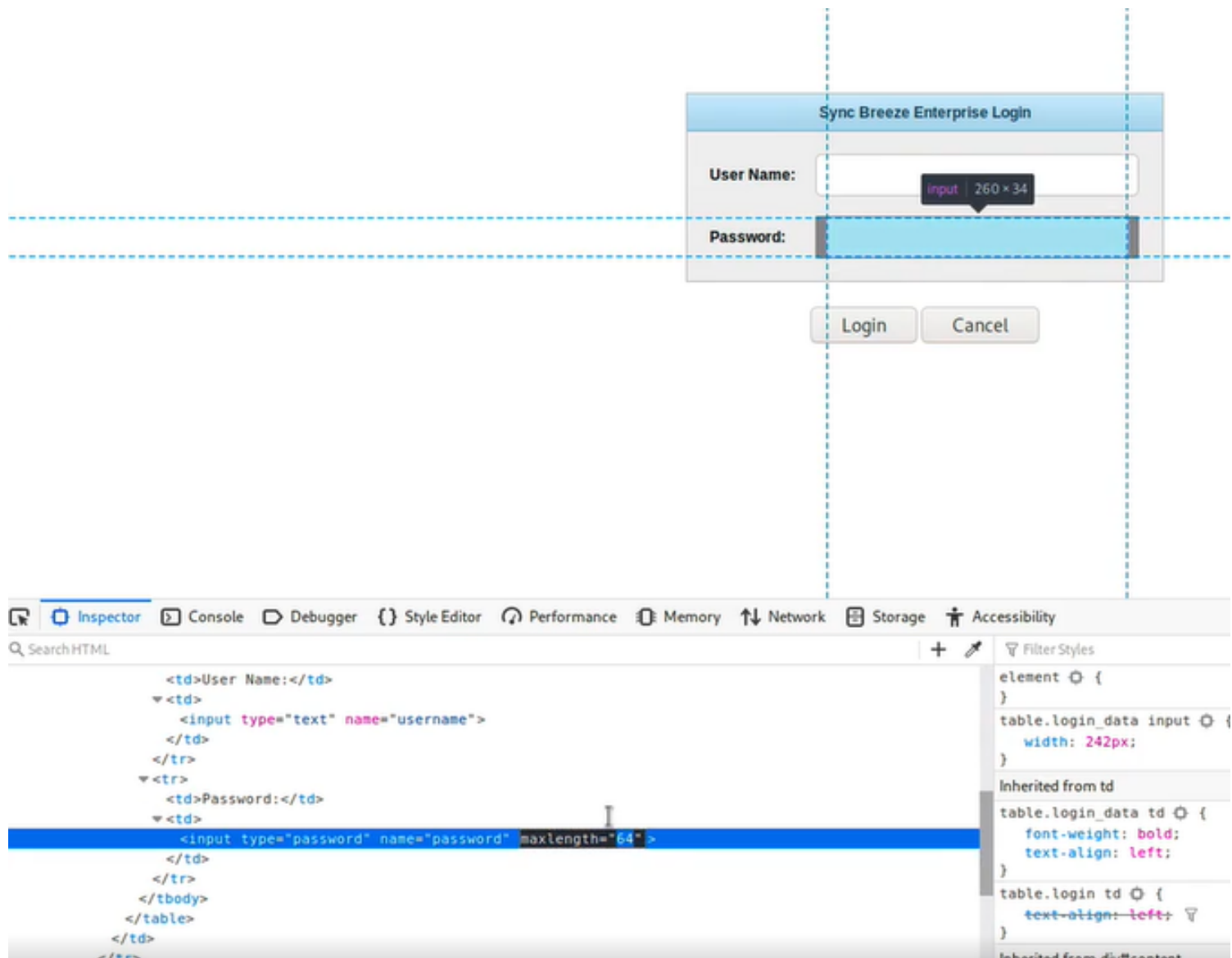


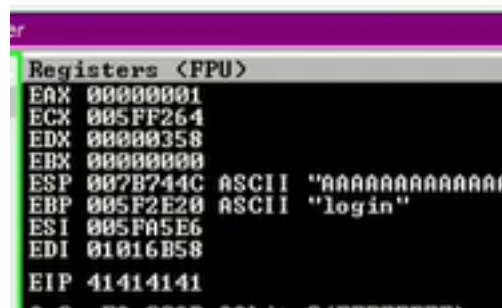
Identificando a Vulnerabilidade

+ 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

[illegible]

→ 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

Connection Settings

Configure Proxy Access to the Internet

☐ No proxy
☐ Auto-detect proxy settings for this network
☐ Use system proxy settings
☒ Manual proxy configuration

HTTP Proxy: 127.0.0.1 Port: 8080
☒ Use this proxy server for all protocols

SSL Proxy: 127.0.0.1 Port: 8080
 FTP Proxy: 127.0.0.1 Port: 8080
 SOCKS Host: 127.0.0.1 Port: 8080
☐ SOCKS v4 ☒ SOCKS v5

☐ Automatic proxy configuration URL

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

☐ Do not prompt for authentication if password is saved
☐ Proxy DNS when using SOCKS v5
☐ Enable DNS over HTTPS

Use Provider: Cloudflare (Default)

→ Ajuste manual das configurações do proxy

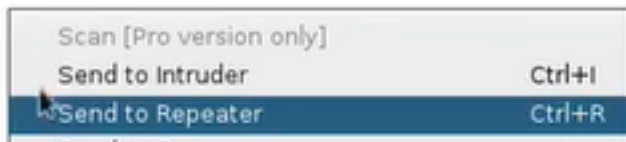
→ Ou seja, estamos falando para o navegador que tudo o que fizermos será interceptado pelo proxy

→ Na aba Intercept poderemos ver a requisição feita

```

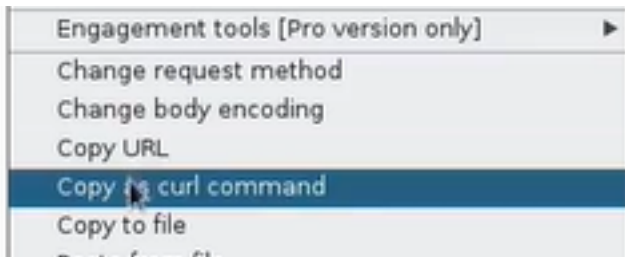
1 POST /login HTTP/1.1
2 Host: 192.168.0.5
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.0.5/login
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 29
10 DNT: 1
11 Connection: close
12 Upgrade-Insecure-Requests: 1
13
14 username=teste&password=teste
  
```

→ 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'
```