DNS Security configuration check Chameleon website

CHAMELEON

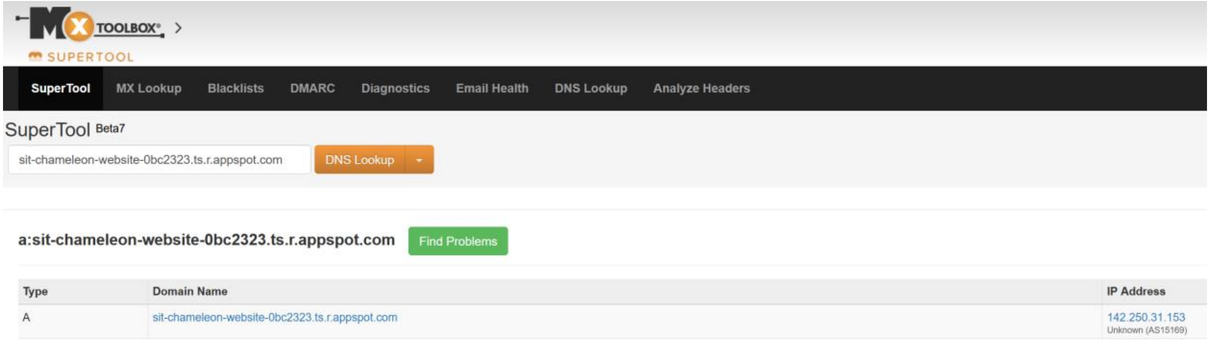
FOR OUR SMARTER WORLD

Jason Galletti.

Monitoring a web applications Domain Name System (DNS) enables you to check the security of the communication between the browser users and the web application and services it is using. Monitoring DNS settings can also mitigate against DNS attacks including DNS Hijacking and DNS Poisoning, Distributed Denial of Service (DDoS) and Denial of Service(Dos).

DNS Check for Chameleon Web application

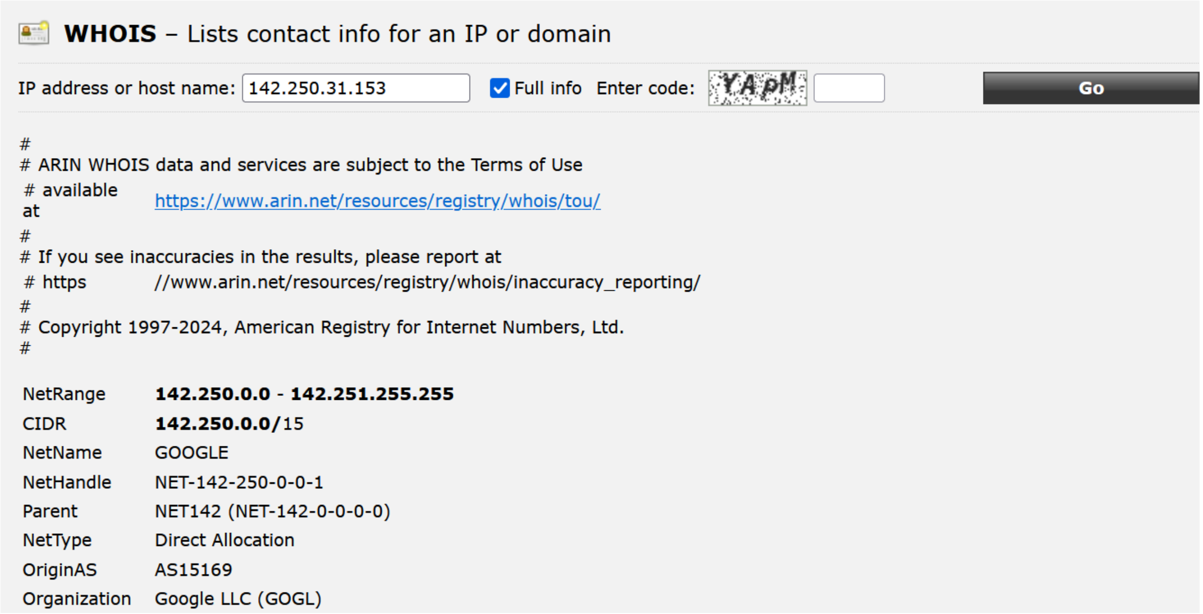
sit-chameleon-website-0bc2323.ts.r.appspot.com Resolves to 142.250.31.153, which confirms the Application is hosted on Google GCP.



sit-chameleon-website-0bc2323.ts.r.appspot.com

a:sit-chameleon-website-0bc2323.ts.r.appspot.com

Type	Domain Name	IP Address
A	sit-chameleon-website-0bc2323.ts.r.appspot.com	142.250.31.153 Unknown (AS15169)



WHOIS – Lists contact info for an IP or domain

IP address or host name: 142.250.31.153 ☑ Full info Enter code: YApM

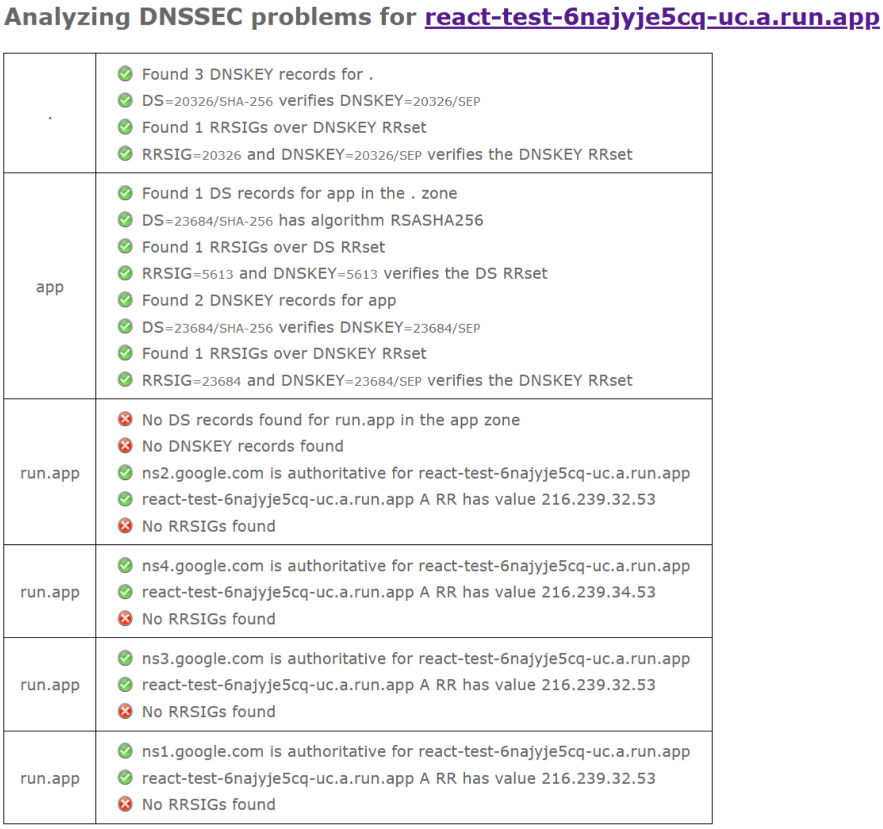
```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at   https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https        //www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American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

NetRange      142.250.0.0 - 142.251.255.255
CIDR          142.250.0.0/15
NetName       GOOGLE
NetHandle     NET-142-250-0-0-1
Parent        NET142 (NET-142-0-0-0-0)
NetType       Direct Allocation
OriginAS      AS15169
Organization  Google LLC (GOGL)
```

DNS Security (DNSSEC)

DNS itself was initially designed without security in focus, using DNSSEC information in the DNS can be cryptographic signed, this enables clients to ensure data is not modified in transit and making DNS attacks harder.

DNSSEC works adding digital signatures to the existing DNS record alongside the common record types, A, MX, CNAME. By checking the associated signature, you can verify it is indeed from the authoritative name server and not tampered by a malicious actor in transit.

DNSSEC Check for Chameleon Web application.



Analyzing DNSSEC problems for react-test-6najyje5cq-uc.a.run.app

.	✓ Found 3 DNSKEY records for . ✓ DS=20326/SHA-256 verifies DNSKEY=20326/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
app	✓ Found 1 DS records for app in the . zone ✓ DS=23684/SHA-256 has algorithm RSASHA256 ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=5613 and DNSKEY=5613 verifies the DS RRset ✓ Found 2 DNSKEY records for app ✓ DS=23684/SHA-256 verifies DNSKEY=23684/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=23684 and DNSKEY=23684/SEP verifies the DNSKEY RRset
run.app	✗ No DS records found for run.app in the app zone ✗ No DNSKEY records found ✓ ns2.google.com is authoritative for react-test-6najyje5cq-uc.a.run.app ✓ react-test-6najyje5cq-uc.a.run.app A RR has value 216.239.32.53 ✗ No RRSIGs found
run.app	✓ ns4.google.com is authoritative for react-test-6najyje5cq-uc.a.run.app ✓ react-test-6najyje5cq-uc.a.run.app A RR has value 216.239.34.53 ✗ No RRSIGs found
run.app	✓ ns3.google.com is authoritative for react-test-6najyje5cq-uc.a.run.app ✓ react-test-6najyje5cq-uc.a.run.app A RR has value 216.239.32.53 ✗ No RRSIGs found
run.app	✓ ns1.google.com is authoritative for react-test-6najyje5cq-uc.a.run.app ✓ react-test-6najyje5cq-uc.a.run.app A RR has value 216.239.32.53 ✗ No RRSIGs found

The above results shows that the web application is missing the RRSIG (which contains the cryptographic signature) and DNSKEY (public signing key) which **confirms that the web application is not using DNSSEC**.

Tools Used: Mx Toolbox, ping.eu, Verisign Labs

https://blog.apnic.net/2017/05/11/dnssec-validation-enabled/

https://www.cloudflare.com/en-au/dns/dnssec/how-dnssec-works/

dnssec-analyzer.verisignlabs.com/