SCENARIO

The application a serialization-based session mechanism and is vulnerable to authentication bypass as a result. We will try to edit the serialized object in the session cookie to exploit this vulnerability and gain administrative privileges.

**PROCEDURE**

1. Go the application and login using the given credentials to act as an user.
2. Navigate to the **My Account** page.
3. Open the BurpSuite’s Proxy’s HTTP History and study the request carefully.
4. We notice that the session cookie is encoded in Base64 and then in URL encoding.
5. We decode it in BurpSuite and we can see that it appears in the format below:

**O:4:"User":2:{s:8:"username";s:6:"wiener";s:12:"access\_token";s:32:"y4esqtkxwo718kbom0duosnt6nvln9f5";}**

1. So, we inject the payload in place of the above value.
2. Now we access the **Admin Panel** using the response we got and delete the user by hitting the endpoint we found in the page.

**PAYLOAD**

O:4:"User":2:{s:8:"username";s:13:"administrator";s:12:"access\_token";i:0;}

**REMEDIATION**