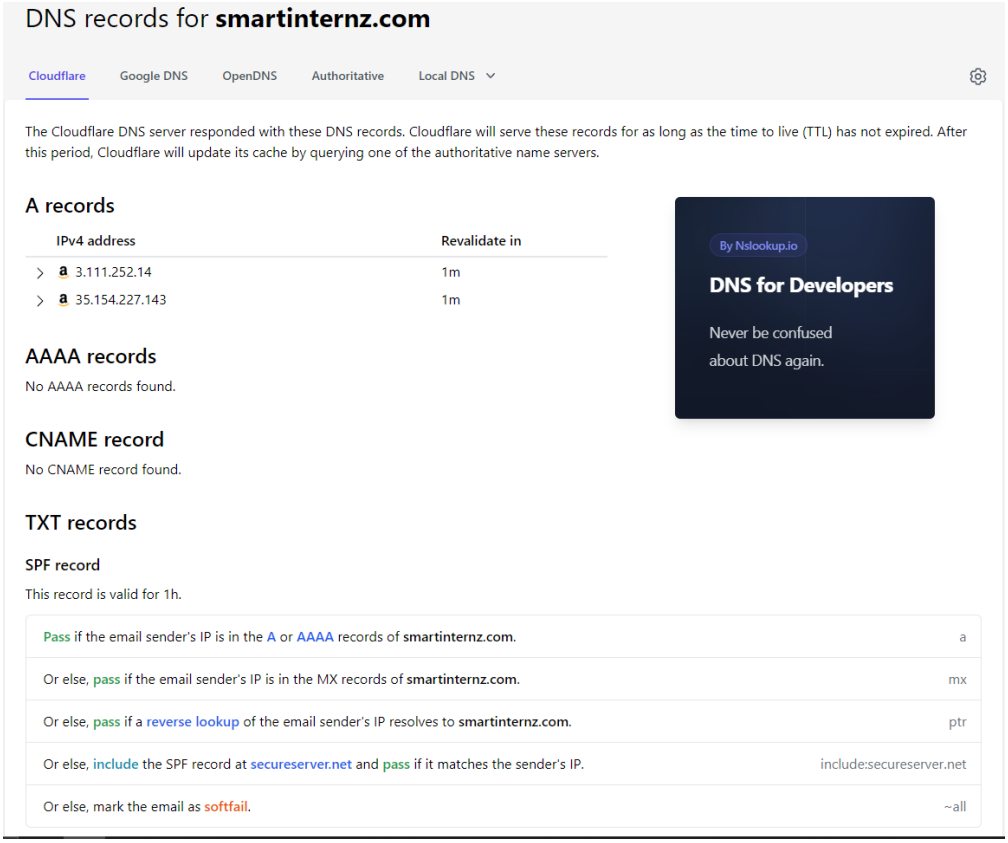
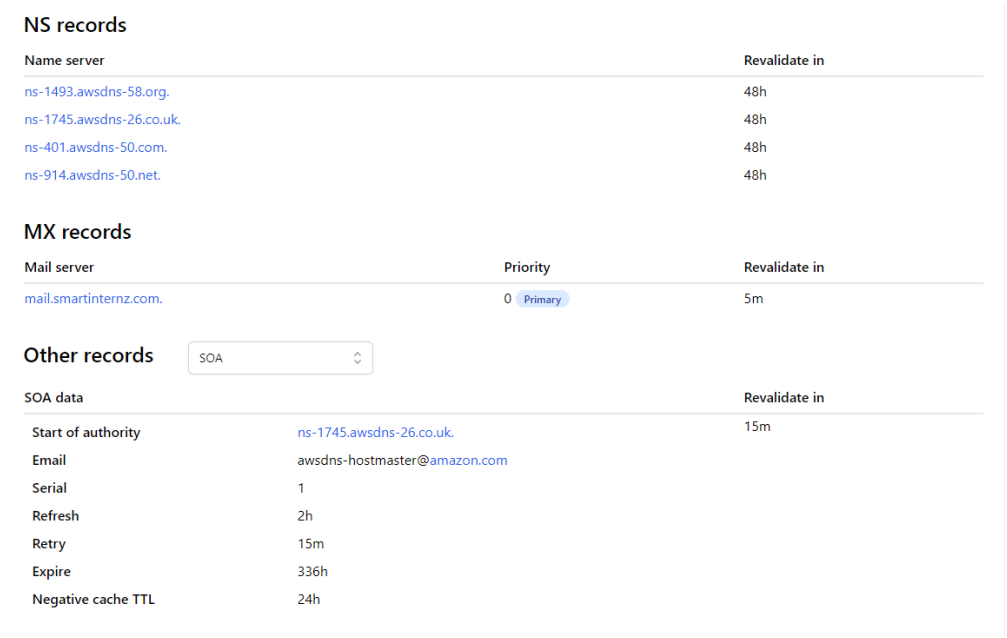
Footprinting and Reconnaissance

NSLookup is a network administration tool for querying the Domain Name System (DNS) to obtain the mapping between domain name and IP address, or other DNS records.

Now I shall use NSLookup to get DNS records of Smartinternz.com.





```
RAW Output
A records

        QUESTION
                dig @ smartinternz.com. A

        ANSWER
                smartinternz.com.       60      A       3.111.252.14
                smartinternz.com.       60      A       35.154.227.143

        AUTHORITY

        ADDITIONAL
                .       0       OPT      ; payload 1232, xrcode 0, version
0, flags 0

AAAA records

        QUESTION
                dig @ smartinternz.com. AAAA

        ANSWER

        AUTHORITY
                smartinternz.com.       900     SOA     ns-1745.awsdns-
26.co.uk. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

        ADDITIONAL
                .       0       OPT      ; payload 1232, xrcode 0, version
0, flags 0

CNAME record

        QUESTION
                dig @ smartinternz.com. CNAME
```

```
        ANSWER

        AUTHORITY
                smartinternz.com.       900     SOA     ns-1745.awsdns-
26.co.uk. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

        ADDITIONAL
                .       0       OPT      ; payload 1232, xrcode 0, version
0, flags 0

TXT records

        QUESTION
                dig @ smartinternz.com. TXT

        ANSWER
                smartinternz.com.       3600    TXT     "v=spf1 a mx ptr
include:secureserver.net ~all"

        AUTHORITY

        ADDITIONAL
                .       0       OPT      ; payload 1232, xrcode 0, version
0, flags 0

NS records

        QUESTION
                dig @ smartinternz.com. NS

        ANSWER
                smartinternz.com.       172800  NS      ns-1493.awsdns-
58.org.
                smartinternz.com.       172800  NS      ns-1745.awsdns-
26.co.uk.
```

```
                smartinternz.com.       172800  NS      ns-401.awsdns-
50.com.
                smartinternz.com.       172800  NS      ns-914.awsdns-
50.net.

        AUTHORITY

        ADDITIONAL
                .       0       OPT      ; payload 1232, xrcode 0, version
0, flags 0

MX records

        QUESTION
                dig @ smartinternz.com. MX

        ANSWER
                smartinternz.com.       300     MX      0
mail.smartinternz.com.

        AUTHORITY

        ADDITIONAL
                .       0       OPT      ; payload 1232, xrcode 0, version
0, flags 0

Other records

        QUESTION
                dig @ smartinternz.com. SOA

        ANSWER
                smartinternz.com.       900     SOA     ns-1745.awsdns-
26.co.uk. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

        AUTHORITY
```

```
        ADDITIONAL
                .       0       OPT      ; payload 1232, xrcode 0, version
0, flags 0
```

From the output of nslookup, we can find out

- The IP addresses of the website
- The Mail servers
- Website is running on AWS
- SOA Data

Analyzing this data will allow us to find vulnerabilities in the website. Then we can use exploit-db to find exploits for the website.