Baba-OAuth

Web Services // 120 points

Description

It was reported that an intern managed to use a discount coupon from the intern's boss. The discount coupon feature is implemented with OAuth. The intern only had his own credentials and the username of his boss. You will be using Baba's Oauth web application for this challenge. Connect to http://p7ju6oidw6ayykt9zeglwyxired60yct.ctf.sg:2416 to try it out.

Find out what the intern did to access the boss's discount coupon to retrieve the flag.

Please refer to the provided details below.

Intern's credentials: - username = intern@baba.com - password = internP@ssw0rd123

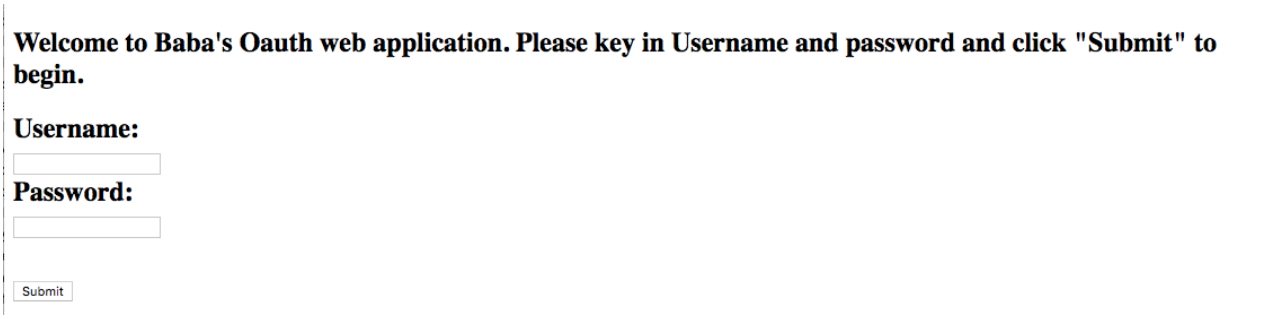
Boss's credentials: - username = internBoss@baba.com

List of all the scopes that the OAuth server accepts:
Y29tLmN5YmVydGhvbi5MQHpAbUAtZGkkYzB1bnQ=
Y29tLmN5YmVydGhvbi5ENkB5LWRpJGMwdW50
Y29tLmN5YmVydGhvbi5QMDA5LWRpJGMwdW50
Y29tLmN5YmVydGhvbi5CQDEwckAtZGkkYzB1bnQ=
Y29tLmN5YmVydGhvbi5CQGJALWRpJGMwdW50
Y29tLmN5YmVydGhvbi5DQHIwdTZ1eS1kaSRjMHVudA==
Y29tLmN5YmVydGhvbi5CMXUzbUBydC1kaSRjMHVudA==
Y29tLmN5YmVydGhvbi5EaTVoMG4zNXRiMzMtZGkkYzB1bnQ=
Y29tLmN5YmVydGhvbi5BMWloQGhALWRpJGMwdW50
Y29tLmN5YmVydGhvbi5CQDBUQDAtZGkkYzB1bnQ=

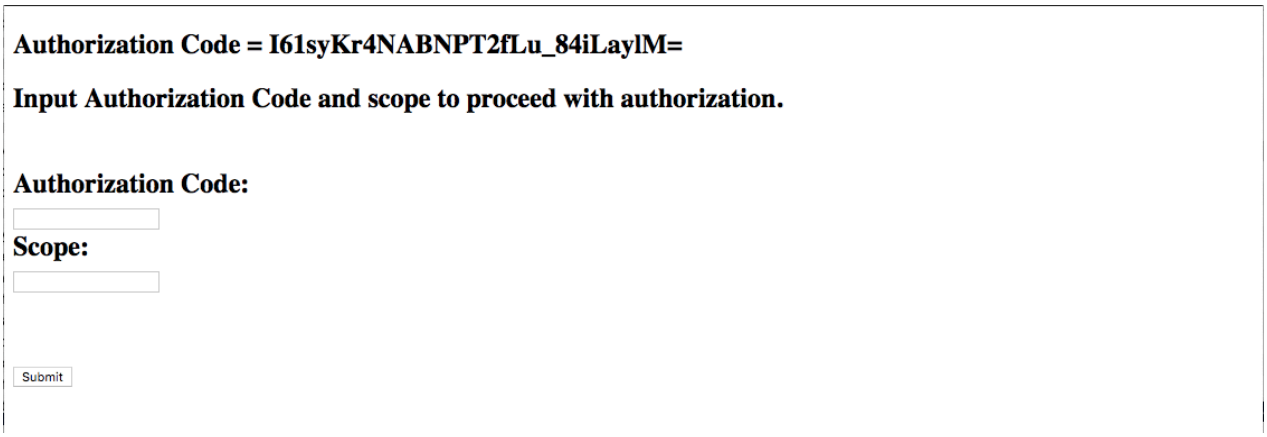
- The scopes are encoded such that it is safe to use in the URL.

Solution

Opening up the link gave us a simple login page, and all we needed to do is to key in the provided intern username and password.

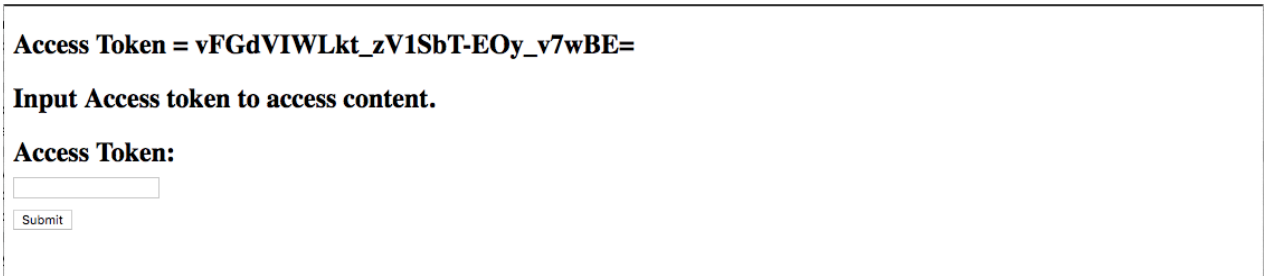


On successful login, we reach the page where they ask us to enter the authorization code and scope. However, we know that the authorization code generated belongs to the intern and not the boss, therefore there must be something to change to gain access to the boss's account.



With close inspection to the URL, we notice that at the end there is a `username=intern%40baba.com`. We know that `%40` is the url encoded representation for the `@` sign and thus it is the username of the account.

Changing that to `internBoss%40baba.com`, we get a new authorization token to use. Putting in the first scope (well no harm trying every one of them) and the code we get to a new access page.



The access page just needs us to copy the token, and which we do, leading us to the discounts page. However, there is not a discount as the scope provided has no discount.

So after trial and error by trying all the scopes, we finally found the one that works and obtain our flag.

Takeaways

- The challenge honestly wasn't very well done, when you take too long to copy the code and go to the next page, the code might have expired and only gives you some information that might make you think otherwise about the error. This might be very misleading as OAuth has quite a number of other parameters that might be missing in this challenge.