WEB: Ajax Not Soap

The webpage looks like the following:

Our goal is probably to find a proper *username* and *password* that gives us access to the system and prints us (?) a flag. If you play a bit by inserting random strings inside the *textboxes* you see a message that says "*username incorrect*" or "*password incorrect*".

We can analyze the *javascript.*

```
$('#name').on('keypress',function(){
  // get the value that is in element with id='name'
  var that = $('#name');
  $.ajax('webhooks/get_username.php',{
  }).done(function(data){ // once the request has been completed, run this function
      data = data.replace(/(\r\n|\n|\r)/gm,""); // remove newlines from returned data
      if(data==that.val()){ // see if the data matches what the user typed in
        that.css('border', '1px solid green'); // if it matches turn the border green
        $('#output').html('Username is correct'); // state that the user was correct
      }else{ // if the user typed in something incorrect
        that.css('border', ''); // set input box border to default color
        $('#output').html('Username is incorrect'); // say the user was incorrect
      }
    }
  );
});
// dito ^ but for the password input now
$('#pass').on('keypress', function(){
  var that = $('#pass');
  $.ajax('webhooks/get_pass.php?username='+$('#name').val(),{
  }).done(function(data){
      data = data.replace(/(\r\n|\n|\r)/gm,"");
      if(data==that.val()){
        that.css('border', '1px solid green');
        $('#output').html(data);
      }else{
        that.css('border', '');
        $('#output').html('Password is incorrect');
      }
    }
  );
});
```

There are two main functions, one that checks the *username*, and one that checks the *password*. The correct pairs of username-passwords are retrieved using a “webhooks” *ajax* function.

Well, since this is a client-side control, we can use the browser debugger and set two breakpoints on the lines that clean the *data* variable (i.e., *data = data.replace([...])*). Thus, we can just type random stuffs on the username, and the breakpoint shows us the real value of *username*:

Username = MrClean

Great! We know the username, and thus we can insert this correct value on its username field. We can do the same for getting the password (we type random characters).

This time the content of the password is the flag itself!

Flag = flag{hj38dsjk324nkeasd9}