

Forum:[Hack Forums](#)

Thread: [Fastest way to find mass websites which has this in their url?](#)

xreD - May 27, 2020, 11:08 pm

Hello,

I am trying to find a way where I can bulk check if the newly registered domain has a particular address in it.

For eg each software has a default address when installed on a domain like, I want to see all the domains where a mail software is installed and its default address is "domain.com/mailer/"

So I want to find all the domains that has that particular mail software installed.

Is this doable?

One way I can think of is mass add millions of domain and then get some sort of checker that can keep on checking all the domains.

I hope you guys understand what I am asking. I am very new to this kind of thing. Any help would be appreciated.

Cheers!

frank3nstien - May 28, 2020, 2:04 am

If you are sure default address is likely the same as mentioned, you should try Google index of search queries (we call them dorks or GHDB) used to find publicly available information you can search first in exploit-db if someone already shared about particular software

xreD - May 28, 2020, 5:27 am

(May 28, 2020 02:04 AM)frank3nstien Wrote: [CITE](#) If you are sure default address is likely the same as mentioned, you should try Google index of search queries (we call them dorks or GHDB) used to find publicly available information you can search first in exploit-db if someone already shared about particular software

Yes I am 100% sure about the address as I myself have installed the same app 100 times on my servers.

Thanks I'll look in exploit-db as you said, although its not a very commonly used software probably only 1-2k people have it.

edit: Can you please point me to the exploit-db that you're talking about? i browsed but didn't find it.

Gee4rce - May 28, 2020, 9:09 am

Making a google dork for the URL mentioned is not that effective as you may get many hits for that when using dork. It's not unique enough. Anyways a dork would be `inurl:".com/mailer/"`

(change .com to .whatever toplevel domain you want to include).

You may have better chances by checking if that mailserver has Ports open which are specific to that mail software. If it has for example Port 3301 then you can use IP searchengines like Shodan or Censys to find machines that run this specifc mailer Software.

Maybe write a script that automates all this in one move, like:
check IP searchengine => dump found ip's by Port, check
then if webpanel is reachabel under https://some-ip:443/mailer/

Cheers, Gee.

frank3nstien - May 28, 2020, 10:58 pm

(May 28, 2020 05:27 AM)xreD Wrote: [\[CITE\]](#) Yes I am 100% sure about the address as I myself have installed the same app 100 times on my servers.

Thanks I'll look in exploit-db as you said, although its not a very commonly used software probably only 1-2k people have it.

edit: Can you please point me to the exploit-db that you're talking about? i browsed but didn't find it. I have pointed you in DM related exploit-db and index file queries example ?

(May 28, 2020 09:09 AM)Gee4rce Wrote: [\[CITE\]](#) Making a google dork for the URL mentioned is not that effective

as you may get many hits for that when using dork. It's not unique enough. Anyways a dork would be inurl:".com/mailer/"

(change .com to .whatever toplevel domain you want to include).

You may have better chances by checking if that mailserver has Ports open which are specific to that mail software. If it has for example Port 3301 then you can use IP searchengines like Shodan or Censys to find machines that run this specifc mailer Software.

Maybe write a script that automates all this in one move, like:
check IP searchengine => dump found ip's by Port, check
then if webpanel is reachabel under https://some-ip:443/mailer/

Cheers, Gee.

This is really in detailed explanation for further, well thanks for new insights ?

xreD - June 1, 2020, 7:50 am

(May 28, 2020 09:09 AM)Gee4rce Wrote: [\[CITE\]](#) Making a google dork for the URL mentioned is not that effective

as you may get many hits for that when using dork. It's not unique enough. Anyways a dork would be inurl:".com/mailer/"

(change .com to .whatever toplevel domain you want to include).

You may have better chances by checking if that mailserver has Ports open which are specific to that mail software. If it has for example Port 3301 then you can use IP searchengines like Shodan or Censys to find machines that run this specifc mailer Software.

Maybe write a script that automates all this in one move, like:
check IP searchengine => dump found ip's by Port, check
then if webpanel is reachabel under https://some-ip:443/mailer/

Cheers, Gee.

The thing is I know the default login id this software script generates and almost every time no one changes the default ones.

That mailing software(its mumara) mostly uses port 2525.
I'll look into what you said about searching open ports but I have absolutely no idea since this is the first time I've heard that haha. :)

(May 28, 2020 10:58 PM)frank3nstien Wrote: [\[CITE\]](#) I have pointed you in DM related exploit-db and index file queries example ?

This is really in detailed explanation for further, well thanks for new insights ?Thanks for your PM too, I dind't knew that site. Looks like a gem :D

Thanks a lot guys :)

This is the exact type of file the software generates so this file should be on the server. The address for this file is "/root/mailamigos-scripts/Readme.info"

So is it possible to find domains/servers with this file?

Code ---> MailAmigos.com License Information

- License Email Address:

---> MySQL + phpMyAdmin

- Access to phpMyAdmin on <http://n-fakty.info/phpmyadmin>
- For: mumara
- Internal user: root
- Password: ajemrum2

- External user: kontakt
- Password: vipbfcebaebe7fa

---> Mumara Installation

- Mumara Admin Panel - <http://n-fakty.info/mailer/login.php>
- Username: admin
- Password: admin ####== CHANGE AS SOON AS POSSIBLE ==####

---> SMTP data

- Email address: kontakt@n-fakty.info
- User: kontakt
- Password: vipbfcebaebe7fa

- Receiving via IMAP:
- Secure connection = STARTTLS / Port: 143

- Sending via SMTP:
- Insecure Connection / Port: 2525

- Webmail address: <http://n-fakty.info/webmail>
- User: kontakt
- Password: vipbfcebaebe7fa

- Reply Email Address
- User: reply
- Pass: reply*p5348*vip

- Return Bounces (errors)
- Return User bounces: return
- Pass: return*p5348*vip

- Admin
- User: admin
- Password: admin*p5347*vip

- FBL (Feedback Loop)
- User: fbl
- Password: fbl*p5348*vip

- Abuse (Complaints)
- User: abuse
- Password: abuse*p5348*vip

Postmaster (Complaints)

- User: postmaster
- Password: postmaster*p5348*vip

---> Monitoring data will be sent to:

- E-mail: rebeccahoppkins@gmail.com

---> SSH Connection

- Users access the SSH on port 22
- The kontakt has access to SSH with password vipbfcebaebe7fa

Mumara backups are located at /root/mailamigos-scripts/backup-local/ if you've opted out for ftp backups

###

```
<=====
=====> ###
```

---> Server information and PMTA useful commands

The sending limit per hour of this server is 10000

To stop powerMTA - "service pmta stop"
To start powerMTA - "service pmta start"
To restart PowerMTA - "service pmta restart"

To stop powerMTA management console - "service pmtahttp stop"
To start powerMTA management console - "service pmtahttp start"
To restart PowerMTA management console - "service pmtahttp restart"

To debug your powerMTA installation to find errors - "pmtad --debug"

<=====

Reverse DNS Information

This is an example of how you should set your Reverse DNS or pass it to your server company, you will find all of your Reverse DNS entries within your DNS settings below:

mta0.domain.com POINTS TO ==> 100.100.100.1

<=====

DNS information :
\$TTL 38400
@ IN SOA ns1.n-fakty.info. postmaster.n-fakty.info. (
20190605150653 ; serial
90M ; refresh
15M ; retry
14D ; expire
3600 ; default_ttl
)

n-fakty.info. 14400 IN NS ns1.n-fakty.info.
n-fakty.info. 14400 IN NS ns2.n-fakty.info.

ns1 14400 IN A 51.255.52.183
ns2 14400 IN A 51.255.52.183

n-fakty.info. 14400 IN A 51.255.52.183

localhost 14400 IN A 127.0.0.1

n-fakty.info. 14400 IN MX 0 n-fakty.info.

server IN A 51.255.52.183
www IN A 51.255.52.183

mail0 IN A 51.255.52.183

n-fakty.info. IN TXT "v=spf1 a mx ptr a:n-fakty.info ip4:51.255.52.0/24 ?all"

_adsp._domainkey.n-fakty.info. IN TXT "dkim=all"

_domainkey.n-fakty.info. IN TXT "o=~; r=abuse@n-fakty.info"

_dmarc.n-fakty.info. IN TXT "v=DMARC1; pct=100; ruf=mailto:abuse@n-fakty.info;
rua=mailto:abuse@n-fakty.info; p=reject; adkim=r; aspf=r"

default._domainkey IN TXT ("v=DKIM1; k=rsa; "

"p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC+4hDNhlwexbSQTxHTEfPgkdR4
IT++C0NuRcouTQiHGFVyUDZE/wBZ8OQHSYGBpkzUED92M4iy1QE6QZO4eJu2fPzZhhHZrkmpW
PjtKrtIA1gC7cpnJYHIQ+djJcJrj+6TrjBQWIIEBriAhZ3eAmHvqO30jcsqS5k2zurmuBMwAwIDAQAB"
) ; ----- DKIM key default for n-fakty.info
chmod: cannot access `/root/clean.sh': No such file or directory
sh: /root/clean.sh: No such file or directory

Script Installed = = Success!

Wait for the restart and point the domain as per the instructions above.

Cleaning installation ...

Broadcast message from root@server.n-fakty.info
(/dev/pts/0) at 15:13 ...

The system is going down for reboot NOW!

Gee4rce - June 12, 2020, 6:28 am

The script you are showing looks like its a script on your machine in local root folder.
You won't be able to find these remotely. I thought you are looking for a way to find
ip's/url's that run this type of mailsoftware. Incase it's "mailamigos" (as seen in your
code snippet), then you could find machines running this software for example with
a google dork:

intitle:"Welcome to MailAmigos.com Ultimate Email Marketing Solution"

Cheers, Gee.

xreD - June 13, 2020, 3:24 am

(Jun 12, 2020 06:28 AM)Gee4rce Wrote: [\[CITE\]](#) The script you are showing looks like its a script on
your machine in local root folder.

You won't be able to find these remotely. I thought you are looking for a way to find
ip's/url's that run this type of mailsoftware. Incase it's "mailamigos" (as seen in your
code snippet), then you could find machines running this software for example with
a google dork:

intitle:"Welcome to MailAmigos.com Ultimate Email Marketing Solution"

Cheers, Gee.
Holy shit yes this works!!!

I just need to modify a few things so that I can get tons of results :)

Thank you so much!

Jacov Cross - June 15, 2020, 4:49 am

Checkout sqliv by the-robot on GitHub.

xreD - June 29, 2020, 8:58 am

(Jun 15, 2020 04:49 AM)Jacov Cross Wrote: [\[CITE\]](#) Checkout sqliv by the-robot on GitHub.
Thanks a lot.

I've never tried scanning and all I'll give it a try.

linkinpork - June 29, 2020, 10:38 am

(Jun 29, 2020 08:58 AM)xreD Wrote: [\[CITE\]](#) Thanks a lot.

I've never tried scanning and all I'll give it a try.
Hey, am I too late?

Not sure but wfuzz on Kali might do the job.

PHP Code

<?php

apt-get update

apt-get install wfuzz

wfuzz -h

I use it for directory bruteforcing, never tried it with putting a domain as a fuzz point though.

My use case tends to be

PHP Code

<?php

https://domain.com/FUZZ

But in your case on a sunny day this might work:

PHP Code

<?php

https://FUZZ.com/webmail

xreD - July 1, 2020, 12:15 am

(Jun 29, 2020 10:38 AM)linkinpork Wrote: [\[CITE\]](#) Hey, am I too late?

Not sure but wfuzz on Kali might do the job.

PHP Code

<?php

apt-get update

apt-get install wfuzz

wfuzz -h

I use it for directory bruteforcing, never tried it with putting a domain as a fuzz point though.

My use case tends to be

PHP Code

```
<?php
```

```
https://domain.com/FUZZ
```

But in your case on a sunny day this might work:

PHP Code

```
<?php
```

```
https://FUZZ.com/webmail
```

You're not late haha.

I have never done any of this before at all so my head is spinning a bit lol.

So you find open directories?? Actually my aim is that only... finding open directories and then looking for email databases.

Since this is a mail sending application I thought people will upload mail lists and all and I can just export that data...

linkinpork - July 1, 2020, 1:57 am

(Jul 1, 2020 12:15 AM)xreD Wrote: [\[CITE\]](#) You're not late haha.

I have never done any of this before at all so my head is spinning a bit lol.

So you find open directories?? Actually my aim is that only... finding open directories and then looking for email databases.

Since this is a mail sending application I thought people will upload mail lists and all and I can just export that data...

If it's for open directories, why not forge a dork for it? Gee4rce has mentioned a dork on finding the websites, but maybe you can add this for the directory itself:

PHP Code

```
<?php
```

```
intitle:"index of"
```

Better yet add the filename of the email database itself (let's say the filename is accounts.sql)

PHP Code

```
<?php
```

```
intitle:"index of" "accounts.sql"
```

Good luck! -Porky