Dear Team Security onebrick.io,

I checked for one brick.io API sandbox, one brick has how many domains like

<https://app.onebrick.io/user-access> (52.84.66.28)

<https://technical-docs.onebrick.io/docs/signup> (104.18.211.56)

<https://sandbox.onebrick.io/v1/auth/> (52.76.244.176)

we will check the sandbox vulnerability by doing the nmap command. here I found the open Kerberos ports, namely ports 88 and 749

└─$ nmap -sT 52.76.244.176

Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-16 02:25 EDT

Nmap scan report for ec2-52-76-244-176.ap-southeast-1.compute.amazonaws.com (52.76.244.176)

Host is up (0.020s latency).

PORT STATE SERVICE

1/tcp open tcpmux

3/tcp open compressnet

4/tcp open unknown

6/tcp open unknown

7/tcp open echo

9/tcp open discard

13/tcp open daytime

17/tcp open qotd

19/tcp open chargen

20/tcp open ftp-data

21/tcp open ftp

22/tcp open ssh

23/tcp open telnet

24/tcp open priv-mail

25/tcp filtered smtp

26/tcp open rsftp

30/tcp open unknown

32/tcp open unknown

33/tcp open dsp

37/tcp open time

42/tcp open nameserver

43/tcp open whois

49/tcp open tacacs

53/tcp open domain

70/tcp open gopher

79/tcp open finger

80/tcp open http

81/tcp open hosts2-ns

82/tcp open xfer

83/tcp open mit-ml-dev

84/tcp open ctf

85/tcp open mit-ml-dev

88/tcp open kerberos-sec

89/tcp open su-mit-tg

90/tcp open dnsix

99/tcp open metagram

100/tcp open newacct

106/tcp open pop3pw

109/tcp open pop2

110/tcp open pop3

111/tcp open rpcbind

113/tcp open ident

119/tcp open nntp

125/tcp open locus-map

135/tcp open msrpc

139/tcp open netbios-ssn

143/tcp open imap

144/tcp open news

146/tcp open iso-tp0

161/tcp open snmp

163/tcp open cmip-man

179/tcp open bgp

199/tcp open smux

211/tcp open 914c-g

212/tcp open anet

222/tcp open rsh-spx

254/tcp open unknown

255/tcp open unknown

256/tcp open fw1-secureremote

259/tcp open esro-gen

264/tcp open bgmp

280/tcp open http-mgmt

301/tcp open unknown

306/tcp open unknown

311/tcp open asip-webadmin

340/tcp open unknown

366/tcp open odmr

389/tcp open ldap

406/tcp open imsp

407/tcp open timbuktu

416/tcp open silverplatter

417/tcp open onmux

425/tcp open icad-el

427/tcp open svrloc

443/tcp open https

444/tcp open snpp

445/tcp open microsoft-ds

458/tcp open appleqtc

464/tcp open kpasswd5

465/tcp open smtps

481/tcp open dvs

497/tcp open retrospect

500/tcp open isakmp

512/tcp open exec

513/tcp open login

514/tcp open shell

515/tcp open printer

524/tcp open ncp

541/tcp open uucp-rlogin

543/tcp open klogin

544/tcp open kshell

545/tcp open ekshell

548/tcp open afp

554/tcp open rtsp

555/tcp open dsf

563/tcp open snews

587/tcp open submission

593/tcp open http-rpc-epmap

616/tcp open sco-sysmgr

617/tcp open sco-dtmgr

625/tcp open apple-xsrvr-admin

631/tcp open ipp

636/tcp open ldapssl

646/tcp open ldp

648/tcp open rrp

666/tcp open doom

667/tcp open disclose

668/tcp open mecomm

683/tcp open corba-iiop

687/tcp open asipregistry

691/tcp open resvc

700/tcp open epp

705/tcp open agentx

711/tcp open cisco-tdp

714/tcp open iris-xpcs

720/tcp open unknown

722/tcp open unknown

726/tcp open unknown

749/tcp open kerberos-adm

765/tcp open webster

777/tcp open multiling-http

783/tcp open spamassassin

787/tcp open qsc

800/tcp open mdbs\_daemon

801/tcp open device

808/tcp open ccproxy-http

843/tcp open unknown

873/tcp open rsync

880/tcp open unknown

888/tcp open accessbuilder

898/tcp open sun-manageconsole

900/tcp open omginitialrefs

901/tcp open samba-swat

902/tcp open iss-realsecure

903/tcp open iss-console-mgr

911/tcp open xact-backup

912/tcp open apex-mesh

981/tcp open unknown

987/tcp open unknown

990/tcp open ftps

992/tcp open telnets

993/tcp open imaps

995/tcp open pop3s

999/tcp open garcon

1000/tcp open cadlock

1001/tcp open webpush

1002/tcp open windows-icfw

1007/tcp open unknown

1009/tcp open unknown

1010/tcp open surf

1011/tcp open unknown

1021/tcp open exp1

1022/tcp open exp2

1023/tcp open netvenuechat

1024/tcp open kdm

1025/tcp open NFS-or-IIS

1026/tcp open LSA-or-nterm

1027/tcp open IIS

1028/tcp open unknown

1029/tcp open ms-lsa

1030/tcp open iad1

1031/tcp open iad2

1032/tcp open iad3

1033/tcp open netinfo

1034/tcp open zincite-a

1035/tcp open multidropper

1036/tcp open nsstp

1037/tcp open ams

1038/tcp open mtqp

1039/tcp open sbl

1040/tcp open netsaint

1041/tcp open danf-ak2

1042/tcp open afrog

1043/tcp open boinc

1044/tcp open dcutility

1045/tcp open fpitp

1046/tcp open wfremotertm

1047/tcp open neod1

1048/tcp open neod2

1049/tcp open td-postman

1050/tcp open java-or-OTGfileshare

1051/tcp open optima-vnet

1052/tcp open ddt

1053/tcp open remote-as

1054/tcp open brvread

1055/tcp open ansyslmd

1056/tcp open vfo

1057/tcp open startron

1058/tcp open nim

1059/tcp open nimreg

1060/tcp open polestar

1061/tcp open kiosk

1062/tcp open veracity

1063/tcp open kyoceranetdev

1064/tcp open jstel

1065/tcp open syscomlan

1066/tcp open fpo-fns

1067/tcp open instl\_boots

1068/tcp open instl\_bootc

1069/tcp open cognex-insight

1070/tcp open gmrupdateserv

1071/tcp open bsquare-voip

1072/tcp open cardax

1073/tcp open bridgecontrol

1074/tcp open warmspotMgmt

1075/tcp open rdrmshc

1076/tcp open sns\_credit

1077/tcp open imgames

1078/tcp open avocent-proxy

1079/tcp open asprovatalk

1080/tcp open socks

1081/tcp open pvuniwien

1082/tcp open amt-esd-prot

1083/tcp open ansoft-lm-1

1084/tcp open ansoft-lm-2

1085/tcp open webobjects

1086/tcp open cplscrambler-lg

1087/tcp open cplscrambler-in

1088/tcp open cplscrambler-al

1089/tcp open ff-annunc

1090/tcp open ff-fms

1091/tcp open ff-sm

1092/tcp open obrpd

1093/tcp open proofd

1094/tcp open rootd

1095/tcp open nicelink

1096/tcp open cnrprotocol

1097/tcp open sunclustermgr

1098/tcp open rmiactivation

1099/tcp open rmiregistry

1100/tcp open mctp

1102/tcp open adobeserver-1

1104/tcp open xrl

1105/tcp open ftranhc

1106/tcp open isoipsigport-1

1107/tcp open isoipsigport-2

1108/tcp open ratio-adp

1110/tcp open nfsd-status

1111/tcp open lmsocialserver

1112/tcp open msql

1113/tcp open ltp-deepspace

1114/tcp open mini-sql

1117/tcp open ardus-mtrns

1119/tcp open bnetgame

1121/tcp open rmpp

1122/tcp open availant-mgr

1123/tcp open murray

1124/tcp open hpvmmcontrol

1126/tcp open hpvmmdata

1130/tcp open casp

1131/tcp open caspssl

1132/tcp open kvm-via-ip

1137/tcp open trim

1138/tcp open encrypted\_admin

1141/tcp open mxomss

1145/tcp open x9-icue

1147/tcp open capioverlan

1148/tcp open elfiq-repl

1149/tcp open bvtsonar

1151/tcp open unizensus

1152/tcp open winpoplanmess

1154/tcp open resacommunity

1163/tcp open sddp

1164/tcp open qsm-proxy

1165/tcp open qsm-gui

1166/tcp open qsm-remote

1169/tcp open tripwire

1174/tcp open fnet-remote-ui

1175/tcp open dossier

1183/tcp open llsurfup-http

1185/tcp open catchpole

1186/tcp open mysql-cluster

1187/tcp open alias

1192/tcp open caids-sensor

1198/tcp open cajo-discovery

1199/tcp open dmidi

1201/tcp open nucleus-sand

1213/tcp open mpc-lifenet

1216/tcp open etebac5

1217/tcp open hpss-ndapi

1218/tcp open aeroflight-ads

1233/tcp open univ-appserver

1234/tcp open hotline

1236/tcp open bvcontrol

1244/tcp open isbconference1

1247/tcp open visionpyramid

1248/tcp open hermes

1259/tcp open opennl-voice

1271/tcp open excw

1272/tcp open cspmlockmgr

1277/tcp open miva-mqs

1287/tcp open routematch

1296/tcp open dproxy

1300/tcp open h323hostcallsc

1301/tcp open ci3-software-1

1309/tcp open jtag-server

1310/tcp open husky

1311/tcp open rxmon

1322/tcp open novation

1328/tcp open ewall

1334/tcp open writesrv

1352/tcp open lotusnotes

1417/tcp open timbuktu-srv1

1433/tcp open ms-sql-s

1434/tcp open ms-sql-m

1443/tcp open ies-lm

1455/tcp open esl-lm

1461/tcp open ibm\_wrless\_lan

1494/tcp open citrix-ica

1500/tcp open vlsi-lm

1501/tcp open sas-3

1503/tcp open imtc-mcs

1521/tcp open oracle

1524/tcp open ingreslock

1533/tcp open virtual-places

1556/tcp open veritas\_pbx

1580/tcp open tn-tl-r1

1583/tcp open simbaexpress

1594/tcp open sixtrak

1600/tcp open issd

1641/tcp open invision

1658/tcp open sixnetudr

1666/tcp open netview-aix-6

1687/tcp open nsjtp-ctrl

1688/tcp open nsjtp-data

1700/tcp open mps-raft

1717/tcp open fj-hdnet

1718/tcp open h323gatedisc

1719/tcp open h323gatestat

1720/tcp open h323q931

1721/tcp open caicci

1723/tcp open pptp

1755/tcp open wms

1761/tcp open landesk-rc

1782/tcp open hp-hcip

1783/tcp open unknown

1801/tcp open msmq

1805/tcp open enl-name

1812/tcp open radius

1839/tcp open netopia-vo1

1840/tcp open netopia-vo2

1862/tcp open mysql-cm-agent

1863/tcp open msnp

1864/tcp open paradym-31

1875/tcp open westell-stats

1900/tcp open upnp

1914/tcp open elm-momentum

1935/tcp open rtmp

1947/tcp open sentinelsrm

1971/tcp open netop-school

1972/tcp open intersys-cache

1974/tcp open drp

1984/tcp open bigbrother

1998/tcp open x25-svc-port

1999/tcp open tcp-id-port

2000/tcp open cisco-sccp

2001/tcp open dc

2002/tcp open globe

2003/tcp open finger

2004/tcp open mailbox

2005/tcp open deslogin

2006/tcp open invokator

2007/tcp open dectalk

2008/tcp open conf

2009/tcp open news

2010/tcp open search

2013/tcp open raid-am

2020/tcp open xinupageserver

2021/tcp open servexec

2022/tcp open down

2030/tcp open device2

2033/tcp open glogger

2034/tcp open scoremgr

2035/tcp open imsldoc

2038/tcp open objectmanager

2040/tcp open lam

2041/tcp open interbase

2042/tcp open isis

2043/tcp open isis-bcast

2045/tcp open cdfunc

2046/tcp open sdfunc

2047/tcp open dls

2048/tcp open dls-monitor

2049/tcp open nfs

2065/tcp open dlsrpn

2068/tcp open avocentkvm

2099/tcp open h2250-annex-g

2100/tcp open amiganetfs

2103/tcp open zephyr-clt

2105/tcp open eklogin

2106/tcp open ekshell

2107/tcp open msmq-mgmt

2111/tcp open kx

2119/tcp open gsigatekeeper

2121/tcp open ccproxy-ftp

2126/tcp open pktcable-cops

2135/tcp open gris

2144/tcp open lv-ffx

2160/tcp open apc-2160

2161/tcp open apc-agent

2170/tcp open eyetv

2179/tcp open vmrdp

2190/tcp open tivoconnect

2191/tcp open tvbus

2196/tcp open unknown

2200/tcp open ici

2222/tcp open EtherNetIP-1

2251/tcp open dif-port

2260/tcp open apc-2260

2288/tcp open netml

2301/tcp open compaqdiag

2323/tcp open 3d-nfsd

2366/tcp open qip-login

2381/tcp open compaq-https

2382/tcp open ms-olap3

2383/tcp open ms-olap4

2393/tcp open ms-olap1

2394/tcp open ms-olap2

2399/tcp open fmpro-fdal

2401/tcp open cvspserver

2492/tcp open groove

2500/tcp open rtsserv

2522/tcp open windb

2525/tcp open ms-v-worlds

2557/tcp open nicetec-mgmt

2601/tcp open zebra

2602/tcp open ripd

2604/tcp open ospfd

2605/tcp open bgpd

2607/tcp open connection

2608/tcp open wag-service

2638/tcp open sybase

2701/tcp open sms-rcinfo

2702/tcp open sms-xfer

2710/tcp open sso-service

2717/tcp open pn-requester

2718/tcp open pn-requester2

2725/tcp open msolap-ptp2

2800/tcp open acc-raid

2809/tcp open corbaloc

2811/tcp open gsiftp

2869/tcp open icslap

2875/tcp open dxmessagebase2

2909/tcp open funk-dialout

2910/tcp open tdaccess

2920/tcp open roboeda

2967/tcp open symantec-av

2968/tcp open enpp

2998/tcp open iss-realsec

3000/tcp open ppp

3001/tcp open nessus

3003/tcp open cgms

3005/tcp open deslogin

3006/tcp open deslogind

3007/tcp open lotusmtap

3011/tcp open trusted-web

3013/tcp open gilatskysurfer

3017/tcp open event\_listener

3030/tcp open arepa-cas

3031/tcp open eppc

3052/tcp open powerchute

3071/tcp open csd-mgmt-port

3077/tcp open orbix-loc-ssl

3128/tcp open squid-http

3168/tcp open poweronnud

3211/tcp open avsecuremgmt

3221/tcp open xnm-clear-text

3260/tcp open iscsi

3261/tcp open winshadow

3268/tcp open globalcatLDAP

3269/tcp open globalcatLDAPssl

3283/tcp open netassistant

3300/tcp open ceph

3301/tcp open unknown

3306/tcp open mysql

3322/tcp open active-net

3323/tcp open active-net

3324/tcp open active-net

3325/tcp open active-net

3333/tcp open dec-notes

3351/tcp open btrieve

3367/tcp open satvid-datalnk

3369/tcp open satvid-datalnk

3370/tcp open satvid-datalnk

3371/tcp open satvid-datalnk

3372/tcp open msdtc

3389/tcp open ms-wbt-server

3390/tcp open dsc

3404/tcp open unknown

3476/tcp open nppmp

3493/tcp open nut

3517/tcp open 802-11-iapp

3527/tcp open beserver-msg-q

3546/tcp open unknown

3551/tcp open apcupsd

3580/tcp open nati-svrloc

3659/tcp open apple-sasl

3689/tcp open rendezvous

3690/tcp open svn

3703/tcp open adobeserver-3

3737/tcp open xpanel

3766/tcp open sitewatch-s

3784/tcp open bfd-control

3800/tcp open pwgpsi

3801/tcp open ibm-mgr

3809/tcp open apocd

3814/tcp open neto-dcs

3826/tcp open wormux

3827/tcp open netmpi

3828/tcp open neteh

3851/tcp open spectraport

3869/tcp open ovsam-mgmt

3871/tcp open avocent-adsap

3878/tcp open fotogcad

3880/tcp open igrs

3889/tcp open dandv-tester

3905/tcp open mupdate

3914/tcp open listcrt-port-2

3918/tcp open pktcablemmcops

3920/tcp open exasoftport1

3945/tcp open emcads

3971/tcp open lanrevserver

3986/tcp open mapper-ws\_ethd

3995/tcp open iss-mgmt-ssl

3998/tcp open dnx

4000/tcp open remoteanything

4001/tcp open newoak

4002/tcp open mlchat-proxy

4003/tcp open pxc-splr-ft

4004/tcp open pxc-roid

4005/tcp open pxc-pin

4006/tcp open pxc-spvr

4045/tcp open lockd

4111/tcp open xgrid

4125/tcp open rww

4126/tcp open ddrepl

4129/tcp open nuauth

4224/tcp open xtell

4242/tcp open vrml-multi-use

4279/tcp open vrml-multi-use

4321/tcp open rwhois

4343/tcp open unicall

4443/tcp open pharos

4444/tcp open krb524

4445/tcp open upnotifyp

4446/tcp open n1-fwp

4449/tcp open privatewire

4550/tcp open gds-adppiw-db

4567/tcp open tram

4662/tcp open edonkey

4848/tcp open appserv-http

4899/tcp open radmin

4900/tcp open hfcs

4998/tcp open maybe-veritas

5000/tcp open upnp

5001/tcp open commplex-link

5002/tcp open rfe

5003/tcp open filemaker

5004/tcp open avt-profile-1

5009/tcp open airport-admin

5030/tcp open surfpass

5033/tcp open jtnetd-server

5050/tcp open mmcc

5051/tcp open ida-agent

5054/tcp open rlm-admin

5060/tcp open sip

5061/tcp open sip-tls

5080/tcp open onscreen

5087/tcp open biotic

5100/tcp open admd

5101/tcp open admdog

5102/tcp open admeng

5120/tcp open barracuda-bbs

5190/tcp open aol

5200/tcp open targus-getdata

5214/tcp open unknown

5221/tcp open 3exmp

5222/tcp open xmpp-client

5225/tcp open hp-server

5226/tcp open hp-status

5269/tcp open xmpp-server

5280/tcp open xmpp-bosh

5298/tcp open presence

5357/tcp open wsdapi

5405/tcp open pcduo

5414/tcp open statusd

5431/tcp open park-agent

5432/tcp open postgresql

5440/tcp open unknown

5500/tcp open hotline

5510/tcp open secureidprop

5544/tcp open unknown

5550/tcp open sdadmind

5555/tcp open freeciv

5560/tcp open isqlplus

5566/tcp open westec-connect

5631/tcp open pcanywheredata

5633/tcp open beorl

5666/tcp open nrpe

5678/tcp open rrac

5679/tcp open activesync

5718/tcp open dpm

5730/tcp open unieng

5800/tcp open vnc-http

5801/tcp open vnc-http-1

5802/tcp open vnc-http-2

5810/tcp open unknown

5811/tcp open unknown

5815/tcp open unknown

5822/tcp open unknown

5825/tcp open unknown

5850/tcp open unknown

5859/tcp open wherehoo

5862/tcp open unknown

5877/tcp open unknown

5900/tcp open vnc

5901/tcp open vnc-1

5902/tcp open vnc-2

5903/tcp open vnc-3

5904/tcp open unknown

5906/tcp open unknown

5907/tcp open unknown

5910/tcp open cm

5911/tcp open cpdlc

5915/tcp open unknown

5922/tcp open unknown

5925/tcp open unknown

5950/tcp open unknown

5952/tcp open unknown

5959/tcp open unknown

5960/tcp open unknown

5961/tcp open unknown

5962/tcp open unknown

5963/tcp open indy

5987/tcp open wbem-rmi

5988/tcp open wbem-http

5989/tcp open wbem-https

5998/tcp open ncd-diag

5999/tcp open ncd-conf

6000/tcp open X11

6001/tcp open X11:1

6002/tcp open X11:2

6003/tcp open X11:3

6004/tcp open X11:4

6005/tcp open X11:5

6006/tcp open X11:6

6007/tcp open X11:7

6009/tcp open X11:9

6025/tcp open x11

6059/tcp open X11:59

6100/tcp open synchronet-db

6101/tcp open backupexec

6106/tcp open isdninfo

6112/tcp open dtspc

6123/tcp open backup-express

6129/tcp open unknown

6156/tcp open unknown

6346/tcp open gnutella

6389/tcp open clariion-evr01

6502/tcp open netop-rc

6510/tcp open mcer-port

6543/tcp open mythtv

6547/tcp open powerchuteplus

6565/tcp open unknown

6566/tcp open sane-port

6567/tcp open esp

6580/tcp open parsec-master

6646/tcp open unknown

6666/tcp open irc

6667/tcp open irc

6668/tcp open irc

6669/tcp open irc

6689/tcp open tsa

6692/tcp open unknown

6699/tcp open napster

6779/tcp open unknown

6788/tcp open smc-http

6789/tcp open ibm-db2-admin

6792/tcp open unknown

6839/tcp open unknown

6881/tcp open bittorrent-tracker

6901/tcp open jetstream

6969/tcp open acmsoda

7000/tcp open afs3-fileserver

7001/tcp open afs3-callback

7002/tcp open afs3-prserver

7004/tcp open afs3-kaserver

7007/tcp open afs3-bos

7019/tcp open doceri-ctl

7025/tcp open vmsvc-2

7070/tcp open realserver

7100/tcp open font-service

7103/tcp open unknown

7106/tcp open unknown

7200/tcp open fodms

7201/tcp open dlip

7402/tcp open rtps-dd-mt

7435/tcp open unknown

7443/tcp open oracleas-https

7496/tcp open unknown

7512/tcp open unknown

7625/tcp open unknown

7627/tcp open soap-http

7676/tcp open imqbrokerd

7741/tcp open scriptview

7777/tcp open cbt

7778/tcp open interwise

7800/tcp open asr

7911/tcp open unknown

7920/tcp open unknown

7921/tcp open unknown

7937/tcp open nsrexecd

7938/tcp open lgtomapper

7999/tcp open irdmi2

8000/tcp open http-alt

8001/tcp open vcom-tunnel

8002/tcp open teradataordbms

8007/tcp open ajp12

8008/tcp open http

8009/tcp open ajp13

8010/tcp open xmpp

8011/tcp open unknown

8021/tcp open ftp-proxy

8022/tcp open oa-system

8031/tcp open unknown

8042/tcp open fs-agent

8045/tcp open unknown

8080/tcp open http-proxy

8081/tcp open blackice-icecap

8082/tcp open blackice-alerts

8083/tcp open us-srv

8084/tcp open websnp

8085/tcp open unknown

8086/tcp open d-s-n

8087/tcp open simplifymedia

8088/tcp open radan-http

8089/tcp open unknown

8090/tcp open opsmessaging

8093/tcp open unknown

8099/tcp open unknown

8100/tcp open xprint-server

8180/tcp open unknown

8181/tcp open intermapper

8192/tcp open sophos

8193/tcp open sophos

8194/tcp open sophos

8200/tcp open trivnet1

8222/tcp open unknown

8254/tcp open unknown

8290/tcp open unknown

8291/tcp open unknown

8292/tcp open blp3

8300/tcp open tmi

8333/tcp open bitcoin

8383/tcp open m2mservices

8400/tcp open cvd

8402/tcp open abarsd

8443/tcp open https-alt

8500/tcp open fmtp

8600/tcp open asterix

8649/tcp open unknown

8651/tcp open unknown

8652/tcp open unknown

8654/tcp open unknown

8701/tcp open unknown

8800/tcp open sunwebadmin

8873/tcp open dxspider

8888/tcp open sun-answerbook

8899/tcp open ospf-lite

8994/tcp open unknown

9000/tcp open cslistener

9001/tcp open tor-orport

9002/tcp open dynamid

9003/tcp open unknown

9009/tcp open pichat

9010/tcp open sdr

9011/tcp open d-star

9040/tcp open tor-trans

9050/tcp open tor-socks

9071/tcp open unknown

9080/tcp open glrpc

9081/tcp open cisco-aqos

9090/tcp open zeus-admin

9091/tcp open xmltec-xmlmail

9099/tcp open unknown

9100/tcp open jetdirect

9101/tcp open jetdirect

9102/tcp open jetdirect

9103/tcp open jetdirect

9110/tcp open unknown

9111/tcp open DragonIDSConsole

9200/tcp open wap-wsp

9207/tcp open wap-vcal-s

9220/tcp open unknown

9290/tcp open unknown

9415/tcp open unknown

9418/tcp open git

9485/tcp open unknown

9500/tcp open ismserver

9502/tcp open unknown

9503/tcp open unknown

9535/tcp open man

9575/tcp open unknown

9593/tcp open cba8

9594/tcp open msgsys

9595/tcp open pds

9618/tcp open condor

9666/tcp open zoomcp

9876/tcp open sd

9877/tcp open x510

9878/tcp open kca-service

9898/tcp open monkeycom

9900/tcp open iua

9917/tcp open unknown

9929/tcp open nping-echo

9943/tcp open unknown

9944/tcp open unknown

9968/tcp open unknown

9998/tcp open distinct32

9999/tcp open abyss

10000/tcp open snet-sensor-mgmt

10001/tcp open scp-config

10002/tcp open documentum

10003/tcp open documentum\_s

10004/tcp open emcrmirccd

10009/tcp open swdtp-sv

10010/tcp open rxapi

10012/tcp open unknown

10024/tcp open unknown

10025/tcp open unknown

10082/tcp open amandaidx

10180/tcp open unknown

10215/tcp open unknown

10243/tcp open unknown

10566/tcp open unknown

10616/tcp open unknown

10617/tcp open unknown

10621/tcp open unknown

10626/tcp open unknown

10628/tcp open unknown

10629/tcp open unknown

10778/tcp open unknown

11110/tcp open sgi-soap

11111/tcp open vce

11967/tcp open sysinfo-sp

12000/tcp open cce4x

12174/tcp open unknown

12265/tcp open unknown

12345/tcp open netbus

13456/tcp open unknown

13722/tcp open netbackup

13782/tcp open netbackup

13783/tcp open netbackup

14000/tcp open scotty-ft

14238/tcp open unknown

14441/tcp open unknown

14442/tcp open unknown

15000/tcp open hydap

15002/tcp open onep-tls

15003/tcp open unknown

15004/tcp open unknown

15660/tcp open bex-xr

15742/tcp open unknown

16000/tcp open fmsas

16001/tcp open fmsascon

16012/tcp open unknown

16016/tcp open unknown

16018/tcp open unknown

16080/tcp open osxwebadmin

16113/tcp open unknown

16992/tcp open amt-soap-http

16993/tcp open amt-soap-https

17877/tcp open unknown

17988/tcp open unknown

18040/tcp open unknown

18101/tcp open unknown

18988/tcp open unknown

19101/tcp open unknown

19283/tcp open keysrvr

19315/tcp open keyshadow

19350/tcp open unknown

19780/tcp open unknown

19801/tcp open unknown

19842/tcp open unknown

20000/tcp open dnp

20005/tcp open btx

20031/tcp open unknown

20221/tcp open unknown

20222/tcp open ipulse-ics

20828/tcp open unknown

21571/tcp open unknown

22939/tcp open unknown

23502/tcp open unknown

24444/tcp open unknown

24800/tcp open unknown

25734/tcp open unknown

25735/tcp open unknown

26214/tcp open unknown

27000/tcp open flexlm0

27352/tcp open unknown

27353/tcp open unknown

27355/tcp open unknown

27356/tcp open unknown

27715/tcp open unknown

28201/tcp open unknown

30000/tcp open ndmps

30718/tcp open unknown

30951/tcp open unknown

31038/tcp open unknown

31337/tcp open Elite

32768/tcp open filenet-tms

32769/tcp open filenet-rpc

32770/tcp open sometimes-rpc3

32771/tcp open sometimes-rpc5

32772/tcp open sometimes-rpc7

32773/tcp open sometimes-rpc9

32774/tcp open sometimes-rpc11

32775/tcp open sometimes-rpc13

32776/tcp open sometimes-rpc15

32777/tcp open sometimes-rpc17

32778/tcp open sometimes-rpc19

32779/tcp open sometimes-rpc21

32780/tcp open sometimes-rpc23

32781/tcp open unknown

32782/tcp open unknown

32783/tcp open unknown

32784/tcp open unknown

32785/tcp open unknown

33354/tcp open unknown

33899/tcp open unknown

34571/tcp open unknown

34572/tcp open unknown

34573/tcp open unknown

35500/tcp open unknown

38292/tcp open landesk-cba

40193/tcp open unknown

40911/tcp open unknown

41511/tcp open unknown

42510/tcp open caerpc

44176/tcp open unknown

44442/tcp open coldfusion-auth

44443/tcp open coldfusion-auth

44501/tcp open unknown

45100/tcp open unknown

48080/tcp open unknown

49152/tcp open unknown

49153/tcp open unknown

49154/tcp open unknown

49155/tcp open unknown

49156/tcp open unknown

49157/tcp open unknown

49158/tcp open unknown

49159/tcp open unknown

49160/tcp open unknown

49161/tcp open unknown

49163/tcp open unknown

49165/tcp open unknown

49167/tcp open unknown

49175/tcp open unknown

49176/tcp open unknown

49400/tcp open compaqdiag

49999/tcp open unknown

50000/tcp open ibm-db2

50001/tcp open unknown

50002/tcp open iiimsf

50003/tcp open unknown

50006/tcp open unknown

50300/tcp open unknown

50389/tcp open unknown

50500/tcp open unknown

50636/tcp open unknown

50800/tcp open unknown

51103/tcp open unknown

51493/tcp open unknown

52673/tcp open unknown

52822/tcp open unknown

52848/tcp open unknown

52869/tcp open unknown

54045/tcp open unknown

54328/tcp open unknown

55055/tcp open unknown

55056/tcp open unknown

55555/tcp open unknown

55600/tcp open unknown

56737/tcp open unknown

56738/tcp open unknown

57294/tcp open unknown

57797/tcp open unknown

58080/tcp open unknown

60020/tcp open unknown

60443/tcp open unknown

61532/tcp open unknown

61900/tcp open unknown

62078/tcp open iphone-sync

63331/tcp open unknown

64623/tcp open unknown

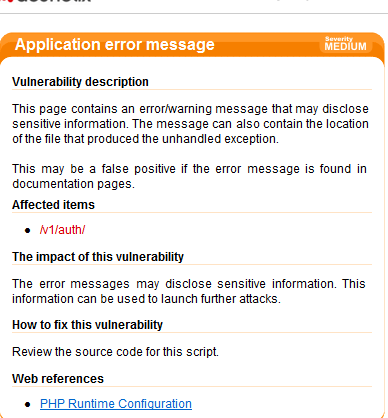
64680/tcp open unknown

65000/tcp open unknown

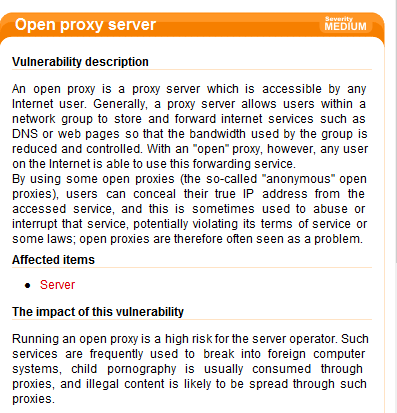
65129/tcp open unknown

65389/tcp open unknown

I also checked using acunetix, here are some findings that acunetix checked



And acunetix found a gap vulnerability in the port



I also checked <https://sandbox.onebrick.io/v1/auth/> (52.76.244.176) with the nikto command, they don't find The X-XSS-Protection and The anti-clickjacking X-Frame-Options header doesn't show up.

└─$ nikto -h http://52.76.244.176

- Nikto v2.1.6

---------------------------------------------------------------------------

+ Target IP: 52.76.244.176

+ Target Hostname: 52.76.244.176

+ Target Port: 80

+ Start Time: 2022-07-16 02:17:01 (GMT-4)

---------------------------------------------------------------------------

+ Server: awselb/2.0

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ 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

+ Root page / redirects to: https://52.76.244.176:443/

+ No CGI Directories found (use '-C all' to force check all possible dirs)

On another onebrick domain (technical-docs.onebrick.io) found vulnerable to AngularJS client-side template injection vulnerability.

**Vulnerability description**

This web application is vulnerable to AngularJS client-side template injection vulnerability. AngularJS client-side template injection vulnerabilities occur when user-input is dynamically embedded on a page where AngularJS client-side templating is used. By using curly braces it's possible to inject AngularJS expressions in the AngularJS client-side template that is being used by the application.These expressions will be evaluated on the client-side by AngularJS and when combined with a sandbox escape they allow an attacker to execute arbitrary JavaScript code.

**Affected items**

* /discuss/

**The impact of this vulnerability**

An attacker can inject AngularJS expressions that will be evaluated on the client-side. Normally AngularJS expressions are not very dangerous, but when combined with a sandbox escape they allow an attacker to execute arbitrary JavaScript code.

**How to fix this vulnerability**

It should not be possible for an attacker to inject AngularJS expressions by using curly braces. The application needs to either treat curly braces in user input as highly dangerous or avoid server-side reflection of user input entirely.

then i check with shodan command

─(kali㉿kali)-[~] └─$ curl -X GET "<https://api.shodan.io/shodan/host/52.76.244.176?key=HhYCrvvlQ555ODywots5yfXkO15zNEWG>" {"region\_code": "01", "tags": ["cloud"], "ip": 877458608, "area\_code": null, "domains": ["onebrick.io", "amazonaws.com"], "hostnames": ["ec2-52-76-244-176.ap-southeast-1.compute.amazonaws.com", "id-demo-app.onebrick.io"], "country\_code": "SG", "org": "Amazon Technologies Inc.", "data": [{"hash": -1668925014, "product": "AWS ELB", "http": {"status": 301, "robots\_hash": null, "redirects": [], "securitytxt": null, "title": "301 Moved Permanently", "sitemap\_hash": null, "robots": null, "server": "awselb/2.0", "headers\_hash": 1258854265, "host": "52.76.244.176", "html": "\r\n<title>301 Moved Permanently</title>\r\n\r\n

# 301 Moved Permanently

\r\n\r\n\r\n", "location": "/", "components": {}, "html\_hash": 1949896279, "sitemap": null, "securitytxt\_hash": null}, "os": null, "tags": ["cloud"], "timestamp": "2022-07-14T00:47:35.549560", "isp": "Amazon.com, Inc.", "transport": "tcp", "shodan": {"region": "eu", "ptr": true, "module": "http", "id": "b4dc3c04-0e40-470e-bf40-e3be9254d494", "options": {}, "crawler": "f4bb88763d8ed3a0f3f91439c2c62b77fb9e06f3"}, "asn": "AS16509", "cloud": {"region": "ap-southeast-1", "service": "AMAZON", "provider": "Amazon"}, "hostnames": ["ec2-52-76-244-176.ap-southeast-1.compute.amazonaws.com"], "location": {"city": "Singapore", "region\_code": "01", "area\_code": null, "longitude": 103.85007, "latitude": 1.28967, "country\_code": "SG", "country\_name": "Singapore"}, "version": "2.0", "ip": 877458608, "domains": ["amazonaws.com"], "org": "Amazon Technologies Inc.", "data": "HTTP/1.1 301 Moved Permanently\r\nServer: awselb/2.0\r\nDate: Thu, 14 Jul 2022 00:47:35 GMT\r\nContent-Type: text/html\r\nContent-Length: 134\r\nConnection: keep-alive\r\nLocation: [https://52.76.244.176:443/\r\n\r\n](https://52.76.244.176/r/n/r/n)", "port": 80, "opts": {}, "ip\_str": "52.76.244.176"}, {"ip": 877458608, "http": {"status": 200, "robots\_hash": null, "redirects": [], "securitytxt": null, "title": "Onebrick", "sitemap\_hash": null, "html\_hash": -1221646999, "robots": null, "favicon": {"hash": 1403223205, "data": "iVBORw0KGgoAAAANSUhEUgAAAPgAAADgCAYAAAAuVKv9AAAACXBIWXMAABYlAAAWJQFJUiTwAAAA\nAXNSR0IArs4c6QAAAARnQU1BAACxjwv8YQUAAAnfSURBVHgB7d1dVtvoHcfx3yOnp5dlB3FWELID\nsQIMs4A4dz3TTHBWAKwgkMxF74AFFJwVxFlBmBVE3YF713Na9PQv2RCmM8lIxo/s/P39nEDMqzD4\nq0dvloKAe+LLQa5etmu3cin07V1b849c29uFSr1Xr5yEk3GhNRVHgy3dZENlempv5vbSn39oah8t\n7H5c66Z8H34ej+VcEKA6iqFidqgvMfyRE4XydJ1Cr8MuswN7VI90N2P6pmqGdRzeXZ7LKQLfcHUU\nMVzZQyFXe4VFvmeRX2vF7H5s2wzK7kfjGdT9r54oxBfrvFSyKALfYBZF36L4oIWiuP+NwjC8/ceF\nViS++uG5BXqiZqP211Qzqx1vkRP4hpqN3NknPTTuW7M4JurYfOSuZlIPiftWFfkzux9TOZEJmylm\nb7SsuGff76yeaXRovgRSLZYva7rV9zuTIwS+geot5dJQy9Wfb6TrTrQNasucSc0MbMaRywkC30S9\nkCrEYVejeD16q95anuCbh25nVAkR+IaZhbHQFvMmZvufu5ErmZDHv+0/lgMEvnlypZTFXXUhhudK\nKdOeHCDwTVOGbSWV+vt3NJ3ZUXDfPQLfNCH5A3ero/XwxNOIfTlA4Fi+/2R/EdYCgQOOETjgGIED\njhE44BiBA44ROOAYgQOOETjgGIEDjhE44BiBA44ROOAYgQOOETjgGIEDjhE44BiBA44ROOAYgQOO\nETjgGIEDjhE44BiBA44ROOAYgQOOETjg2KOmn1hfb+rf6uTaz8Aa2Ip/ra9B3lr4+7jQmvhm4PHH\nwbYeZbsKcaAYtvVnARuieryHz1pAPNif2utrleFCvXISTlYX/O8GXl8kPmZv7OZg9p4gAI3Zkm7I\nbQU4t46K+Gr/PLy9PNYK/GYd3OK20Tr7pLu4ATxA38bHIxvVP9cDZ8d+FXh89cNzi/tKYl0bWLJq\nqfhD15HfBV6P3CGeC0Aqt5F3NoDWgd9b5waQVtXaoToyG8FnE+wLQBdGNqjm6kA2XycYCkB3Yuhk\nFK9G8FwAOhbyLtbFM8XergB07yZLviu6GsH7AtC9kL49CzxuC0D3gh4rMZ5NBjhWBT4VAJcs8FAI\ngEu2Fb38KAAuZcriWABcysLJeGJb0icC4M5sK3qIK3kyOoC06sBno7hYVAec+bIfPJQv7HUhAG7c\nBW6j+NQi3xGRA2786ki26uyP4fTyiWI8FYDv3u8eqhreXo1sNK9CvxCA79ZXz4s+P5fzMI4GR/b/\ntsqQK4THtkttgeew2temNTsPNdbDn+K/lFzqXbvZlocnYiU/4fn8fG8LnUC+xVQm4fRqR8CSxJeD\nXL3sg9I6t1XiF0qIZ5MBjhE44BiBA44ROOAYgQOOETjgGIEDjhE44BiBA44ROOAYgQOOETjgGIED\njhE44BiBA44ROOAYgQOOETjgGIEDjhE44BiBA44ROOAYgQOOETjgGIEDjhE44BiBA44ROOAYgQOO\nETjgGIEDjhE44BiBA449EpYq/jjYVk/bNu/cUtCW0EwsC0UV9oi8DifjqbAUBL4E8eUgVy/btZtD\neyHqRYT5wmS0fwd7E5XhIry7PBcehMAfII4GW4rZod0cCUsUclt5zOPB/qFKHRP64lgHX5DF3be4\nP4m4U+rbI/Qsvto/FBZC4AuYx/1B1QMQ6QUdEfliCLwl4l6RKvKf9llaaonA25qtc/eF7mU6rGew\naIzAW5g/uIbCqthGzXAmNEbgbcxGb6xUyOu9F2iEwNvJhdW7yYZCIwTekI0a22Ldez2EmAuNEHhT\n/+31hfUQwlOhEQJvKsS+sC5YB2+IwAHHCLypXskznNZGLIRGCLy5a2E9RP1TaITAGwon4ypwRvF1\nEMNYaITA24jxQli9XjkRGiHwNrLIyLF657Y0VQiNEHgL9sCa2Ch+KqxOKI+Fxgi8rSwe2etC6F7Q\nMaN3OwTeUn1CwFDuiMi7Vcd9eSS0QuALqEcRIu8OcS+MwBd0Fzlb1lOqf8fEvTgCf4Aq8vD2amgP\nwifz0NlPvhRxolKv7ff6rN6wiYVx2uQlmG/4GVa3755WepP1ufBBC1lZaDaDnHDhg+Uh8CWbH/HG\nYa1YCyyiA44ROOAYgQOOETjgGIEDjhE44BiBA44ROOAYgQOOETjgGIEDjhE44BiBA44ROOAYgQOO\nETjgGIEDjhE44BiBA44ROOAYgQOOETjgGIEDjhE44BiBA44ROOAYgQOOETjgGIEDjhE44BiBA44R\nOOAYgQOOBSUWR4O+YvZZaU1tStdKqQwX4d3luRKKP+2PlMVdYR1sWR7bSquwv3qh1kKhUr8oltfh\n5/HkW5/5SD5Uf4xcKQV9VGohbie/H1gnfft797WIbPYqHuxXsR9/bfBhER34vvWt4jML/bMtLf9m\niYPAAR+qVeFP8dX+4f13EjjgSdBRvS1njsABbzK9uV1cJ3DAoxjeVP8ROOBSyG0Uzwkc8CqGQwIH\n3AqM4IBnBA44RuCAYwQOOJY88HAyLgRgJboawQsB6Fw3gcf4XgC6VnQTeBbHAtC1SSeB23r4xIbx\niQB0J5TH3W1FD/G1AHQj6LjawN1Z4Daxa5sokQPJhetwcnlU3ep0P7hN9KSaswhAIsEG0pud27c6\nP9ClnrMQOZDCuIrblpant+9YyZFss8jLJ2x4A5ZiWq3+htPLvftxV1Z22uT5EW471ZPSVYah/YBP\nOzgPNeDF7FoAIZ7a7cn/h31r5edFn+1CU/VSXSRhS/U5zlvLFbMz4Y/dlHv2V097kQgk1/QQ8LW6\n8MF8LjRt+3Xx5aBQT2jikaY8P2Bz8GwywDECBxwjcMAxAgccI3DAMQIHHCNwwDECBxwjcMAxAgcc\nI3DAMQIHHCNwwDECBxwjcMAxAgccI3DAMQIHHCNwwDECBxwjcMAxAgccI3DAMQIHHCNwwDECBxwj\n8PXS+rJNwLf4CPyRCqUWO4gvhkLpceHBDeIi8PnF9NIG2CvTh5F+GsXXLjMLn/wsosf4XukU88sc\nJzWfRsoAJ8JG8RN4Fs+VzkRdiTpVKqG8EDaKm8Bno1+caPmmFsaxupKV50oyisdJF0shWC++tqKH\n+FrLFnQ6X8fvRD2toOXPUEJ8IWwcV4FbHNcWxzIjH4eTyyN1zKZ5stSlEfuddDmTwvpwtx+8jmMp\nI6AFFsrVjXoh7tnP8PCt6va7mM0wsImCnIqj/ZFtsDq0m1tqK0RbLL8aaQ3EV3s2wwoHam86G7kv\nz4WN5fZIttlIXj6z3WctthzXo/bOusRdCW/tZwmljeatDuY5r+47ccPtCH5fHA36uskGtitt1+5y\n397Vn39oWi8GR/1iHxuv+1Zmux+5yjCwv9pTux/b+rJ0Uqg6Qq3UR/XKcw5mwa3/AZ5ipJz4jVsa\nAAAAAElFTkSuQmCC\n", "location": "<https://brick-io-assets.s3-ap-southeast-1.amazonaws.com/favicon/favicon.png>"}, "headers\_hash": 680691815, "host": "52.76.244.176", "html": "\n\n\n <title>Onebrick</title>\n <meta content="text/html; charset=UTF-8" http-equiv="Content-Type"/>\n <link href="<https://brick-io-assets.s3-ap-southeast-1.amazonaws.com/favicon/favicon.png>" rel="icon"\n type="image/png"/>\n <link href="<https://brick-io-assets.s3-ap-southeast-1.amazonaws.com/static/stylesheets/main.css>" media="screen"\n rel="stylesheet"/>\n <link href="<https://brick-io-assets.s3-ap-southeast-1.amazonaws.com/static/stylesheets/bootstrap.min.css>" media="screen"\n rel="stylesheet"/>\n <link href="<https://brick-io-assets.s3-ap-southeast-1.amazonaws.com/static/stylesheets/permission.css>" media="screen"\n rel="stylesheet"/>\n\n <script src="[https://ajax.googleapis.com/ajax/libs/jquery/3.4.1/jquery.min.js"></script>\n](https://ajax.googleapis.com/ajax/libs/jquery/3.4.1/jquery.min.js%22%3E%3C/script%3E/n) <script src="[https://brick-io-assets.s3-ap-southeast-1.amazonaws.com/static/javascripts/bootstrap.min.js"></script>\n](https://brick-io-assets.s3-ap-southeast-1.amazonaws.com/static/javascripts/bootstrap.min.js%22%3E%3C/script%3E/n) <script src="[https://unpkg.com/feather-icons"></script>\n](https://unpkg.com/feather-icons%22%3E%3C/script%3E/n)\n\n<div class="center">\n <div class="content-box">\n <div class="brick-logo">\n <img class="img-fluid" src="[https://brick-io-assets.s3-ap-southeast-1.amazonaws.com/brick-logo.png">\n](https://brick-io-assets.s3-ap-southeast-1.amazonaws.com/brick-logo.png%22%3E/n) \n

# Server is Up and Running

\n \n\n\n<script language="javascript" type="text/javascript">\n function windowClose() {\n window.close();\n }\n</script>\n\n\n", "location": "/", "components": {"jQuery": {"categories": ["JavaScript libraries"]}, "Google Hosted Libraries": {"categories": ["CDN"]}, "Bootstrap": {"categories": ["UI frameworks"]}, "Unpkg": {"categories": ["CDN"]}}, "server": "nginx/1.20.0", "sitemap": null, "securitytxt\_hash": null}, "port": 443, "transport": "tcp", "version": "1.20.0", "cloud": {"region": "ap-southeast-1", "service": "AMAZON", "provider": "Amazon"}, "location": {"city": "Singapore", "region\_code": "01", "area\_code": null, "longitude": 103.85007, "latitude": 1.28967, "country\_code": "SG", "country\_name": "Singapore"}, "product": "nginx", "hash": 1191281077, "tags": ["cloud"], "timestamp": "2022-07-14T15:31:58.796786", "ssl": {"chain\_sha256": ["f199e37f08490eb42a7f9c9b02b41039457db0ce63b18765e9b5b213e1f74f8a", "52274c57ce4dee3b49db7a7ff708c040f771898b3be88725a86fb4430182fe14", "4348a0e9444c78cb265e058d5e8944b4d84f9662bd26db257f8934a443c70161"], "jarm": "29d29d00029d29d00029d29d29d29d4d0c5eed338ce212ffe821a67732ded8", "chain": ["-----BEGIN CERTIFICATE-----\nMIIG8jCCBdqgAwIBAgIQAy9IyNQKaPO1GtLtWBPKCjANBgkqhkiG9w0BAQsFADBP\nMQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMSkwJwYDVQQDEyBE\naWdpQ2VydCBUTFMgUlNBIFNIQTI1NiAyMDIwIENBMTAeFw0yMjA2MDcwMDAwMDBa\nFw0yMzA2MjkyMzU5NTlaMIGOMQswCQYDVQQGEwJJRDEmMCQGA1UECBMdRGFlcmFo\nIEtodXN1cyBJYnVrb3RhIEpha2FydGExGDAWBgNVBAcTD0pha2FydGEgU2VsYXRh\nbjElMCMGA1UEChMcUFQgQnJpY2sgVGVrbm9sb2dpIEluZG9uZXNpYTEWMBQGA1UE\nAwwNKi5vbmVicmljay5pbzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB\nALajgtZOSaO/nGsdtkLtp5kfAINYSQG/tzLmLW9dYC9TODRRT8nL53dBxaEUE3Sv\n+wUtxJjM9gjvlVMbaCM2+Eji9Qf+vuAHpyJV7t75JR5hvO5CQWxKdw70/jZN5QoC\ndWghMT2aEZwdPGY5XPGb/6RI5g+CcNey2QDMmjFp8Gl/FEYXLHhmtupIrpfwad8F\nKrb66/SQTqJlM28TvluhgV1FtUIX64tE8/UG3juGe8qRuq5+e4WlJ87CDBw769gR\nL0A2yhXC7mW0PNg71nbn4zyVtOq+TyteVY5iH7PNEVke9AEBC5SmUSHqNDZzAShO\n0KrJJIWawdkLg/h2ZQrbAGkCAwEAAaOCA4gwggOEMB8GA1UdIwQYMBaAFLdrouqo\nqoSMeeq02g+YssWVdrn0MB0GA1UdDgQWBBQiEkQxp/23Mq+b7wDptqmhRCd2FzAx\nBgNVHREEKjAogg0qLm9uZWJyaWNrLmlvghdpZC1kZW1vLWFwcC5vbmVicmljay5p\nbzAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMC\nMIGPBgNVHR8EgYcwgYQwQKA+oDyGOmh0dHA6Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9E\naWdpQ2VydFRMU1JTQVNIQTI1NjIwMjBDQTEtNC5jcmwwQKA+oDyGOmh0dHA6Ly9j\ncmw0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydFRMU1JTQVNIQTI1NjIwMjBDQTEtNC5j\ncmwwPgYDVR0gBDcwNTAzBgZngQwBAgIwKTAnBggrBgEFBQcCARYbaHR0cDovL3d3\ndy5kaWdpY2VydC5jb20vQ1BTMH8GCCsGAQUFBwEBBHMwcTAkBggrBgEFBQcwAYYY\naHR0cDovL29jc3AuZGlnaWNlcnQuY29tMEkGCCsGAQUFBzAChj1odHRwOi8vY2Fj\nZXJ0cy5kaWdpY2VydC5jb20vRGlnaUNlcnRUTFNSU0FTSEEyNTYyMDIwQ0ExLTEu\nY3J0MAkGA1UdEwQCMAAwggGABgorBgEEAdZ5AgQCBIIBcASCAWwBagB2AOg+0No+\n9QY1MudXKLyJa8kD08vREWvs62nhd31tBr1uAAABgTyG444AAAQDAEcwRQIhAIce\nfd96tcOJwpHglU3bSJM0r+vFU/tVFVrijbcacsLwAiAw8v4zFAcqx4xCQLzL76Pe\nu10R/1XsDJKJu8SwBJdGmQB3ADXPGRu/sWxXvw+tTG1Cy7u2JyAmUeo/4SrvqAPD\nO9ZMAAABgTyG480AAAQDAEgwRgIhAJ6UA4jaMt6ISvjcN2PLPtyYRhWtMyKrnT0K\ncHBAYsdaAiEA5IRfx8ZZrAszibtG+sDG+AezFcrXqrhrqLCBf40C5KsAdwC3Pvsk\n35xNunXyOcW6WPRsXfxCz3qfNcSeHQmBJe20mQAAAYE8huPFAAAEAwBIMEYCIQDD\nBRZNNJ1EQLCWpv3FuV7ub7Tn+O5XT/8vX6vCmHe/8QIhAICjhPbuohvpVsl2hU1r\n6cjRXBsXiT8JzQVUi9Aa+I41MA0GCSqGSIb3DQEBCwUAA4IBAQAvzBDDIIG4NRA/\niFLid4Jt7M6a2RB/WXC/tkCegYdkGGq66gMcIK9OzWgocV5IE/+vIkfnTk/evPMM\nb1sem0u9qCswWt6kjBWRBXqicagZWIXzDqtB3+iHFOJMmCK/KJadKzo1vvQEqlS6\naSIOKrHHjsq2vQVtZ8q0JwE77KL1gmYS+asuu9NgPukftt9O6Z1SCW86nSDXPGad\ni+PTpFDnovE1BDN5V3pw6EHAbX8zE8qdE5FZJZGsORwm1nb+KRnzTaK9LmPihNz6\nRH7K8pKERjB+lVyqSavDyQ7Jclecgz7QLTYcowLGHtcCngLMzp+j1TsE6WdzAkXy\nornpTURW\n-----END CERTIFICATE-----\n", "-----BEGIN CERTIFICATE-----\nMIIEvjCCA6agAwIBAgIQBtjZBNVYQ0b2ii+nVCJ+xDANBgkqhkiG9w0BAQsFADBh\nMQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3\nd3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD\nQTAeFw0yMTA0MTQwMDAwMDBaFw0zMTA0MTMyMzU5NTlaME8xCzAJBgNVBAYTAlVT\nMRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxKTAnBgNVBAMTIERpZ2lDZXJ0IFRMUyBS\nU0EgU0hBMjU2IDIwMjAgQ0ExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC\nAQEAwUuzZUdwvN1PWNvsnO3DZuUfMRNUrUpmRh8sCuxkB+Uu3Ny5CiDt3+PE0J6a\nqXodgojlEVbbHp9YwlHnLDQNLtKS4VbL8Xlfs7uHyiUDe5pSQWYQYE9XE0nw6Ddn\ng9/n00tnTCJRpt8OmRDtV1F0JuJ9x8piLhMbfyOIJVNvwTRYAIuE//i+p1hJInuW\nraKImxW8oHzf6VGo1bDtN+I2tIJLYrVJmuzHZ9bjPvXj1hJeRPG/cUJ9WIQDgLGB\nAfr5yjK7tI4nhyfFK3TUqNaX3sNk+crOU6JWvHgXjkkDKa77SU+kFbnO8lwZV21r\neacroicgE7XQPUDTITAHk+qZ9QIDAQABo4IBgjCCAX4wEgYDVR0TAQH/BAgwBgEB\n/wIBADAdBgNVHQ4EFgQUt2ui6qiqhIx56rTaD5iyxZV2ufQwHwYDVR0jBBgwFoAU\nA95QNVbRTLtm8KPiGxvDl7I90VUwDgYDVR0PAQH/BAQDAgGGMB0GA1UdJQQWMBQG\nCCsGAQUFBwMBBggrBgEFBQcDAjB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGG\nGGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0LmNvbTBABggrBgEFBQcwAoY0aHR0cDovL2Nh\nY2VydHMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0R2xvYmFsUm9vdENBLmNydDBCBgNV\nHR8EOzA5MDegNaAzhjFodHRwOi8vY3JsMy5kaWdpY2VydC5jb20vRGlnaUNlcnRH\nbG9iYWxSb290Q0EuY3JsMD0GA1UdIAQ2MDQwCwYJYIZIAYb9bAIBMAcGBWeBDAEB\nMAgGBmeBDAECATAIBgZngQwBAgIwCAYGZ4EMAQIDMA0GCSqGSIb3DQEBCwUAA4IB\nAQCAMs5eC91uWg0Kr+HWhMvAjvqFcO3aXbMM9yt1QP6FCvrzMXi3cEsaiVi6gL3z\nax3pfs8LulicWdSQ0/1s/dCYbbdxglvPbQtaCdB73sRD2Cqk3p5BJl+7j5nL3a7h\nqG+fh/50tx8bIKuxT8b1Z11dmzzp/2n3YWzW2fP9NsarA4h20ksudYbj/NhVfSbC\nEXffPgK2fPOre3qGNm+499iTcc+G33Mw+nur7SpZyEKEOxEXGlLzyQ4UfaJbcme6\nce1XR2bFuAJKZTRei9AqPCCcUZlM51Ke92sRKw2Sfh3oius2FkOH6ipjv3U/697E\nA7sKPPcw7+uvTPyLNhBzPvOk\n-----END CERTIFICATE-----\n", "-----BEGIN CERTIFICATE-----\nMIIDrzCCApegAwIBAgIQCDvgVpBCRrGhdWrJWZHHSjANBgkqhkiG9w0BAQUFADBh\nMQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3\nd3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD\nQTAeFw0wNjExMTAwMDAwMDBaFw0zMTExMTAwMDAwMDBaMGExCzAJBgNVBAYTAlVT\nMRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j\nb20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IENBMIIBIjANBgkqhkiG\n9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLeqKTTo1eqUKKPC3eQyaKl7hLOllsB\nCSDMAZOnTjC3U/dDxGkAV53ijSLdhwZAAIEJzs4bg7/fzTtxRuLWZscFs3YnFo97\nnh6Vfe63SKMI2tavegw5BmV/Sl0fvBf4q77uKNd0f3p4mVmFaG5cIzJLv07A6Fpt\n43C/dxC//AH2hdmoRBBYMql1GNXRor5H4idq9Joz+EkIYIvUX7Q6hL+hqkpMfT7P\nT19sdl6gSzeRntwi5m3OFBqOasv+zbMUZBfHWymeMr/y7vrTC0LUq7dBMtoM1O/4\ngdW7jVg/tRvoSSiicNoxBN33shbyTApOB6jtSj1etX+jkMOvJwIDAQABo2MwYTAO\nBgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUA95QNVbR\nTLtm8KPiGxvDl7I90VUwHwYDVR0jBBgwFoAUA95QNVbRTLtm8KPiGxvDl7I90VUw\nDQYJKoZIhvcNAQEFBQADggEBAMucN6pIExIK+t1EnE9SsPTfrgT1eXkIoyQY/Esr\nhMAtudXH/vTBH1jLuG2cenTnmCmrEbXjcKChzUyImZOMkXDiqw8cvpOp/2PV5Adg\n06O/nVsJ8dWO41P0jmP6P6fbtGbfYmbW0W5BjfIttep3Sp+dWOIrWcBAI+0tKIJF\nPnlUkiaY4IBIqDfv8NZ5YBberOgOzW6sRBc4L0na4UU+Krk2U886UAb3LujEV0ls\nYSEY1QSteDwsOoBrp+uvFRTp2InBuThs4pFsiv9kuXclVzDAGySj4dzp30d8tbQk\nCAUw7C29C79Fv1C5qfPrmAESrciIxpg0X40KPMbp1ZWVbd4=\n-----END CERTIFICATE-----\n"], "dhparams": null, "versions": ["-TLSv1", "-SSLv2", "-SSLv3", "-TLSv1.1", "TLSv1.2", "-TLSv1.3"], "acceptable\_cas": [], "tlsext": [{"id": 65281, "name": "renegotiation\_info"}, {"id": 11, "name": "ec\_point\_formats"}, {"id": 35, "name": "session\_ticket"}], "ja3s": "ccc514751b175866924439bdbb5bba34", "cert": {"sig\_alg": "sha256WithRSAEncryption", "issued": "20220607000000Z", "expires": "20230629235959Z", "expired": false, "version": 2, "extensions": [{"data": "0\x16\x80\x14\xb7k\xa2\xea\xa8\xaa\x84\x8cy\xea\xb4\xda\x0f\x98\xb2\xc5\x95v\xb9\xf4", "name": "authorityKeyIdentifier"}, {"data": "\x04\x14"\x12D1\xa7\xfd\xb72\xaf\x9b\xef\x00\xe9\xb6\xa9\xa1D\'v\x17", "name": "subjectKeyIdentifier"}, {"data": "0(\x82\r\*.onebrick.io\x82\x17id-demo-app.onebrick.io", "name": "subjectAltName"}, {"critical": true, "data": "\x03\x02\x05\xa0", "name": "keyUsage"}, {"data": "0\x14\x06\x08+\x06\x01\x05\x05\x07\x03\x01\x06\x08+\x06\x01\x05\x05\x07\x03\x02", "name": "extendedKeyUsage"}, {"data": "0\x81\x840@\xa0>\xa0<\x86:[http://crl3.digicert.com/DigiCertTLSRSASHA2562020CA1-4.crl0@\xa0>\xa0<\x86:http://crl4.digicert.com/DigiCertTLSRSASHA2562020CA1-4.crl](http://crl3.digicert.com/DigiCertTLSRSASHA2562020CA1-4.crl0@/xa0%3E/xa0%3C/x86:http:/crl4.digicert.com/DigiCertTLSRSASHA2562020CA1-4.crl)", "name": "crlDistributionPoints"}, {"data": "0503\x06\x06g\x81\x0c\x01\x02\x020)0\'\x06\x08+\x06\x01\x05\x05\x07\x02\x01\x16\x1bhttp://[www.digicert.com/CPS](http://www.digicert.com/CPS)", "name": "certificatePolicies"}, {"data": "0q0$\x06\x08+\x06\x01\x05\x05\x070\x01\x86\x18[http://ocsp.digicert.com0I\x06\x08+\x06\x01\x05\x05\x070\x02\x86=http://cacerts.digicert.com/DigiCertTLSRSASHA2562020CA1-1.crt](http://ocsp.digicert.com0i/x06/x08+/x06/x01/x05/x05/x070/x02/x86=http:/cacerts.digicert.com/DigiCertTLSRSASHA2562020CA1-1.crt)", "name": "authorityInfoAccess"}, {"data": "0\x00", "name": "basicConstraints"}, {"data": "\x04\x82\x01l\x01j\x00v\x00\xe8>\xd0\xda>\xf5\x0652\xe7W(\xbc\x89k\xc9\x03\xd3\xcb\xd1\x11k\xec\xebi\xe1w}m\x06\xbdn\x00\x00\x01\x81<\x86\xe3\x8e\x00\x00\x04\x03\x00G0E\x02!\x00\x87\x1e}\xdfz\xb5\xc3\x89\xc2\x91\xe0\x95M\xdbH\x934\xaf\xeb\xc5S\xfbU\x15Z\xe2\x8d\xb7\x1ar\xc2\xf0\x02 0\xf2\xfe3\x14\x07\*\xc7\x8cB@\xbc\xcb\xef\xa3\xde\xbb]\x11\xffU\xec\x0c\x92\x89\xbb\xc4\xb0\x04\x97F\x99\x00w\x005\xcf\x19\x1b\xbf\xb1lW\xbf\x0f\xadLmB\xcb\xbb\xb6\' &Q\xea?\xe1\*\xef\xa8\x03\xc3;\xd6L\x00\x00\x01\x81<\x86\xe3\xcd\x00\x00\x04\x03\x00H0F\x02!\x00\x9e\x94\x03\x88\xda2\xde\x88J\xf8\xdc7c\xcb>\xdc\x98F\x15\xad3"\xab\x9d=\npp@b\xc7Z\x02!\x00\xe4\x84\xc7\xc6Y\xac\x0b3\x89\xbbF\xfa\xc0\xc6\xf8\x07\xb3\x15\xca\xd7\xaa\xb8k\xa8\xb0\x81\x7f\x8d\x02\xe4\xab\x00w\x00\xb7>\xfb$\xdf\x9cM\xbau\xf29\xc5\xbaX\xf4l]\xfcB\xcfz\x9f5\xc4\x9e\x1d\t\x81%\xed\xb4\x99\x00\x00\x01\x81<\x86\xe3\xc5\x00\x00\x04\x03\x00H0F\x02!\x00\xc3\x05\x16M4\x9dD@\xb0\x96\xa6\xfd\xc5\xb9^\xeeo\xb4\xe7\xf8\xeeWO\xff/\_\xab\xc2\x98w\xbf\xf1\x02!\x00\x80\xa3\x84\xf6\xee\xa2\x1b\xe9V\xc9v\x85Mk\xe9\xc8\xd1\\\x1b\x17\x89?\t\xcd\x05T\x8b\xd0\x1a\xf8\x8e5", "name": "ct\_precert\_scts"}], "fingerprint": {"sha256": "f199e37f08490eb42a7f9c9b02b41039457db0ce63b18765e9b5b213e1f74f8a", "sha1": "969137123a7f66ee9e996d3c4113f5619768bc1e"}, "serial": 4233198184453257252434701422207158794, "subject": {"C": "ID", "L": "Jakarta Selatan", "CN": "\*.onebrick.io", "O": "PT Brick Teknologi Indonesia", "ST": "Daerah Khusus Ibukota Jakarta"}, "pubkey": {"type": "rsa", "bits": 2048}, "issuer": {"C": "US", "CN": "DigiCert TLS RSA SHA256 2020 CA1", "O": "DigiCert Inc"}}, "cipher": {"version": "TLSv1.2", "bits": 128, "name": "ECDHE-RSA-AES128-GCM-SHA256"}, "trust": {"revoked": false, "browser": {"mozilla": true, "apple": true, "microsoft": true}}, "handshake\_states": ["before SSL initialization", "SSLv3/TLS write client hello", "SSLv3/TLS read server hello", "SSLv3/TLS read server certificate", "SSLv3/TLS read server key exchange", "SSLv3/TLS read server done", "SSLv3/TLS write client key exchange", "SSLv3/TLS write change cipher spec", "SSLv3/TLS write finished", "SSLv3/TLS read server session ticket", "SSLv3/TLS read change cipher spec", "SSLv3/TLS read finished", "SSL negotiation finished successfully"], "alpn": ["h2", "http/1.1"], "ocsp": {}}, "hostnames": ["ec2-52-76-244-176.ap-southeast-1.compute.amazonaws.com", "id-demo-app.onebrick.io"], "org": "Amazon Technologies Inc.", "data": "HTTP/1.1 200 \r\nDate: Thu, 14 Jul 2022 15:31:58 GMT\r\nContent-Type: text/html;charset=UTF-8\r\nTransfer-Encoding: chunked\r\nConnection: keep-alive\r\nServer: nginx/1.20.0\r\nVary: Origin\r\nVary: Access-Control-Request-Method\r\nVary: Access-Control-Request-Headers\r\nX-Content-Type-Options: nosniff\r\nX-XSS-Protection: 1; mode=block\r\nCache-Control: no-cache, no-store, max-age=0, must-revalidate\r\nPragma: no-cache\r\nExpires: 0\r\nStrict-Transport-Security: max-age=31536000 ; includeSubDomains\r\nX-Frame-Options: DENY\r\nContent-Language: en-US\r\n\r\n", "asn": "AS16509", "cpe23": ["cpe:2.3🅰️jquery:jquery", "cpe:2.3🅰️getbootstrap:bootstrap", "cpe:2.3🅰️igor\_sysoev:nginx:1.20.0"], "isp": "Amazon.com, Inc.", "cpe": ["cpe:/a:jquery:jquery", "cpe:/a:getbootstrap:bootstrap", "cpe:/a:igor\_sysoev:nginx:1.20.0"], "domains": ["amazonaws.com", "onebrick.io"], "ip\_str": "52.76.244.176", "os": null, "\_shodan": {"region": "eu", "ptr": true, "module": "https", "id": "71065d26-a194-425b-bda3-06759d0b37ee", "options": {}, "crawler": "f4bb88763d8ed3a0f3f91439c2c62b77fb9e06f3"}, "opts": {"vulns": [], "heartbleed": "2022/07/14 15:32:23 52.76.244.176:443 - SAFE\n"}}], "asn": "AS16509", "city": "Singapore", "latitude": 1.28967, "isp": "Amazon.com, Inc.", "longitude": 103.85007, "last\_update": "2022-07-14T15:31:58.796786", "country\_name": "Singapore", "ip\_str": "52.76.244.176", "os": null, "ports": [80, 443]}

I am still a NOOB and learn every day I do my best to succeed in ethical hacking because it is my hobby

I wish success for everyone on this journey.

if you have any questions ping me on whatsapp.

thank you for reading my first writeup.