Python

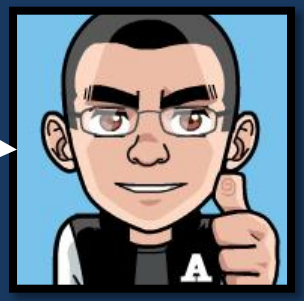
Para Análises de Segurança

Daniel Marques

I Escola Regional de Sistemas de Informação

Novembro - 2014

Daniel Marques
@0xc0da



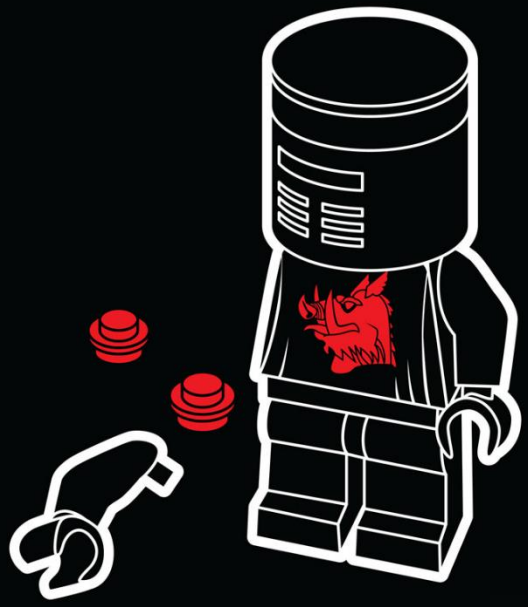
```
0xc0da['pentester'] = True
0xc0da['pesquisa'] = ['python',
                      'password cracking',
                      'web apps']
```

Um lembrete
(é, o mesmo de sempre)

O conteúdo apresentado representa minhas próprias conclusões e opiniões e não as de meus empregadores, clientes e afins.

Não há intenção de causar nenhum dano. A utilização do conteúdo apresentado é fruto de pesquisa e deve ser utilizado apenas quando autorizados.

Algumas dicas iniciais



Estruturas Interessantes

```
pythons = [‘Eric’, ‘John’, ‘Michael’]
```

Listas

```
filmes = {‘Titulo’: ‘Holy Grail’, ‘Ano’: 1975}
```

Dicionários

```
eps = ‘Dead Parrot’, ‘Cheese Shop’
```

Tuplas

```
what = (‘spam’, ’ham’)
```

Sets

Programas servem para Resolver problemas

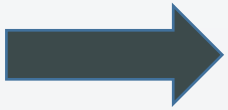
Objetivo?

Restrições?

Regras?

Dividir um grande problema em problemas menores

Extrair links de uma página web



Carregar a página

Interpretar código HTML

Para cada tag a, extrair atribute href

Usando módulos como Blocos de montar

```
import requests

import csv
```

Pacotes separados da instalação real

virtualenv(wrapper)

Ambientes virtuais FTW

Sujando um pouco as mãos

Análise de Logs
Estudo de Caso 1

Ler arquivos de log

Interpretar formato

Gravar arquivo CSV

Análise de PCAPs
Estudo de Caso 2

Ler pacotes →  pycap, dpkt

Extrair Geolocalização →  pygeoip

Bruteforce
Estudo de Caso 3

Carregar página

requests

Interpretar HTML

Preencher formulário

BeautifulSoup

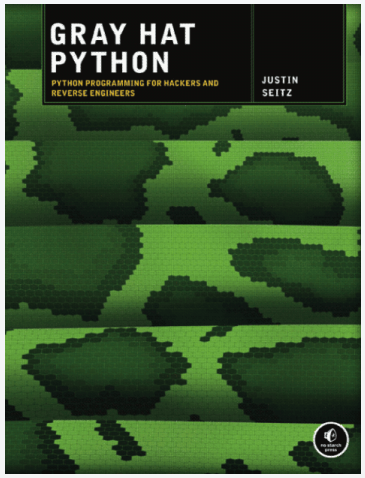
mechanize

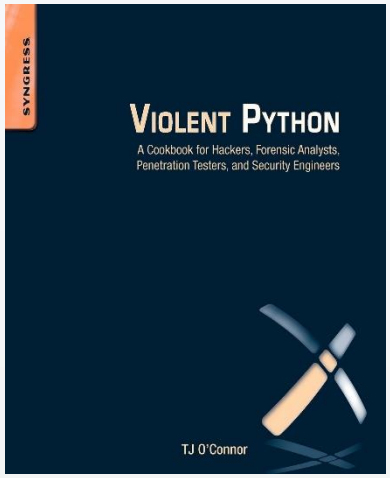
Aplicação BING API

Para enumeração

Finalizando

Sugestões para estudar





SecurityTube Python Scripting Expert

Não da Mechanize.
A Documentação é Péssima.

Obrigado!

daniel@codalabs.net

@0xc0da

codalabs.net

/0xc0da