Nmap Scan Results:

```
# Nmap 7.94SVN scan initiated Thu May 16 17:44:28 2024 as: nmap -sV -oN nmap_scan.txt 143.244.222.116
Nmap scan report for 143.244.222.116
Host is up (0.20s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
23/tcp open telnet?
80/tcp open http OpenResty web app server 1.19.3.1
443/tcp open ssl/https?
8443/tcp open ssl/https-alt?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port23-TCP:V=7.94SVN%I=7%D=5/16%Time=6645F8B7%P=x86_64-pc-linux-gnu%r(N
SF:ULL,6,"Host:\x20")%r(GenericLines,27,"Host:\x20Couldn't\x20find\x20unde
SF:rlying\x20service\n")%r(tn3270,6,"Host:\x20")%r(GetRequest,27,"Host:\x2
SF:0Couldn't\x20find\x20underlying\x20service\n")%r(HTTPOptions,27,"Host:\
SF:x20Couldn't\x20find\x20underlying\x20service\n")%r(RTSPRequest,27,"Host
SF::\x20Couldn't\x20find\x20underlying\x20service\n")%r(RPCCheck,6,"Host:\
SF:x20")%r(DNSVersionBindReqTCP,6,"Host:\x20")%r(DNSStatusRequestTCP,6,"Ho
SF:st:\x20")%r(Help,27,"Host:\x20Couldn't\x20find\x20underlying\x20service
SF:\n")%r(SSLSessionReq,27,"Host:\x20Couldn't\x20find\x20underlying\x20ser
SF:vice\n")%r(TerminalServerCookie,27,"Host:\x20Couldn't\x20find\x20underl
SF:ying\x20service\n")%r(TLSSessionReq,27,"Host:\x20Couldn't\x20find\x20un
SF:derlying\x20service\n")%r(Kerberos,27,"Host:\x20Couldn't\x20find\x20und
SF:erlying\x20service\n")%r(SMBProgNeg,6,"Host:\x20")%r(X11Probe,6,"Host:\
SF:x20")%r(FourOhFourRequest,27,"Host:\x20Couldn't\x20find\x20underlying\x
SF:20service\n")%r(LPDString,27,"Host:\x20Couldn't\x20find\x20underlying\x
SF:20service\n")%r(LDAPSearchReq,27,"Host:\x20Couldn't\x20find\x20underlyi
SF:ng\x20service\n")%r(LDAPBindReq,6,"Host:\x20")%r(SIPOptions,27,"Host:\x
SF:20Couldn't\x20find\x20underlying\x20service\n")%r(LANDesk-RC,6,"Host:\x
SF:20")%r(TerminalServer,6,"Host:\x20")%r(NCP,6,"Host:\x20")%r(NotesRPC,6,
SF:"Host:\x20")%r(JavaRMI,6,"Host:\x20")%r(WMSRequest,6,"Host:\x20")%r(ora
SF:cle-tns,6,"Host:\x20")%r(ms-sql-s,6,"Host:\x20")%r(afp,6,"Host:\x20")%r
SF:(giop,6,"Host:\x20");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu May 16 17:46:25 2024 -- 1 IP address (1 host up) scanned in 117.33 seconds
```

WhoIs Results:

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#


NetRange: 143.244.128.0 - 143.244.255.255
CIDR: 143.244.128.0/17
NetName: DIGITALOCEAN-143-244-128-0
```

```
NetHandle: NET-143-244-128-0-1
Parent: NET143 (NET-143-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS14061
Organization: DigitalOcean, LLC (DO-13)
RegDate: 2020-01-09
Updated: 2020-04-03
Comment: Routing and Peering Policy can be found at https://www.as14061.net
Comment:
Comment: Please submit abuse reports at https://www.digitalocean.com/company/contact/#abuse
Ref: https://rdap.arin.net/registry/ip/143.244.128.0



OrgName: DigitalOcean, LLC
OrgId: DO-13
Address: 101 Ave of the Americas
Address: FL2
City: New York
StateProv: NY
PostalCode: 10013
Country: US
RegDate: 2012-05-14
Updated: 2023-10-23
Ref: https://rdap.arin.net/registry/entity/DO-13


OrgNOCHandle: NOC32014-ARIN
OrgNOCName: Network Operations Center
OrgNOCPhone: +1-347-875-6044
OrgNOCEmail: noc@digitalocean.com
OrgNOCRef: https://rdap.arin.net/registry/entity/NOC32014-ARIN

OrgTechHandle: NOC32014-ARIN
OrgTechName: Network Operations Center
OrgTechPhone: +1-347-875-6044
OrgTechEmail: noc@digitalocean.com
OrgTechRef: https://rdap.arin.net/registry/entity/NOC32014-ARIN

OrgAbuseHandle: ABUSE5232-ARIN
OrgAbuseName: Abuse, DigitalOcean
OrgAbusePhone: +1-347-875-6044
OrgAbuseEmail: abuse@digitalocean.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/ABUSE5232-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#
```

Dig Results:

```
; <<>> DiG 9.19.21-1-Debian <<>> 143.244.222.116
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 37323
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;143.244.222.116. IN A

;; AUTHORITY SECTION:
. 86375 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2024051600 1800 900 604800 86400

;; Query time: 4 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Thu May 16 17:46:26 IST 2024
;; MSG SIZE rcvd: 119
```

Nikto Scan Results:

```
- Nikto v2.5.0/
+ Target Host: hacktify-credential-conundrum.chals.io
+ Target Port: 443
+ GET /: Retrieved x-powered-by header: PHP/7.4.33.
+ GET /: The anti-clickjacking X-Frame-Options header is not present. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options:
+ GET /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security:
+ GET /: The X-Content-Type-Options header is not set. This could allow the user agent to render
the content of the site in a different fashion to the MIME type. See:
https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/:
+ GET Server is using a wildcard certificate: *.chals.io. See:
https://en.wikipedia.org/wiki/Wildcard_certificate:
```

SQLMap Scan Results:

WPScan Results:

```
__ ________ ______
\ \ / / __ \ / _____|
\ \ /\ / /| |__) | (___ ___ __ _ _ __ ®
\ \/ \/ / | ___/ \___ \ / __|/ _` | '_ \
\ /\ / | | _____) | (__| (_| | | | |
\/ \/ |_| |______/ \___|\__,_|_| |_|

WordPress Security Scanner by the WPScan Team
Version 3.8.25
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

Scan Aborted: The remote website is up, but does not seem to be running WordPress.

SSLScan Results:

```
Version: ■[32m2.1.3-static■[0m
OpenSSL 3.0.12 24 Oct 2023
■[0m
■[32mConnected to 143.244.222.116■[0m

Testing SSL server ■[32mhacktify-credential-conundrum.chals.io■[0m on port ■[32m443■[0m
using SNI name ■[32mhacktify-credential-conundrum.chals.io■[0m

■[1;34mSSL/TLS Protocols:■[0m
SSLv2 ■[32mdisabled■[0m
SSLv3 ■[32mdisabled■[0m
TLSv1.0 ■[32mdisabled■[0m
TLSv1.1 ■[32mdisabled■[0m
TLSv1.2 enabled
TLSv1.3 ■[33mdisabled■[0m

■[1;34mTLS Fallback SCSV:■[0m
Server ■[32msupports■[0m TLS Fallback SCSV

■[1;34mTLS renegotiation:■[0m
Session renegotiation ■[32mnot supported■[0m

■[1;34mTLS Compression:■[0m
Compression ■[32mdisabled■[0m

■[1;34mHeartbleed:■[0m
TLSv1.2 ■[32mnot vulnerable■[0m to heartbleed

■[1;34mSupported Server Cipher(s):■[0m
■[32mPreferred■[0m TLSv1.2 ■[32m256■[0m bits ■[32mECDHE-RSA-AES256-GCM-SHA384
■[0m Curve ■[32m25519■[0m DHE 253
Accepted TLSv1.2 ■[32m256■[0m bits ■[32mECDHE-RSA-CHACHA20-POLY1305 ■[0m Curve
■[32m25519■[0m DHE 253
Accepted TLSv1.2 ■[32m256■[0m bits ■[32mECDHE-ARIA256-GCM-SHA384 ■[0m Curve
■[32m25519■[0m DHE 253
Accepted TLSv1.2 ■[32m128■[0m bits ■[32mECDHE-RSA-AES128-GCM-SHA256 ■[0m Curve
■[32m25519■[0m DHE 253
Accepted TLSv1.2 ■[32m128■[0m bits ■[32mECDHE-ARIA128-GCM-SHA256 ■[0m Curve
■[32m25519■[0m DHE 253
Accepted TLSv1.2 ■[32m256■[0m bits ECDHE-RSA-AES256-SHA384 Curve ■[32m25519■[0m
DHE 253
Accepted TLSv1.2 ■[32m256■[0m bits ECDHE-RSA-CAMELLIA256-SHA384 Curve
■[32m25519■[0m DHE 253
Accepted TLSv1.2 ■[32m128■[0m bits ECDHE-RSA-AES128-SHA256 Curve ■[32m25519■[0m
DHE 253
Accepted TLSv1.2 ■[32m128■[0m bits ECDHE-RSA-CAMELLIA128-SHA256 Curve
■[32m25519■[0m DHE 253
Accepted TLSv1.2 ■[32m256■[0m bits ECDHE-RSA-AES256-SHA Curve ■[32m25519■[0m DHE
253
Accepted TLSv1.2 ■[32m128■[0m bits ECDHE-RSA-AES128-SHA Curve ■[32m25519■[0m DHE
253
```

```
Accepted TLSv1.2 ■[32m256■[0m bits AES256-GCM-SHA384
Accepted TLSv1.2 ■[32m256■[0m bits AES256-CCM8
Accepted TLSv1.2 ■[32m256■[0m bits AES256-CCM
Accepted TLSv1.2 ■[32m256■[0m bits ARIA256-GCM-SHA384
Accepted TLSv1.2 ■[32m128■[0m bits AES128-GCM-SHA256
Accepted TLSv1.2 ■[32m128■[0m bits AES128-CCM8
Accepted TLSv1.2 ■[32m128■[0m bits AES128-CCM
Accepted TLSv1.2 ■[32m128■[0m bits ARIA128-GCM-SHA256
Accepted TLSv1.2 ■[32m256■[0m bits AES256-SHA256
Accepted TLSv1.2 ■[32m256■[0m bits CAMELLIA256-SHA256
Accepted TLSv1.2 ■[32m128■[0m bits AES128-SHA256
Accepted TLSv1.2 ■[32m128■[0m bits CAMELLIA128-SHA256
Accepted TLSv1.2 ■[32m256■[0m bits AES256-SHA
Accepted TLSv1.2 ■[32m256■[0m bits CAMELLIA256-SHA
Accepted TLSv1.2 ■[32m128■[0m bits AES128-SHA
Accepted TLSv1.2 ■[32m128■[0m bits CAMELLIA128-SHA

■[1;34mServer Key Exchange Group(s):■[0m
TLSv1.2 ■[32m128■[0m bits secp256r1 (NIST P-256)■[0m
TLSv1.2 ■[32m192■[0m bits secp384r1 (NIST P-384)■[0m
TLSv1.2 ■[32m260■[0m bits secp521r1 (NIST P-521)■[0m
TLSv1.2 ■[32m128■[0m bits ■[32mx25519■[0m
TLSv1.2 ■[32m224■[0m bits ■[32mx448■[0m

■[1;34mSSL Certificate:■[0m
Signature Algorithm: ■[32msha256WithRSAEncryption■[0m
RSA Key Strength: ■[32m4096■[0m

Subject: *.chals.io
Altnames: DNS:*.chals.io, DNS:chals.io
Issuer: AlphaSSL CA - SHA256 - G4

Not valid before: ■[32mJun 11 20:49:16 2023 GMT■[0m
Not valid after: ■[32mJul 12 20:49:15 2024 GMT■[0m
```