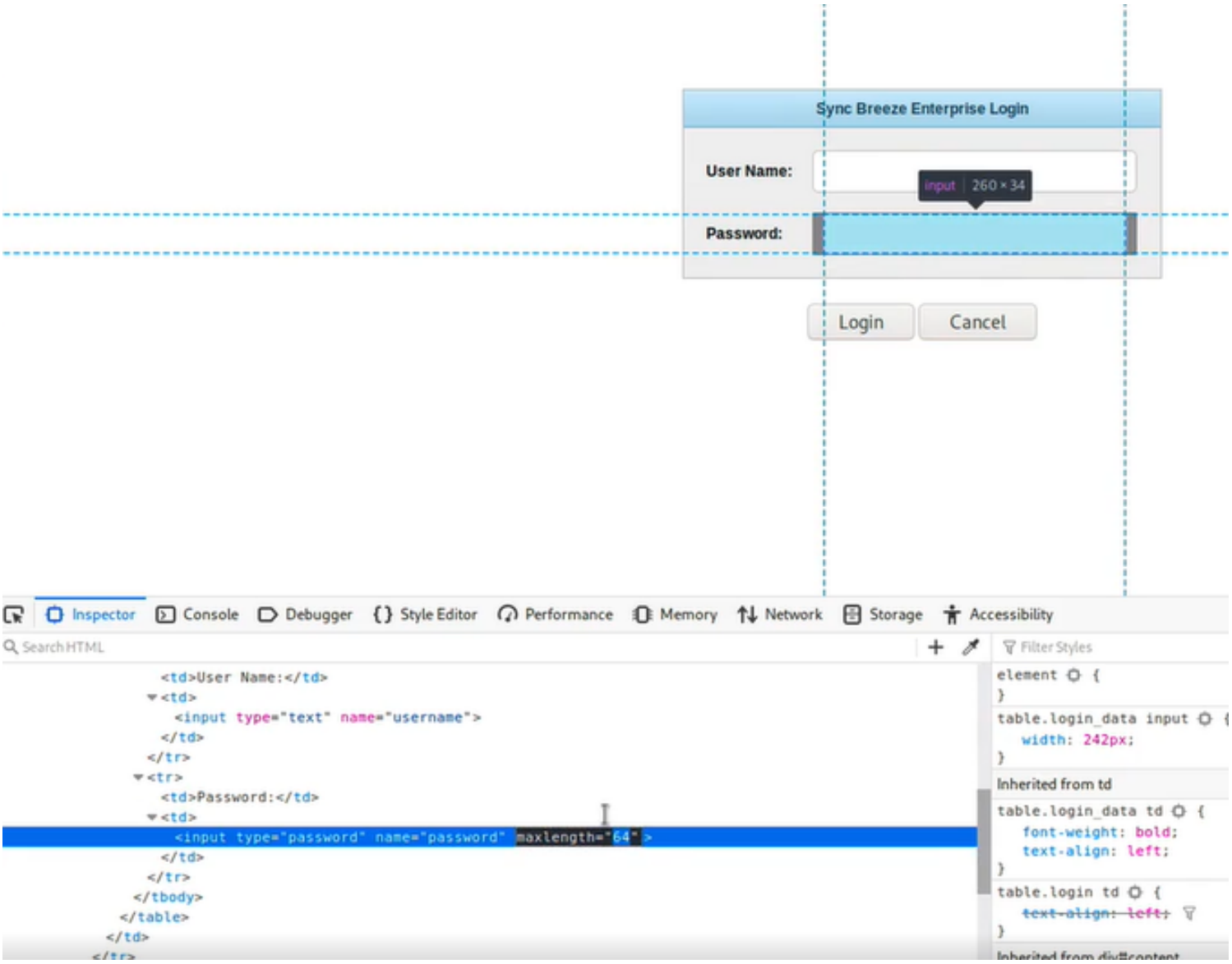
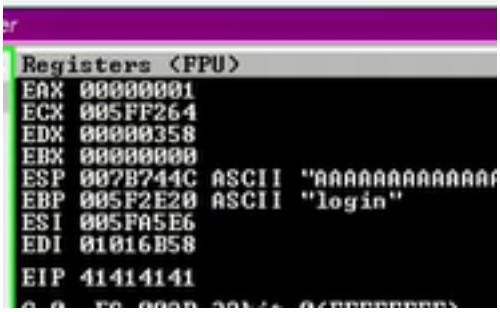
Identificando a Vulnerabilidade

+ Vimos anteriormente que temos dois campos de entrada (usuário e senha)



→ Vamos remover o maxlength

→ Se enviarmos 1000A's no user name, e tbm no pass, veremos a sobrescrição no debugger



→ O EIP foi sobrescrito com os A's

→ Em ESP tbm temos mais A's

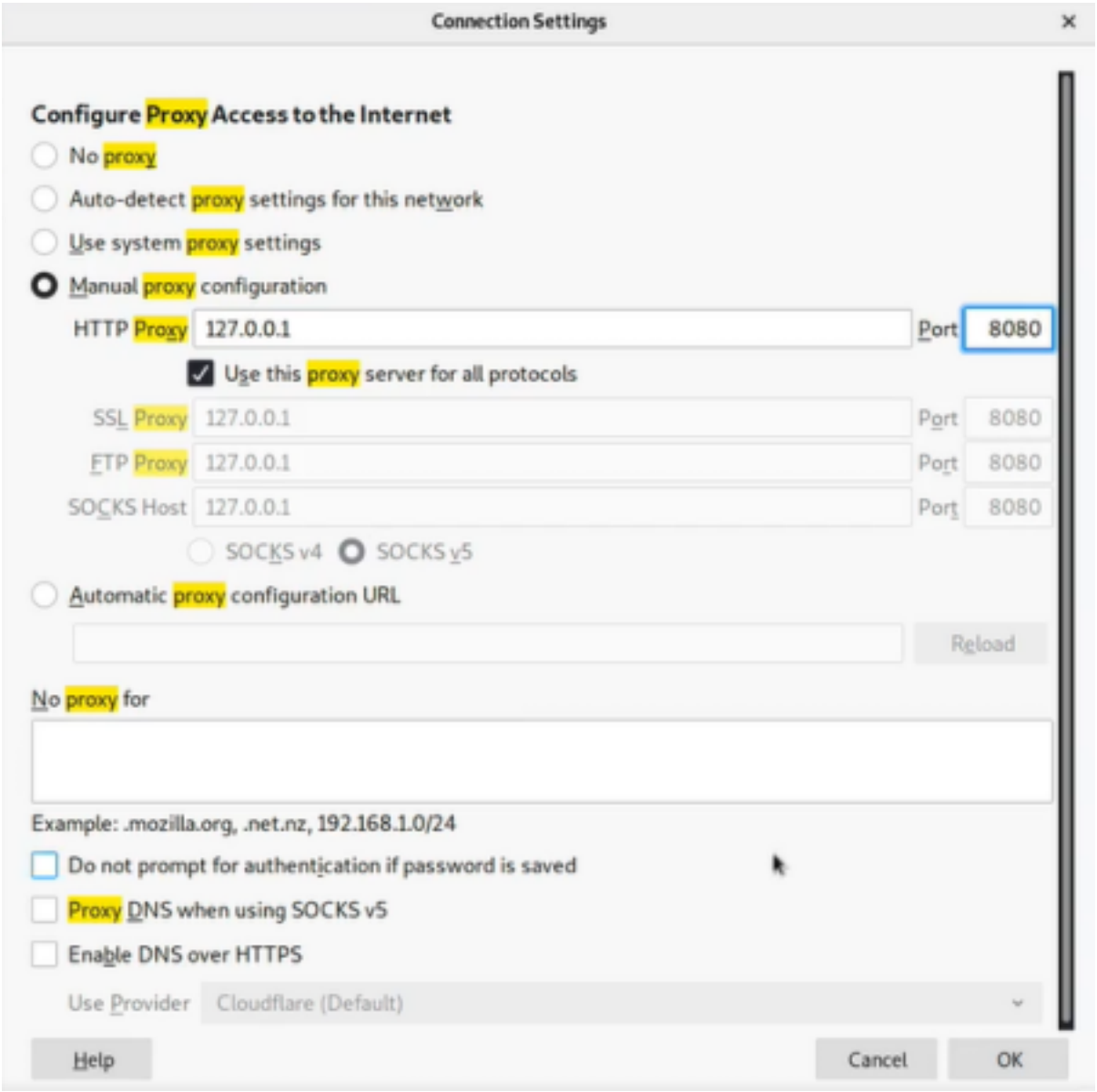
→ Acabamos então de descobrir um bufferoverflow em um software
→ Como isso dá um crash na aplicação, devemos reiniciá-la para conseguir voltar às análises
→ Devemos fazer isso para testar tanto o campo de usuário quanto o campo de pass
→ Vamos usar um proxy pra invés de ficar reiniciando o serviço, nós gerarmos uma requisição única e ficar repetindo ela quantas vezes precisarmos

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

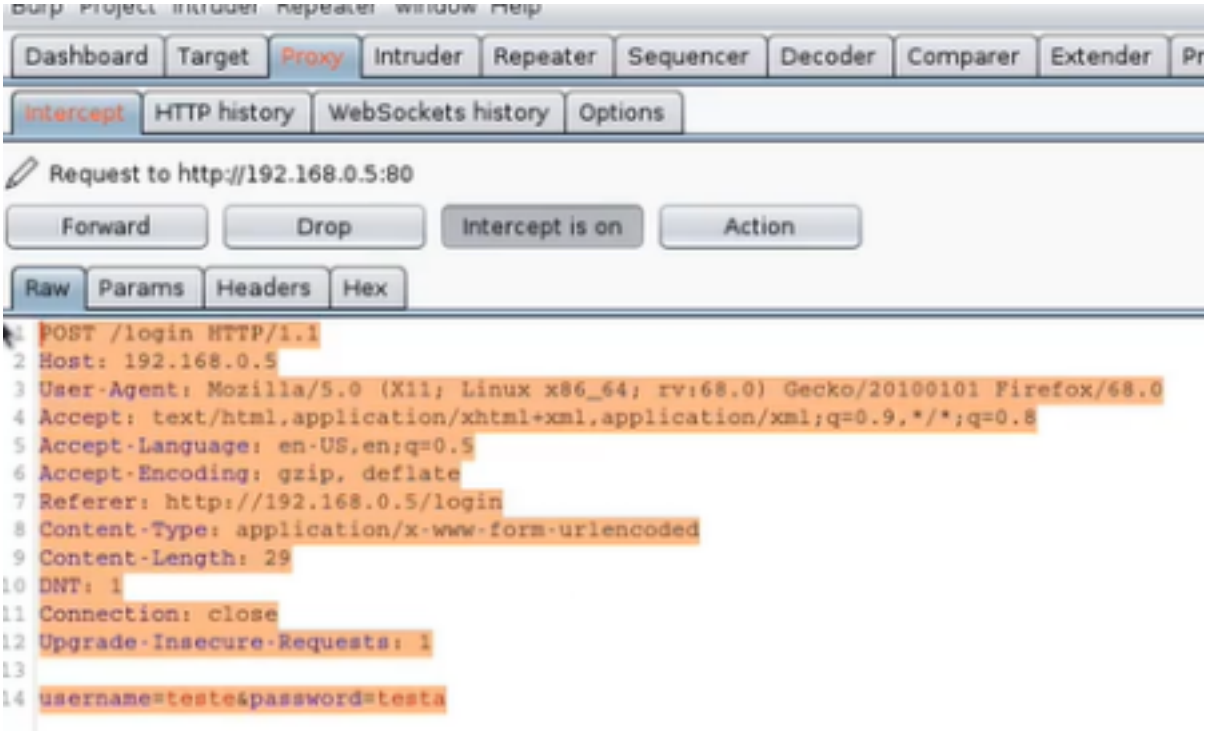
BURPSUITE

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

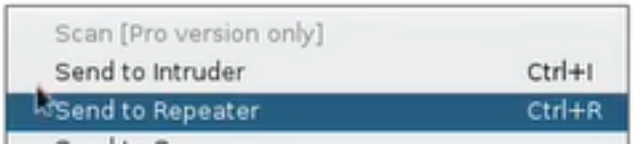
OK → NEXT → START BURP
Devemos primeiro configurar um proxy no navegador



→ Ajuste manual das configurações do proxy
→ Ou seja, estamos falando para o navegador que tudo o que fizermos será interceptado pelo proxy
→ Na aba Intercept poderemos ver a requisição feita

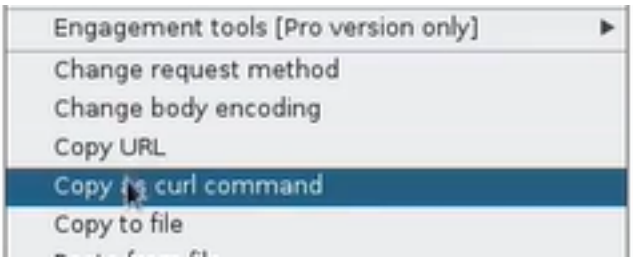


→ Com o botão direito do mouse, podemos enviar para o repeater



→ Podemos desabilitar o intercept

→ Podemos também copiar a requisição como um comando do curl




```
curl -i -s -k -X $'POST' \
    -H $'Host: 192.168.0.5' -H $'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0' -H $'Accept: te
    --data-binary $'username=tasdas&password=asdasda' \
    $'http://192.168.0.5/login'
```