This homework refers to the following website:

http://web.engr.oregonstate.edu/cgi-bin/cgiwrap/rosulekm/ecb-hw.cgi

You can check out the source code here:

http://web.engr.oregonstate.edu/cgi-bin/cgiwrap/rosulekm/highlight.cgi?ecb-hw.cgi

This form allows you to create a new account on a system. When creating a new account, you receive a cookie with a cryptographic token that grants access to this account. The “admin” username is special. If anyone accesses the page with a valid token for admin, some secret administrative announcement will be displayed. However, the page does not allow you to create a new account named admin. Nevertheless, your goal in this homework is to obtain the secret admin announcement.

Note: A significant challenge in this homework is mentally managing the many different layers of encodings that are going on (encryption, URL-encoding, base64-encoding). You can help yourself out by always keeping track of which levels of encoding are present at each step.

1. What is the name of the cookie that is set by this page?

2. Authentication tokens are made by encrypting (then base-64 encoding) some raw data. Looking at the source code of the script, what must a token for the admin user contain as its raw data?

3. The token data is encrypted with a block cipher in ECB mode. If you weren’t told that it used ECB, and you didn’t have access to the source code, how could you verify that indeed used ECB?

4. How can you determine the block-length of the block cipher, just from the observable behavior of the website? What is the block-length used in this page? (your answer should be a number with units!)

5. What parts of the token raw-data can you (as the attacker) control?
6. You will need to get an admin token, which means you need to get encrypted blocks that encode the raw data you described in problem 2. What should you submit to the form in order to get these encrypted blocks? Why is it necessary/helpful to know the block-length for this step?

7. In the previous step, you would have obtain some kind of cookie token. Describe in full detail how you can use this cookie to obtain an admin token.

8. Find out how to use javascript to set a cookie for a page. Then manually set the cookie for this page to one of your own choosing, by using your browser's developer tools. For me, in Chrome, it's the “console” tab of the developer tools, where I can type in javascript that is executed in the context of the page.

    Note: With javascript you can set the raw cookie value, as would be sent in the HTTP headers. This raw value has the form “cookie1=val; cookie2=val; ...”, where each val is URL-encoded! You may find it convenient to use the javascript function encodeURIComponent.

9. What is the secret admin message?