SPF messing flag

Background Concept about Missing / insufficient SPF record

- Sender Policy Framework, or SPF, is a technical standard that helps protect email senders and recipients from spam, spoofing, and phishing. It is a form of email authentication.
- Specifically, it defines a way to validate that an email message was sent from an authorized mail server, in order to detect forgery and to prevent spam. It was designed to supplement SMTP, the basic protocol used to send email, because SMTP does not itself include any authentication mechanisms.

2 / 3

domain don't have SPF -> Vulnerable.
domain have SPF -> secure.

What is an SPF record?

- An SPF record is included in an organization's DNS database. An SPF record is a specially-formatted version of a standard DNS TXT record. An SPF record looks something like this:

v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com include:_spf-ssg-a.microsoft.com include:spf-a.hotmail.com ip4:147.243.128.24 ip4:147.243.128.26 ip4:147.243.1.153 ip4:147.243.1.47 ip4:147.243.1.48 -all

3 / 3

How to check that domain have spf Record or Not ?

- Go to - http://www.kitterman.com/spf/validate.html
- Or Go to - https://mxtoolbox.com

Exploitation of SPF

- You can use any fake mailer to forge the mail of a vulnerable domain .
- Go to https://anonymousemail.me/

.... Report ....

SPF/TXT Records

An SPF record is a type of Domain Name Service (DNS) record that identifies which mail servers are permitted to send email on **behalf of your domain**. The purpose of an SPF record is to prevent spammers from sending messages with forged From addresses at your domain.
Checking Missing SPF:-
There Are Various Ways of Checking Missing SPF Records on a website But the Most Common and Popular way is kitterman.com

Steps to Check SPF Records on a website:-
Go to http://www.kitterman.com/spf/validate.html

Enter Target Website simplify.com

If You seem any SPF Record than Domain is Not Vulnerable But if you see Nothing Here then "HURRAY! You Found a Bug"

Attack Scenario & PoC:-

Once There is No SPF Records.

An Attacker Can Spoof Email Via any Fake Mailer Like anonymousemail.me

Attacker Can Send Email From name "Support" and Email: **"support@simplify.com"** With Social Engineering Attack He Can TakeOver User Account

Let Victim Knows the Phishing Attack but When He See The Email from the Authorized Domain.

He Got tricked Easily.