Red Hawk

Target information

Domain
payvand.com

IP Address
144.208.67.248

Date
08/31/2021 10:59 a.m.

Shodan

Gathered information

Technology:

- IP: 144.208.67.248
- Service Provider: InMotion Hosting, Inc.
- Operating System: None

Ports

465
Info: 220-vps23791.inmotionhosting.com ESMTP Exim 4.93 #2 Mon, 30 Aug 2021 08:41:22 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail. 250-vps23791.inmotionhosting.com Hello 155.60.224.205 [155.60.224.205] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250 HELP

2087
Info: HTTP/1.1 301 Moved Content-length: 125 Location: https://vps23791.inmotionhosting.com:2087 Content-type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache <html><head><META HTTP-EQUIV="refresh" CONTENT="2;URL=https://vps23791.inmotionhosting.com:2087"></head><body></body></html>

443
Info: HTTP/1.1 200 OK Date: Mon, 30 Aug 2021 04:58:05 GMT Server: Apache Transfer-Encoding: chunked Content-Type: text/html

2083
Info: HTTP/1.1 200 OK Connection: close Content-Type: text/html; charset="utf-8" Date: Sun, 29 Aug 2021 23:44:04 GMT Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: cpsession=%3aEJdJqE1ePq_gkI6w%2cce623d0690d8f6b4d1b638efea996cac; HttpOnly; path=/; port=2083; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=144.208.67.248; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: Horde=expired; HttpOnly; domain=.144.208.67.248; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.144.208.67.248; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=2083; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: imp_key=expired; HttpOnly; domain=144.208.67.248; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: Horde=expired; HttpOnly; domain=.144.208.67.248; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.144.208.67.248; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083 Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 40718

3306
Info: \x04Host \'195.34.185.252\' is not allowed to connect to this MariaDB server

110
Info: +OK Dovecot ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE STLS USER SASL PLAIN LOGIN .

995
Info: +OK Dovecot ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE USER SASL PLAIN LOGIN .

21
Info: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220-You are user number 1 of 150 allowed. 220-Local time is now 18:04. Server port: 21. 220-This is a private system - No anonymous login 220-IPv6 connections are also welcome on this server. 220 You will be disconnected after 30 minutes of inactivity. 530 Login authentication failed 214-The following SITE commands are recognized ALIAS CHMOD IDLE UTIME 214 Pure-FTPd - http://pureftpd.org/ 211-Extensions supported: EPRT IDLE MDTM SIZE MFMT REST STREAM MLST

type*;size*;sizd*;modify*;UNIX.mode*;UNIX.uid*;UNIX.gid*;unique*; MLSD AUTH TLS PBSZ PROT UTF8 TVFS ESTA PASV EPSV SPSV ESTP 211 End.

2082
Info: HTTP/1.1 200 OK Connection: close Content-Type: text/html; charset="utf-8" Date: Tue, 17 Aug 2021 18:12:28 GMT Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082 Set-Cookie: cpsession=%3aa_TzkZkmRqrSd2Py%2c14d80a9e5c2e3e3205ca5f702f3f207d; HttpOnly; path=/; port=2082 Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082 Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=144.208.67.248; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082 Set-Cookie: Horde=expired; HttpOnly; domain=.144.208.67.248; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.144.208.67.248; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082 Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082 Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=2082 Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082 Set-Cookie: imp_key=expired; HttpOnly; domain=144.208.67.248; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082 Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 37674

587
Info: 220-vps23791.inmotionhosting.com ESMTP Exim 4.93 #2 Mon, 16 Aug 2021 18:04:22 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail. 250-vps23791.inmotionhosting.com Hello 134.39.128.79 [134.39.128.79] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP

143
Info: * OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ STARTTLS AUTH=PLAIN AUTH=LOGIN] Dovecot ready. * CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ STARTTLS AUTH=PLAIN AUTH=LOGIN A001 OK Pre-login capabilities listed, post-login capabilities have more. * ID ("name" "Dovecot") A002 OK ID completed. A003 BAD Error in IMAP command received by server. * BYE Logging out A004 OK Logout completed.

2086
Info: HTTP/1.1 200 OK Connection: close Content-Type: text/html; charset="utf-8" Date: Thu, 12 Aug 2021 14:11:28 GMT Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Set-Cookie: whostmgrrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086 Set-Cookie: whostmgrsession=%3a9RKytuLv19ybLDRq%2c0a88e46c889cfa87f008381296366b82; HttpOnly; path=/; port=2086 Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086 Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=144.208.67.248; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086 Set-Cookie: Horde=expired; HttpOnly; domain=.144.208.67.248; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.144.208.67.248; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086 Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086 Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=2086 Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086 Set-Cookie: imp_key=expired; HttpOnly; domain=144.208.67.248; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086 Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 37327

80
Info: HTTP/1.1 200 OK Date: Wed, 11 Aug 2021 16:56:12 GMT Server: Apache Transfer-Encoding: chunked Content-Type: text/html

993
Info: * OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ AUTH=PLAIN AUTH=LOGIN] Dovecot ready. * CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ AUTH=PLAIN AUTH=LOGIN A001 OK Pre-login capabilities listed, post-login capabilities have more. * ID ("name" "Dovecot") A002 OK ID completed. A003 BAD Error in IMAP command received by server. * BYE Logging out A004 OK Logout completed.

Vulnerabilities

The host which you are trying to scan seems to be no vulnerable in Shodan

Wapiti - Web Application Vulnerability Scanner

The host which you are trying to scan is unreachable, there is a WAF blocking the requests or you chose Discovery or CMS scanning mode

WPScan - WordPress Vulnerability Scanner

Gathered Information

It seems that host is reachable but it isn't running WordPress as CMS

CMSeek - CMS Scanner (Joomla)

Gathered information

ⓘ **It seems that host is reachable but it isn't running Joomla as CMS**