like Nmap, something else, etc)

Reference Documents:

This network examination utilized multiple references for compliance and utilization purposes.

- Learn Kali Linux 2019 - Glen D. Singh
- Mastering Kali Linux for Web Penetration Testing - Michael McPhee
- Mastering Kali Linux for Advanced Penetration Testing – Vijay Kumar Velu

Disclaimer

This document is confidential and only for use by the company receiving this information. Interstellar Security is not responsible for the loss of misuse of this document. The information presented in this document is provided as is and without warranty. Vulnerability assessments

are a “point in time” analysis and as such it is possible that something in the environment could have changed since the tests reflected in this report were run. Also, it is possible that new vulnerabilities may have been discovered since the tests were run. For this reason, this report should be considered a guide, not a 100% representation of the risk threatening your systems, networks and applications.

Reconnaissance Narrative:

This section walks through all steps made investigating the target.

Information Gathering:

Multiple searches were conducted through search engines for user information.

Email Addresses:

Using hunter.io, we discovered a 131 email address exposed to the internet. (Link: https://hunter.io/search/wordpress.org)

Examples include:

- otto@wordpress.org
- siobhan@wordpress.org
- admin@wordpress.org
- user@wordpress.org
- security@wordpress.org

Domain Hunting:

Next we searched for information from the domain. Whois.com was used for the initial information hunting, then used securitytrails.com/dns-trails for server and DNS information.

Domain:
wordpress.org

Registrar:
MarkMonitor Inc.

Registered On:
2003-03-28

Expires On:
2022-03-28

Updated On:
2020-02-25

Status:
clientDeleteProhibited
clientTransferProhibited
clientUpdateProhibited

Name Servers:
ns1.wordpress.org
ns2.wordpress.org
ns3.wordpress.org
ns4.wordpress.org

DNS Information

Website is hosted by SingleHop LLC at 198.143.164.252. SingleHop LLC. is an IT hosting company and services provider based out of Chicago, Illinois, USA. The company has data centers in Chicago, Arizona, and the Netherlands. SingleHop provides bare metal dedicated servers, public and private clouds, as well as managed services to more than 4,000 clients in 114 countries.

A Record: 198.143.164.252

MX Record: 0 mail.wordpress.org

SOA Records: hostmaster.wordpress.org

NS Records:

Automattic, Inc

ns4.wordpress.org 25

ns3.wordpress.org 25

ns2.wordpress.org 26

ns1.wordpress.org 26

Based on this, we know wordpress.org is hosted by an outside company, SingleHop, and most likely is used exclusively used for their webhosting.

SingleHop LLC has a variety of IP addresses:

https://mxtoolbox.com/SuperTool.aspx?action=arin%3a198.143.164.252++&run=toolpage

NetRange: 198.143.128.0 - 198.143.191.255
CIDR: 198.143.128.0/18
NetName: SINGLEHOP
NetHandle: NET-198-143-128-0-1
Parent: NET198 (NET-198-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS32475
Organization: SingleHop LLC (SL-1370)
RegDate: 2012-05-16
Updated: 2018-02-27
Ref: https://rdap.arin.net/registry/ip/198.143.128.0

Passive Sniffing

Using NMAP, we scanned the server that was hosting wordpress.com's web server.

Host is up (0.033s latency).
Not shown: 997 filtered ports
PORT STATE SERVICE
53/tcp closed domain
80/tcp open http
443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 56.58 seconds

Server blocks Pings, preventing NMAP from scanning it with the -A flag.

AMAP did not identify any specific applications on each port.

Protocols

There were only three protocols exposed in the searches.

Protocol on 198.143.164.252:80/tcp matches http
Protocol on 198.143.164.252:443/tcp matches http
Protocol on 198.143.164.252:443/tcp matches ssl

Exposed Files

Via google, there are a number of files that are exposed to the internet.

Google Search: site:wordpress.org filetype:pdf

Using google, 84 pdf files were found, along with a number of other documents from around the site.

Subdomains

ns3.wordpress.org	192.0.74.10	nginx	PHP	WordPress	Domain Helper – Support
ns4.wordpress.org	192.0.75.10	nginx	PHP	WordPress	Domain Helper – Support
mail.wordpress.org	198.143.164.146				
wordpress.org	198.143.164.252	nginx	PHP		Blog Tool, Publishing Platform, and CMS — WordPress.org
ns1.wordpress.org	198.181.116.10	nginx	PHP	WordPress	Domain Helper – Support
ns2.wordpress.org	198.181.117.10	nginx	PHP	WordPress	Domain Helper – Support

Above is only as few subdomains.

Python tool sublist3r found 628 subdomains for wordpress.org

Webhosting Server:

Detailed information about the wordpress.org server and hosting application. In summary, it uses nginx web server

Status : 301 Moved Permanently
Title : 301 Moved Permanently
IP : 198.143.164.252
Country : UNITED STATES, US

Summary : HTTPServer[nginx], nginx, RedirectLocation[https://wordpress.org/]

Detected Plugins:
[HTTPServer]
HTTP server header string. This plugin also attempts to
identify the operating system from the server header.

String : nginx (from server string)

[RedirectLocation]

HTTP Server string location. used with http-status 301 and 302

String : https://wordpress.org/ (from location)

[nginx]
Nginx (Engine-X) is a free, open-source, high-performance HTTP server and reverse proxy, as well as an IMAP/POP3 proxy server.

Website : http://nginx.net/

HTTP Headers:
HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Thu, 24 Sep 2020 02:47:06 GMT
Content-Type: text/html
Content-Length: 162
Connection: close
Location: https://wordpress.org/

WhatWeb report for https://wordpress.org/
Status : 200 OK
Title : Blog Tool, Publishing Platform, and CMS — WordPress.org
IP : 198.143.164.252
Country : UNITED STATES, US

Summary : Open-Graph-Protocol[website], Script[application/ld+json,text/javascript], Frame, HTTPServer[nginx], HTML5, nginx, UncommonHeaders[x-olaf,x-nc], Strict-Transport-Security[max-age=360], JQuery, X-Frame-Options[SAMEORIGIN]

Detected Plugins:
[Frame]
This plugin detects instances of frame and iframe HTML elements.

[HTML5]
HTML version 5, detected by the doctype declaration

[HTTPServer]
HTTP server header string. This plugin also attempts to identify the operating system from the server header.

String : nginx (from server string)

[JQuery]
A fast, concise, JavaScript that simplifies how to traverse

HTML documents, handle events, perform animations, and add AJAX.

Website : http://jquery.com/

[Open-Graph-Protocol]
The Open Graph protocol enables you to integrate your Web pages into the social graph. It is currently designed for Web pages representing profiles of real-world things . things like movies, sports teams, celebrities, and restaurants. Including Open Graph tags on your Web page, makes your page equivalent to a Facebook Page.

Version : website

[Script]
This plugin detects instances of script HTML elements and returns the script language/type.

String : application/ld+json,text/javascript

[Strict-Transport-Security]
Strict-Transport-Security is an HTTP header that restricts a web browser from accessing a website without the security of the HTTPS protocol.

String : max-age=360

[UncommonHeaders]
Uncommon HTTP server headers. The blacklist includes all the standard headers and many non standard but common ones. Interesting but fairly common headers should have their own plugins, eg. x-powered-by, server and x-aspnet-version. Info about headers can be found at www.http-stats.com

String : x-olaf,x-nc (from headers)

[X-Frame-Options]
This plugin retrieves the X-Frame-Options value from the HTTP header. - More Info: http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.aspx

String : SAMEORIGIN

[nginx]
Nginx (Engine-X) is a free, open-source, high-performance

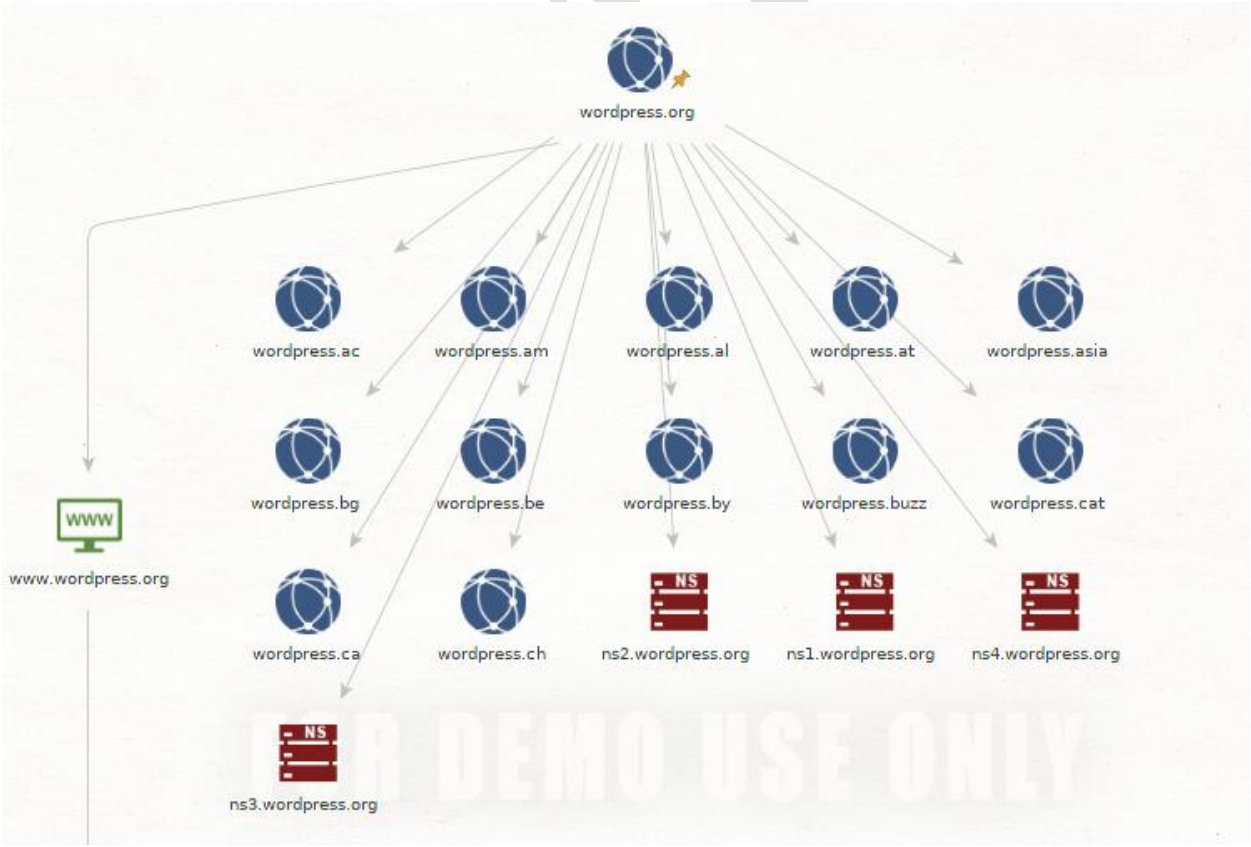
HTTP server and reverse proxy, as well as an IMAP/POP3 proxy server.

Website : http://nginx.net/

HTTP Headers:
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 24 Sep 2020 02:47:07 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
Vary: Accept-Encoding
Strict-Transport-Security: max-age=360

X-Olaf:
X-Frame-Options: SAMEORIGIN
X-nc: HIT ord 2
Content-Encoding: gzip

Domain Map:



Wordpress.org Map created with Maltego.

Conclusion:

Wordpress.org, without running any pentesting functions, seems to be isolated within the platform that they chose to host their website on. Most of their content is secured, and the information they want to have out in the internet isn't harmful.