

Nome: Leonardo "Quazmo" Moura

Pico CTF> Factory Login

Origem: <https://jupiter.challenges.picoctf.org/problem/13594/>

Para fazer está resolução, foi usado o Burp Suite.

O site possui uma tela de login

Factory Login

Home Sign Out

Username

Password

Sign In

© PicoCTF 2019

Temos a dica do próprio CTF que queremos pegar o login do Joe

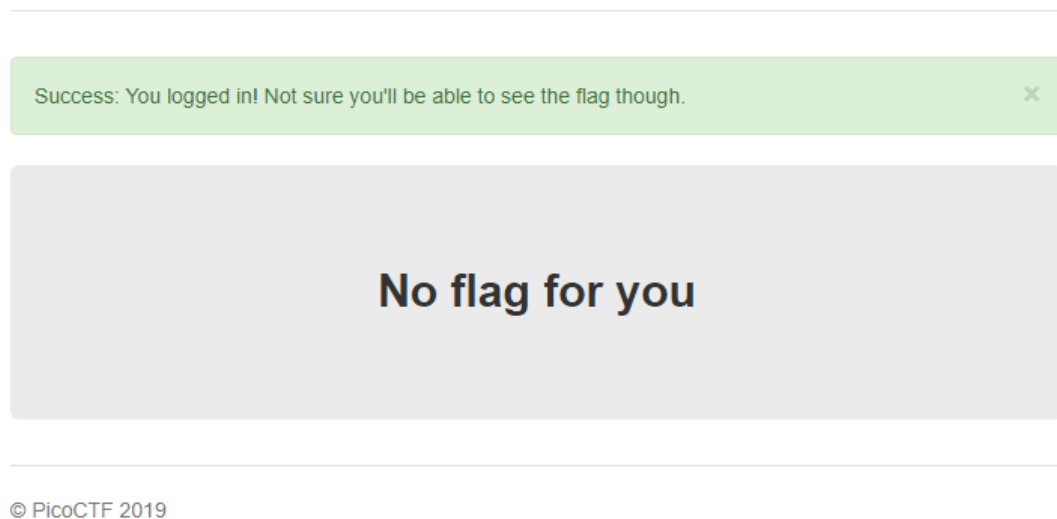
I'm sorry Joe's password is super secure. You're not getting in that way. ✕

Username

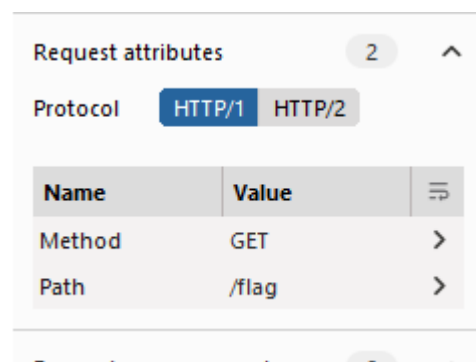
Password

Sign In

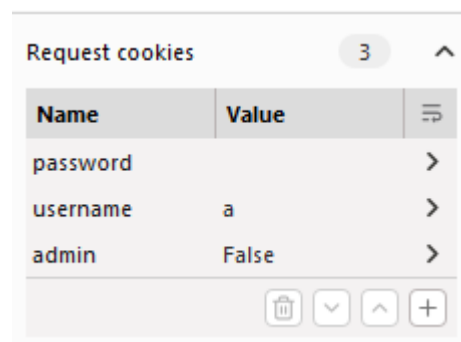
Quando tentamos o username de Joe com qualquer senha temos a resposta acima, e quando tentamos qualquer outro user com uma senha qualquer temos a resposta abaixo:



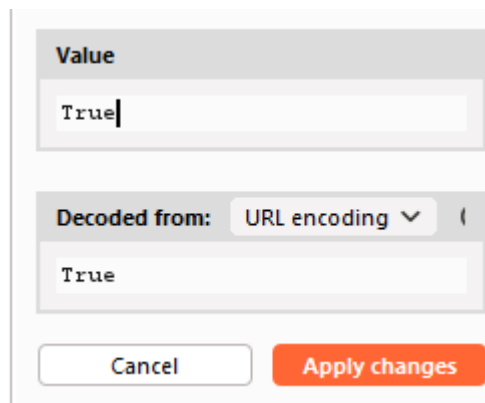
Usando o Proxy Intercept do Burp Suite, vamos mexer no segmento de login do usuário após entrar com um login qualquer. O primeiro intercept nos mostra o caminho /login, que não nos trás nada de muito interessante, mas logo após /login temos um caminho chamado /flag



Podemos ver cookies interessantes neste caminho, que checka se o usuário é um admin



Mudando o valor de false para true e enviando a request:



Value

True

Decoded from: URL encoding

True

Cancel Apply changes

Factory Login

Home

Sign Out

**Flag:**

picoCTF{th3\_c0nsp1r4cy\_l1v3s\_d1c24fef}

© PicoCTF 2019

Bingo.