DMARC report template

No Spoofing Protection on Email Domain

When testing it was found that there was no dmarc record for the domain <target.com>. No record was added and no quarantinee/reject policy was enabled [see it via mxtoolbox and write whatever the case is according to the results]

Overview of the Vulnerability

DMARC policy helps email receiver systems distinguish legitimate and fraudulent emails. If an email doesn't come from an approved domain, the DMARC alerts the receiver systems and tells them how to respond—isolating any potential threats.

Business Impact

If there is no spoofing protection on target website, attacker can impersonate as company and send emails to users from their email. As this vulnerable domain is vulnerable attacker can use this flaw to trick customers reveal victims card details , PII information and eventually lead to fradulent activities and possible account takeover. More impact are:

Higher likelihood of fraudulent financial transactions initiated through deceptive emails, causing direct monetary losses.

Spoofed emails harm the domain's reputation, eroding customer trust and credibility in financial transactions.

Successful email spoofing attacks can lead to immediate financial losses, affecting the organization's bottom line.

Spoofed emails may contain malicious elements, exposing the domain to data breaches and compromising financial information.

Steps to Reproduce

1. Go to ❎ **MX Lookup Tool - Check your DNS MX Records online - MxToolbo...**

2. Search the domain name
3. Verify the misconfigured policy
4. Try sending spoofed email as <target.com> company from using https://www.anonymailer.net/(PoC attached)
5. Verify the issue

Proof of Concept (PoC)

The screenshot(s) below demonstrates the mail server misconfiguration: