

probe

probe

<https://tryhackme.com/room/probe>

```
rustscan -a 10.10.241.94 -- -sC -sV -A | tee scan.txt
```

```
-----END CERTIFICATE-----
http-title: 403 Forbidden
tls-alpn:
  http/1.1
http-server-header: Apache/2.4.41 (Ubuntu)
ssl-date: TLS randomness does not represent time
338/tcp open  ftp      syn-ack vsftpd 2.0.8 or later
443/tcp open  ssl/http    syn-ack Apache httpd 2.4.41 ((Ubuntu))
tls-alpn:
  http/1.1
ssl-cert: Subject: commonName=dev.probe.thm/organizationName=Tester/stateOrProvinceName=Some-State/countryName=US/localityName=city/organizationalUnitName=MHT/emailAddress=probe@probe.thm
Issuer: commonName=dev.probe.thm/organizationName=Tester/stateOrProvinceName=Some-State/countryName=US/localityName=city/organizationalUnitName=MHT/emailAddress=probe@probe.thm
Public Key type: rsa
Public Key bits: 2048
Signature Algorithm: sha256WithRSAEncryption
```

```
ftp 10.10.241.94 -p 1338
```

```
(kali@kali) [~]
$ ftp 10.10.241.94 -p 1338
Connected to 10.10.241.94.
220 THM{WELCOME_101113}
Name (10.10.241.94:kali): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> !log
ftp> exit
221 Goodbye.
```

```
gobuster dir -u http://10.10.241.94:8000 -w
```

```
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,txt,zip -t 20
```

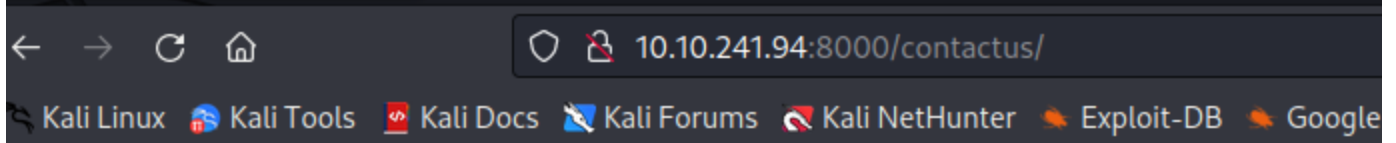
```
$ gobuster dir -u http://10.10.241.94:8000 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,txt,zip -t 20
```

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:             http://10.10.241.94:8000
[+] Method:          GET
[+] Threads:         20
[+] Wordlist:         /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:       gobuster/3.6
[+] Extensions:     php,txt,zip
[+] Timeout:         10s

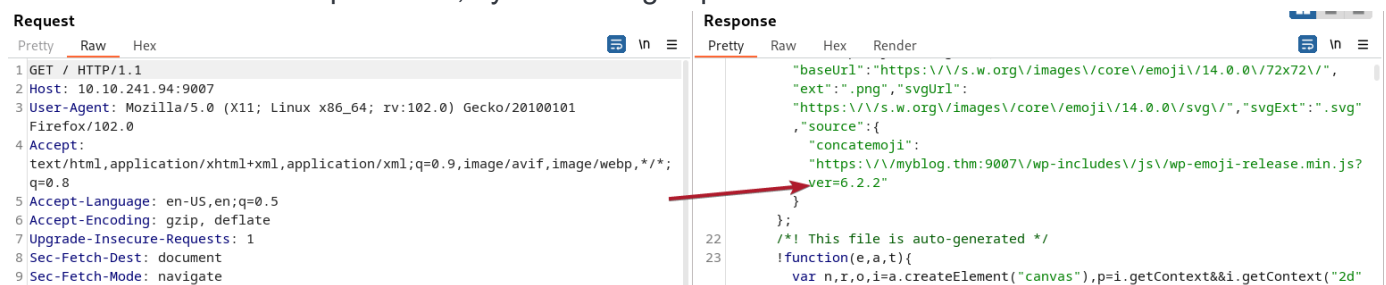
Starting gobuster in directory enumeration mode

/index.php           (Status: 200) [Size: 0]
/.php                (Status: 403) [Size: 279]
/contactus           (Status: 301) [Size: 323] [→ http://10.10.241.94:8000/contactus/]
/javascript           (Status: 301) [Size: 324] [→ http://10.10.241.94:8000/javascript/]
/phpmyadmin          (Status: 301) [Size: 324] [→ http://10.10.241.94:8000/phpmyadmin/]
```



flag: THM{0

```
80/tcp open http syn-ack lighttpd 1.4.55
|_http-server-header: lighttpd/1.4.55
|_http-methods:
|_Supported Methods: OPTIONS GET HEAD POST
|_http-title: 403 Forbidden
```



```
gobuster dir -u https://10.10.241.94:9007 -k -w
```

```
(kali㉿kali)-[~/THM/probe]
$ gobuster dir -u https://10.10.241.94:9007 -k -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,txt,zip -t 20
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                https://10.10.241.94:9007
[+] Method:             GET
[+] Threads:            20
[+] Wordlist:            /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:          gobuster/3.6
[+] Extensions:        zip,php,txt
[+] Timeout:            10s
=====
Starting gobuster in directory enumeration mode
=====
./php                  (Status: 403) [Size: 279]
/index.php             (Status: 301) [Size: 0] [→ https://10.10.241.94:9007/]
/wp-content            (Status: 301) [Size: 325] [→ https://10.10.241.94:9007/wp-content/]
/wp-login.php         (Status: 200) [Size: 5252]
/license.txt          (Status: 200) [Size: 19915]
/wp-includes          (Status: 301) [Size: 326] [→ https://10.10.241.94:9007/wp-includes/]
/javascript            (Status: 301) [Size: 325] [→ https://10.10.241.94:9007/javascript/]
/wp-trackback.php     (Status: 200) [Size: 135]
/wp-admin             (Status: 301) [Size: 323] [→ https://10.10.241.94:9007/wp-admin/]
Progress: 32429 / 882244 (3.68%)
```

```
[i] No DB Exports Found.

[+] Enumerating Medias (via Passive and Aggressive Methods) (Permalink setting must be set to "Plain" for
Brute Forcing Attachment IDs - Time: 00:00:03 ←=====
[+] Enumerating Medias (via Passive and Aggressive Methods)
Brute Forcing Attachment IDs - Time: 00:00:03 ←=====
[i] No Medias Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 ←=====
[i] User(s) Identified:

[+] Joomla
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Sat Nov 11 08:09:32 2023
[+] Requests Done: 3559
[+] Cached Requests: 7
[+] Data Sent: 1019.22 KB
[+] Data Received: 733.121 KB
[+] Memory used: 272.625 MB
[+] Elapsed time: 00:00:51
```

PHP extension build

https://10.10.241.94:1443	
Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Shift Cipher - Online D...	
Build Date	Jun 27 2023 15:49:59
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-mysqld.ini, /etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/15-xml.ini, /etc/php/7.4/apache2/conf.d/20-bz2.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-curl.ini, /etc/php/7.4/apache2/conf.d/20-dom.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-fli.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gd.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-json.ini, /etc/php/7.4/apache2/conf.d/20-mbstring.ini, /etc/php/7.4/apache2/conf.d/20-mysqli.ini, /etc/php/7.4/apache2/conf.d/20-pdo_mysqli.ini, /etc/php/7.4/apache2/conf.d/20-phar.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-readline.ini, /etc/php/7.4/apache2/conf.d/20-shmop.ini, /etc/php/7.4/apache2/conf.d/20-simplexml.ini, /etc/php/7.4/apache2/conf.d/20-sockets.ini, /etc/php/7.4/apache2/conf.d/20-sysmsg.ini, /etc/php/7.4/apache2/conf.d/20-syssem.ini, /etc/php/7.4/apache2/conf.d/20-sysshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini, /etc/php/7.4/apache2/conf.d/20-xmlreader.ini, /etc/php/7.4/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.4/apache2/conf.d/20-xsl.ini, /etc/php/7.4/apache2/conf.d/20-zip.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902.NTS
PHP Extension Build	API20190902.NTS
Debug Build	no
Thread Safety	disabled
Zend Shared Libraries	enabled