GAME OF HASHES

QUEBRANDO, PASSANDO E LIBERTANDO SENHAS

DANIEL MARQUES

CoOL BSIDES SÃO PAULO

NOVEMBRO 2013

UM LEMBRETE

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

Não há intenção de causar nenhum dano a terceiros. O conteúdo apresentado é fruto de pesquisa e deve ser utilizado apenas em ambientes autorizados.

@0XC0DA

> Pentester

> Curte o hacking moleque, malemolente, de várzea

> Não é “password cracker profissional”

Esta é uma pesquisa em fase embrionária.

Quer colaborar?
É só me procurar!

Estamos usando as wordlists certas?

Talvez.


PERFORMANCE DAS
WORDLISTS

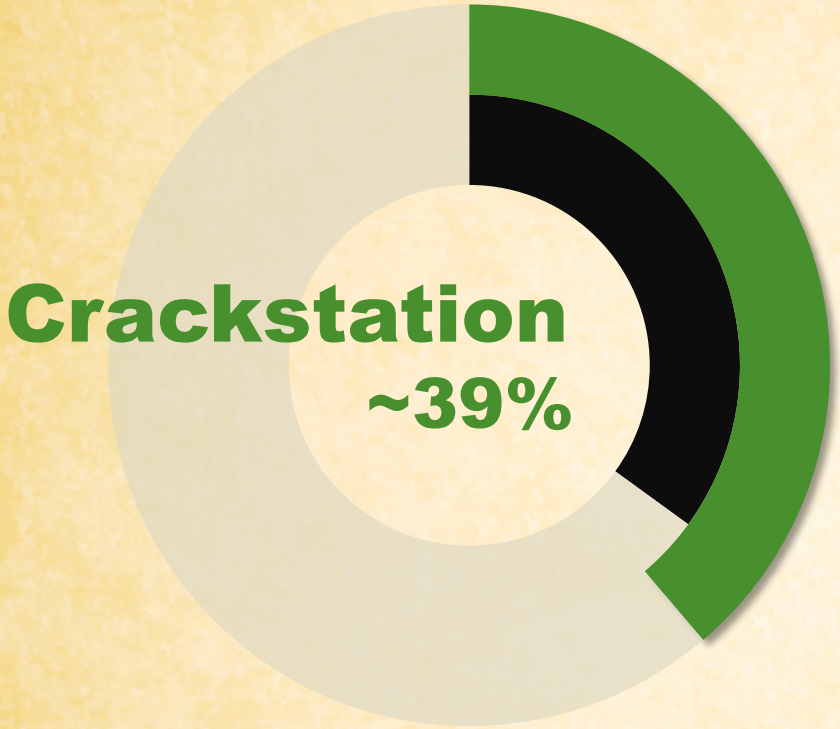
5 Wordlists

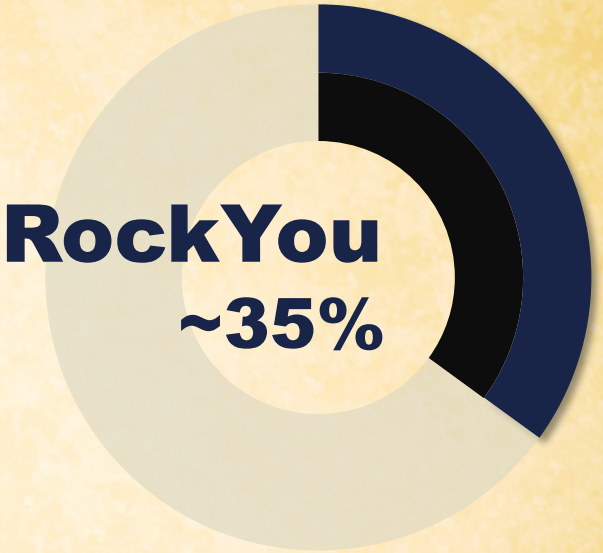
Crackstation Human Only
InsidePro 2012
RockYou
Cain & Abel
John The Ripper
500 Worst Passwords

3 Cenarios

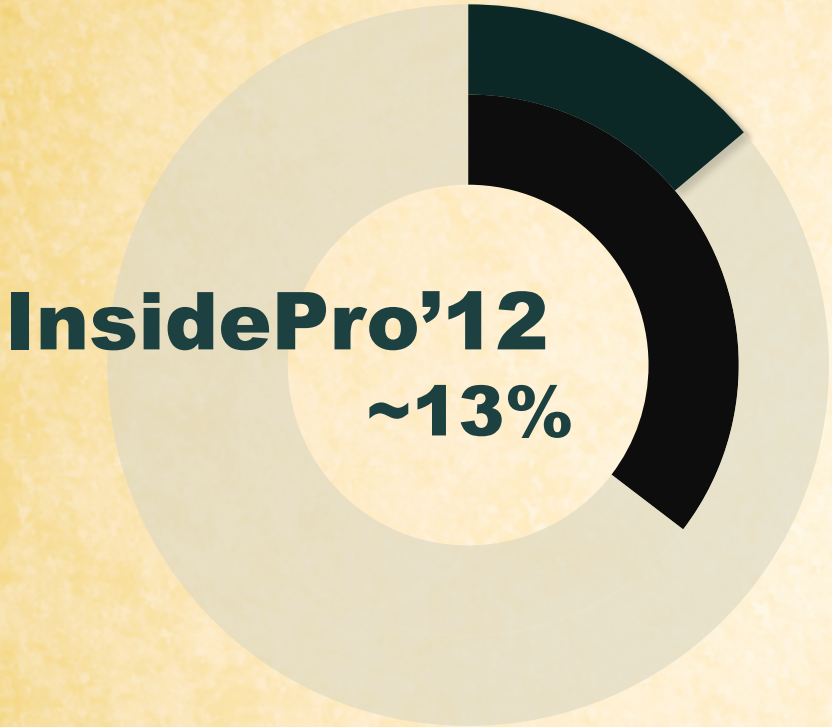
Sem política de senhas
8 Caracteres alfanuméricos
6 Caracteres alfanuméricos + 1 especial

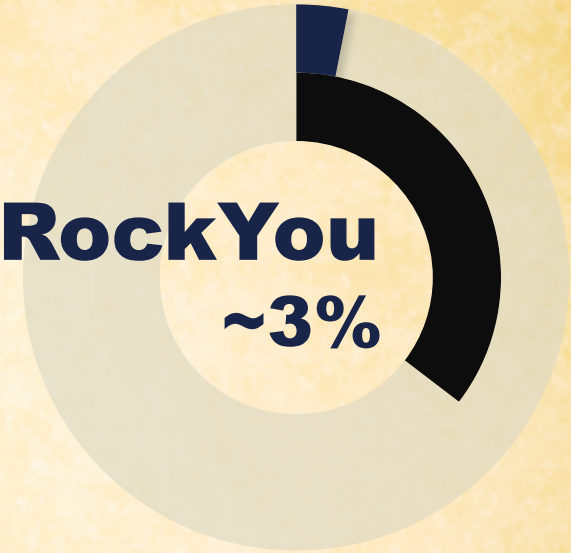
i · sem política aplicada

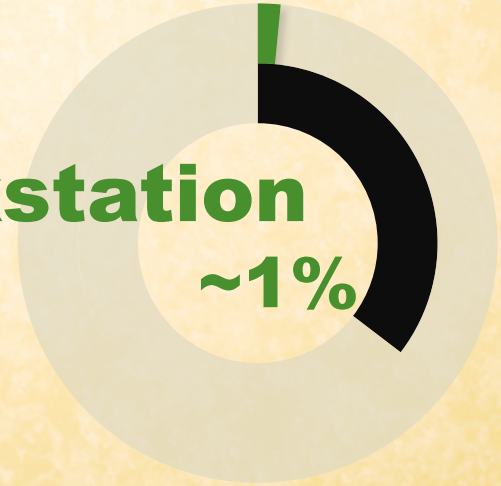




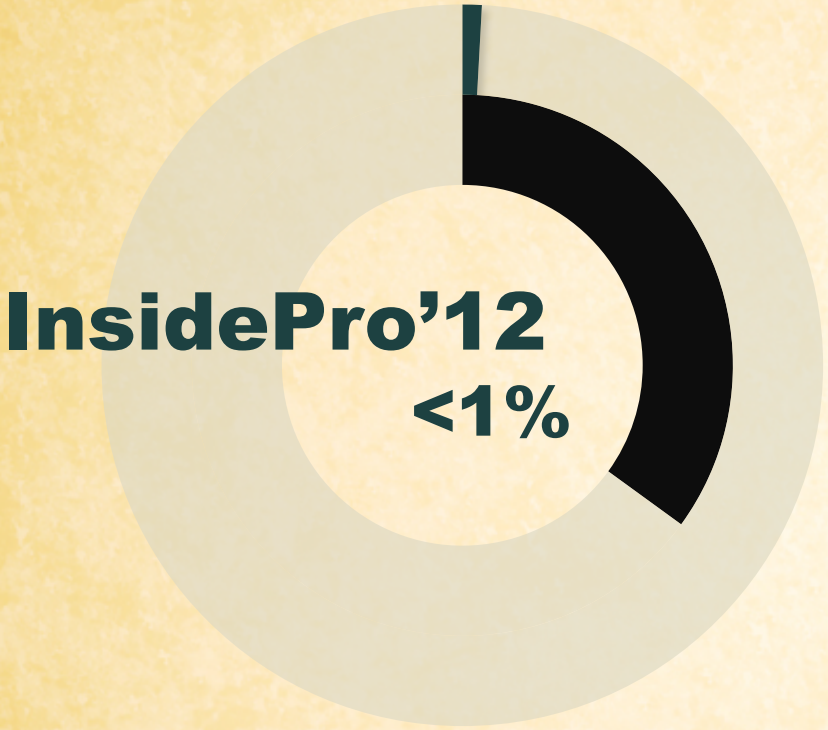
ii · 8 chars + alfanum

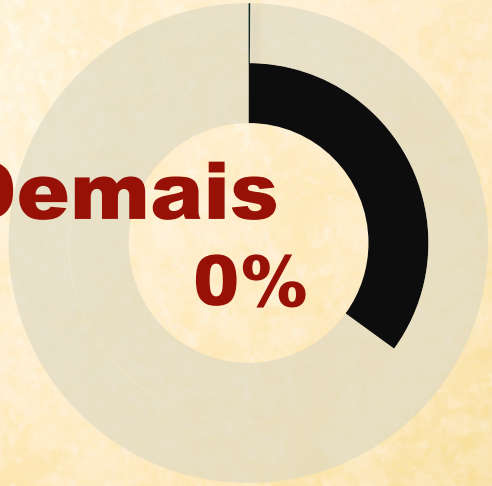




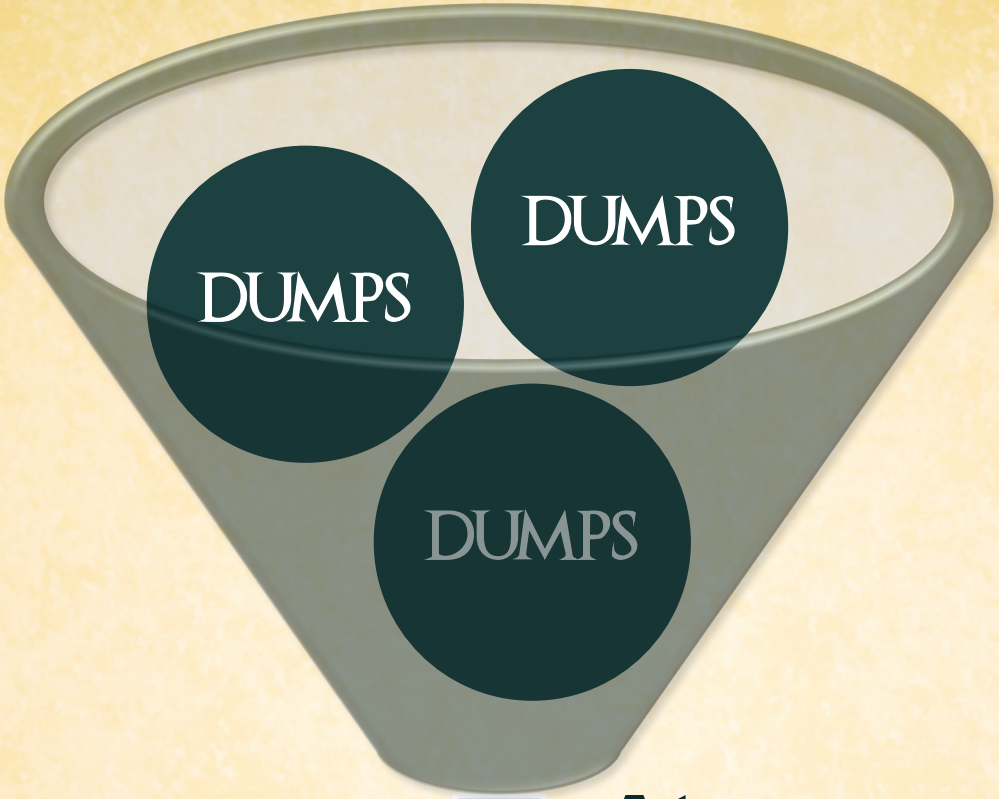


iii · 6 chars + alfanum + especial





UMA WORDLIST PT-BR



Atacar os hashes
Analisar resultados

Wordlist

desafio 1

Poucos dumps .br Disponíveis publicamente

Desafio 2

Hashes truncados

Listas com hashes

Dumps sem padrão

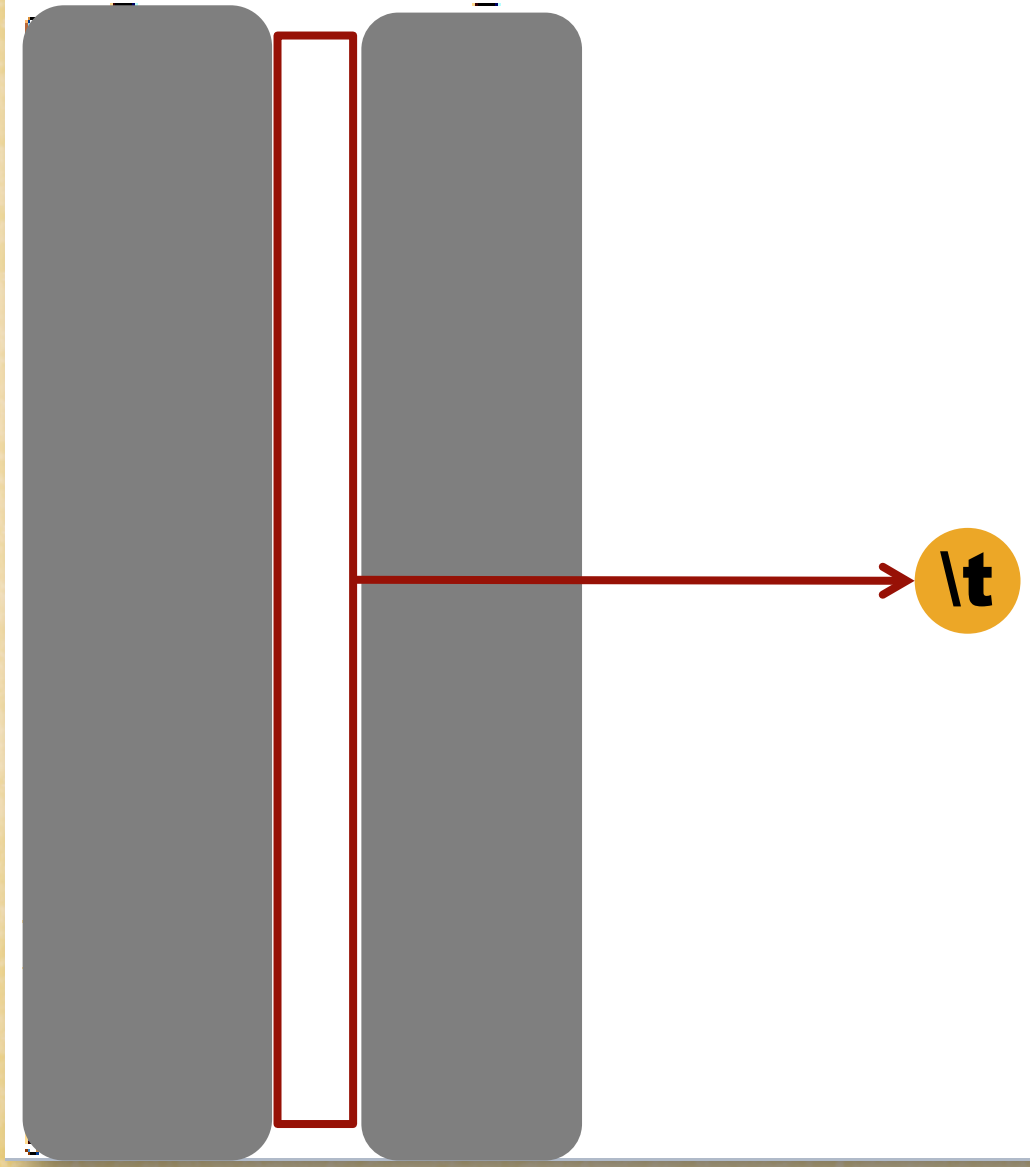
Usuários/senhas separados por tab

Saída do sqlmap

Arquivos CSV

SITE:
http://www.[redacted]com.br/

user_name user_passwd



Site:http://www.[redacted].br

Não esqueçam de descriptografar as senhas :)

tabela usuario nome & email & senha

nome:[redacted] email:[redacted] senha:[redacted]

nome:[redacted] email:[redacted] senha:[redacted]

Desafio 3

Inexistente?

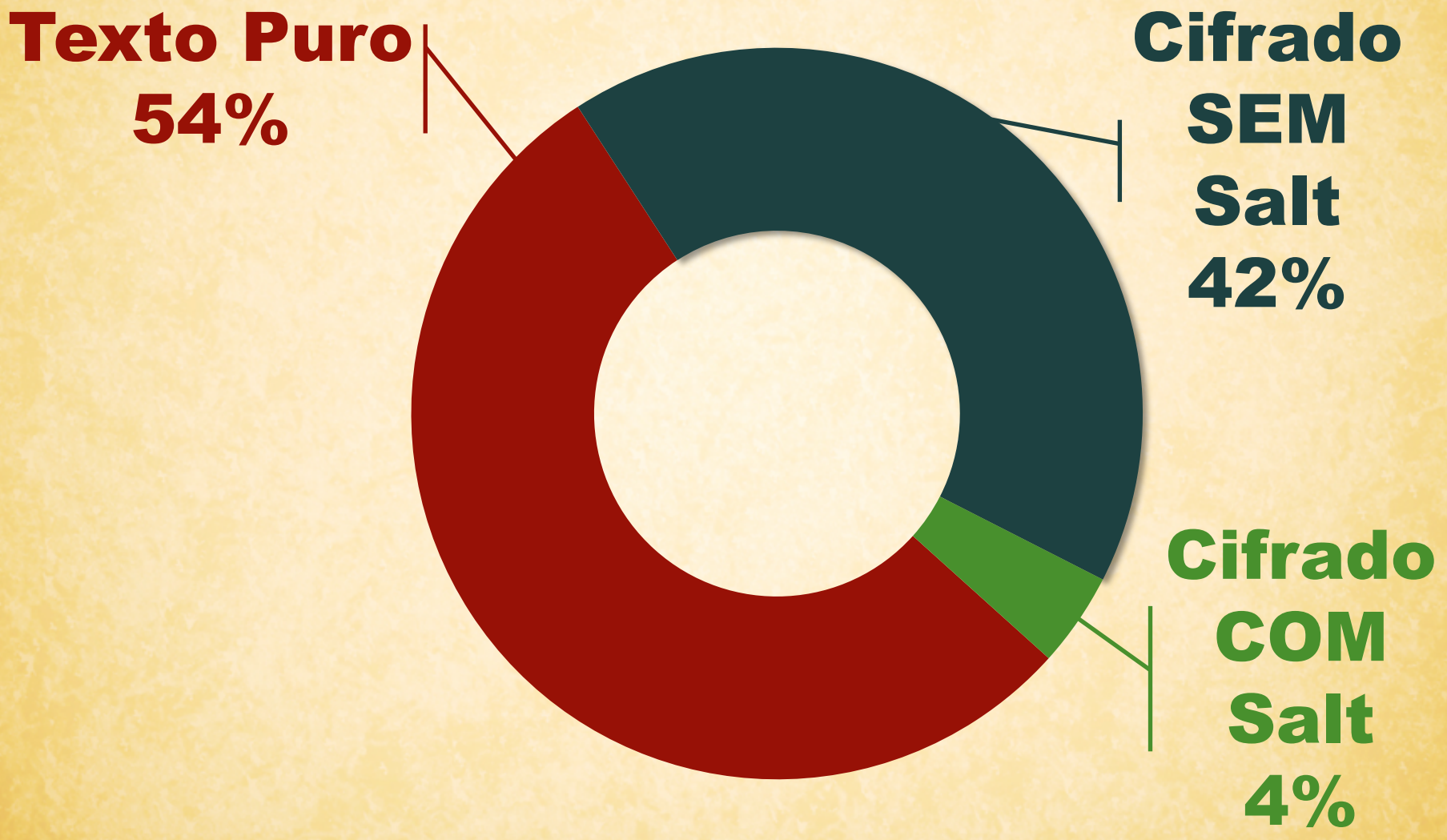
Caracteres especiais?

Identificar políticas

Maíusculas e Minúsculas?

Palavras proibidas?

curiosade sobre os dumps



Fontes de dados para wordlists

Redes Sociais

Wikipedia

Arquivos .pot

ALGUNS PADRÕES OBSERVADOS

sem política de senhas?

6 - 8 Caracteres

Apenas Números

Nome do Sistema

maiúsculas + alfanúmericas?

Bsidessp1

José2

maiúscula + alfanum + especial?

maiúscula + alfanum + especial

Jose@123

JDS.123

BÔNUS: SENHAS INTERESSANTES

soeusei


O RLY?

Euamovosse


JUSTIÇA
TAH SERTO !

taradinhogostosinhovemnaminhavem


O quê...

winteriscomingpracar***o

winteriscomingpracar***o

Códigos no GitHub

OBRIGADO

daniel@codalabs.net


@0xc0da


codalabs.net

/0xc0da