DNS Configuration Check



Contents

[What is DNS? 3](#_Toc144662016)

[Why check the DNS configuration? 3](#_Toc144662017)

[Tools Used 3](#_Toc144662018)

[Results 3](#_Toc144662019)

[Confirmation of Lack of DNSSEC 5](#_Toc144662020)

[Works Cited 5](#_Toc144662021)

# What is DNS?

To put it simply DNS is how users interact with websites, instead of having to remember a random IP address such as 192.168.1.5 in IPv4 or something like 2400:cb00:2048:1::c629:d7a2, we can simply type in the name of a website and access it (for example ebay.com). This makes it easy for people to access websites. (Cloudflare) In this report there will be a few tests run just to determine what the DNS security is on the MOP website and if there are any improvements that could be made to make the website more secure.

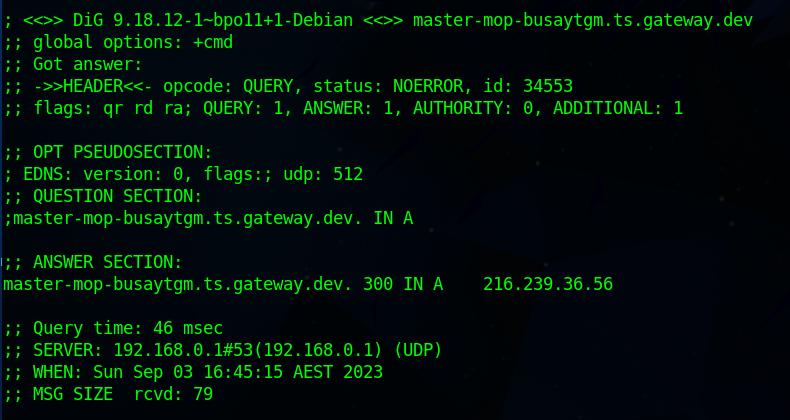
# Why check the DNS configuration?

Checking the DNS configuration is a key step in maintaining security and reliability of any website, as DNS is crucial to connectivity. If there is anything that is misconfigured it could lead to many different vulnerabilities and open a website up to different attacks. By ensuring DNS has been properly configured in the MOP website the web dev team can ensure that there is protection against any DNS related attack (such as spoofing or poisoning) while maintaining a smooth user experience. Checking DNS is staying to proactive and ensuring we are beating attackers to exposing website vulnerabilities.

# Tools Used

* ParrotOS
* ChatGPT
* DiG
* Internet.nl

# Results



To further understand what this response means I consulted ChatGPT.

The first line (Got Answer) is self-explanatory, we did receive a dns response with this query.

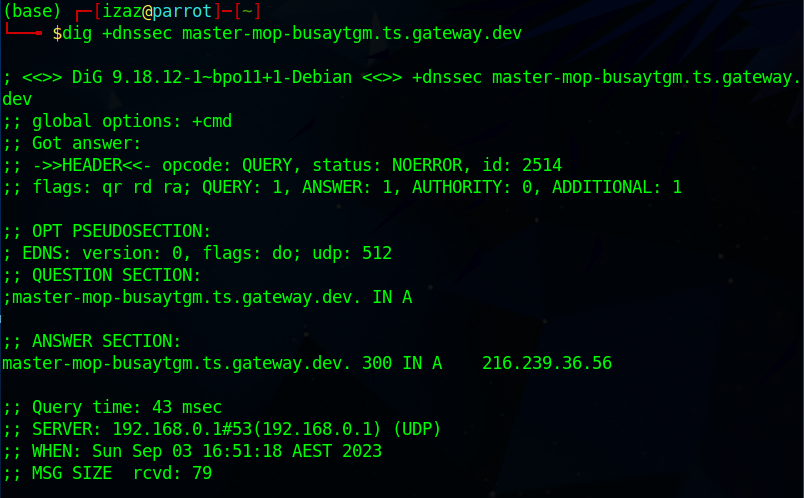
The next line (->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34553) shows that this was a standard query and that there were no errors in processing this. The ID is unique to the query.

Within the next line( flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1 we can see the status flags regarding the DNS query), in this case qr means it is responding to the DNS query that we made with the command, rd (recursion desired) means that we asked the server to look information up for us and ra (recursion available) means that the server can fulfil this request. It also provides us with the one answer regarding the one address we investigated (the MOP Page)

Within the OPT Pseudosection we can see information regarding EDNS (Extension mechanisms for DNS) which can be helpful to find additional information regarding DNS

Finally, we are given the IP address to which the MOP home page belongs to (219.239.36.56)

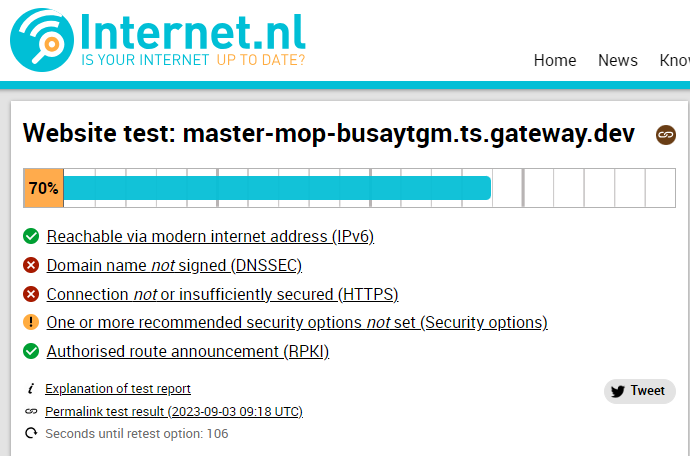
My next test was to ensure that the DNS security extensions were configured as they should be, and the results are as below



While most results are the same as the above test what we can see from the command that I used above the results is that I was trying to disclose the DNSSEC (Domain Name System Security Extensions) however we aren’t able to find any within the response when prompting the server. This can indicate that there is no DNSSEC in place. If it is implemented and hidden that is fine however if it isn’t enabled then that could expose the MOP website to many different vulnerabilities such as DNS Cache Poisoning, Man in the middle attacks, phishing, and DNS hijacking. (AuthenticWeb)

## Confirmation of Lack of DNSSEC

After finding a few tools that Can check for DNSSEC I put the MOP link into there, this scanned the domain and was able to find the Domain name is not signed showing that the website could become vulnerable to these kinds of attacks mentioned above. While implementation of DNSSEC can be time consuming, it is best to invest the time and effort into it as if it were a public website.



# Works Cited

AuthenticWeb. “The Real Risks of Not Deploying DNSSEC.” *Authentic Web*, 5 Feb. 2020, authenticweb.com/domains-dns-and-tls-certificates/the-real-risks-of-not-deploying-dnssec/#:~:text=Without%20DNSSEC%20in%20place%20to. Accessed 3 Sept. 2023.

Cloudflare. “What Is DNS? | How DNS Works.” *Cloudflare*, Cloudflare, 2019, www.cloudflare.com/learning/dns/what-is-dns/.