SecureSuite Report for juice-shop.herokuapp.com

NMAP SCAN RESULTS

Starting Nmap 7.95 (https://nmap.org) at 2025-07-28 17:36 IST

Nmap scan report for juice-shop.herokuapp.com (54.220.192.176)

Host is up (0.024s latency).

Other addresses for juice-shop.herokuapp.com (not scanned): 46.137.15.86 54.73.53.134

rDNS record for 54.220.192.176: ec2-54-220-192-176.eu-west-1.compute.amazonaws.com

Not shown: 997 filtered tcp ports (no-response)

PORT   STATE SERVICE   VERSION

53/tcp open domain   ISC BIND 9.18.36

80/tcp open http   heroku-router

443/tcp open ssl/https heroku-router

2 services unrecognized despite returning data. If you know the service/version, please submit the following

fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port80-TCP:V=7.95%I=7%D=7/28%Time=688767BB%P=x86_64-pc-linux-gnu%r(GetR

SF:equest,BF,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nCache-Control:\x20no-c

SF:ache,\x20no-store\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nDa

SF:te:\x202025-07-28\x2012:08:07\.86020112\x20\+0000\x20UTC\r\nServer:\x20

SF:heroku-router\r\nContent-Length:\x200\r\n\r\n")%r(HTTPOptions,C0,"HTTP/

SF:1\.0\x20400\x20Bad\x20Request\r\nCache-Control:\x20no-cache,\x20no-stor

SF:e\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nDate:\x202025-07-2

SF:8\x2012:08:08\.529047285\x20\+0000\x20UTC\r\nServer:\x20heroku-router\r

SF:\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,C0,"HTTP/1\.0\x204

SF:00\x20Bad\x20Request\r\nCache-Control:\x20no-cache,\x20no-store\r\nCont

SF:ent-Type:\x20text/html;\x20charset=utf-8\r\nDate:\x202025-07-28\x2012:0

SF:8:19\.314617639\x20\+0000\x20UTC\r\nServer:\x20heroku-router\r\nContent

SF:-Length:\x200\r\n\r\n");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port443-TCP:V=7.95%T=SSL%I=7%D=7/28%Time=688767C5%P=x86_64-pc-linux-gnu

SF:%r(GetRequest,C0,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nCache-Control:\

SF:x20no-cache,\x20no-store\r\nContent-Type:\x20text/html;\x20charset=utf-

SF:8\r\nDate:\x202025-07-28\x2012:08:16\.378390774\x20\+0000\x20UTC\r\nSer

SF:ver:\x20heroku-router\r\nContent-Length:\x200\r\n\r\n")%r(HTTPOptions,C

SF:0,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nCache-Control:\x20no-cache,\x2

SF:0no-store\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nDate:\x202

SF:025-07-28\x2012:08:18\.939023877\x20\+0000\x20UTC\r\nServer:\x20heroku-

SF:router\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,BF,"HTTP/1

SF:\.0\x20400\x20Bad\x20Request\r\nCache-Control:\x20no-cache,\x20no-store

SF:\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nDate:\x202025-07-28

SF:\x2012:08:19\.61859878\x20\+0000\x20UTC\r\nServer:\x20heroku-router\r\n

SF:Content-Length:\x200\r\n\r\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 230.50 seconds

OSINT INFO

WHOIS Info:

No match for "JUICE-SHOP.HEROKUAPP.COM".

>>> Last update of whois database: 2025-07-28T12:11:24Z <<<

NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and automated except as reasonably necessary to register domain names or modify existing registrations; the Data in VeriSign Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. VeriSign does not guarantee its accuracy. By submitting a Whois query, you agree to abide by the following terms of use: You agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to VeriSign (or its computer systems). The compilation, repackaging, dissemination or other use of this Data is expressly prohibited without the prior written consent of VeriSign. You agree not to use electronic processes that are automated and high-volume to access or query the Whois database except as reasonably necessary to register domain names or modify existing registrations. VeriSign reserves the right

to restrict your access to the Whois database in its sole discretion to ensure operational stability. VeriSign may restrict or terminate your access to the Whois database for failure to abide by these terms of use. VeriSign reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.

DNS Info:

; <<>> DiG 9.20.9-1-Debian <<>> juice-shop.herokuapp.com

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39369

;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 1232

; COOKIE: a6a05eb1bd7707a501000000688768fe63040d96e81bb26b (good)

;; QUESTION SECTION:

;juice-shop.herokuapp.com. IN A

;; ANSWER SECTION:

juice-shop.herokuapp.com. 11 IN A 54.220.192.176

juice-shop.herokuapp.com. 11 IN A 46.137.15.86

juice-shop.herokuapp.com. 11 IN A 54.73.53.134

;; Query time: 55 msec

;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)

;; WHEN: Mon Jul 28 17:39:54 IST 2025

;; MSG SIZE rcvd: 129

WEB VULNERABILITY SCAN

Web scan failed: HTTPConnectionPool(host='juice-shop.herokuapp.com', port=80): Read timed out. (read timeout=5)