What is Spoofing in cybersecurity | How to do Email Spoofing, Message Spoofing, IP and UserAgent Spoofing

Published on August 5, 2024 by Osama Ellahi

Introduction to Spoofing

Spoofing is mimicking some entity and asking the user to perform certain action according to the intention of an attacker. It includes both technical and non-technical stuff. Mostly it is dependent on the information that you use for tricking the victim. If the information is more related to the victim than there is more chance that he/she can be tricked. Spoofing is a major part of phishing, without better spoofing phishing campaign may result in failure.

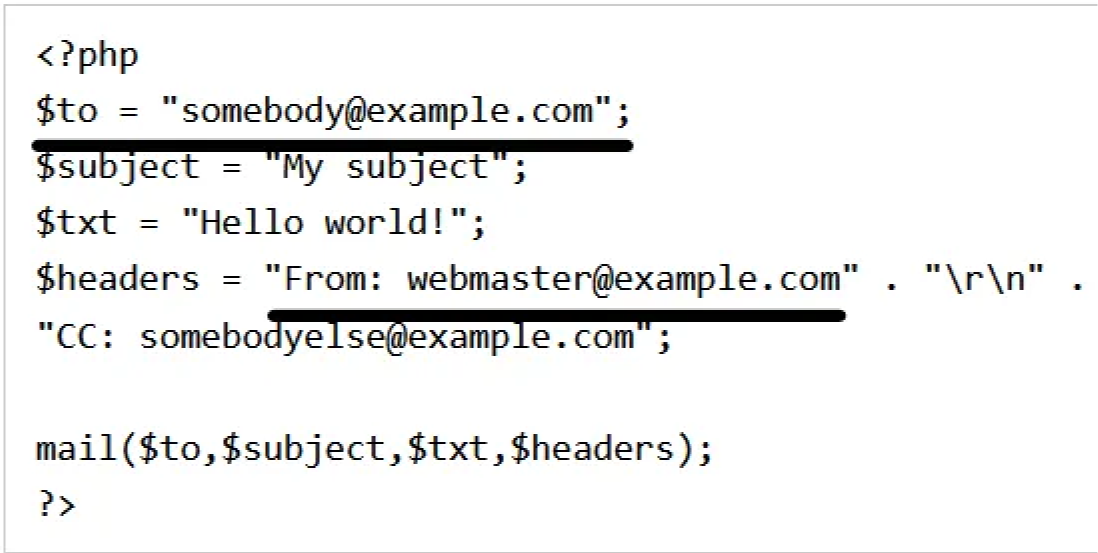
Almost every organization have great security control but when it comes to spoofing every **organization is vulnerable**, just need the right information. In this blog, we will show you how its done and how to mitigate them. Well there is one mitigation that you may have already known which is proper awareness but it needs to be updated because the techniques in phishing are also being updated. Nowadays attackers did not just message you and pretends like your friend and ask for some money, it could be way more worst than that.

Email Spoofing

Cyber criminals use a lot of techniques when it comes to email spoofing because this is the main entry point for their attack path. Email spoofing can be done through many sources, there are public tools available for spoofing. But we will show you the spoofing which will not blocked by the email-gateways because it will be a legitimate email to email-gateways also. Actually lets first understand how the email spoofing is done.

When you are sending email form your public server from "**PHP"** or some other language you have to tell the server put this email in header in place of **"From email"** and send the mail using this following function.

```
mail($to,$subject,$txt,$headers);
```

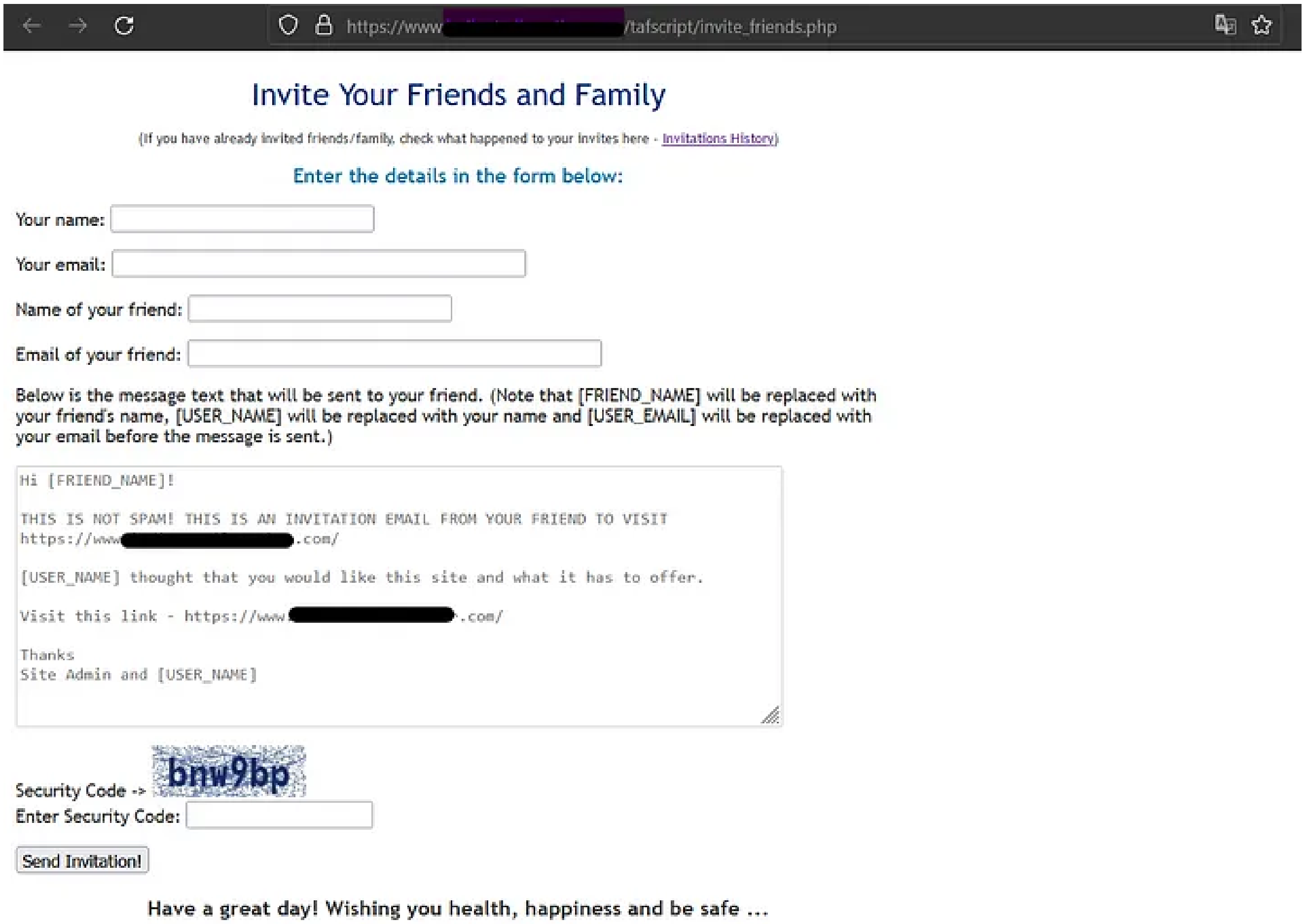


```
<?php
$to = "somebody@example.com";
$subject = "My subject";
$txt = "Hello world!";
$headers = "From: webmaster@example.com" . "\r\n" .
"CC: somebodyelse@example.com";

mail($to,$subject,$txt,$headers);
?>
```

With this function email can be sent from anybody’s email to anyone’s email. But there is some limitation behind it. There is “email-gateway” and “email scanners” who checks every email, when they see that sending mail’s domain is not matching the real server, they mark is suspicious and then this email go to spam or in junk mail box. There are other checks also for email scanning like they even checks the reputation of sending domain and most importantly if email is signed or not. There are flags used for this all process like **DKIM** which is “email receiver will run a **DNS query** to search for the public key for that domain.” **Sender Policy Framework (SPF)** is an email authentication protocol that domain owners use to specify the email servers they send email from, making it harder for fraudsters to spoof sender information.

So this email function could not help us here in email spoofing. But wait, there is legitimate use of the **mail()** function is also there. So lets understand it once again.

Some websites have a API/interface for inviting the friends to there website using email and everyone can send the email to invite the friends. These APIs are vulnerable because the user can even set the **“FROM email”** in headers which makes them dangerous.



https://www[redacted]/tafscript/invite_friends.php

Invite Your Friends and Family

(If you have already invited friends/family, check what happened to your invites here - Invitations History)

Enter the details in the form below:

Your name:

Your email:

Name of your friend:

Email of your friend:

Below is the message text that will be sent to your friend. (Note that [FRIEND_NAME] will be replaced with your friend's name, [USER_NAME] will be replaced with your name and [USER_EMAIL] will be replaced with your email before the message is sent.)

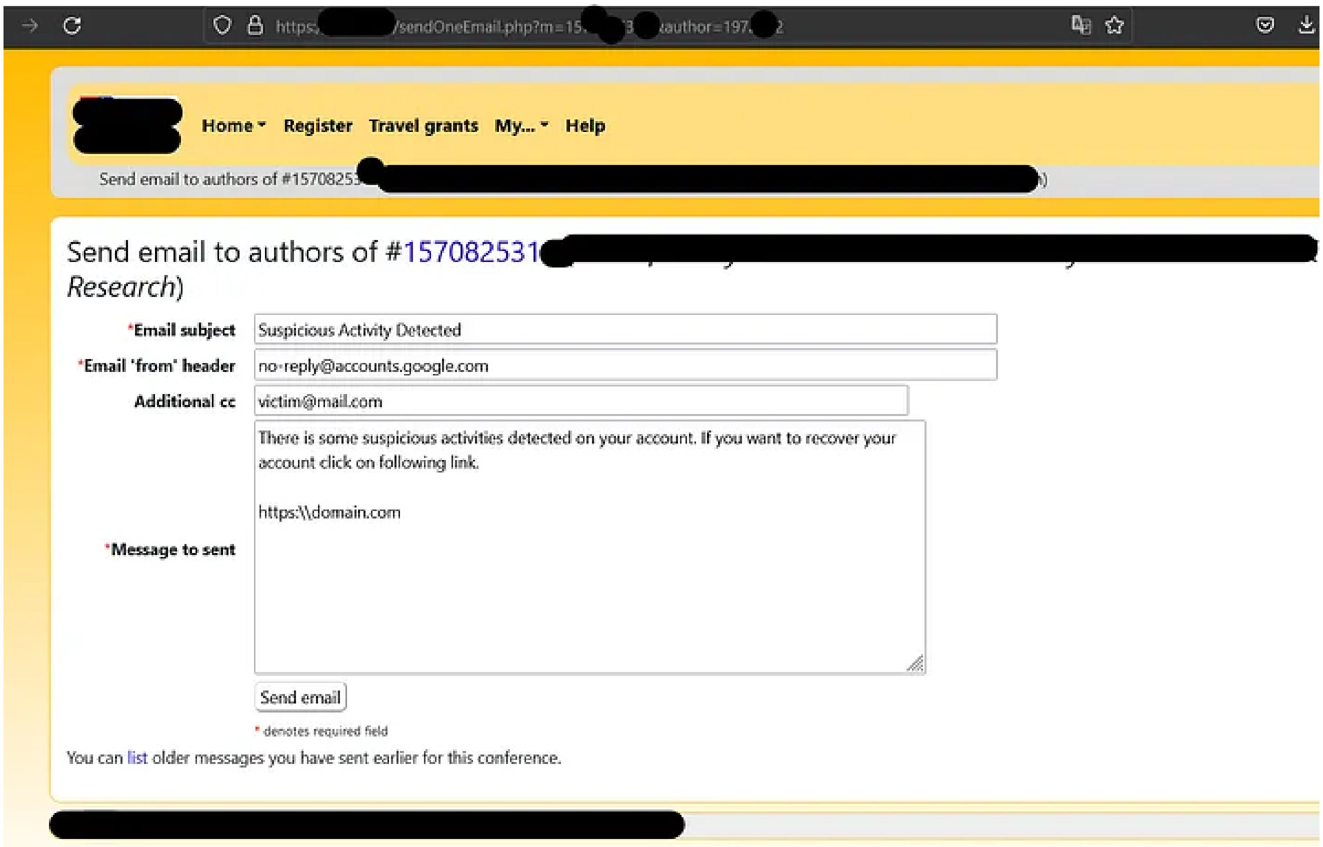
```
Hi [FRIEND_NAME]!

THIS IS NOT SPAM! THIS IS AN INVITATION EMAIL FROM YOUR FRIEND TO VISIT
https://www[redacted].com/

[USER_NAME] thought that you would like this site and what it has to offer.

Visit this link - https://www[redacted].com/

Thanks
Site Admin and [USER_NAME]
```

Security Code -> bnw9bp

Enter Security Code:

Have a great day! Wishing you health, happiness and be safe ...

This is not only one case, there are thousands of websites publicly available and open for attackers. Like look at this case this website required a user to signup and it is actually a well known conference by famous publishers. **For test case we send a dummy paper.**


https:[redacted]/sendOneEmail.php?m=15[redacted]3[redacted]author=197[redacted]2
[redacted]
Home
Register
Travel grants
My...
Help

Send email to authors of #1570825[redacted])

Send email to authors of #157082531[redacted] *Research*)

*Email subject	Suspicious Activity Detected
*Email 'from' header	no-reply@accounts.google.com
Additional cc	victim@mail.com
*Message to sent	There is some suspicious activities detected on your account. If you want to recover your account click on following link. https:\\domain.com

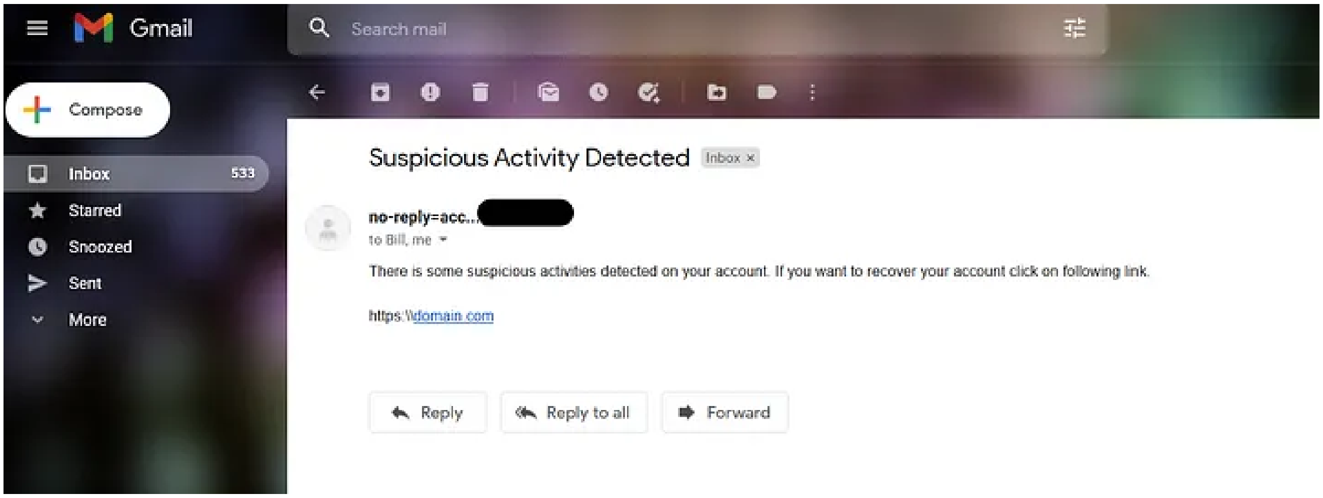
Send email

* denotes required field

You can list older messages you have sent earlier for this conference.

[redacted]

These message comes straight to your **inbox.**



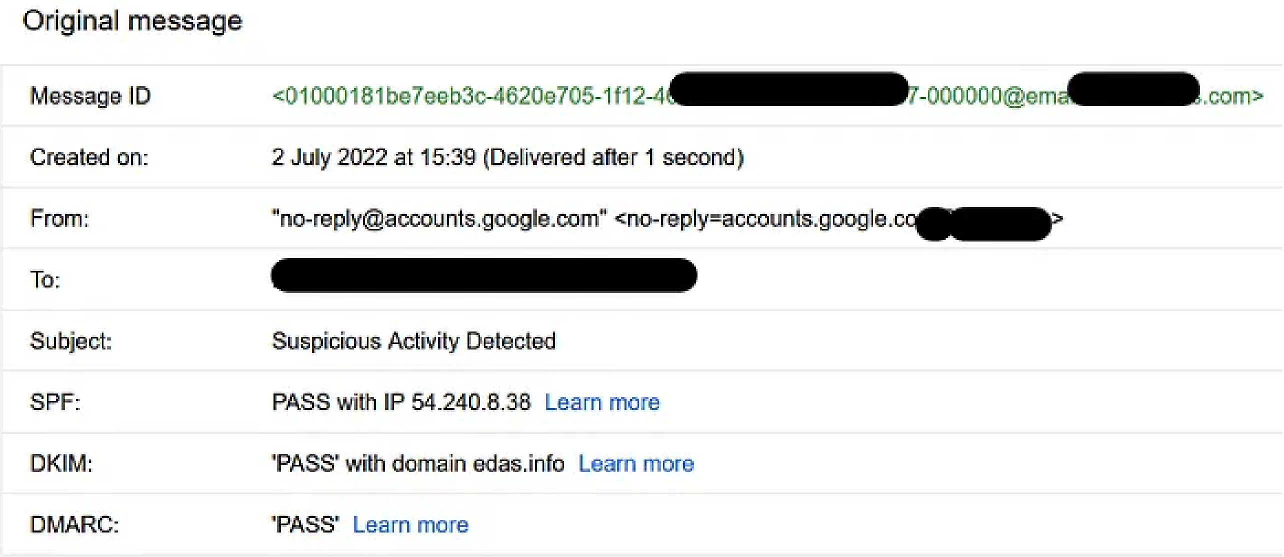
Suspicious Activity Detected Inbox ×

no-reply=acc...[redacted]
to Bill, me

There is some suspicious activities detected on your account. If you want to recover your account click on following link.

https:\\domain.com

Now lets look at the original message of over mail. As you can see it shows nothing malicious because the message is signed by the website and it also have some popularity. You can also see the flags and subject of mail which we send **“Suspicious Activity Detected”**. By the way you need to avoid some words like “**suspicious**” and “click on link” etc to get more accuracy.



Original message

Message ID	<01000181be7eeb3c-4620e705-1f12-4[redacted]7-000000@ema[redacted].com>
Created on:	2 July 2022 at 15:39 (Delivered after 1 second)
From:	"no-reply@accounts.google.com" <no-reply=accounts.google.co[redacted]>
To:	[redacted]
Subject:	Suspicious Activity Detected
SPF:	PASS with IP 54.240.8.38 Learn more
DKIM:	'PASS' with domain edas.info Learn more
DMARC:	'PASS' Learn more

In this mail still they are sending their domain name which may looks suspicious for some users. But there are thousands of websites who works very fine with spoofing.

Message Spoofing

We sometimes see a suspicious message that comes form legitimate number, so start believing that it is not suspicious. Like let me give you a practical example here the OTP (One Time Pass-code) that you have set up for Facebook or google or some other domains, they send you message from **56789**. Using online messaging services we can send message anybody from **“56789”**. This shows that this number did not belong to any entity and everyone can use it for their own benefits.

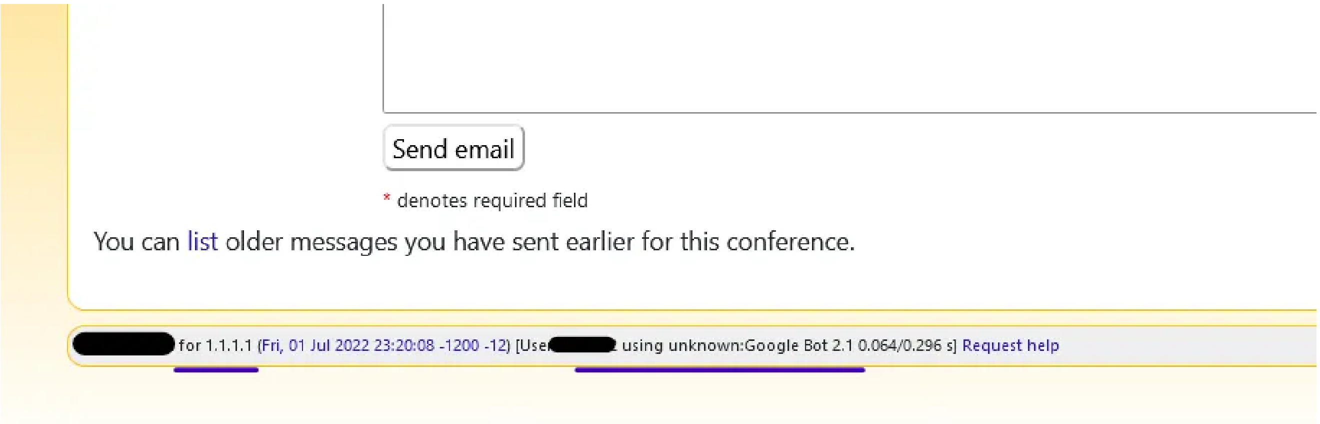
Only thing that can be copyright is the name like if you see a message from “Google” that might be legitimate. But some attackers can even bypass human eye with character playing. Like they can send you message from **“g00gle” or “G00GLE”**. For demo you can use any online messaging service.

IP and UserAgent Spoofing

The request identifies the user. If user is using a browser there will be a user agent which tells the server that user is using which browser, which OS and which version of (OS / browser). But when it comes to IP, some servers use them for identification and logs. Like if an attack happened on a organization, there will be IP which tell the location of the user. Yes and attacker might be using VPN but let me show you another very interesting aspect of it which is IP spoofing. There are IPs that be set up in your browser and some servers use these IPs as the primary source of the user information. These are called **X-Forwarded-For.**

The **X-Forwarded-For (XFF)** request header is a de-facto standard header for identifying the originating IP address of a client connecting to a web server through a proxy server.The amazing part it if we can change them to whatever we want, we can set our XFF to Google's public IP or even our victim's public IP.

And user-agent can also be easily changed, if you are sending the request from any programming language you can set user-agent to whatever you want, if you are using browser there are add-ons and extension available just search **"user-agent switcher"** and you are good to go. Lets see this example it is same example from email spoofing. So apparently they are even recording my IP and user agent also for the record.

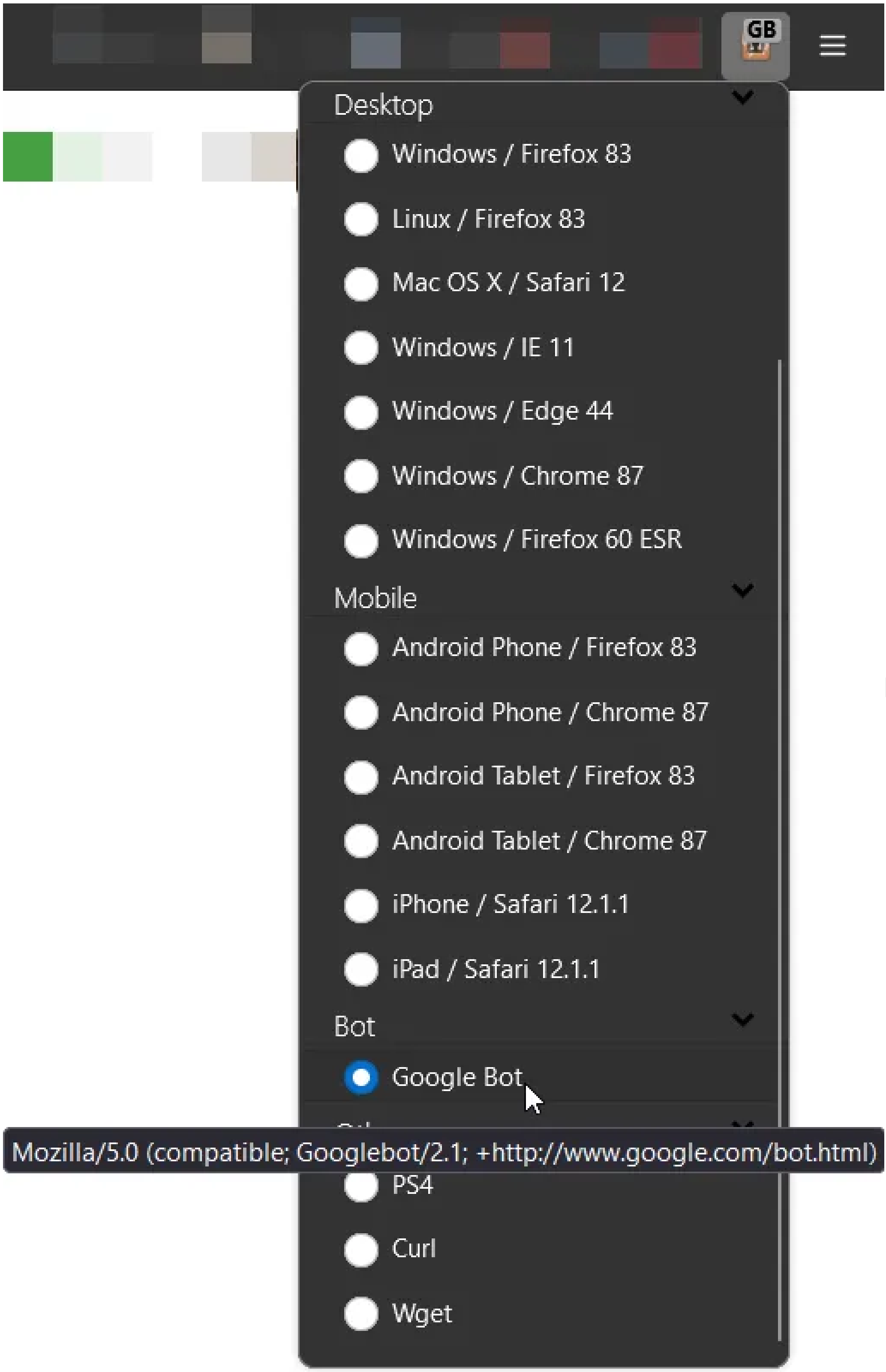


* denotes required field

You can list older messages you have sent earlier for this conference.

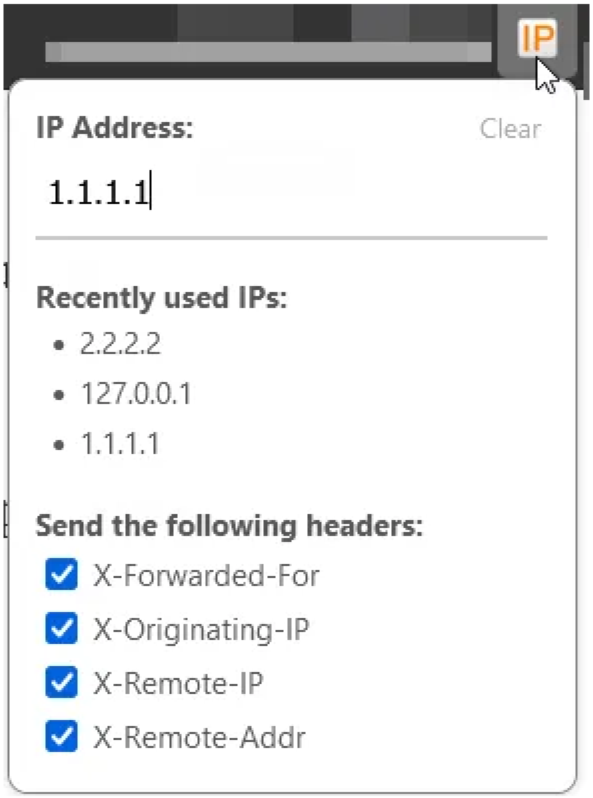
[redacted] for 1.1.1.1 (Fri, 01 Jul 2022 23:20:08 -1200 -12) [Use[redacted] using unknown:Google Bot 2.1 0.064/0.296 s] Request help

For user-agent switching we use **"user-agent switcher"** and set me like we are **Google Bot.**



Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

For IP switching we use **“X-Forwarder-For header”**. But keep in mind if server is getting the real client IP it can’t be changed only **x-forwarded-For, X-Origininating-IP, X-Remote-IP and X-Remote-Addr** can be changed because these are send in request headers.



IP Address: Clear

1.1.1.1

Recently used IPs:

- 2.2.2.2
- 127.0.0.1
- 1.1.1.1

Send the following headers:

☑ X-Forwarded-For

☑ X-Originating-IP

☑ X-Remote-IP

☑ X-Remote-Addr

Views: 220