Report: Investigating Website IP Addresses and DNS

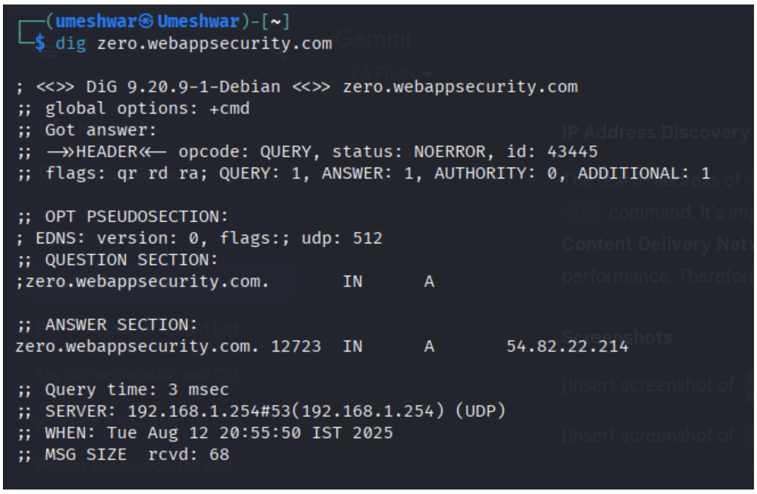
Introduction

This report details the process of finding the IP address for the website zero.webappsecurity.com and explains the underlying mechanism of how the internet locates websites using the Domain Name System (DNS). The tools dig and nmap -sL were used to gather information about the website.

IP Address Discovery

The real IP address of zero.webappsecurity.com was found to be 54.82.22.214 using the dig command. It's important to note that a website can have multiple IP addresses due to a Content Delivery Network (CDN), which distributes traffic across multiple servers to improve performance. Therefore, the IP address can vary depending on your location.

Screenshots



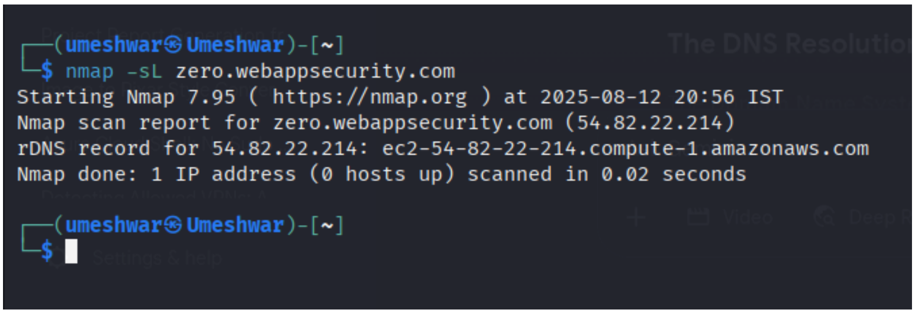
```
┌──(umeshwar㉿Umeshwar)-[~]
└─$ dig zero.webappsecurity.com

; <<>> DiG 9.20.9-1-Debian <<>> zero.webappsecurity.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43445
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
zero.webappsecurity.com. 12723  IN      A       54.82.22.214

;; Query time: 3 msec
;; SERVER: 192.168.1.254#53(192.168.1.254) (UDP)
;; WHEN: Tue Aug 12 20:55:50 IST 2025
;; MSG SIZE  rcvd: 68
```



```
┌──(umeshwar㉿Umeshwar)-[~]
└─$ nmap -sL zero.webappsecurity.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-12 20:56 IST
Nmap scan report for zero.webappsecurity.com (54.82.22.214)
rDNS record for 54.82.22.214: ec2-54-82-22-214.compute-1.amazonaws.com
Nmap done: 1 IP address (0 hosts up) scanned in 0.02 seconds

┌──(umeshwar㉿Umeshwar)-[~]
└─$ 
```

The DNS Resolution Process

The Domain Name System (DNS) acts as a phone book for the internet, translating human-readable domain names into machine-readable IP addresses. This process, known as DNS resolution, is how your computer finds the server hosting a website.

The flowchart below illustrates this process:

1. User Request: You type zero.webappsecurity.com into your browser.
2. Recursive DNS Server Query: Your browser sends a query to a recursive DNS server, usually provided by your internet service provider (ISP).
3. Root Server Query: The recursive server, if it doesn't have the IP address cached, asks a root name server for the IP of the Top-Level Domain (TLD) server for .com.
4. TLD Server Query: The recursive server queries the .com TLD server, which directs it to the authoritative name server for webappsecurity.com.
5. Authoritative Name Server Query: The recursive server queries the authoritative name server, which holds the actual IP address for zero.webappsecurity.com.
6. IP Address Returned: The authoritative server sends the IP address (e.g., 54.82.22.214) back to the recursive DNS server. The recursive server then sends it to your browser.
7. Browser Connection: Your browser uses the IP address to connect to the website's server and load the webpage.

Tool Analysis

- dig (Domain Information Groper): This is a command-line tool for querying DNS. It's the most effective and reliable tool for finding the specific IP address of a domain. It shows the A record, which is the DNS record that maps a domain name to its IPv4 address. The dig command successfully revealed the IP address of zero.webappsecurity.com.
- nmap -sL: This command is used for list scanning. The -sL flag tells nmap to simply list the hosts within a given range without performing a full port scan. While it can be used for host discovery, it does not actively query DNS to find the specific IP address of a single domain. It's more of a reconnaissance tool for seeing what is in a network rather than for resolving a single hostname to an IP address.