Assignment 3

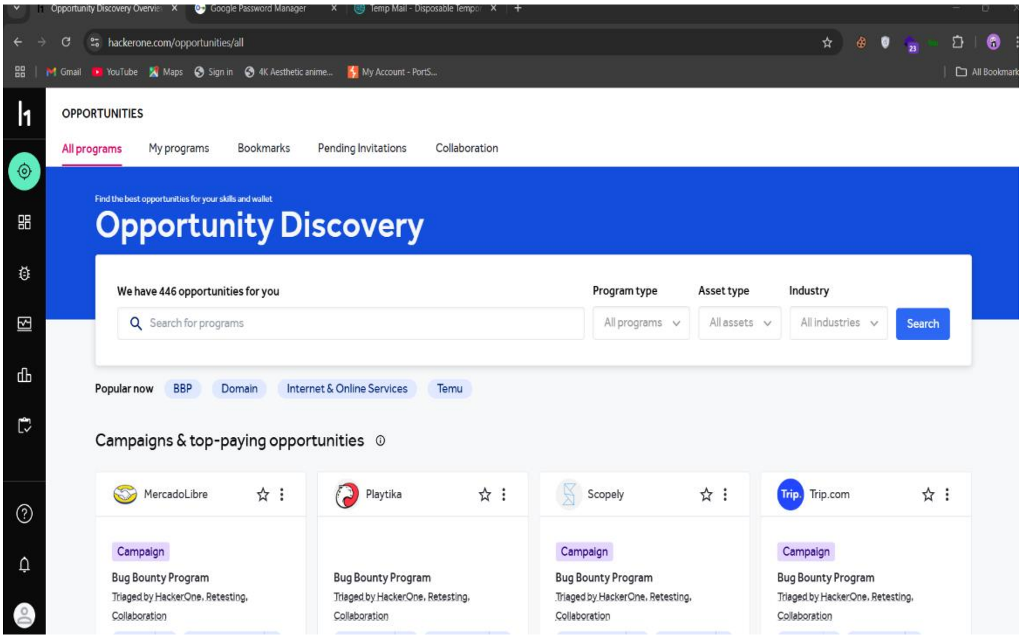
TASK -1:

1. TITLE: Find Subdomains for Any 3 targets that you need to select targets from the HackerOne platform.

2. OBJECTIVE OF TASK: to retrieve the information of subdomains for the any 3 targets in the HackerOne platform using the various subdomains finding tools and websites. This was done in the phase of information gathering

3. STEP BY STEP PROCEDURE:

   1. OPEN THE WEBSITE: https://hackerone.com

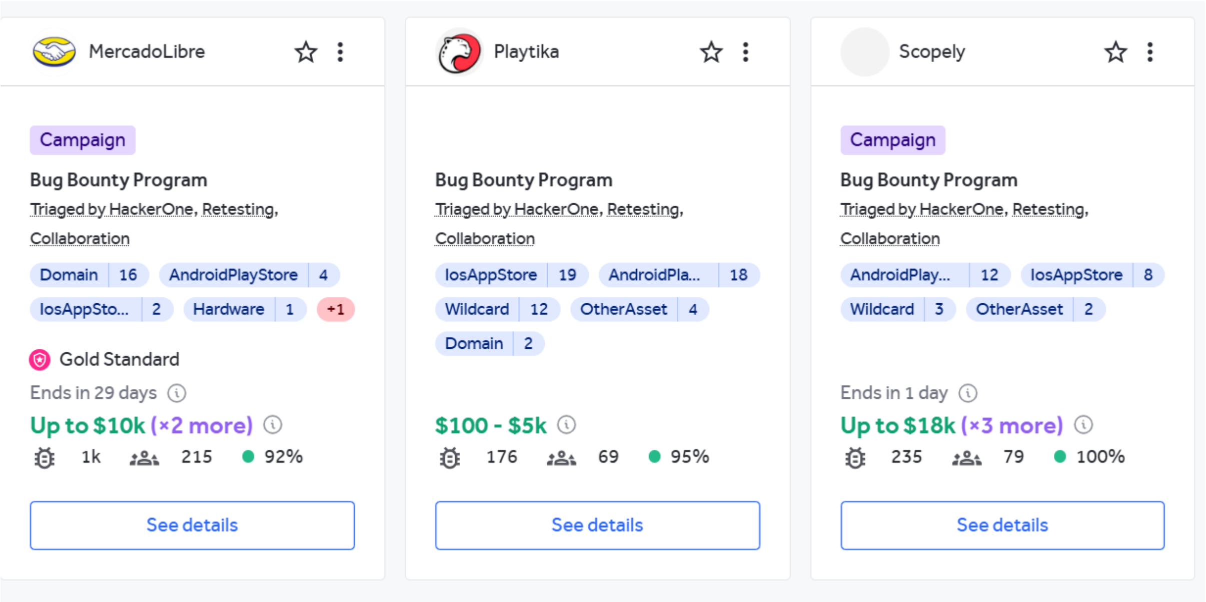


   2. NOW SELECT THE 3 TARGETED WEBSITES:

      TARGET 1: https://www.mercadolibre.com

      TARGET 2: https://www.playtika.com

      TARGET 3: https://www.scopely.com



MercadoLibre

Campaign

Bug Bounty Program

Triaged by HackerOne, Retesting, Collaboration

Domain 16 | AndroidPlayStore 4 | IosAppSto... 2 | Hardware 1 | +1

Gold Standard

Ends in 29 days

Up to $10k (×2 more)

1k 215 ● 92%

See details

Playtika

Bug Bounty Program

Triaged by HackerOne, Retesting, Collaboration

IosAppStore 19 | AndroidPla... 18 | Wildcard 12 | OtherAsset 4 | Domain 2

$100 - $5k

176 69 ● 95%

See details

Scopely

Campaign

Bug Bounty Program

Triaged by HackerOne, Retesting, Collaboration

AndroidPlay... 12 | IosAppStore 8 | Wildcard 3 | OtherAsset 2

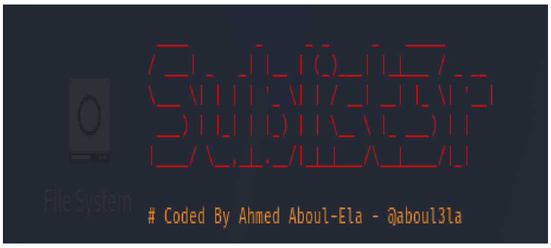
Ends in 1 day

Up to $18k (×3 more)

235 79 ● 100%

See details

3. Now go to the kali Linux and install the sublist3r to find subdomains



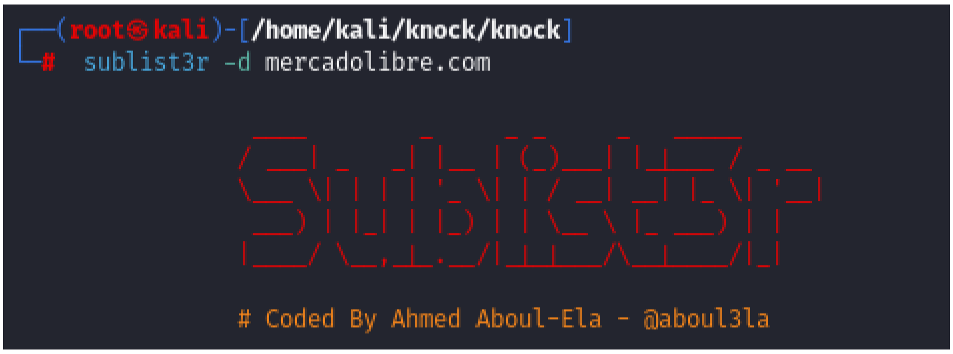
```
# Coded By Ahmed Aboul-Ela - @aboul3la
```

4. Now write command of sublist3r to run on kali with website url to find all sub domains.

SYNTAX: sublist3r -d –url--

Now for target 1:

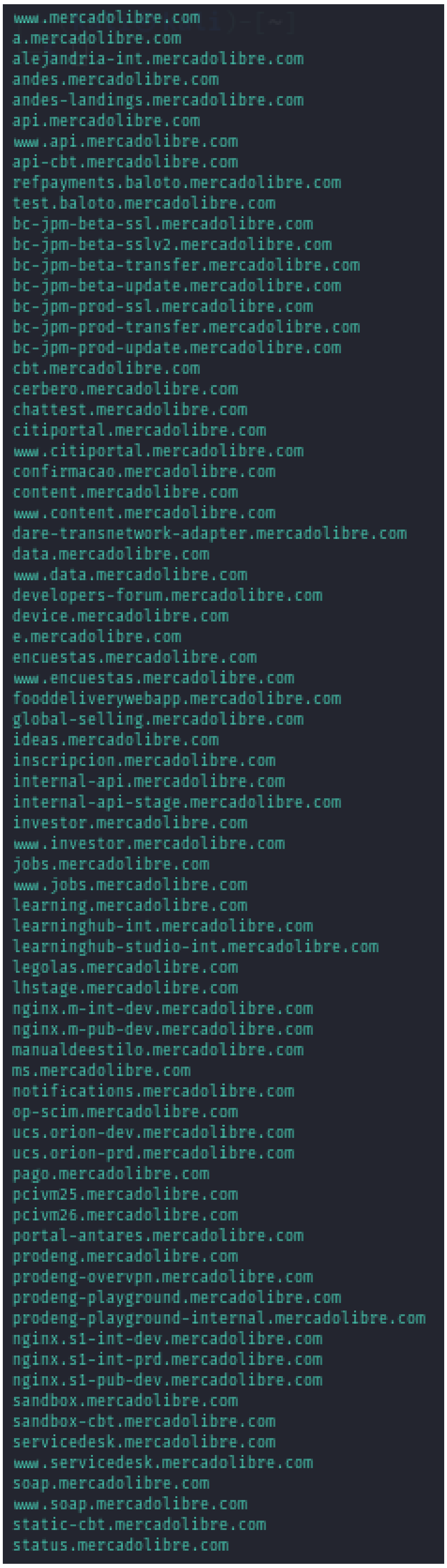
The command implementation:



```
┌──(root㉿kali)-[/home/kali/knock/knock]
└─#  sublist3r -d mercadolibre.com

                 ____        _     _ _     _   _____
                / ___| _   _| |__ | (_)___| |_|___ / _ __
                \___ \| | | | '_ \| | / __| __| |_ \| '__|
                 ___) | |_| | |_) | | \__ \ |_ ___) | |
                |____/ \__,_|_.__/|_|_|___/\__|____/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la
```

The output for the target 1:

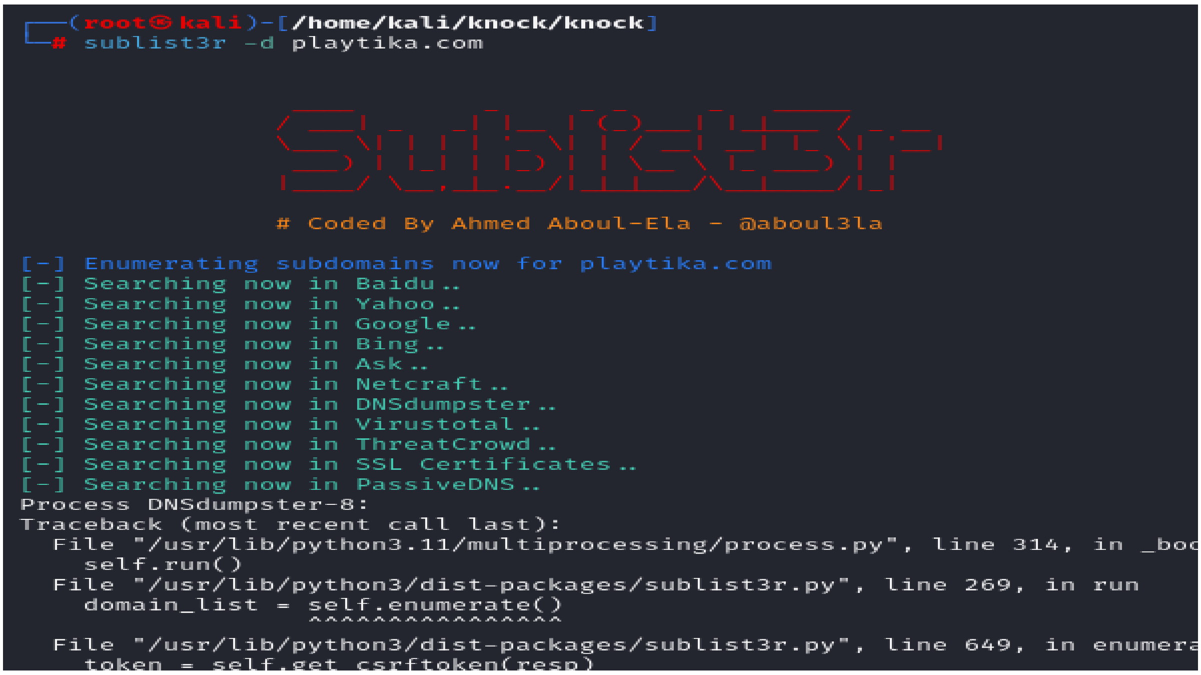
In this we retrieve the subdomains of the respected target websites



```
www.mercadolibre.com
a.mercadolibre.com
alejandria-int.mercadolibre.com
andes.mercadolibre.com
andes-landings.mercadolibre.com
api.mercadolibre.com
www.api.mercadolibre.com
api-cbt.mercadolibre.com
refpayments.baloto.mercadolibre.com
test.baloto.mercadolibre.com
bc-jpm-beta-ssl.mercadolibre.com
bc-jpm-beta-sslv2.mercadolibre.com
bc-jpm-beta-transfer.mercadolibre.com
bc-jpm-beta-update.mercadolibre.com
bc-jpm-prod-ssl.mercadolibre.com
bc-jpm-prod-transfer.mercadolibre.com
bc-jpm-prod-update.mercadolibre.com
cbt.mercadolibre.com
cerbero.mercadolibre.com
chattest.mercadolibre.com
citiportal.mercadolibre.com
www.citiportal.mercadolibre.com
confirmacao.mercadolibre.com
content.mercadolibre.com
www.content.mercadolibre.com
dare-transnetwork-adapter.mercadolibre.com
data.mercadolibre.com
www.data.mercadolibre.com
developers-forum.mercadolibre.com
device.mercadolibre.com
e.mercadolibre.com
encuestas.mercadolibre.com
www.encuestas.mercadolibre.com
fooddeliverywebapp.mercadolibre.com
global-selling.mercadolibre.com
ideas.mercadolibre.com
inscripcion.mercadolibre.com
internal-api.mercadolibre.com
internal-api-stage.mercadolibre.com
investor.mercadolibre.com
www.investor.mercadolibre.com
jobs.mercadolibre.com
www.jobs.mercadolibre.com
learning.mercadolibre.com
learninghub-int.mercadolibre.com
learninghub-studio-int.mercadolibre.com
legolas.mercadolibre.com
lhstage.mercadolibre.com
nginx.m-int-dev.mercadolibre.com
nginx.m-pub-dev.mercadolibre.com
manualdeestilo.mercadolibre.com
ms.mercadolibre.com
notifications.mercadolibre.com
op-scim.mercadolibre.com
ucs.orion-dev.mercadolibre.com
ucs.orion-prd.mercadolibre.com
pago.mercadolibre.com
pcivm25.mercadolibre.com
pcivm26.mercadolibre.com
portal-antares.mercadolibre.com
prodeng.mercadolibre.com
prodeng-overvpn.mercadolibre.com
prodeng-playground.mercadolibre.com
prodeng-playground-internal.mercadolibre.com
nginx.s1-int-dev.mercadolibre.com
nginx.s1-int-prd.mercadolibre.com
nginx.s1-pub-dev.mercadolibre.com
sandbox.mercadolibre.com
sandbox-cbt.mercadolibre.com
servicedesk.mercadolibre.com
www.servicedesk.mercadolibre.com
soap.mercadolibre.com
www.soap.mercadolibre.com
static-cbt.mercadolibre.com
status.mercadolibre.com
```

Now for target 2:

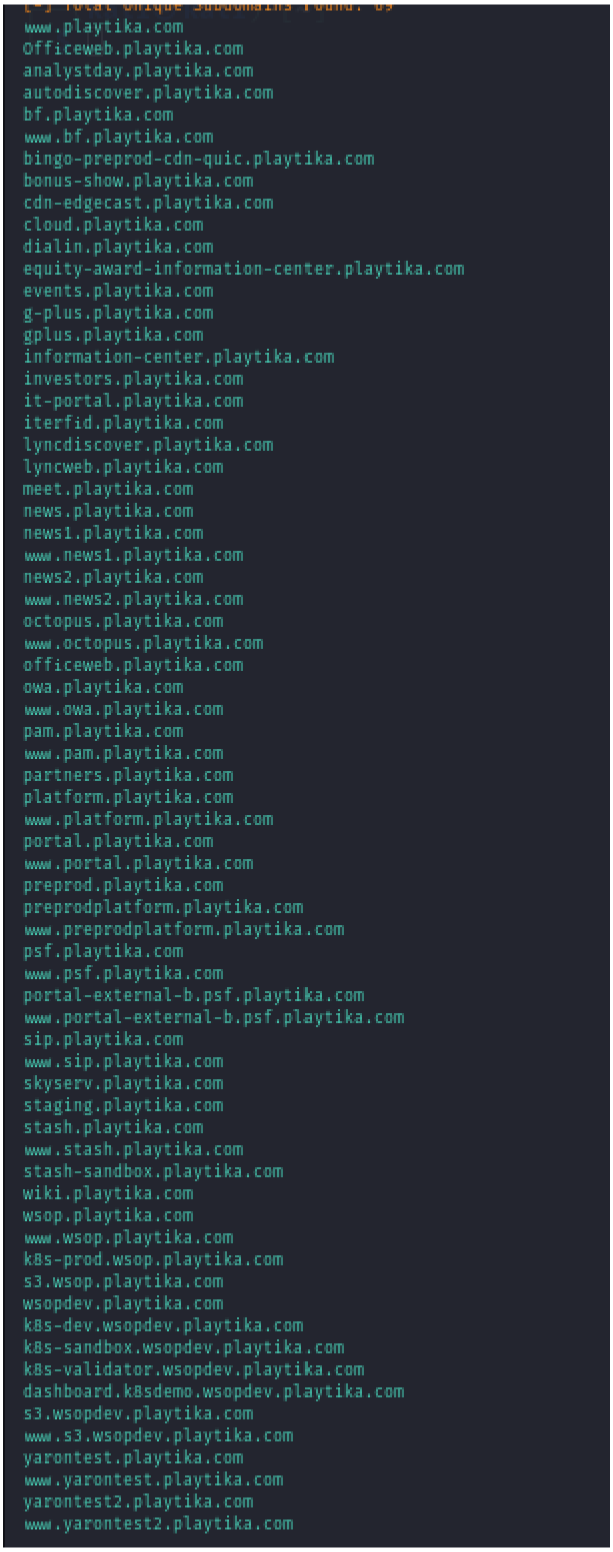
The command implementation:



```
┌──(root㉿kali)-[/home/kali/knock/knock]
└─# sublist3r -d playtika.com


                 ____        _     _ _     _   _____
                / ___| _   _| |__ | (_)___| |_|___ / _ __
                \___ \| | | | '_ \| | / __| __| |_ \| '__|
                 ___) | |_| | |_) | | \__ \ |_ ___) | |
                |____/ \__,_|_.__/|_|_|___/\__|____/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for playtika.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
Process DNSdumpster-8:
Traceback (most recent call last):
  File "/usr/lib/python3.11/multiprocessing/process.py", line 314, in _boo
    self.run()
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 269, in run
    domain_list = self.enumerate()
                  ^^^^^^^^^^^^^^^^

  File "/usr/lib/python3/dist-packages/sublist3r.py", line 649, in enumera
    token = self.get_csrftoken(resp)
```

Now output of the 2nd target :

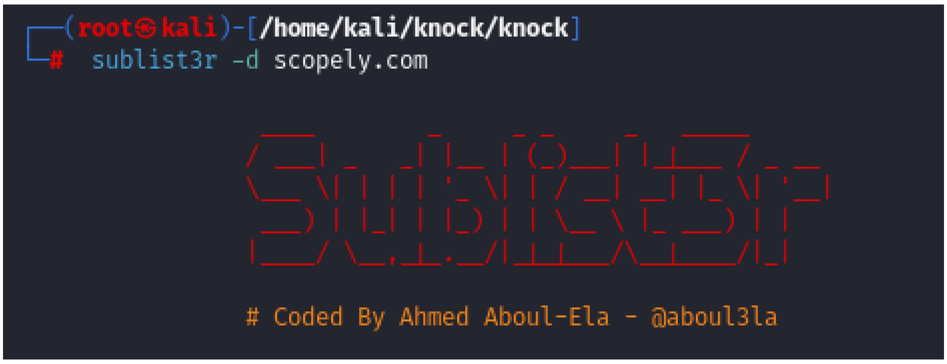
In this we retrieve the subdomains of the respected target websites



```
[-] Total Unique Subdomains Found: 69
www.playtika.com
Officeweb.playtika.com
analystday.playtika.com
autodiscover.playtika.com
bf.playtika.com
www.bf.playtika.com
bingo-preprod-cdn-quic.playtika.com
bonus-show.playtika.com
cdn-edgecast.playtika.com
cloud.playtika.com
dialin.playtika.com
equity-award-information-center.playtika.com
events.playtika.com
g-plus.playtika.com
gplus.playtika.com
information-center.playtika.com
investors.playtika.com
it-portal.playtika.com
iterfid.playtika.com
lyncdiscover.playtika.com
lyncweb.playtika.com
meet.playtika.com
news.playtika.com
news1.playtika.com
www.news1.playtika.com
news2.playtika.com
www.news2.playtika.com
octopus.playtika.com
www.octopus.playtika.com
officeweb.playtika.com
owa.playtika.com
www.owa.playtika.com
pam.playtika.com
www.pam.playtika.com
partners.playtika.com
platform.playtika.com
www.platform.playtika.com
portal.playtika.com
www.portal.playtika.com
preprod.playtika.com
preprodplatform.playtika.com
www.preprodplatform.playtika.com
psf.playtika.com
www.psf.playtika.com
portal-external-b.psf.playtika.com
www.portal-external-b.psf.playtika.com
sip.playtika.com
www.sip.playtika.com
skyserv.playtika.com
staging.playtika.com
stash.playtika.com
www.stash.playtika.com
stash-sandbox.playtika.com
wiki.playtika.com
wsop.playtika.com
www.wsop.playtika.com
k8s-prod.wsop.playtika.com
s3.wsop.playtika.com
wsopdev.playtika.com
k8s-dev.wsopdev.playtika.com
k8s-sandbox.wsopdev.playtika.com
k8s-validator.wsopdev.playtika.com
dashboard.k8sdemo.wsopdev.playtika.com
s3.wsopdev.playtika.com
www.s3.wsopdev.playtika.com
yarontest.playtika.com
www.yarontest.playtika.com
yarontest2.playtika.com
www.yarontest2.playtika.com
```

Now for target 3:

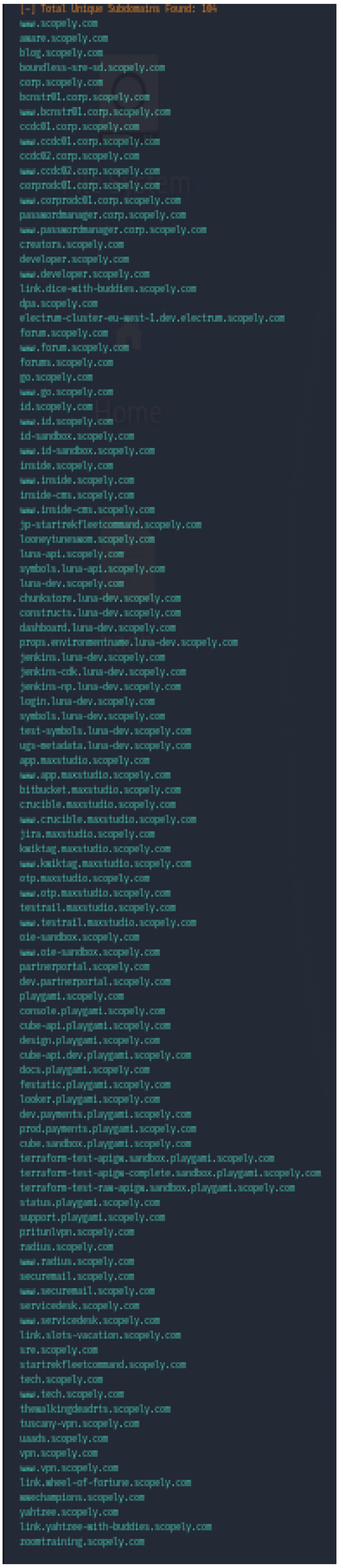
The command implementation:



```
┌──(root㉿kali)-[/home/kali/knock/knock]
└─# sublist3r -d scopely.com

                 ____        _     _ _     _   _____
                / ___| _   _| |__ | (_)___| |_|___ / _ __
                \___ \| | | | '_ \| | / __| __| |_ \| '__|
                 ___) | |_| | |_) | | \__ \ |_ ___) | |
                |____/ \__,_|_.__/|_|_|___/\__|____/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la
```

Now output of the 3rd target:

In this we retrieve the subdomains of the respected target websites



```
[-] Total Unique Subdomains Found: 104
www.scopely.com
aware.scopely.com
blog.scopely.com
boundless-sre-sd.scopely.com
corp.scopely.com
bcnstr01.corp.scopely.com
www.bcnstr01.corp.scopely.com
ccdc01.corp.scopely.com
www.ccdc01.corp.scopely.com
ccdc02.corp.scopely.com
www.ccdc02.corp.scopely.com
corprodc01.corp.scopely.com
www.corprodc01.corp.scopely.com
passwordmanager.corp.scopely.com
www.passwordmanager.corp.scopely.com
creators.scopely.com
developer.scopely.com
www.developer.scopely.com
link.dice-with-buddies.scopely.com
dps.scopely.com
electrum-cluster-eu-west-1.dev.electrum.scopely.com
forum.scopely.com
www.forum.scopely.com
forums.scopely.com
go.scopely.com
www.go.scopely.com
id.scopely.com
www.id.scopely.com
id-sandbox.scopely.com
www.id-sandbox.scopely.com
inside.scopely.com
www.inside.scopely.com
inside-cms.scopely.com
www.inside-cms.scopely.com
jp-startrekfleetcommand.scopely.com
looneytuneswom.scopely.com
luna-api.scopely.com
symbols.luna-api.scopely.com
luna-dev.scopely.com
chunkstore.luna-dev.scopely.com
constructs.luna-dev.scopely.com
dashboard.luna-dev.scopely.com
props.environmentname.luna-dev.scopely.com
jenkins.luna-dev.scopely.com
jenkins-cdk.luna-dev.scopely.com
jenkins-np.luna-dev.scopely.com
login.luna-dev.scopely.com
symbols.luna-dev.scopely.com
test-symbols.luna-dev.scopely.com
ugs-metadata.luna-dev.scopely.com
app.maxstudio.scopely.com
www.app.maxstudio.scopely.com
bitbucket.maxstudio.scopely.com
crucible.maxstudio.scopely.com
www.crucible.maxstudio.scopely.com
jira.maxstudio.scopely.com
kaiktag.maxstudio.scopely.com
www.kaiktag.maxstudio.scopely.com
otp.maxstudio.scopely.com
www.otp.maxstudio.scopely.com
testrail.maxstudio.scopely.com
www.testrail.maxstudio.scopely.com
oie-sandbox.scopely.com
www.oie-sandbox.scopely.com
partnerportal.scopely.com
dev.partnerportal.scopely.com
playgami.scopely.com
console.playgami.scopely.com
cube-api.playgami.scopely.com
design.playgami.scopely.com
cube-api.dev.playgami.scopely.com
docs.playgami.scopely.com
festatic.playgami.scopely.com
looker.playgami.scopely.com
dev.payments.playgami.scopely.com
prod.payments.playgami.scopely.com
cube.sandbox.playgami.scopely.com
terraform-test-apigw.sandbox.playgami.scopely.com
terraform-test-apigw-complete.sandbox.playgami.scopely.com
terraform-test-raw-apigw.sandbox.playgami.scopely.com
status.playgami.scopely.com
support.playgami.scopely.com
pritunlvpn.scopely.com
radius.scopely.com
www.radius.scopely.com
securemail.scopely.com
www.securemail.scopely.com
servicedesk.scopely.com
www.servicedesk.scopely.com
link.slots-vacation.scopely.com
sre.scopely.com
startrekfleetcommand.scopely.com
tech.scopely.com
www.tech.scopely.com
thewalkingdeadrts.scopely.com
tuscany-vpn.scopely.com
uaads.scopely.com
vpn.scopely.com
www.vpn.scopely.com
link.wheel-of-fortune.scopely.com
wwechampions.scopely.com
yahtzee.scopely.com
link.yahtzee-with-buddies.scopely.com
zoomtraining.scopely.com
```

4. Conclusion: here we scan the websites one after one and it shows the results of the subdomains of their own respective domain here we use the sublist3r scan to find all sub domains. Here I concluded that the three targets have subdomains.

5. Summary of the task: the summary of the task is here we select the targets from the hackerone website and scan the three websites or targets using **sublist3r** tool in kali which gives the subdomains of given website it will help in information gathering for the attacker to access and known the subdomains of the target

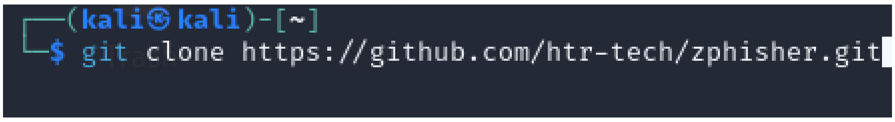
TASK-2:

1. Title: Create a fake login page for 3 social media handles given below and detect if the link is malicious or not, using tools like Virustotal or Netcraft extension.

2. Objective of the Task: to make a fake phishing links of applications like Gmail, microsoft365, LinkedIn to gather information from the target by acting our phishing link as a real application link, so that he can add his details or information.

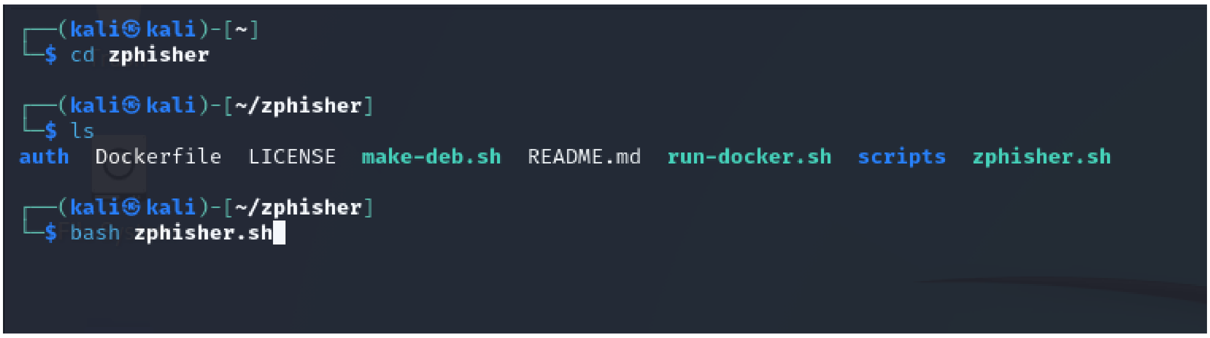
3. step by step procedure:

1. Now go to the Kali Linux and go to command prompt and install the Zphishers in the github



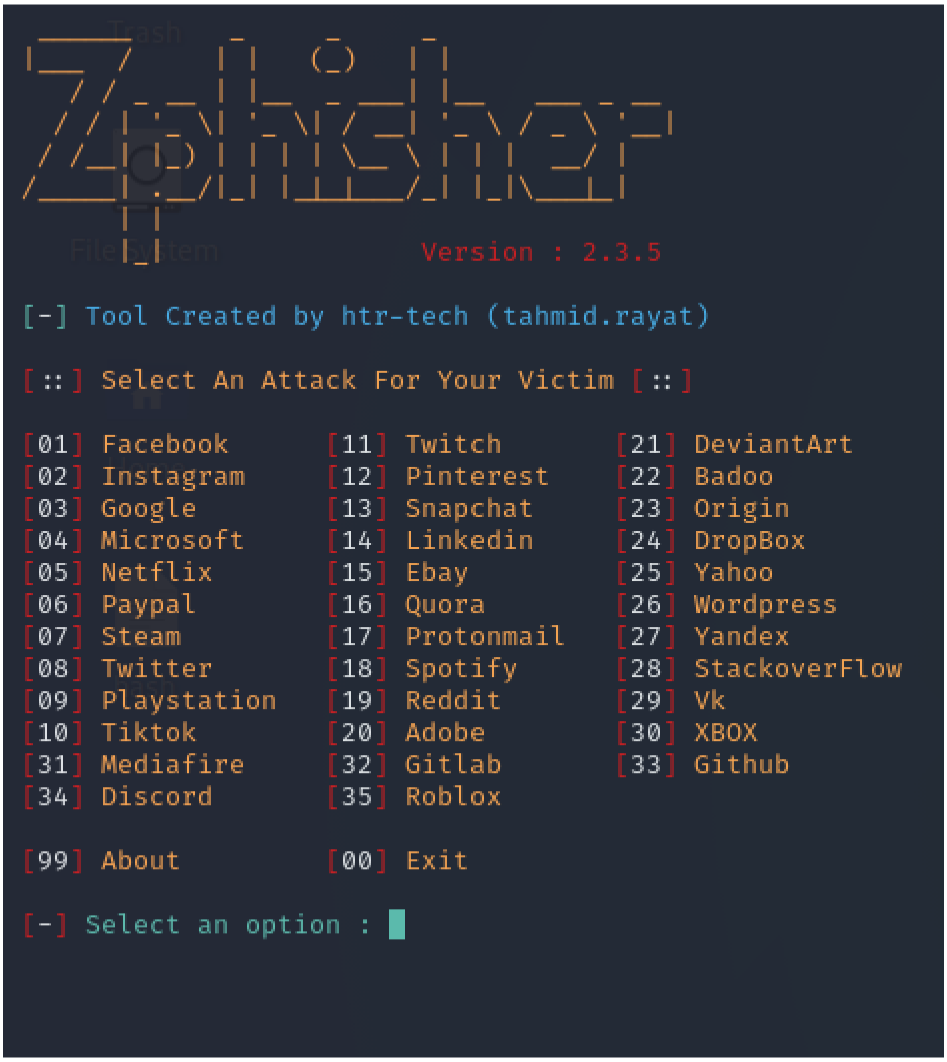
```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/htr-tech/zphisher.git
```

2. Now go to the zphisher tool and run the zphisher using below displayed way



```
┌──(kali㉿kali)-[~]
└─$ cd zphisher

┌──(kali㉿kali)-[~/zphisher]
└─$ ls
auth  Dockerfile  LICENSE  make-deb.sh  README.md  run-docker.sh  scripts  zphisher.sh

┌──(kali㉿kali)-[~/zphisher]
└─$ bash zphisher.sh
```

3. Now we run the zphisher it display as like below mentioned way of interface



```
                              Version : 2.3.5

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook        [11] Twitch          [21] DeviantArt
[02] Instagram       [12] Pinterest       [22] Badoo
[03] Google          [13] Snapchat        [23] Origin
[04] Microsoft       [14] Linkedin        [24] DropBox
[05] Netflix         [15] Ebay            [25] Yahoo
[06] Paypal          [16] Quora           [26] Wordpress
[07] Steam           [17] Protonmail      [27] Yandex
[08] Twitter         [18] Spotify         [28] StackoverFlow
[09] Playstation     [19] Reddit          [29] Vk
[10] Tiktok          [20] Adobe           [30] XBOX
[31] Mediafire       [32] Gitlab          [33] Github
[34] Discord         [35] Roblox

[99] About           [00] Exit

[-] Select an option :
```

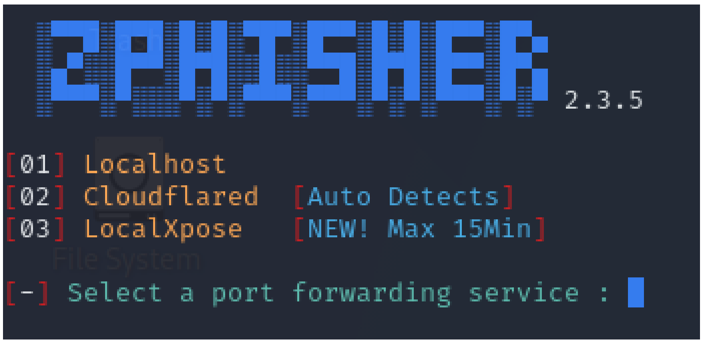
4. Now here we get three profiles phishing links to build

SECTION 1:

1. Now build the phishing link for LinkedIn

2. Go to the zphisher and select option “14”

3. Now after select of option we get interface to select url type

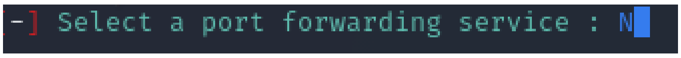


```
  ZPHISHER 2.3.5

[01] Localhost
[02] Cloudflared  [Auto Detects]
[03] LocalXpose   [NEW! Max 15Min]

[-] Select a port forwarding service :
```

4. Here we select the option 2 for cloudflared links for generate phishing links

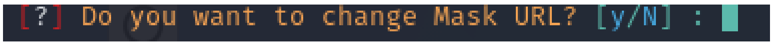
5. Now after generate we use go select any ports

6. But here we select no at that input



```
-] Select a port forwarding service : N
```

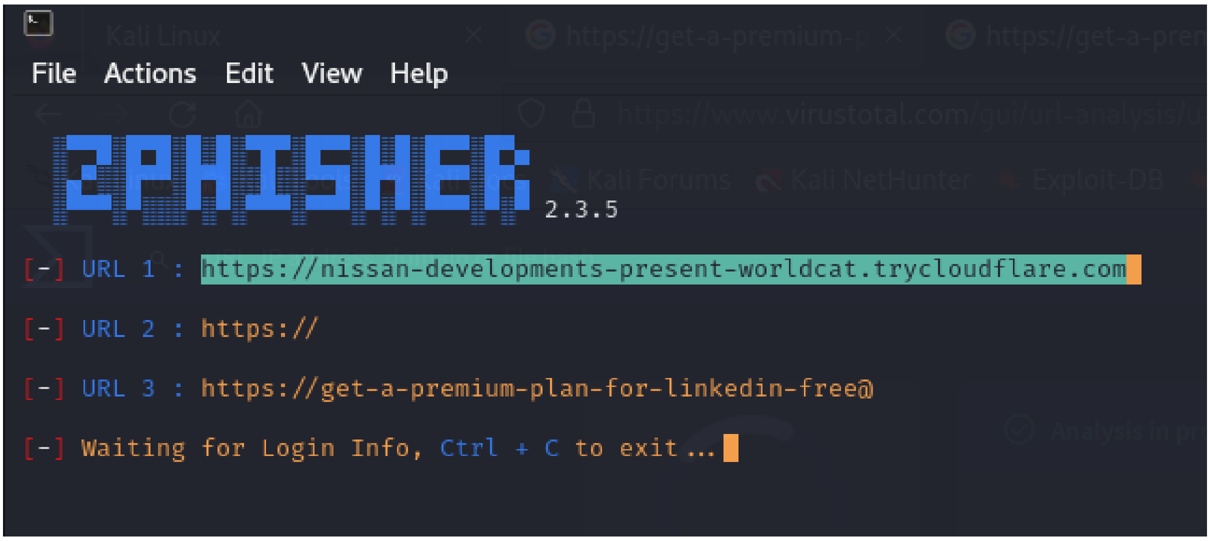
7. Now after it ask for any URL mask



```
[?] Do you want to change Mask URL? [y/N] :
```

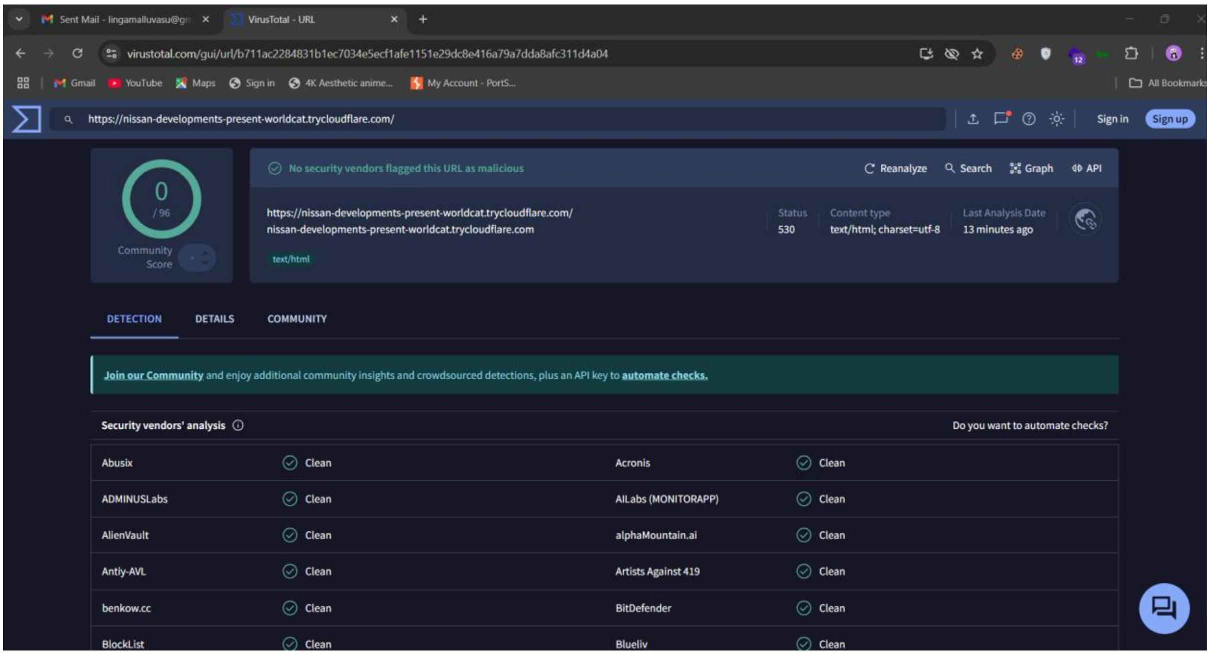
8. Then simply no for URL mask

9. Then we get output of phishing URL



```
[-] URL 1 : https://nissan-developments-present-worldcat.trycloudflare.com

[-] URL 2 : https://

[-] URL 3 : https://get-a-premium-plan-for-linkedin-free@

[-] Waiting for Login Info, Ctrl + C to exit ...
```

10. Now place the phishing links in the virus total website URL to find it shows vulnerable or not



virustotal.com/gui/url/b711ac2284831b1ec7034e5ecf1afe1151e29dc8e416a79a7dda8afc311d4a04

https://nissan-developments-present-worldcat.trycloudflare.com/

0 / 96 Community Score

No security vendors flagged this URL as malicious

https://nissan-developments-present-worldcat.trycloudflare.com/
nissan-developments-present-worldcat.trycloudflare.com

text/html

Status 530

Content type text/html; charset=utf-8

Last Analysis Date 13 minutes ago

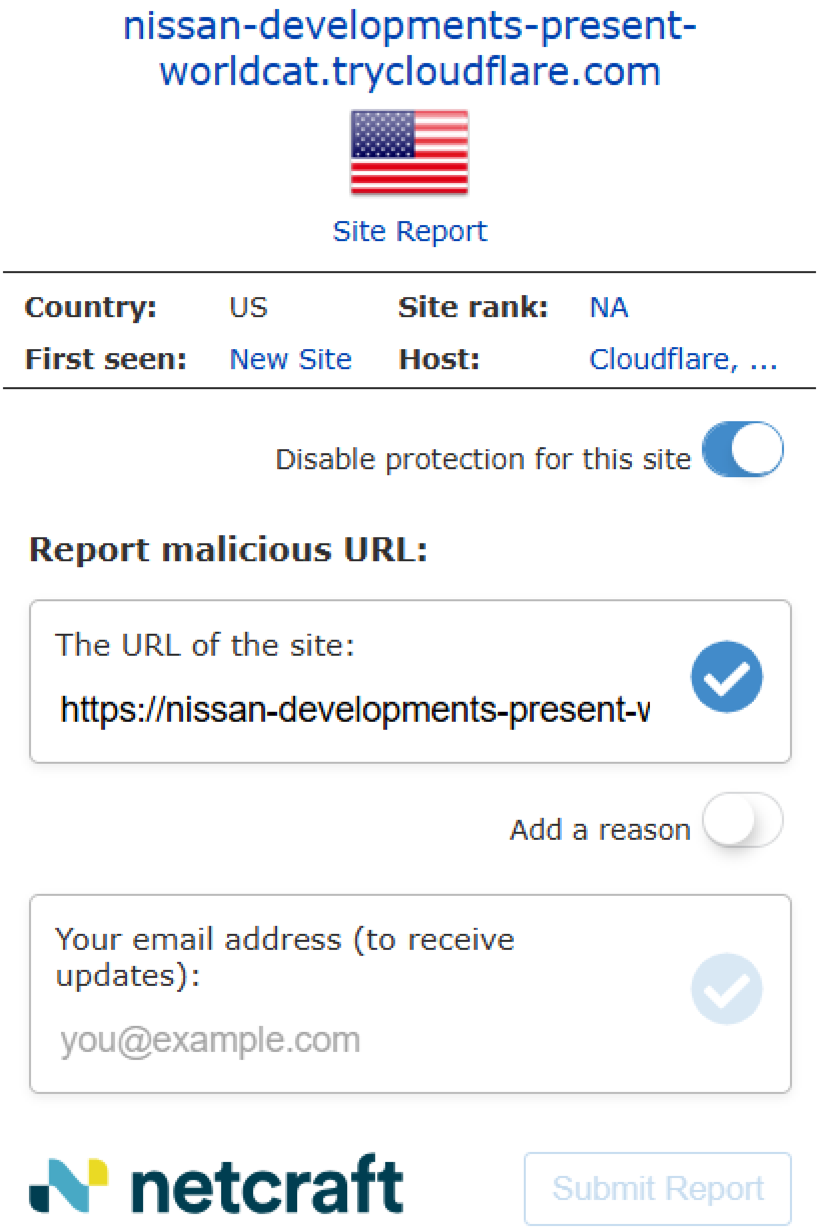
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Security vendors' analysis

Do you want to automate checks?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	alphaMountain.ai	✓ Clean
Antiy-AVL	✓ Clean	Artists Against 419	✓ Clean
benkow.cc	✓ Clean	BitDefender	✓ Clean
BlockList	✓ Clean	Blueliv	✓ Clean

11. Now we get results from the netcraft extention to get the results



nissan-developments-present-worldcat.trycloudflare.com

Site Report

Country:	US	**Site rank:**	NA
First seen:	New Site	**Host:**	Cloudflare, ...

Disable protection for this site

Report malicious URL:

The URL of the site:

https://nissan-developments-present-v

Add a reason

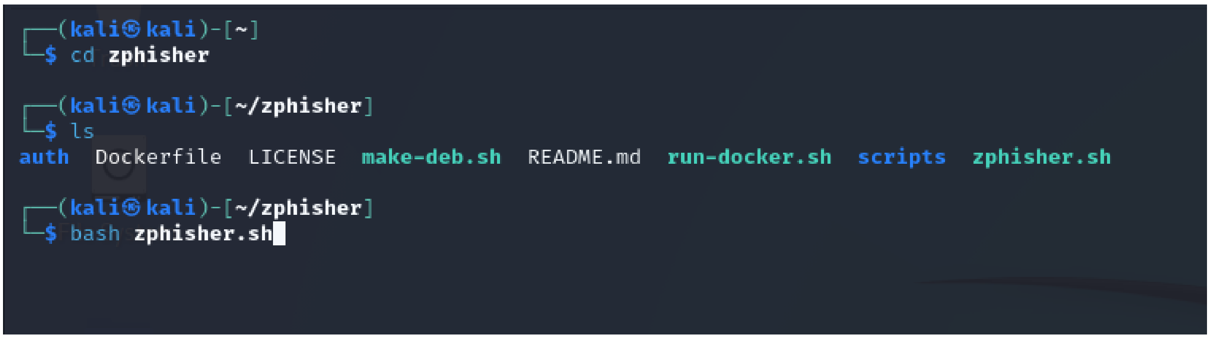
Your email address (to receive updates):

you@example.com

12. Here we observed that there was no any phishing link warns from these two

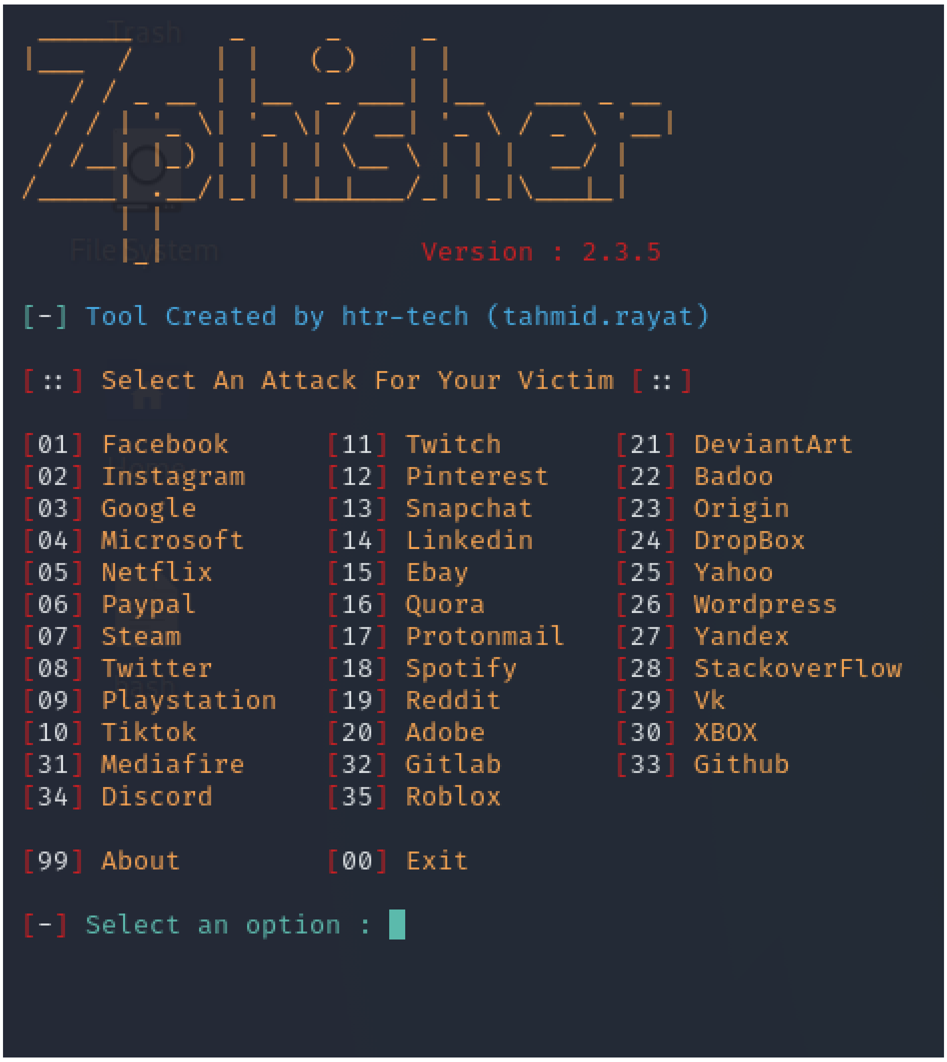
SECTION 2:

1. Here we find the phishing link for the microsoft365
2. To login any Microsoft service we need login Microsoft account
3. Here we use the zphisher tool to made login for the Microsoft
4. Open and run the Zphisher tool kit in kali Linux



```
┌──(kali㉿kali)-[~]
└─$ cd zphisher

┌──(kali㉿kali)-[~/zphisher]
└─$ ls
auth  Dockerfile  LICENSE  make-deb.sh  README.md  run-docker.sh  scripts  zphisher.sh

┌──(kali㉿kali)-[~/zphisher]
└─$ bash zphisher.sh
```

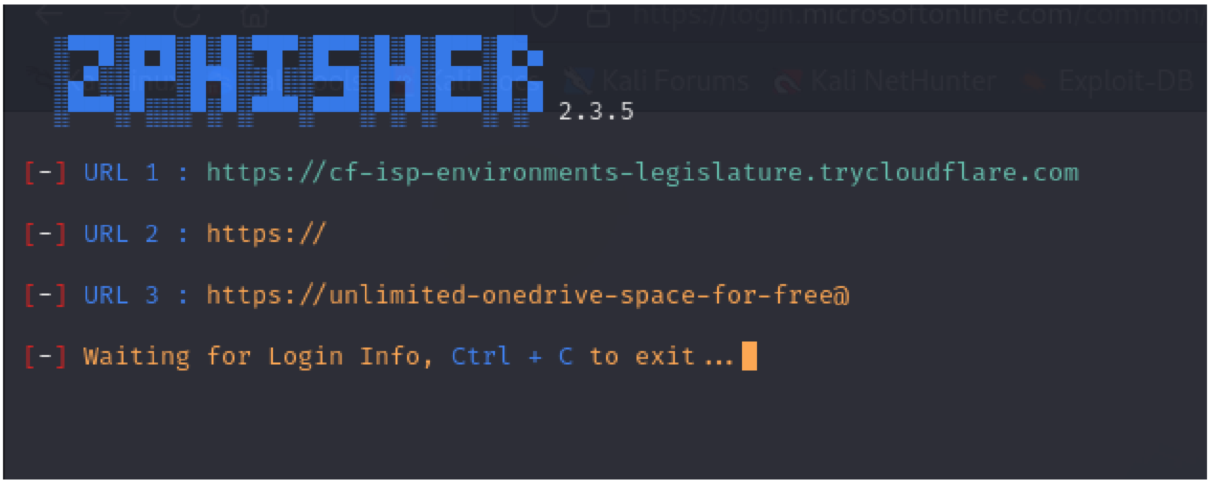
5. After run the above command the instance launch the Zphisher interface



```
 ______      _     _     _
|___  /     | |   (_)   | |
   / / _ __ | |__  _ ___| |__   ___ _ __
  / / | '_ \| '_ \| / __| '_ \ / _ \ '__|
 / /__| |_) | | | | \__ \ | | |  __/ |
/_____| .__/|_| |_|_|___/_| |_|\___|_|
      | |
      |_|                Version : 2.3.5

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook      [11] Twitch       [21] DeviantArt
[02] Instagram     [12] Pinterest    [22] Badoo
[03] Google        [13] Snapchat     [23] Origin
[04] Microsoft     [14] Linkedin     [24] DropBox
[05] Netflix       [15] Ebay         [25] Yahoo
[06] Paypal        [16] Quora        [26] Wordpress
[07] Steam         [17] Protonmail   [27] Yandex
[08] Twitter       [18] Spotify      [28] StackoverFlow
[09] Playstation   [19] Reddit       [29] Vk
[10] Tiktok        [20] Adobe        [30] XBOX
[31] Mediafire     [32] Gitlab       [33] Github
[34] Discord       [35] Roblox

[99] About         [00] Exit

[-] Select an option :
```

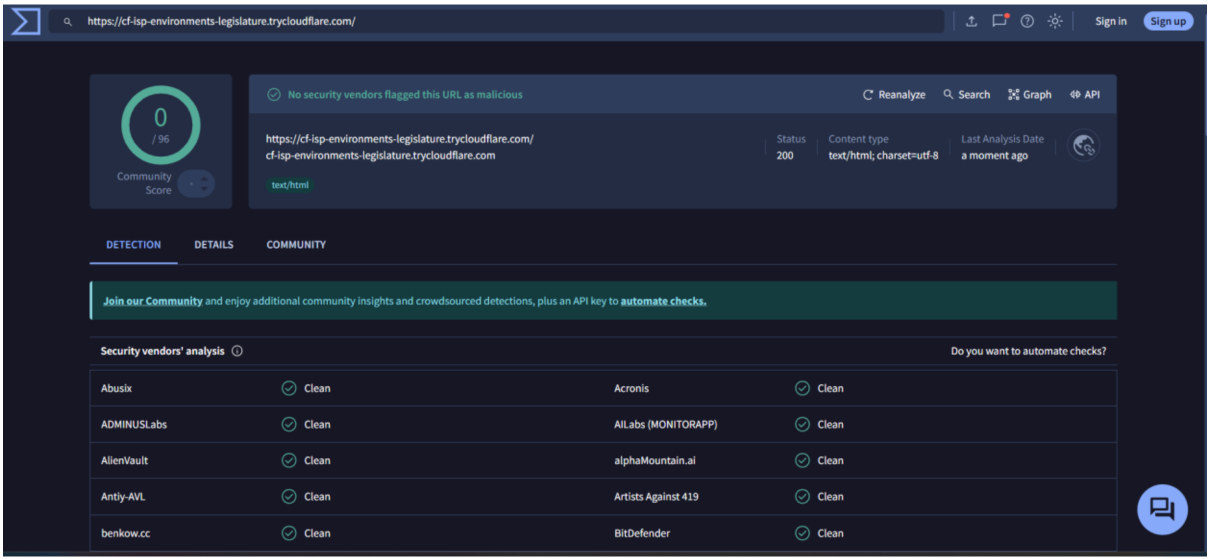
6. Now select the option “04” to create Microsoft account login phishing mail

7. After the same process repeat as the section -1 happen until the URL generated



```
ZPHISHER 2.3.5

[-] URL 1 : https://cf-isp-environments-legislature.trycloudflare.com

[-] URL 2 : https://

[-] URL 3 : https://unlimited-onedrive-space-for-free@

[-] Waiting for Login Info, Ctrl + C to exit...
```

7. Now check the phishing links in the virus total URL and netcraft extension



0
/ 96
Community Score

No security vendors flagged this URL as malicious

https://cf-isp-environments-legislature.trycloudflare.com/
cf-isp-environments-legislature.trycloudflare.com
text/html

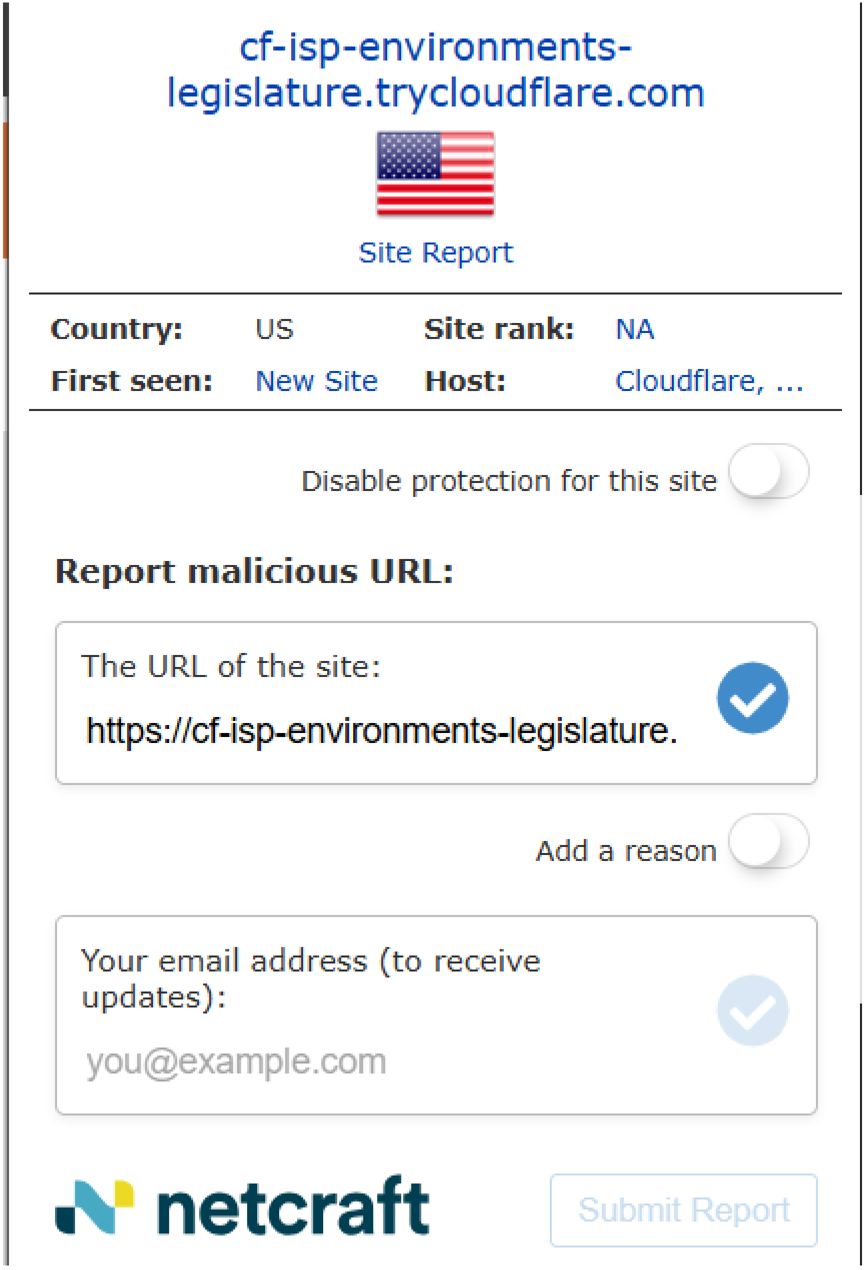
Status 200
Content type text/html; charset=utf-8
Last Analysis Date a moment ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	alphaMountain.ai	✓ Clean
Antiy-AVL	✓ Clean	Artists Against 419	✓ Clean
benkow.cc	✓ Clean	BitDefender	✓ Clean



cf-isp-environments-legislature.trycloudflare.com

Site Report

Country:	US	**Site rank:**	NA
First seen:	New Site	**Host:**	Cloudflare, ...

Disable protection for this site ○

Report malicious URL:

The URL of the site:

https://cf-isp-environments-legislature.

Add a reason ○

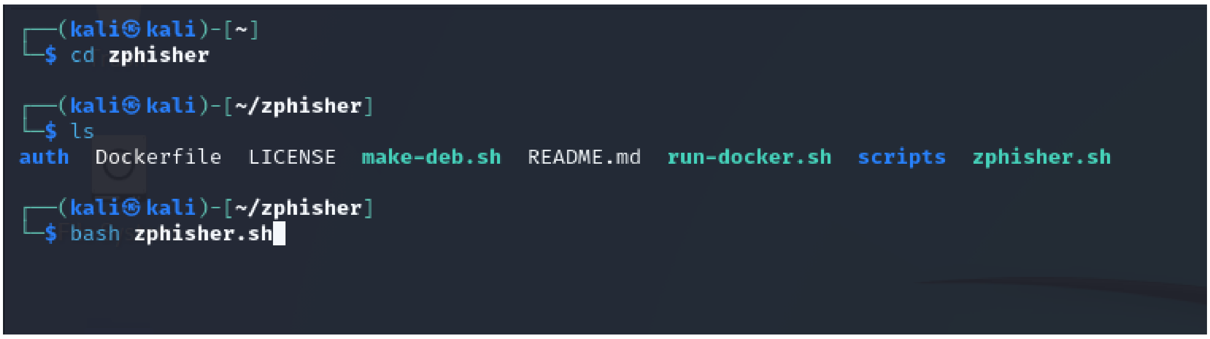
Your email address (to receive updates):

you@example.com

SECTION 3:

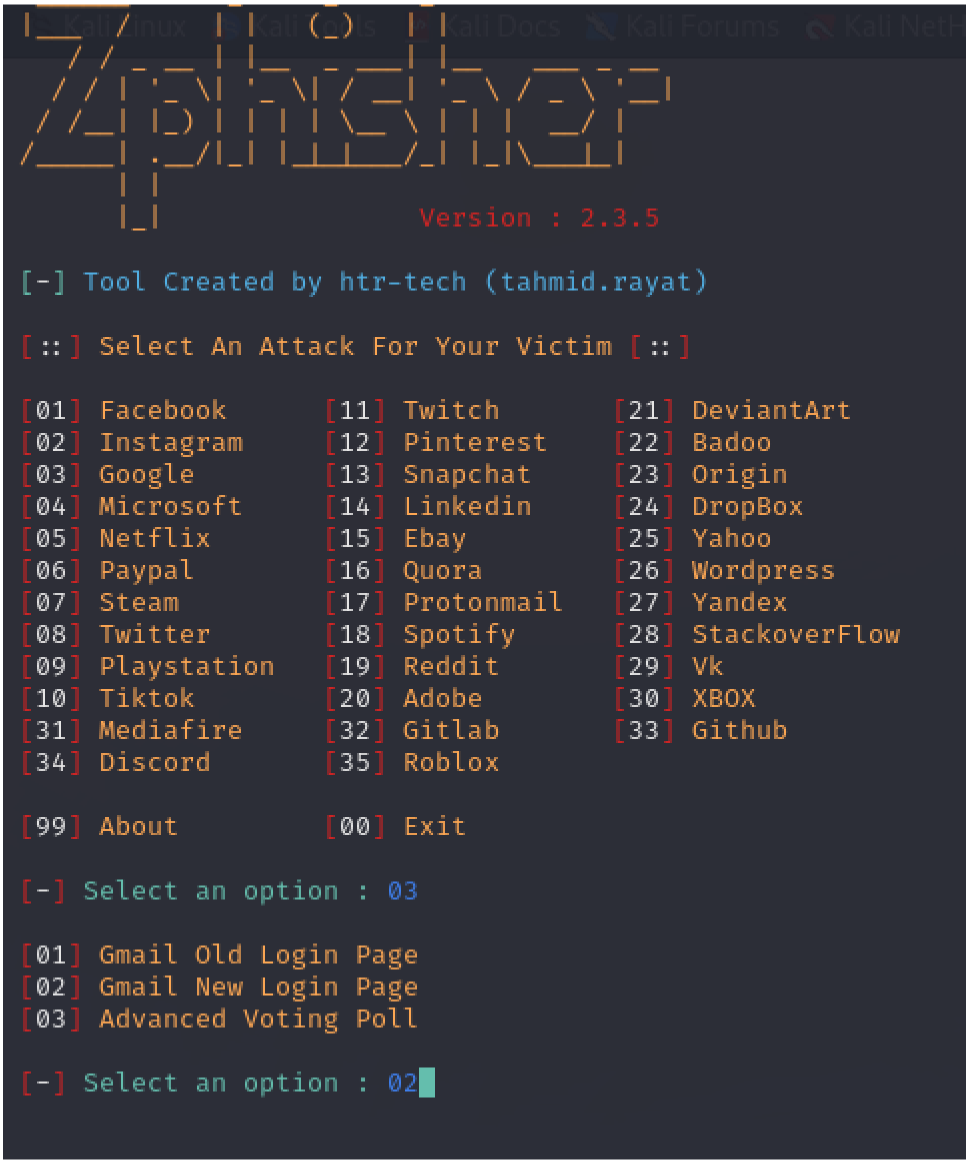
1. Here we done the phishing link generation for the google Gmail.

2. Go to the kali Linux and open the command prompt and open the Zphisher for phishing links



```
┌──(kali㉿kali)-[~]
└─$ cd zphisher

┌──(kali㉿kali)-[~/zphisher]
└─$ ls
auth  Dockerfile  LICENSE  make-deb.sh  README.md  run-docker.sh  scripts  zphisher.sh

┌──(kali㉿kali)-[~/zphisher]
└─$ bash zphisher.sh
```

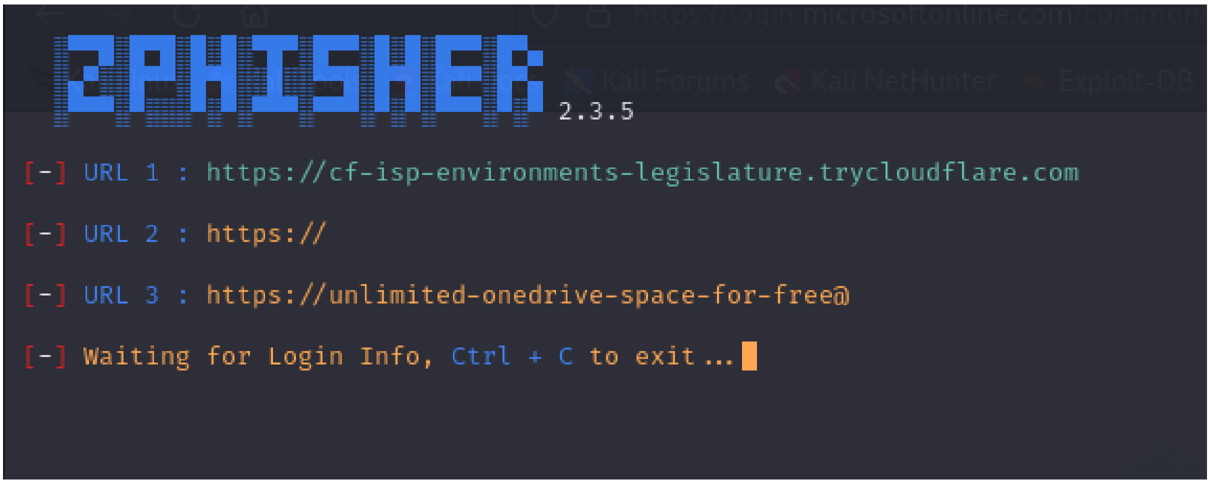
3. Now open the Zphisher and select the google to done the phishing link generation for the Gmail.



```
                              Version : 2.3.5

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook      [11] Twitch       [21] DeviantArt
[02] Instagram     [12] Pinterest    [22] Badoo
[03] Google        [13] Snapchat     [23] Origin
[04] Microsoft     [14] Linkedin     [24] DropBox
[05] Netflix       [15] Ebay         [25] Yahoo
[06] Paypal        [16] Quora        [26] Wordpress
[07] Steam         [17] Protonmail   [27] Yandex
[08] Twitter       [18] Spotify      [28] StackoverFlow
[09] Playstation   [19] Reddit       [29] Vk
[10] Tiktok        [20] Adobe        [30] XBOX
[31] Mediafire     [32] Gitlab       [33] Github
[34] Discord       [35] Roblox

[99] About         [00] Exit

[-] Select an option : 03

[01] Gmail Old Login Page
[02] Gmail New Login Page
[03] Advanced Voting Poll

[-] Select an option : 02
```

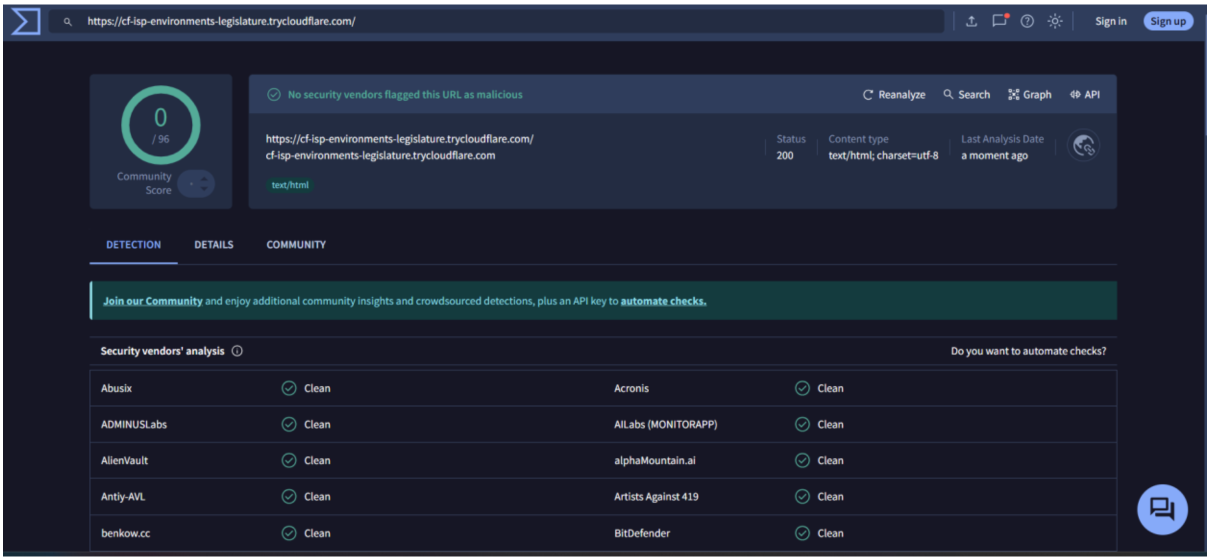
5. Here we select the option “3” for google and then we select the “02” for new gmail login page

6. After we continue steps like at section 1 to generate the links for the URL



```
ZPHISHER 2.3.5

[-] URL 1 : https://cf-isp-environments-legislature.trycloudflare.com

[-] URL 2 : https://

[-] URL 3 : https://unlimited-onedrive-space-for-free@

[-] Waiting for Login Info, Ctrl + C to exit ...
```

7. Now we place at the virus total and netcraft extention to known that it showing the vulnerable or not



0 / 96
Community Score

No security vendors flagged this URL as malicious

https://cf-isp-environments-legislature.trycloudflare.com/
cf-isp-environments-legislature.trycloudflare.com

text/html

Status 200

Content type text/html; charset=utf-8

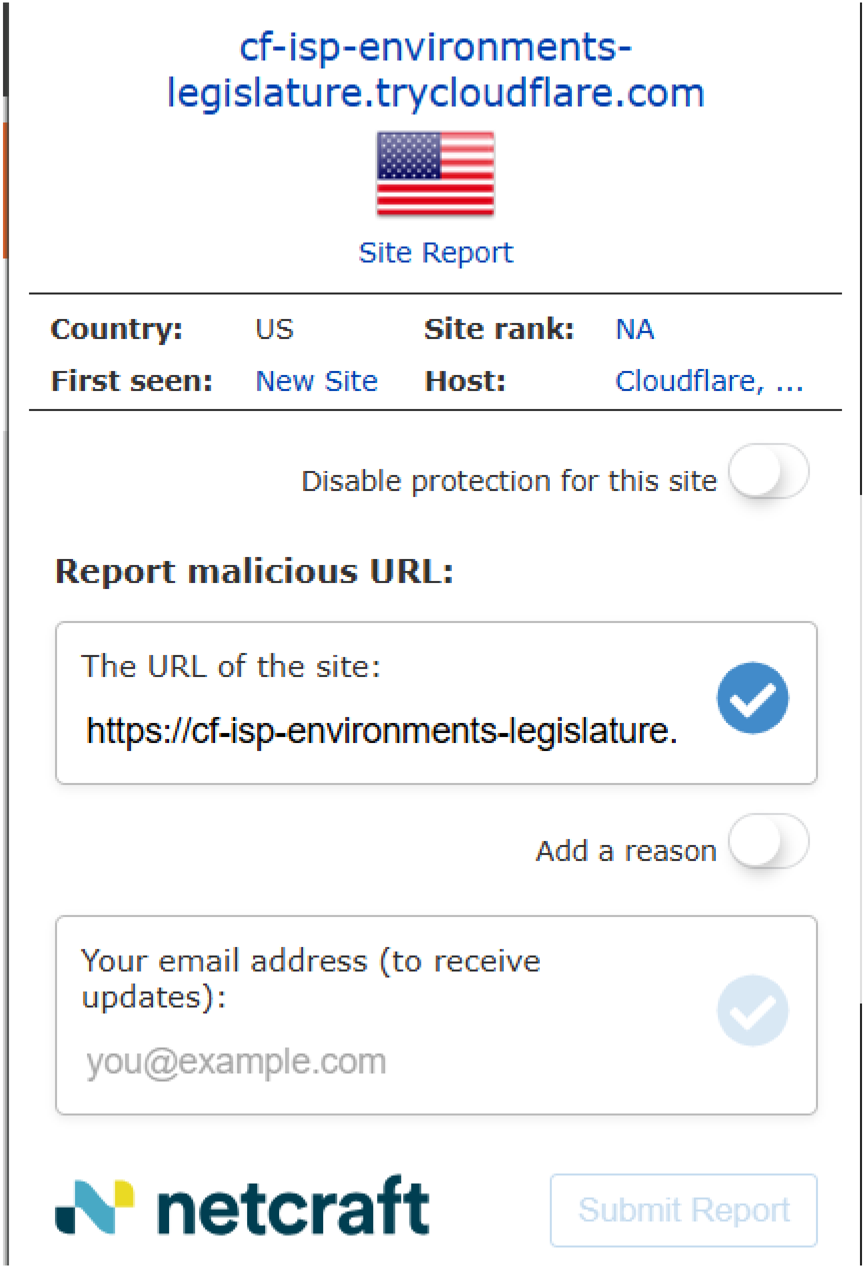
Last Analysis Date a moment ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean
Antiy-AVL	Clean	Artists Against 419	Clean
benkow.cc	Clean	BitDefender	Clean



cf-isp-environments-legislature.trycloudflare.com

Site Report

Country:	US	**Site rank:**	NA
First seen:	New Site	**Host:**	Cloudflare, ...

Disable protection for this site ○

Report malicious URL:

The URL of the site:

https://cf-isp-environments-legislature.

Add a reason ○

Your email address (to receive updates):

you@example.com

4. CONCLUSION: the target phishing links can scan on virus total and netcraft extension they display some are malicious and some or not malicious by pasting the phishing links one by one.

5. SUMMARY OF THE TASK: here we first download or git clone the Zphisher for making malicious links which are need to scan on virus total and netcraft extention and we take three given target to build phishing links like LinkedIn, Microsoft 365, and Gmail.

TASK -3:

1. Title: Identify any 3 Business email IDs where you can do an email spoofing attack

2. Objective of the Task: Here we done the spoofing attack to access the business mails. By this we can find that the mails are vulnerable or not.

3. STEP BY STEP PROCEDURE:

1. Go to google and search for the business mails in the internet

2. Here we gather the emails of different organizations from various domains

Email-1: **grant@deeboodah.org**

Email-2: **admin@jumia.org**

Email-3: **zaid@zsecurity.org**

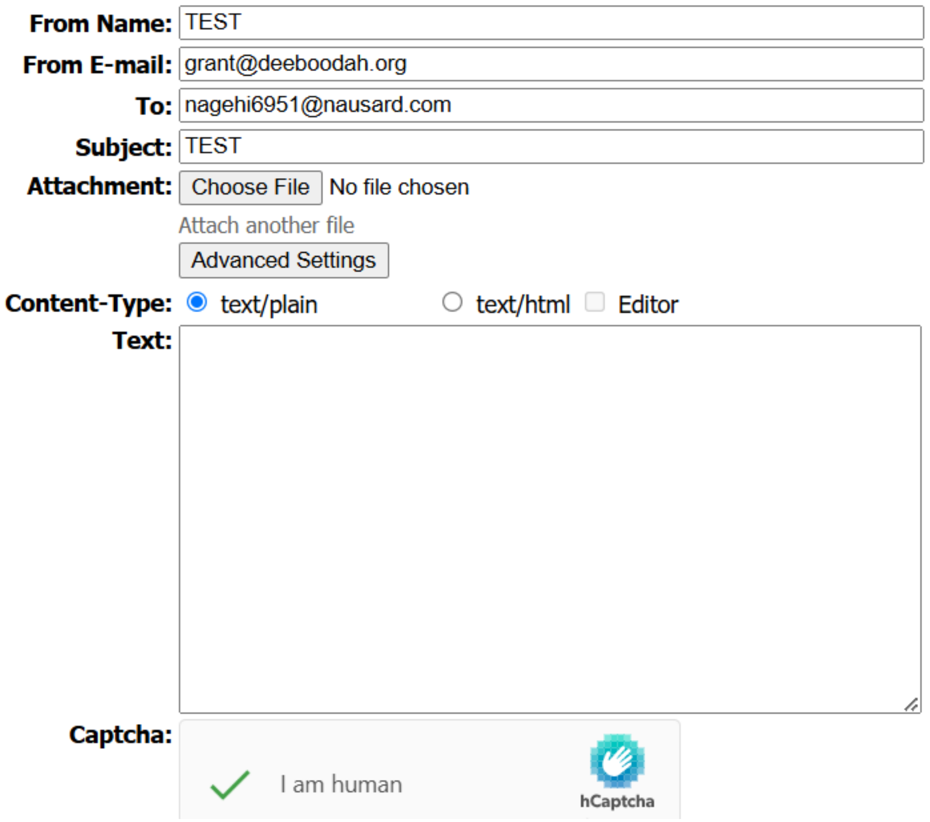
3. Now use EMKEI'S FAKE MAILER to known the organisation mail is vulnerable or not

4. We go to the EMKEI'S FAKE MAILER for testing the email spoofing

5. Now place the vulnerable mails at the "from address" and then

Place the temp mail at the "To address"

6. Now we get the mail in the given temp mail section



From Name: TEST

From E-mail: grant@deeboodah.org

To: nagehi6951@nausard.com

Subject: TEST

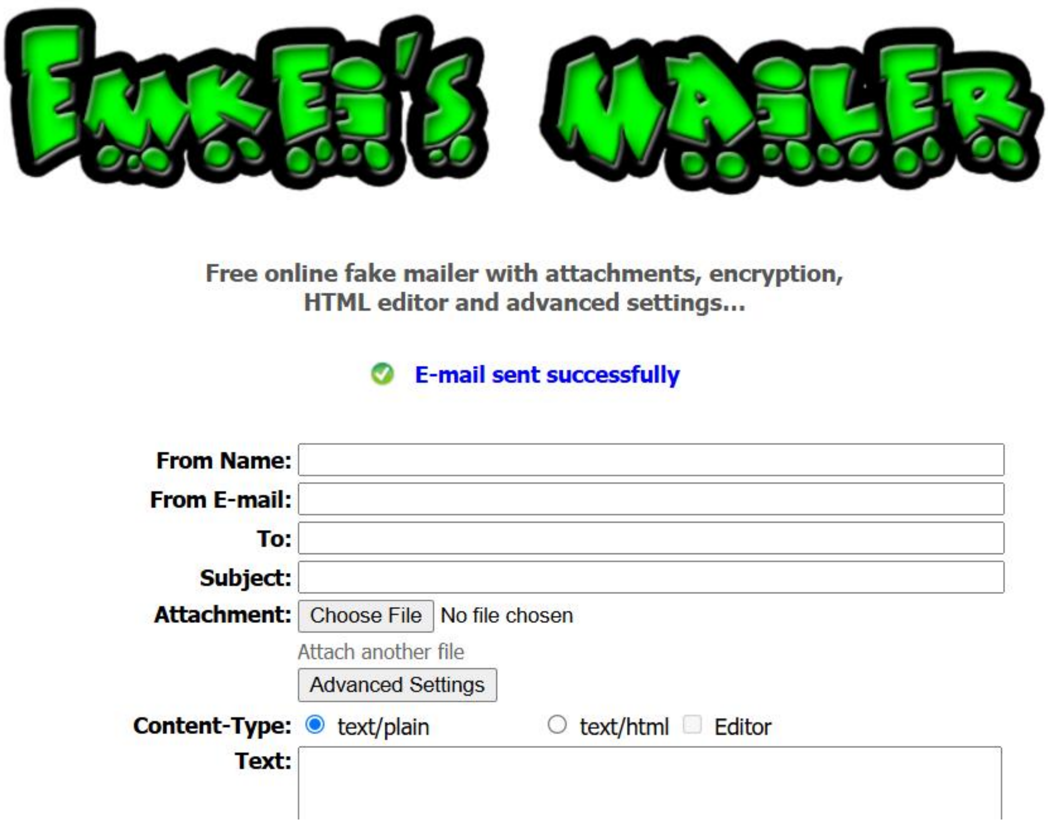
Attachment: Choose File No file chosen

Content-Type: ● text/plain ○ text/html □ Editor

Text:

Captcha: ✓ I am human

8. After we enter all details as mentioned above we get email sent successfully



Free online fake mailer with attachments, encryption, HTML editor and advanced settings...

✓ E-mail sent successfully

From Name:

From E-mail:

To:

Subject:

Attachment: No file chosen

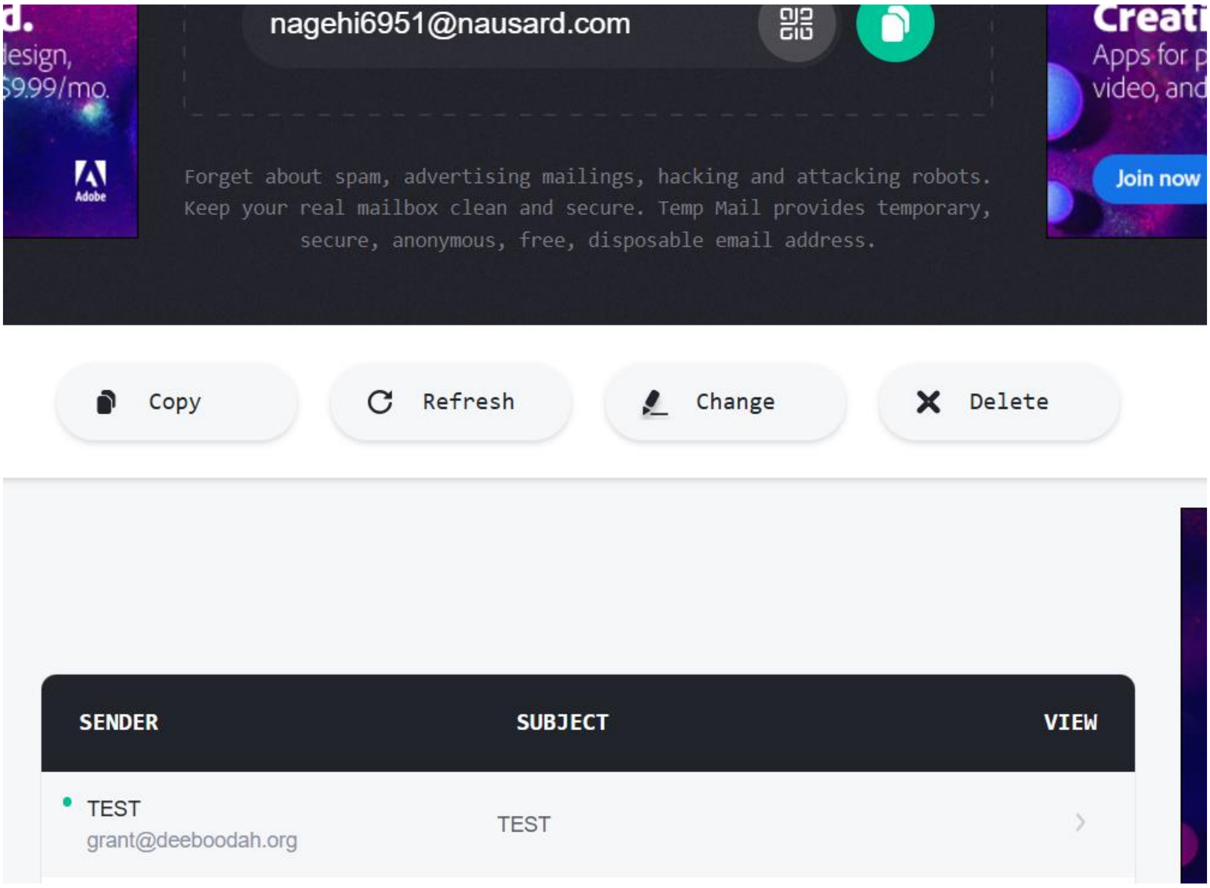
Content-Type: ● text/plain ○ text/html □ Editor

Text:

9. After the message we go to mail and check the mail if we get mail it is vulnerable for email spoofing

10. Here I send the Test subject mail and named as Test

OUTPUT:



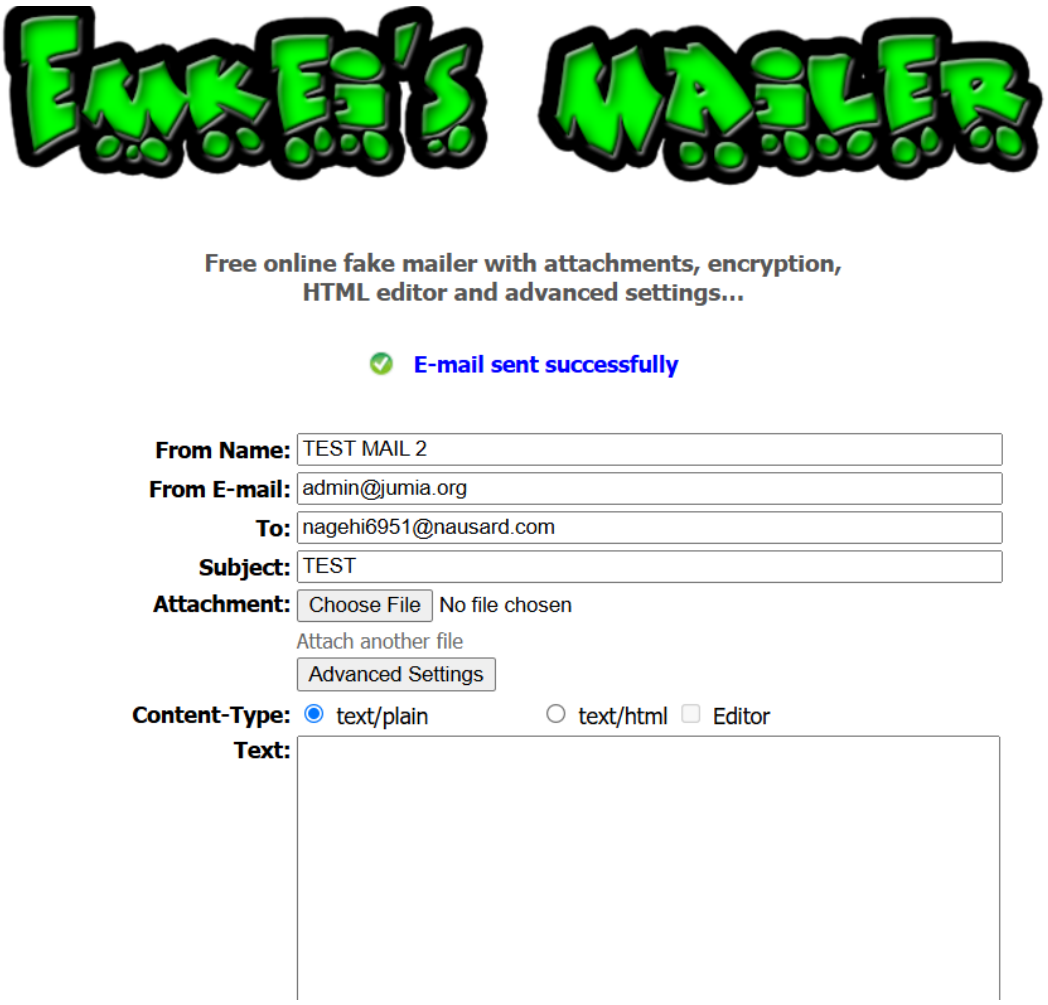
nagehi6951@nausard.com

Forget about spam, advertising mailings, hacking and attacking robots. Keep your real mailbox clean and secure. Temp Mail provides temporary, secure, anonymous, free, disposable email address.

SENDER	SUBJECT	VIEW
● TEST grant@deeboodah.org	TEST	›

SECOND MAIL:

11. Now we done for second mail that is vulnerable or not using same method for first mail.

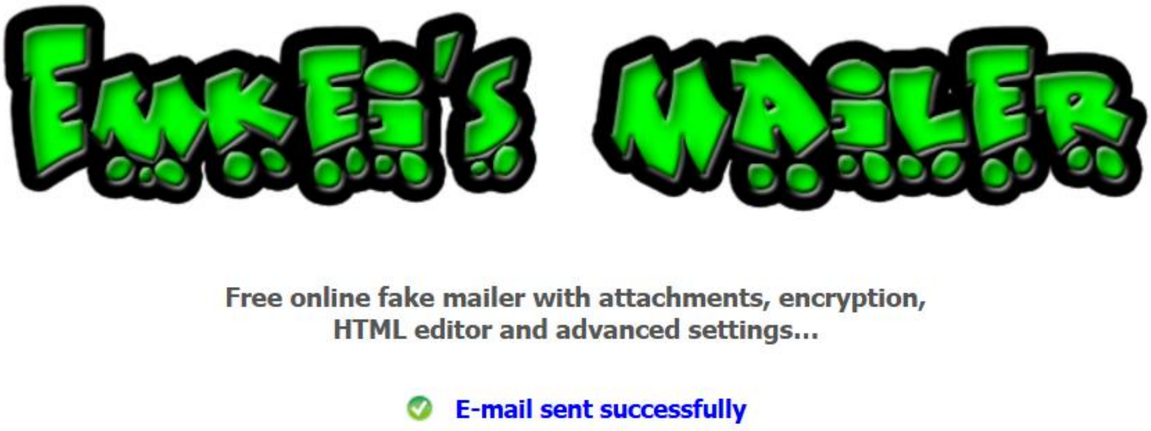


Free online fake mailer with attachments, encryption, HTML editor and advanced settings...

✓ E-mail sent successfully

From Name:	TEST MAIL 2
From E-mail:	admin@jumia.org
To:	nagehi6951@nausard.com
Subject:	TEST
Attachment:	Choose File No file chosen Attach another file Advanced Settings
Content-Type:	● text/plain ○ text/html □ Editor
Text:	

12. We enter the details and press send we get notification as E-mail sent

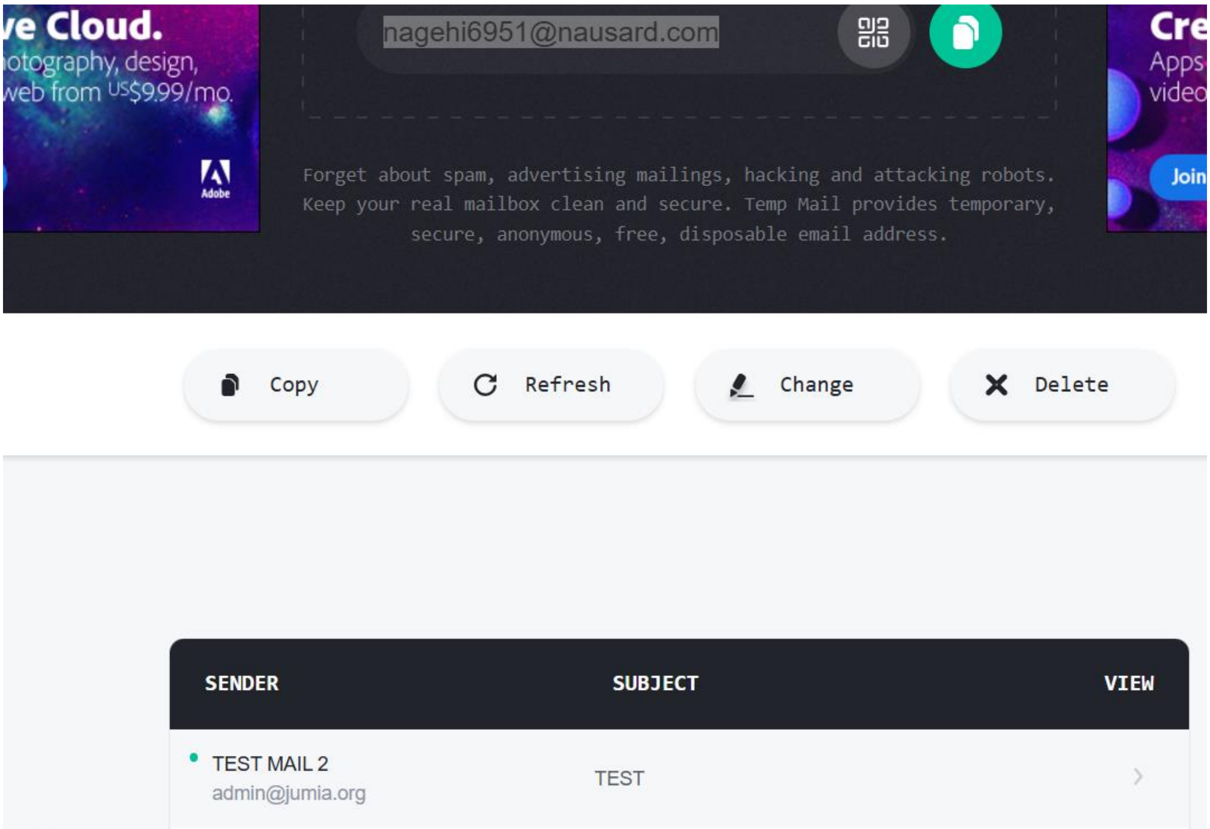


Free online fake mailer with attachments, encryption, HTML editor and advanced settings...

✓ E-mail sent successfully

13. Now we go to the temp mail now we get the mail from the respected business mail.

OUTPUT:

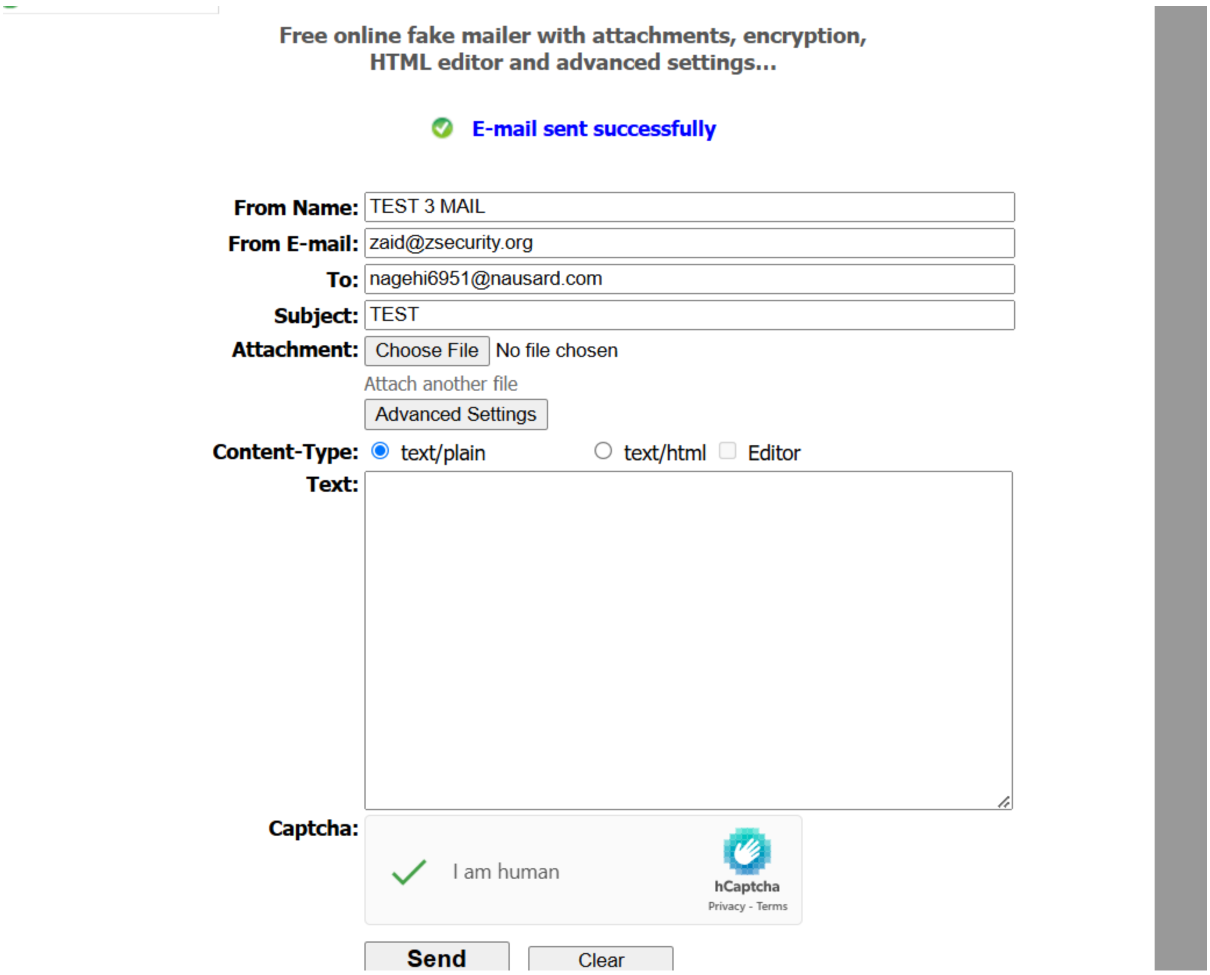


nagehi6951@nausard.com

Forget about spam, advertising mailings, hacking and attacking robots. Keep your real mailbox clean and secure. Temp Mail provides temporary, secure, anonymous, free, disposable email address.

SENDER	SUBJECT	VIEW
TEST MAIL 2 admin@jumia.org	TEST	›

14. Now we done the spoofing attack on the 3rd mail as like above mentioned way

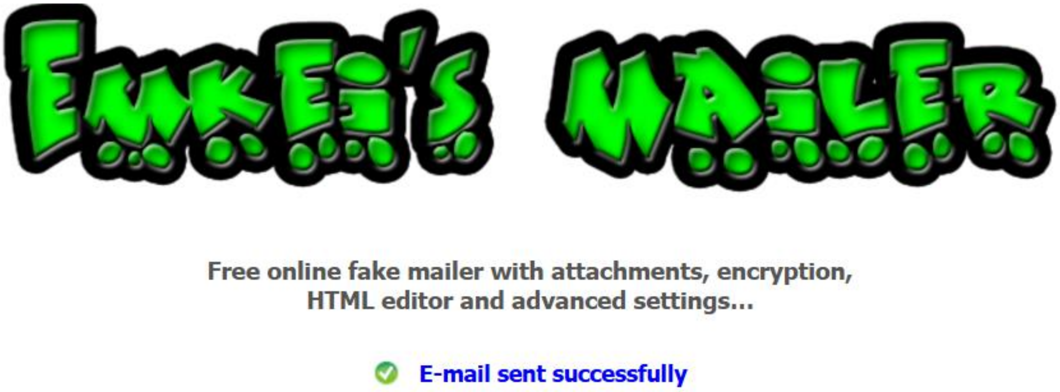


Free online fake mailer with attachments, encryption, HTML editor and advanced settings...

✓ E-mail sent successfully

From Name:	TEST 3 MAIL
From E-mail:	zaid@zsecurity.org
To:	nagehi6951@nausard.com
Subject:	TEST
Attachment:	No file chosen
Content-Type:	● text/plain ○ text/html □ Editor
Text:	
Captcha:	✓ I am human

15. Here we enter the details in the domain, we get the email sent.

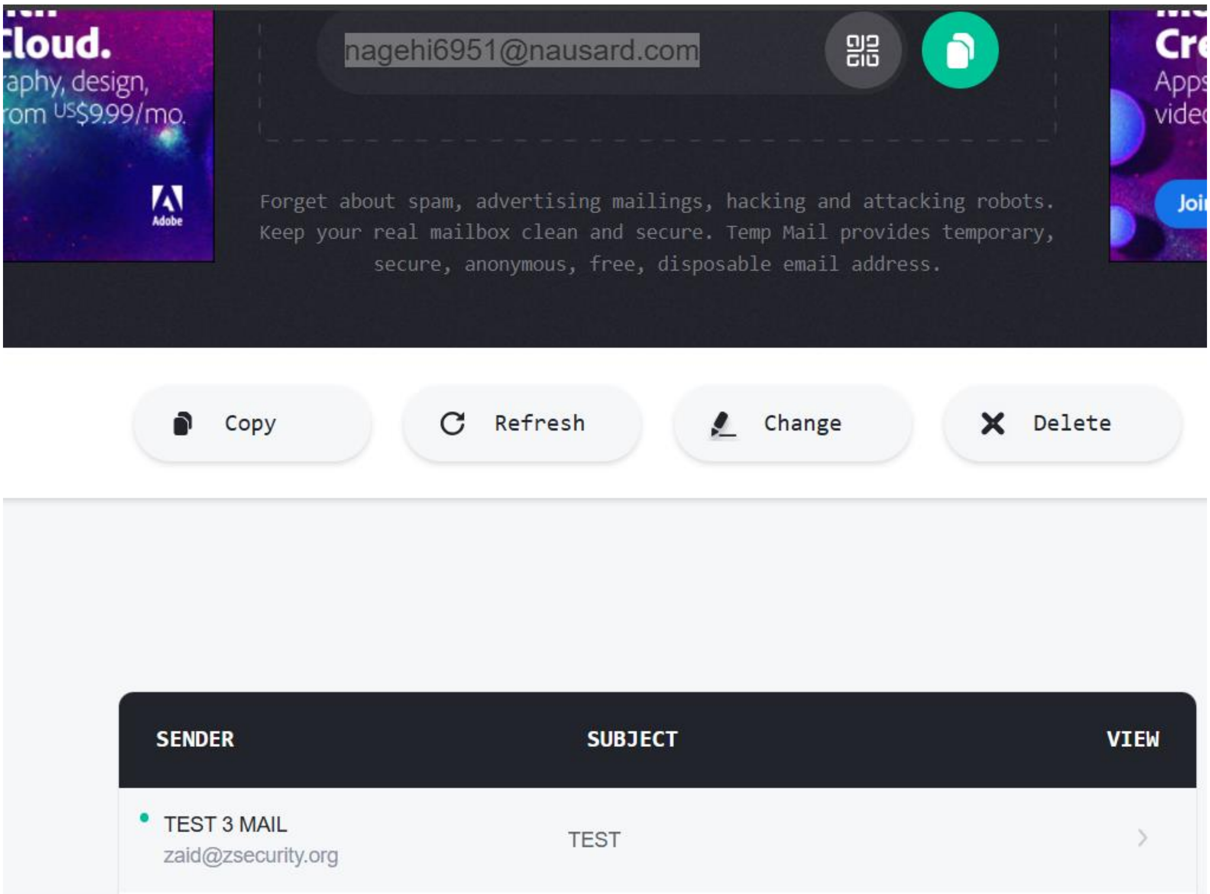


Free online fake mailer with attachments, encryption, HTML editor and advanced settings...

✓ E-mail sent successfully

16. Now we get the mail in the temp mail and if we get it was email spoofing vulnerable.

OUTPUT:



Forget about spam, advertising mailings, hacking and attacking robots. Keep your real mailbox clean and secure. Temp Mail provides temporary, secure, anonymous, free, disposable email address.

SENDER	SUBJECT	VIEW
TEST 3 MAIL zaid@zsecurity.org	TEST	›

<span style="color:red">**4. CONCLUSION:**</span> Here we done the email spoofing attack on different organisation business mails to known that the one are vulnerable or not.

<span style="color:red">**5. SUMMARY OF TASK:**</span> First we go to google and intensively find the various business mails of different organisations and we collect the targeted mails and check if they are email spoofing vulnerable or not, by the using EMKEI’S FAKE MAILER we send test mails by using business mails to the temp mails as “test subject” if we get mail they are vulnerable or else we don’t get any mail it can’t work as email spoofing.