A SONG OF HASHES AND DUMPS

WHAT I'VE LEARNED FROM CRACKING .BR PASSWORDS

Daniel Marques

Black Hat Regional Summit São Paulo

November 2014

Daniel Marques

@0xc0da, your friendly neighbor

Penetration Tester

First time Blackhat Speaker

Not a “professional” password cracker

Disclaimer

This research has no intention to cause any harm. It is only for educational purposes. Opinions on my own, so my employer or clients cannot be hold responsible for what you will see here.

PasswordsCon ‘13

“**50%** of hashes can be cracked with **RockYou + best64**”

Works for
.br hashes?

Collect

.br dumps

Classify

the hashes

Analyze

data

Focus on

lessons learned

during the research

tools rules wordlists

lessons learned

scripts patterns stats

Challenge #1

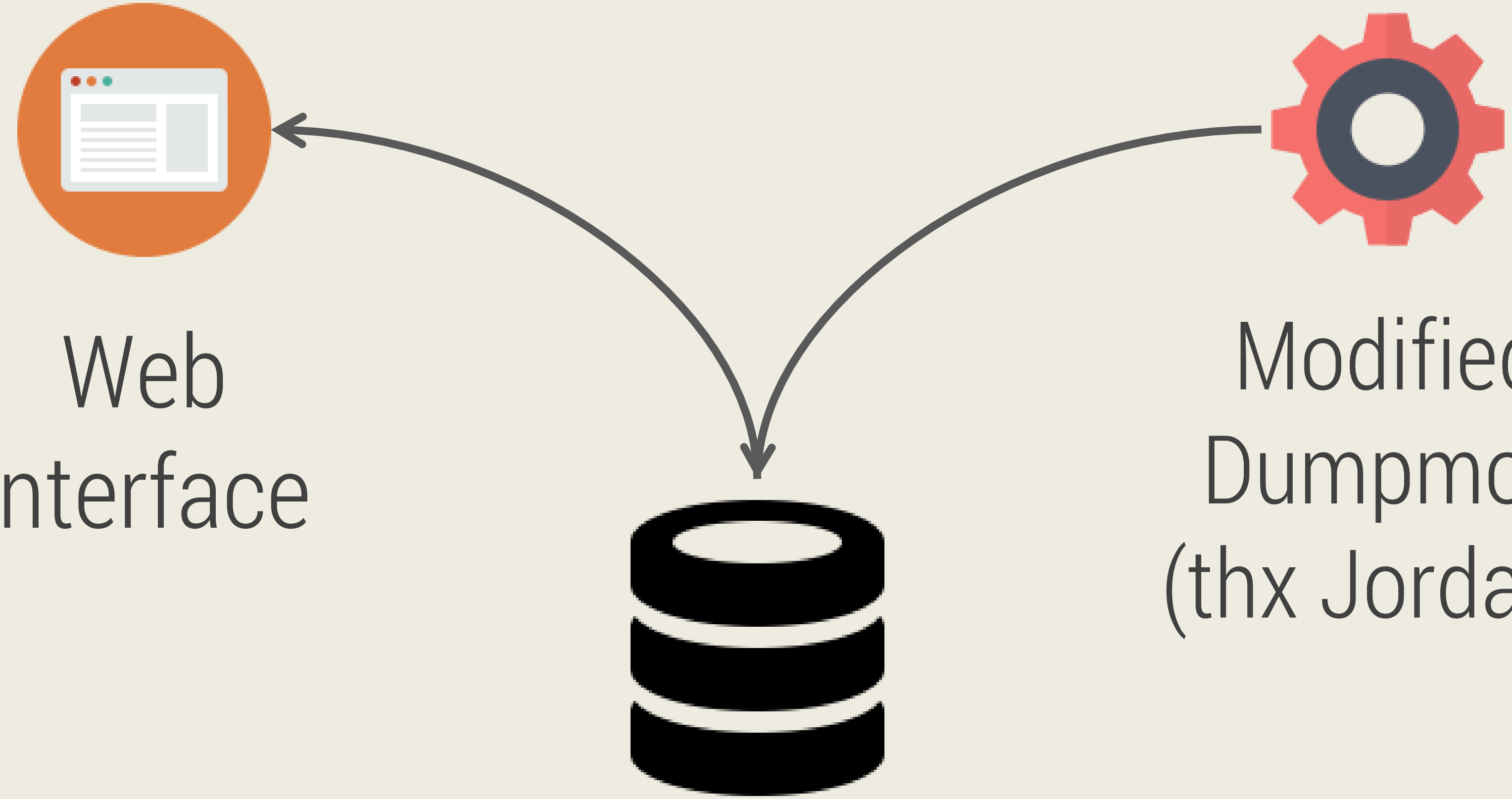
Collecting .br dumps

few dumps available
keeping organized

Enter **pastebot**

Automating dump collection and organization

pastebot



Web interface

Pastebot db

Modified Dumpmon (thx Jordan!)

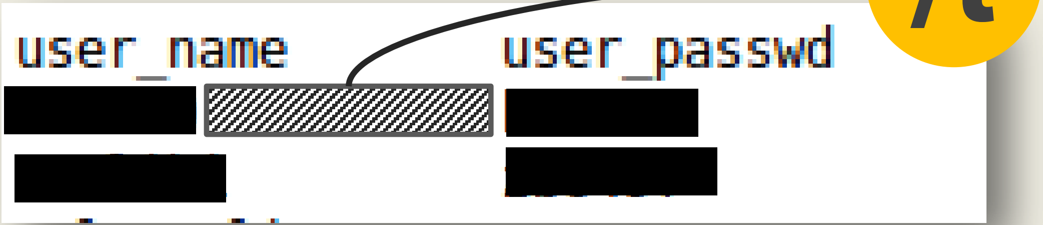
Challenge #2

Extracting dump data

bad formatting

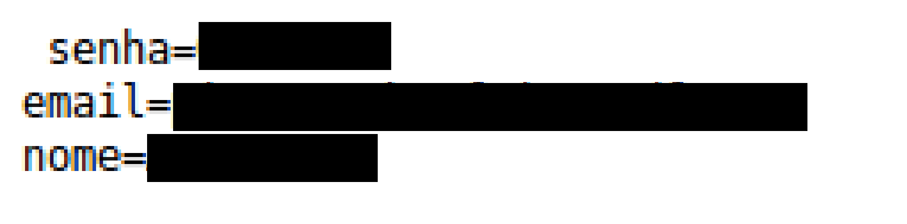
truncated hashes

examples

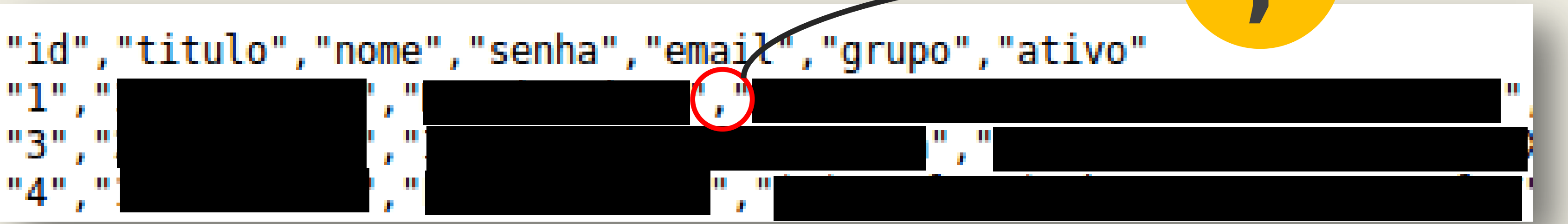


```
user_name                 user_passwd
[redacted]                [redacted]
[redacted]                [redacted]
```

/t



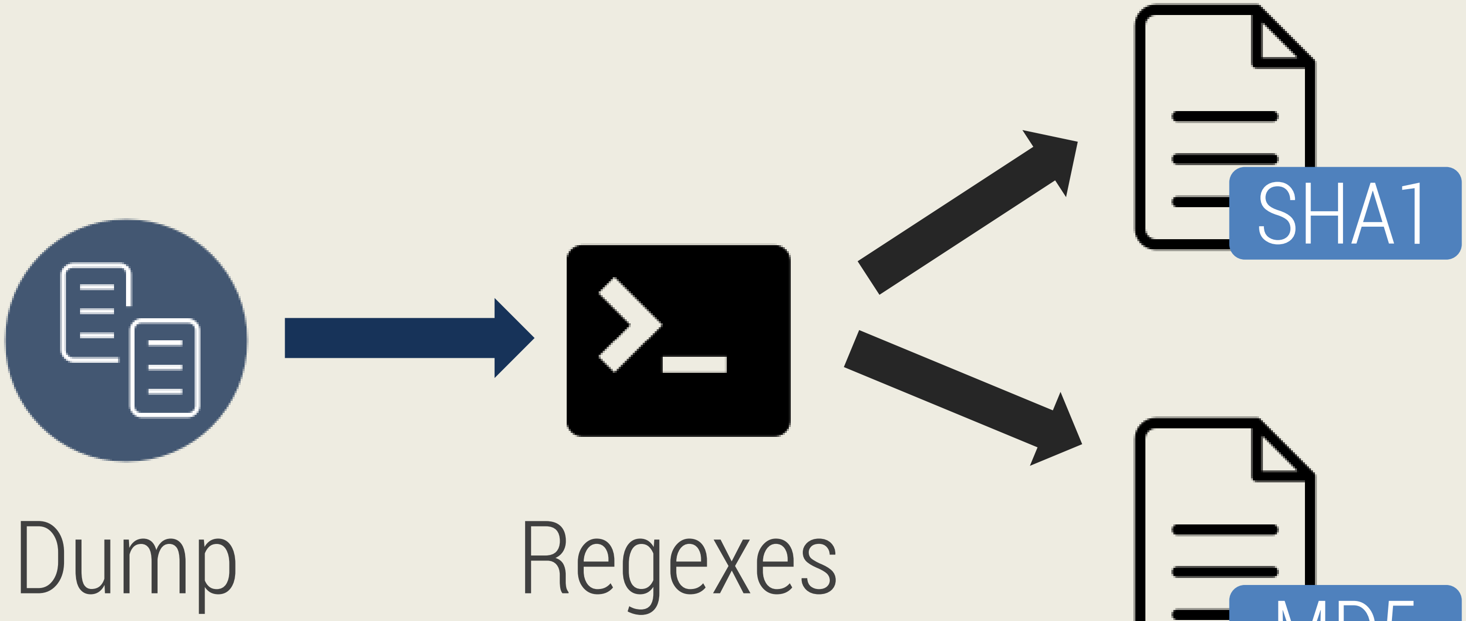
```
 senha=[redacted]
email=[redacted]
nome=[redacted]
```

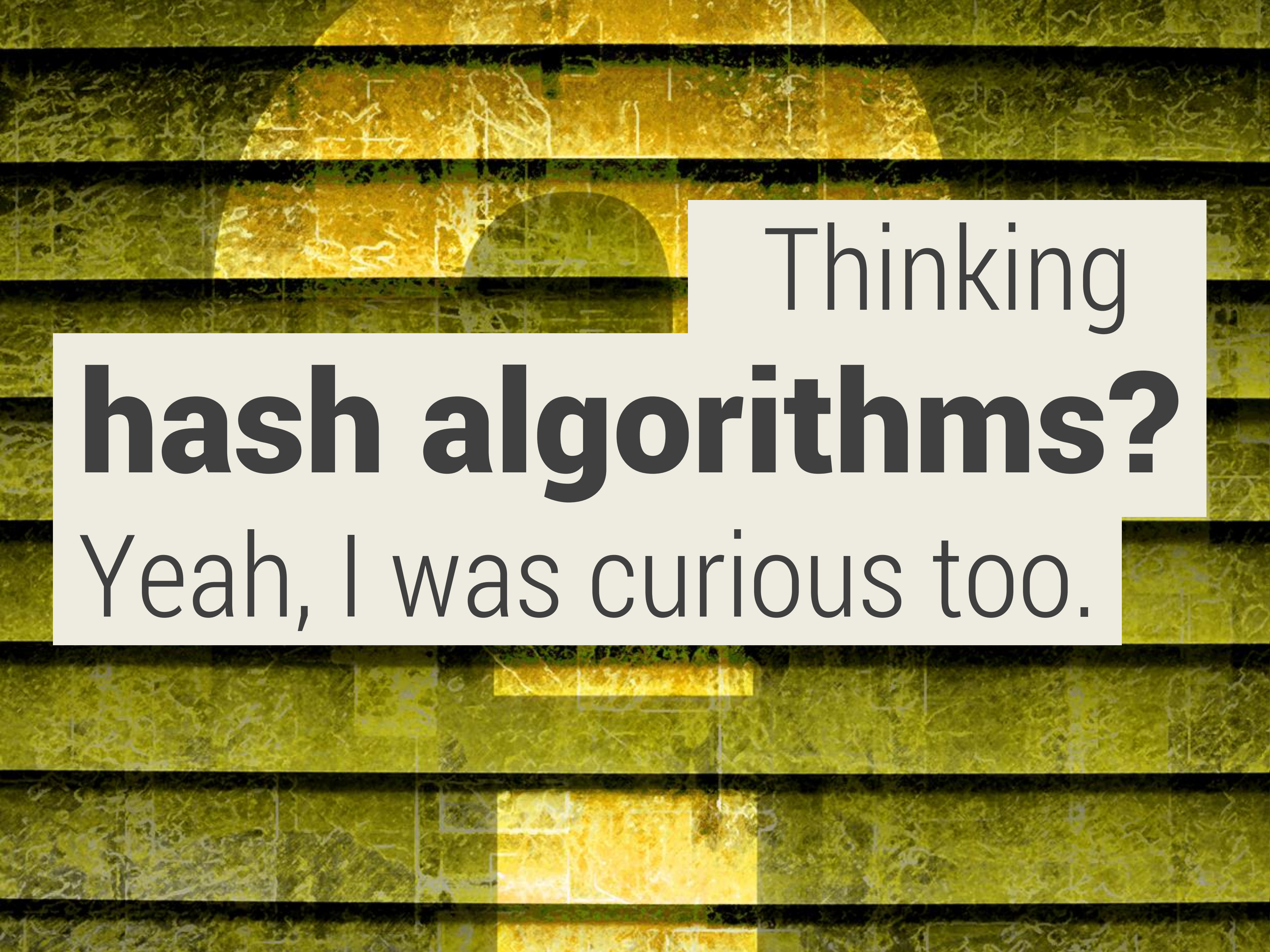


```
"id","titulo","nome","senha","email","grupo","ativo"
"1","[redacted]","[redacted]","[redacted]"
"3","[redacted]","[redacted]","[redacted]
"4","[redacted]","[redacted]","[redacted]
```

,

extract-hashes.py



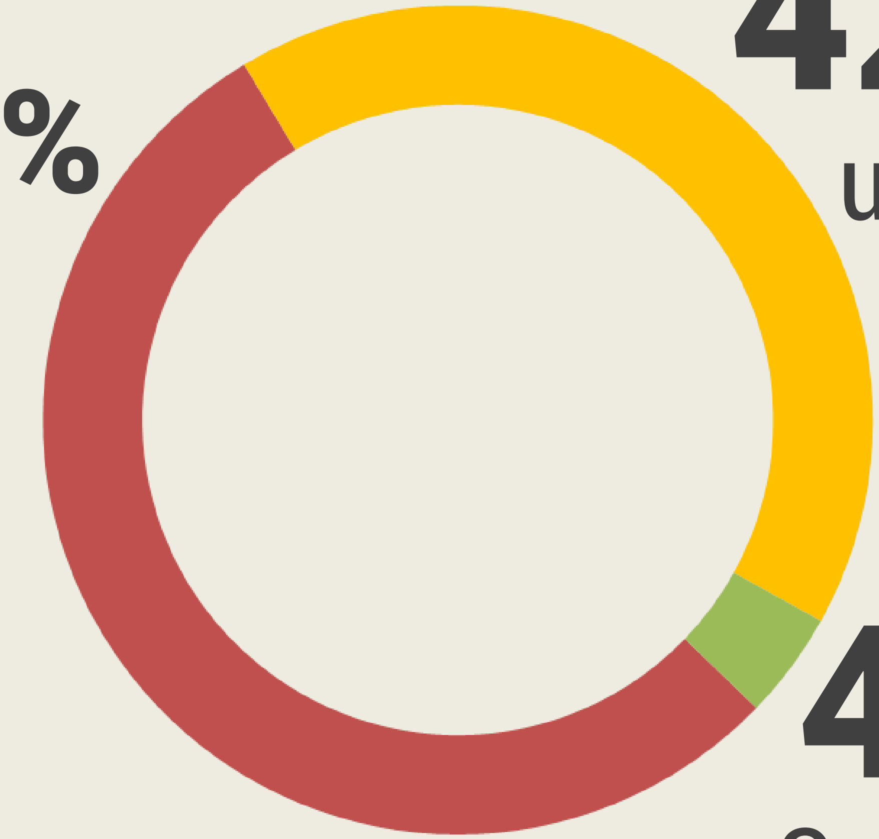


Thinking

hash algorithms?

Yeah, I was curious too.

think again.



Let’s crack some passwords!!

Scenarios

No password policy

8 alphanumeric chars
(uppercase + lowercase)

6 alphanumeric + 1 special chars
(uppercase + lowercase)

Challenge #3

Classifying hashes

Manual classification

Wordlists

Crackstation (Human Only)

InsidePro 2012

RockYou

Cain & Abel

John The Ripper

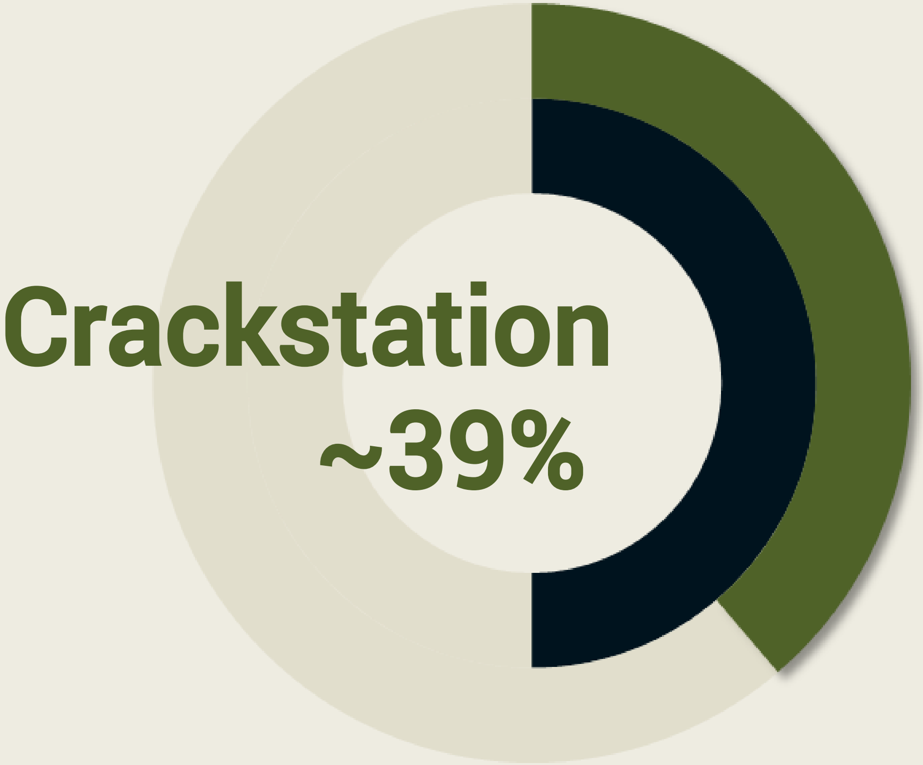
500 Worst Passwords

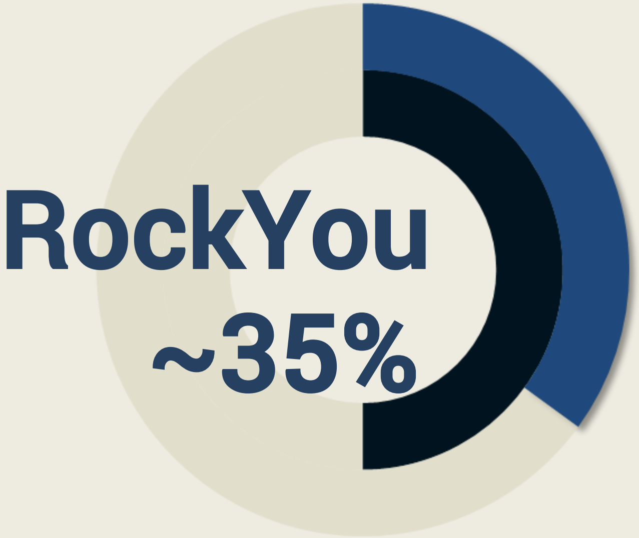
Round #1

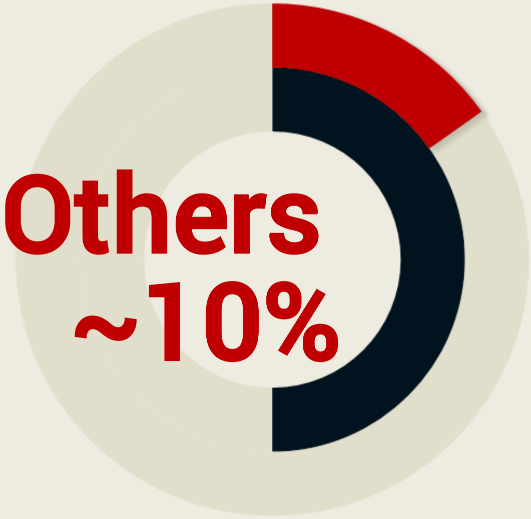
Wordlist only

Hashcat without best64.rule

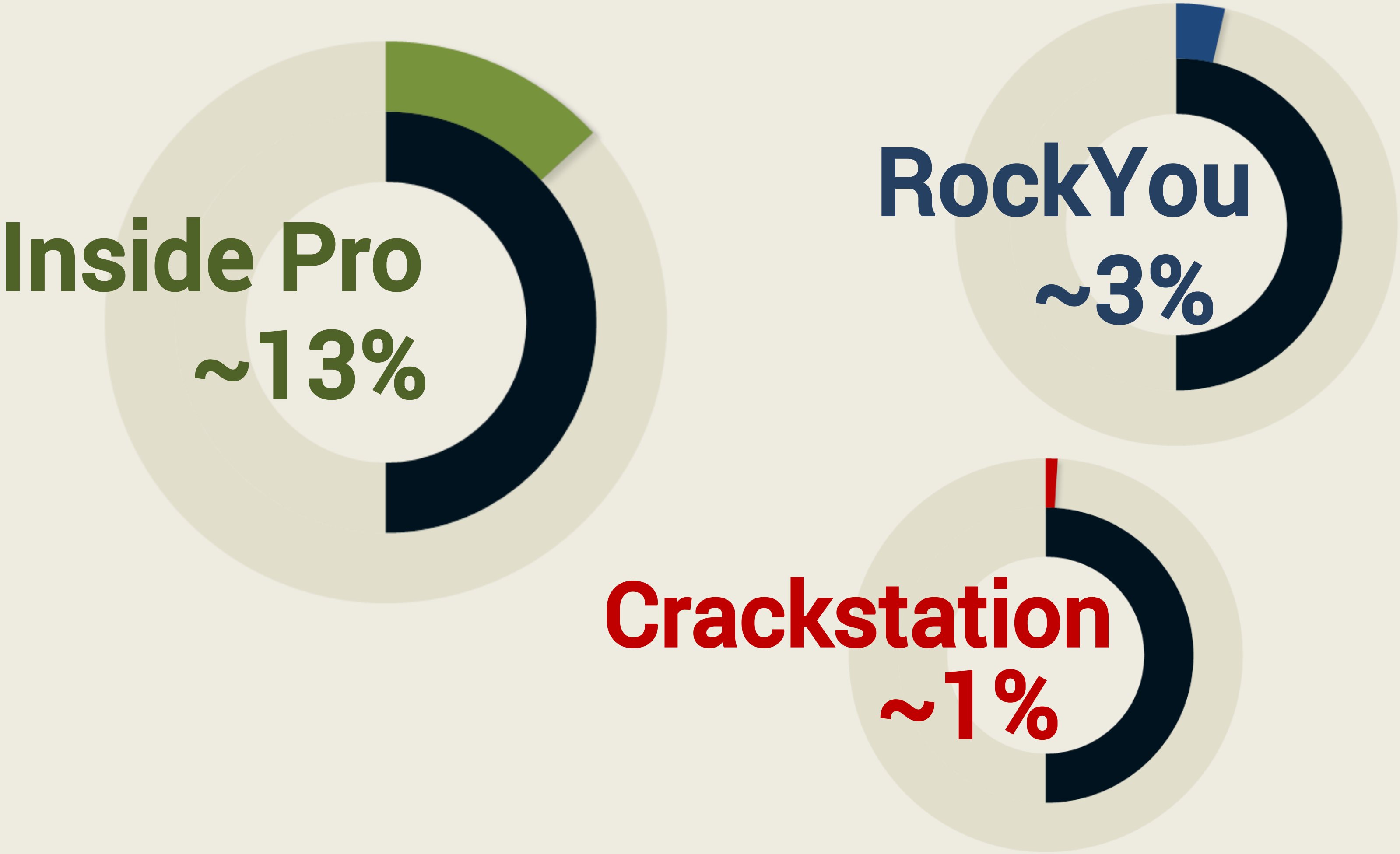
no password policy



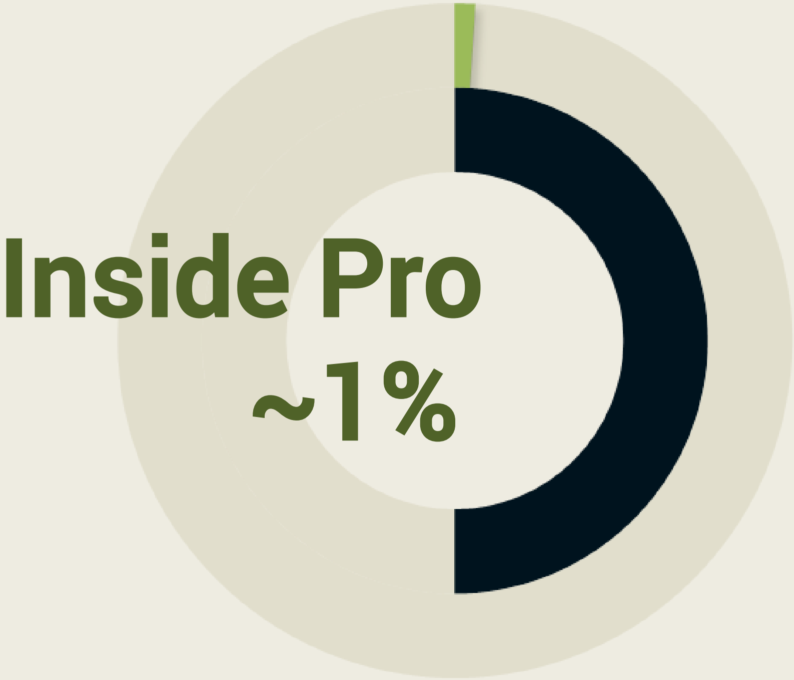


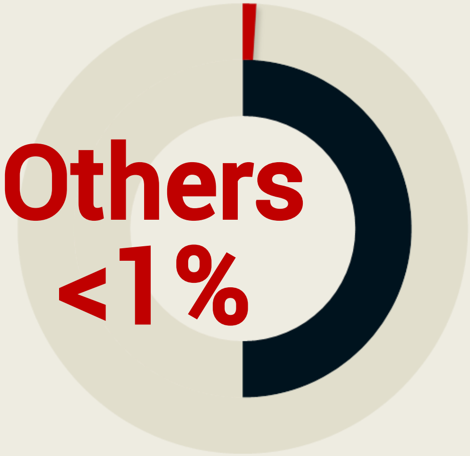


8 alphanum
(uppercase + lowercase)



6 alphanum + special
(uppercase + lowercase)



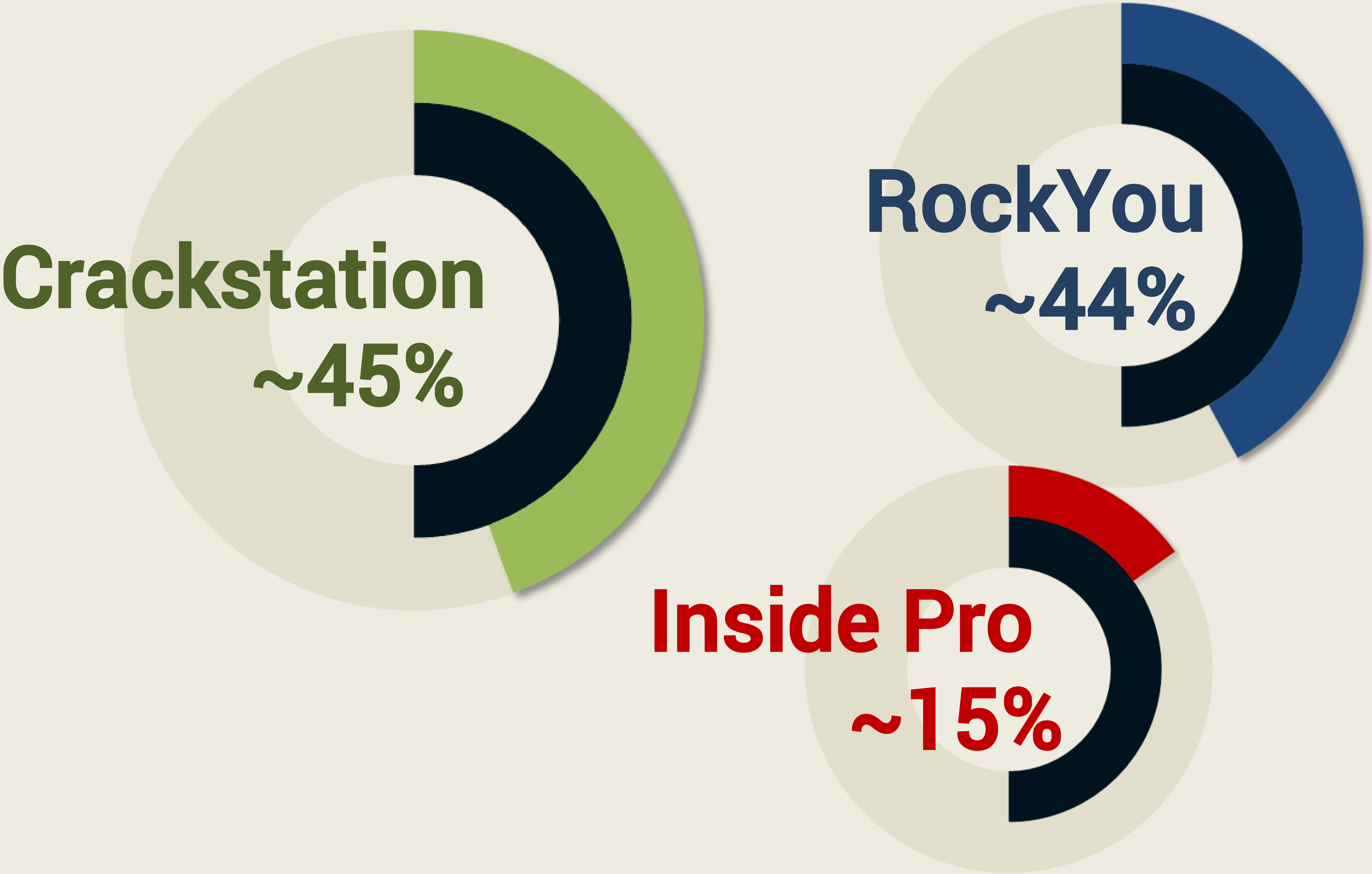


Round #2

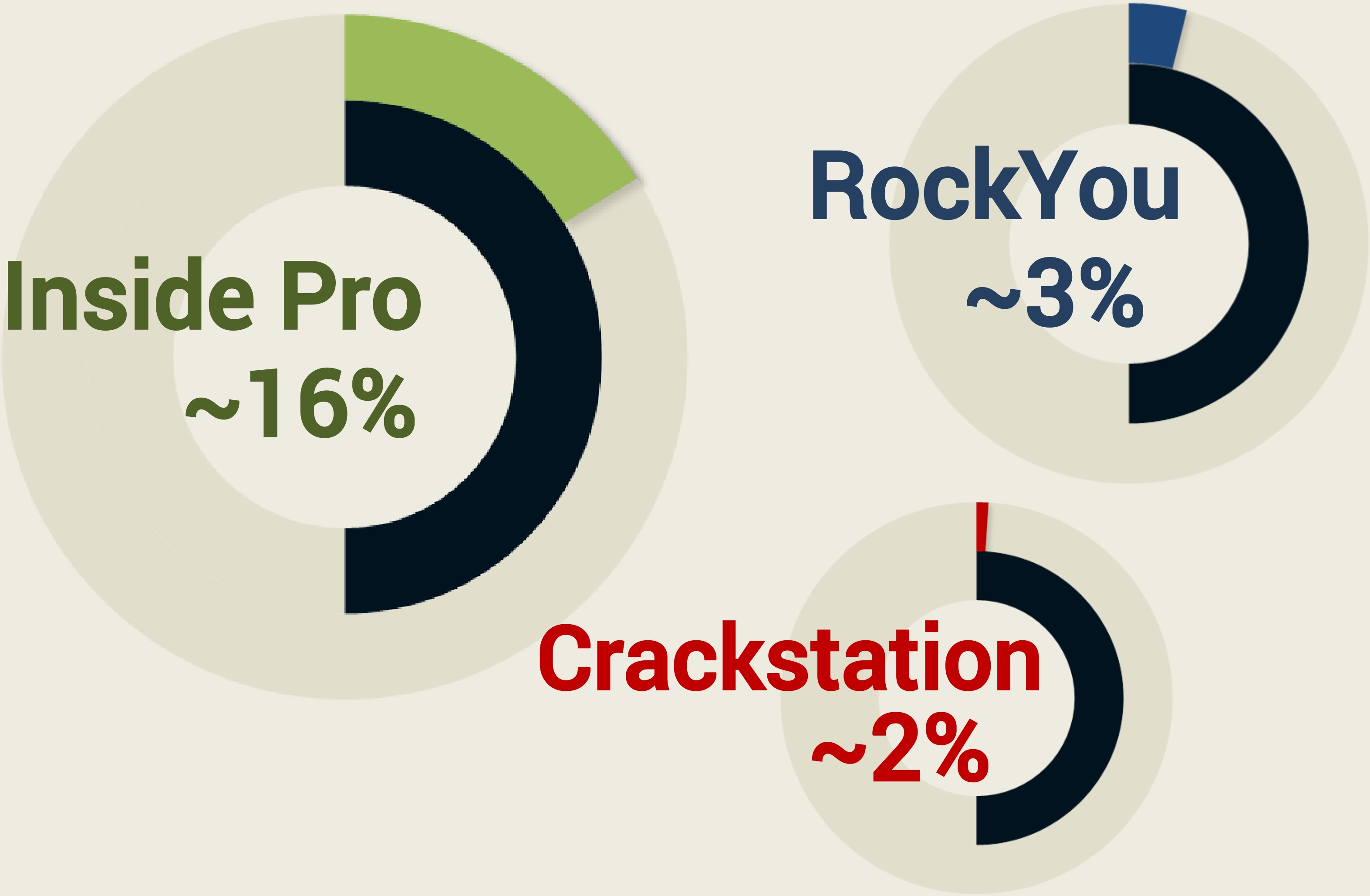
Wordlist + best64

Hashcat with best64.rule

no password policy

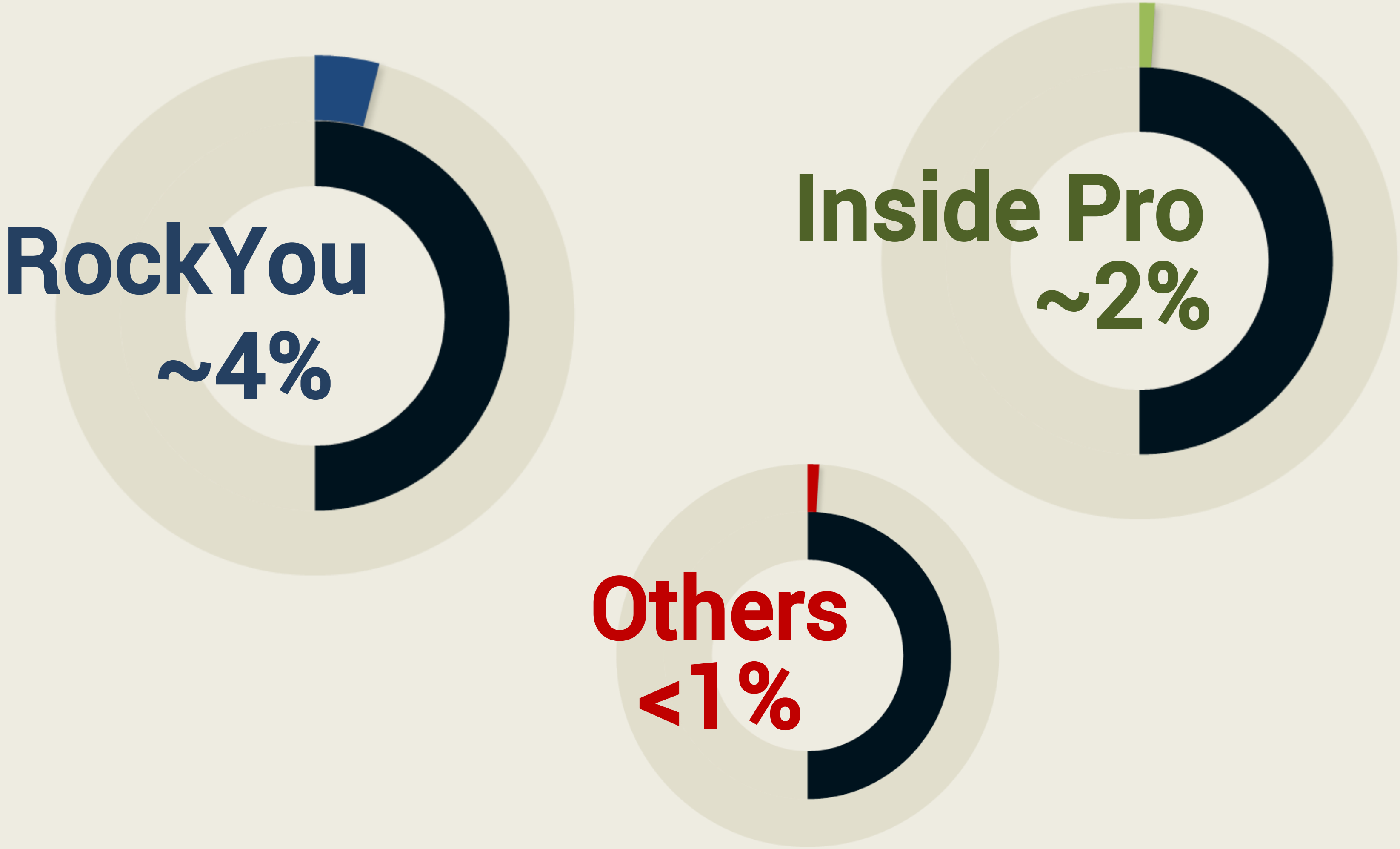


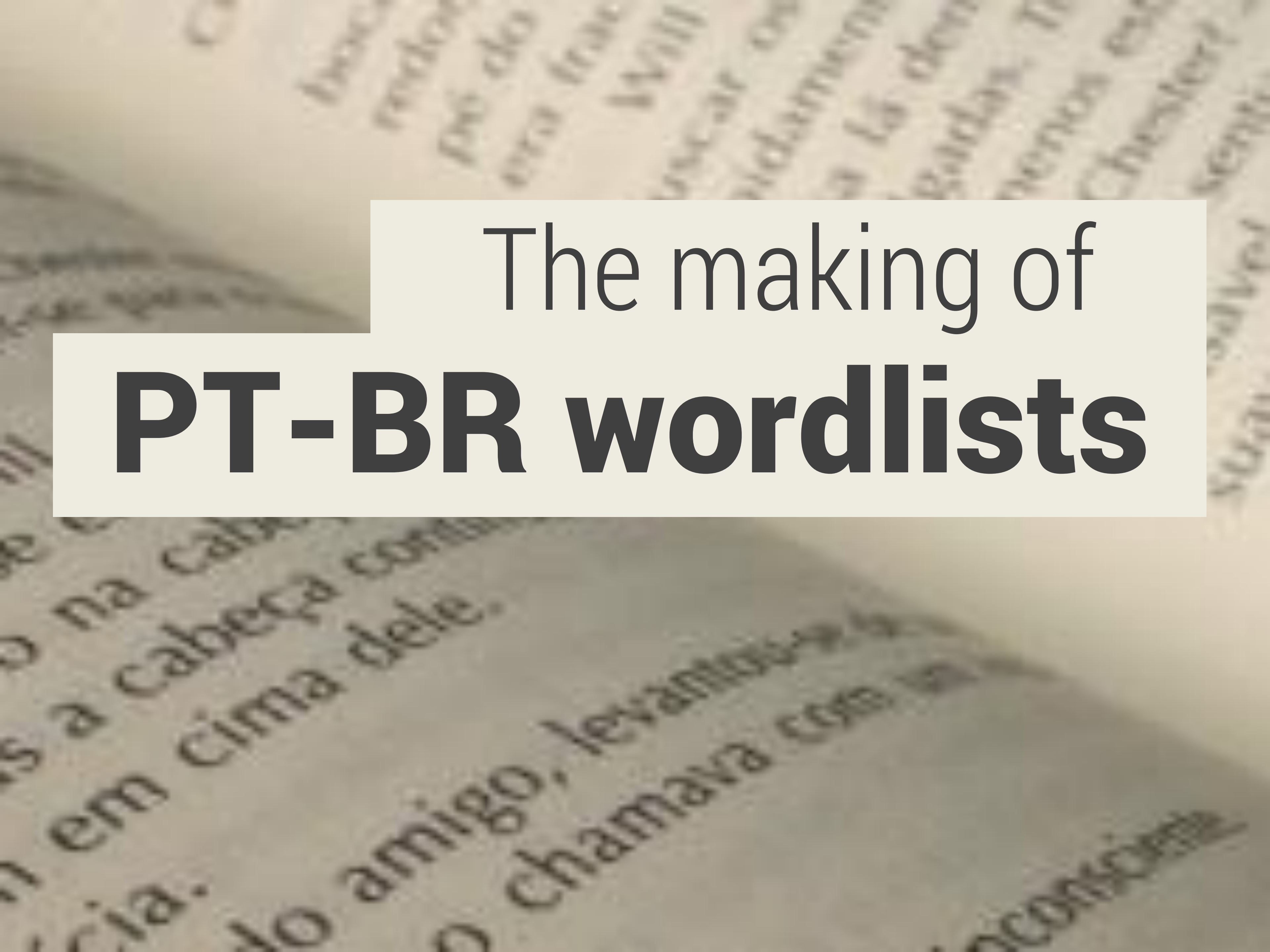
8 alphanum
(uppercase + lowercase)



6 alphanum + special

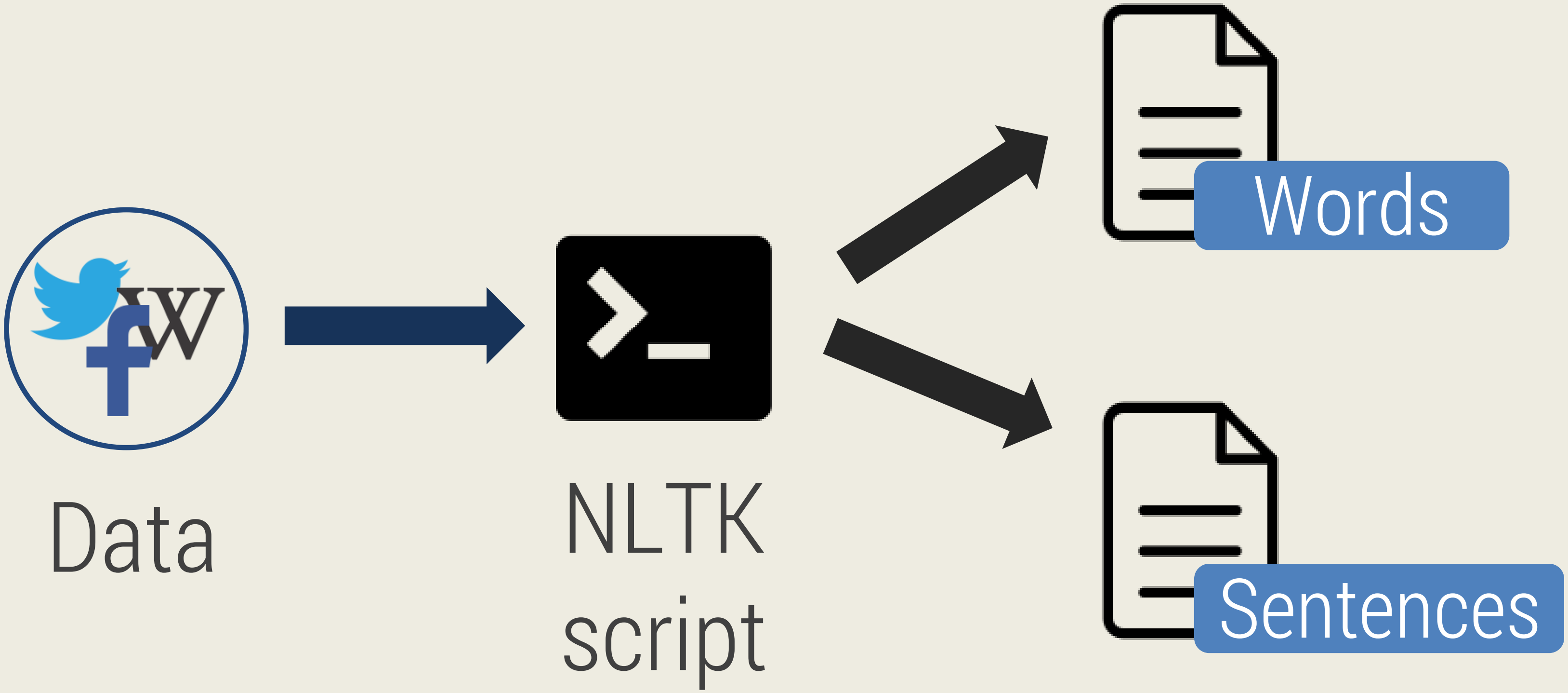
(uppercase + lowercase)





The making of
PT-BR wordlists

wordlists with NLTK

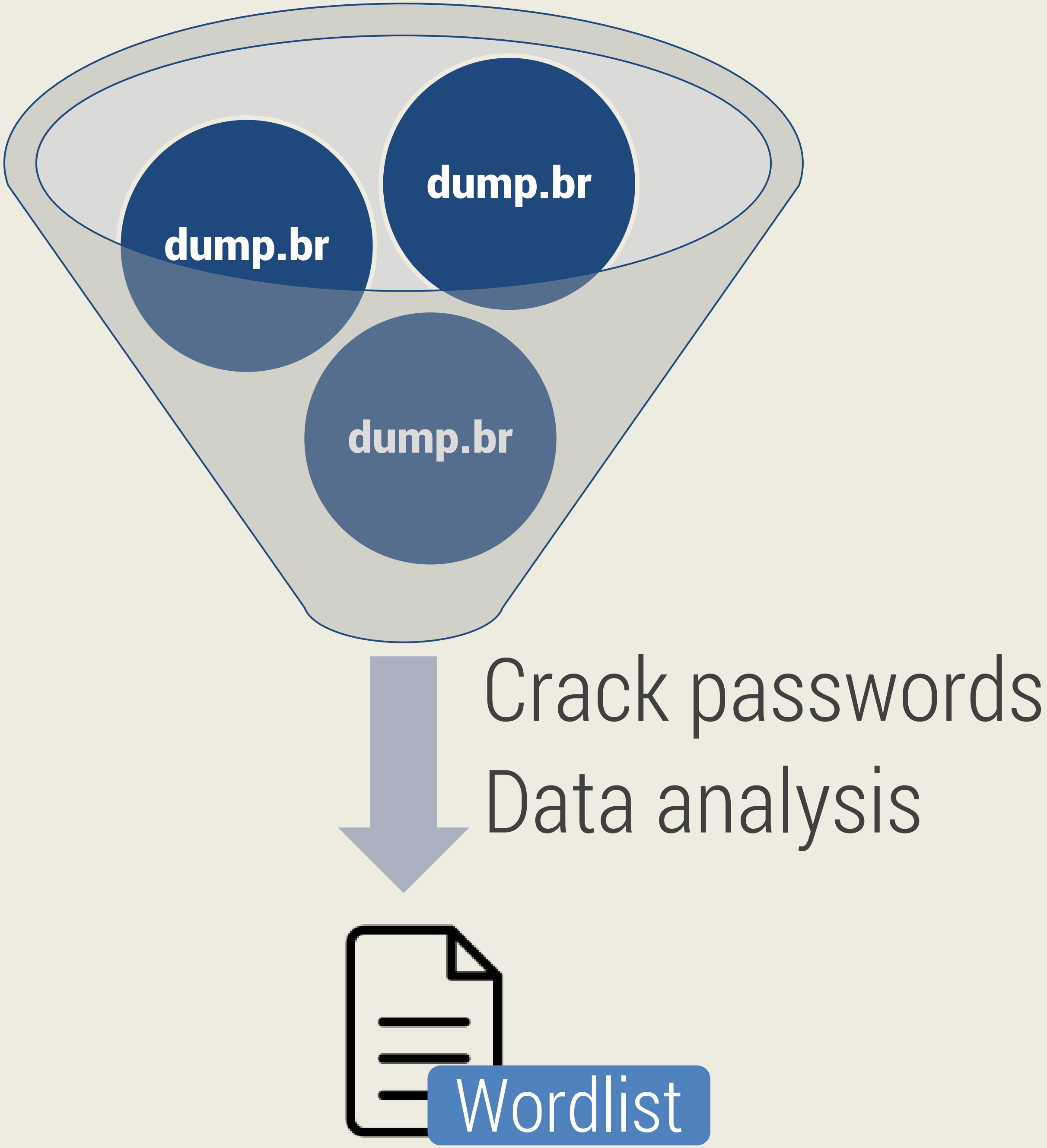


Data

NLTK script

Words

Sentences



dump.br

dump.br

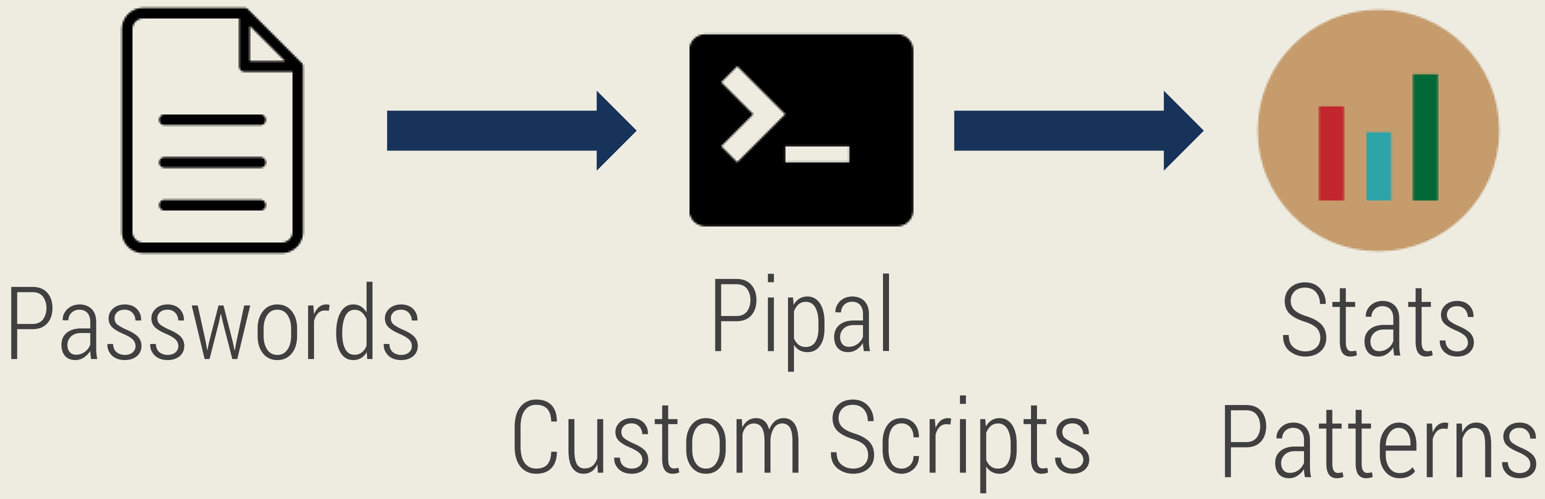
dump.br

Crack passwords

Data analysis

Wordlist

password patterns



Passwords

Pipal
Custom Scripts

Stats
Patterns

Obsevartions on **identified patterns** using the previous scenarios

no password policy

123

6-8
chars

Numbers
only

Service
or tool name

8 alphanum

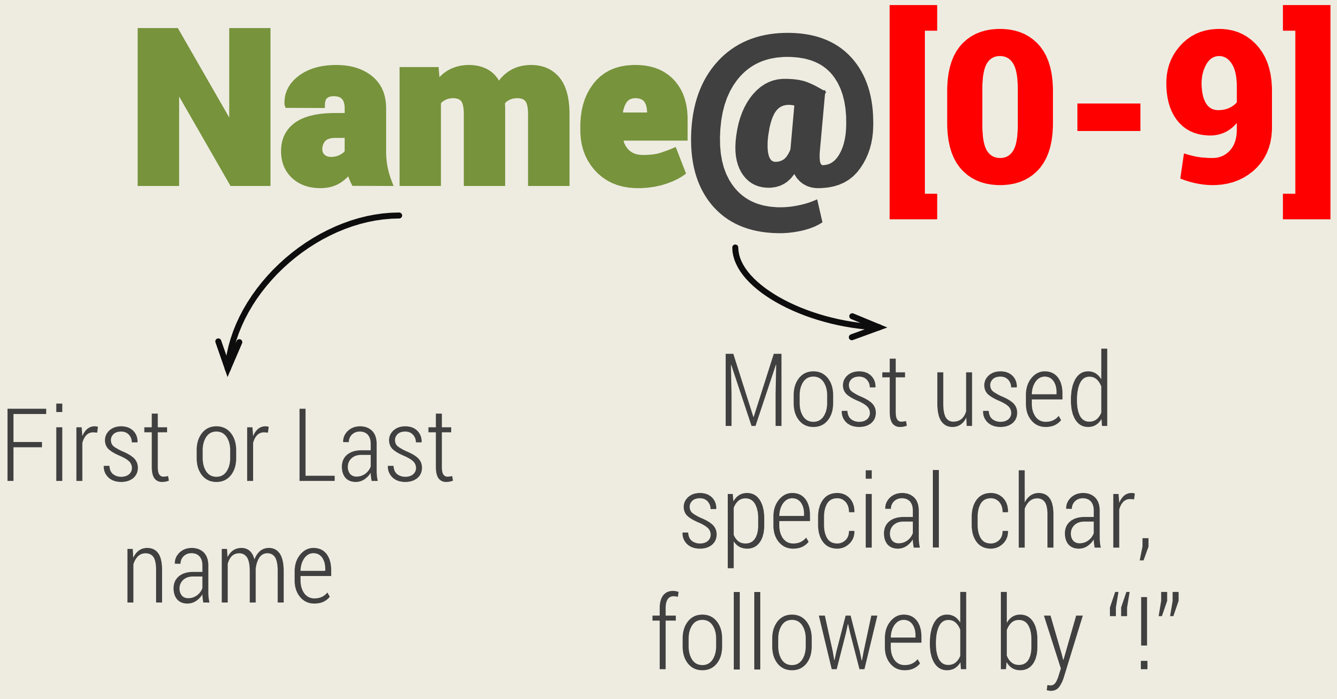
(uppercase + lowercase)

Blackhat1

Renata10

6 alphanum + special

(uppercase + lowercase)



Name@[0-9]

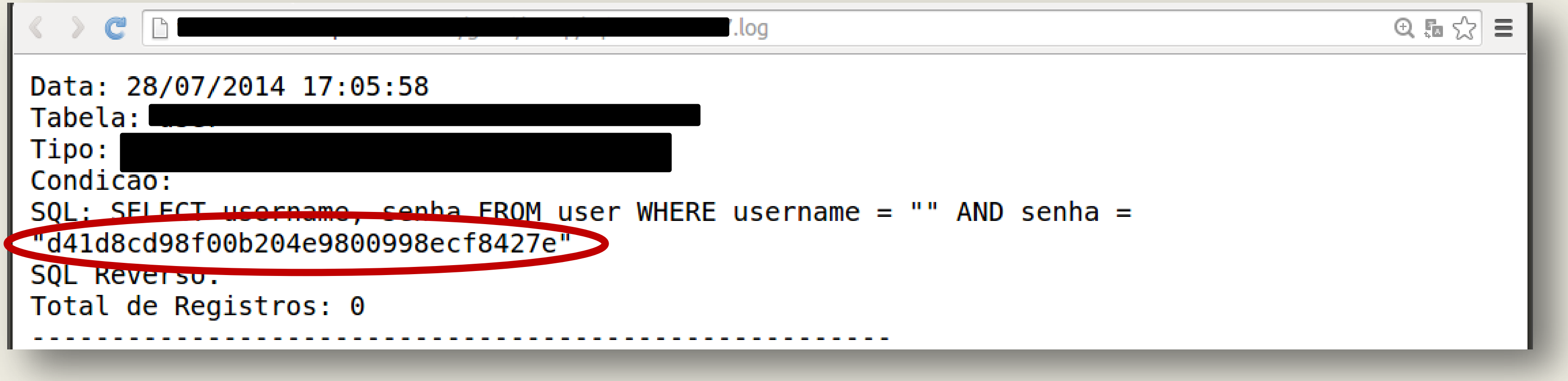
First or Last name

Most used special char, followed by “!”

BONUS STAGE!

world readable logs

SQL Query FTW

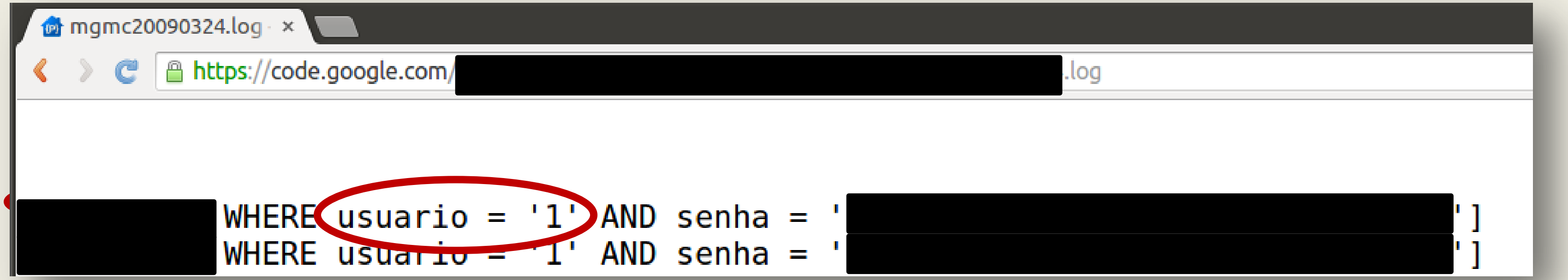


[redacted].log

```
Data: 28/07/2014 17:05:58
Tabela: [redacted]
Tipo: [redacted]
Condicao:
SQL: SELECT username, senha FROM user WHERE username = "" AND senha =
"d41d8cd98f00b204e9800998ecf8427e"
SQL Reverso:
Total de Registros: 0
------------------------------------------------------
```

more log files

Google Code, Yay!



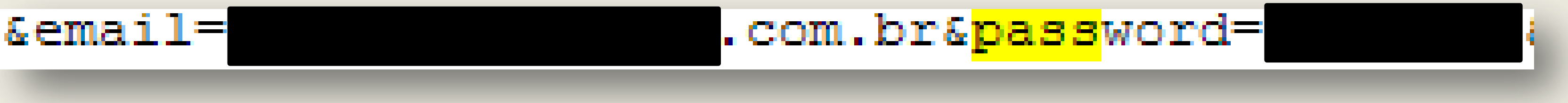
https://code.google.com/[redacted].log

```
[redacted] WHERE usuario = '1' AND senha = '[redacted]']
           WHERE usuario = '1' AND senha = '[redacted]']
```

Guess who user ID =1 is?

plain text in log files

http://xxx.com.br/logs/xxx.log.bkp



```
&email=[redacted].com.br&password=[redacted]&
```

Username + Password (clear text)

~ 6K **UNIQUE** credentials in a single file.

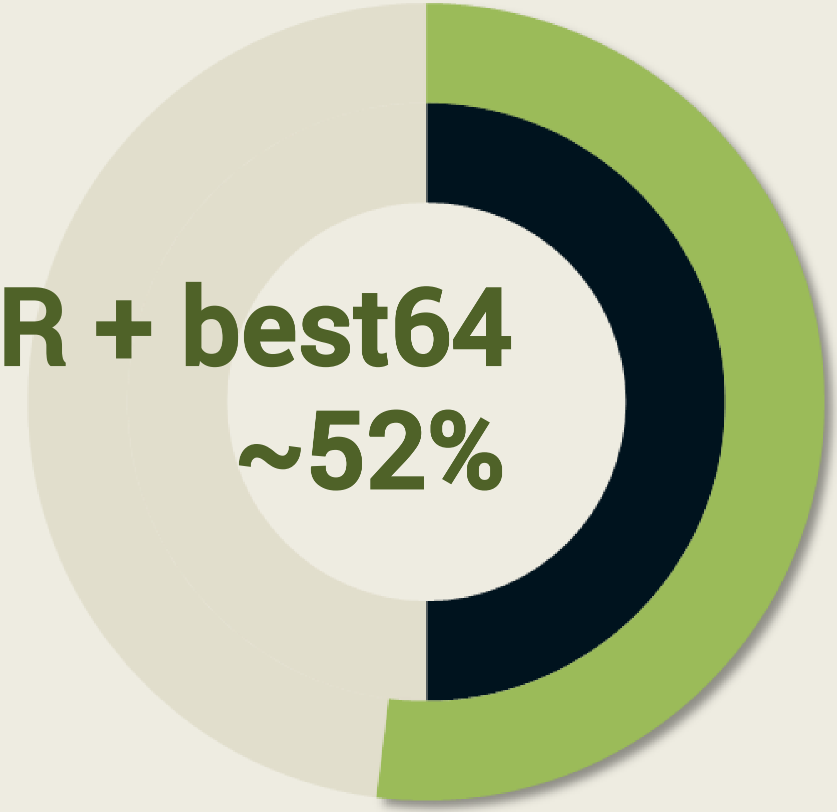
Round #3

Wordlist PT-BR + best64

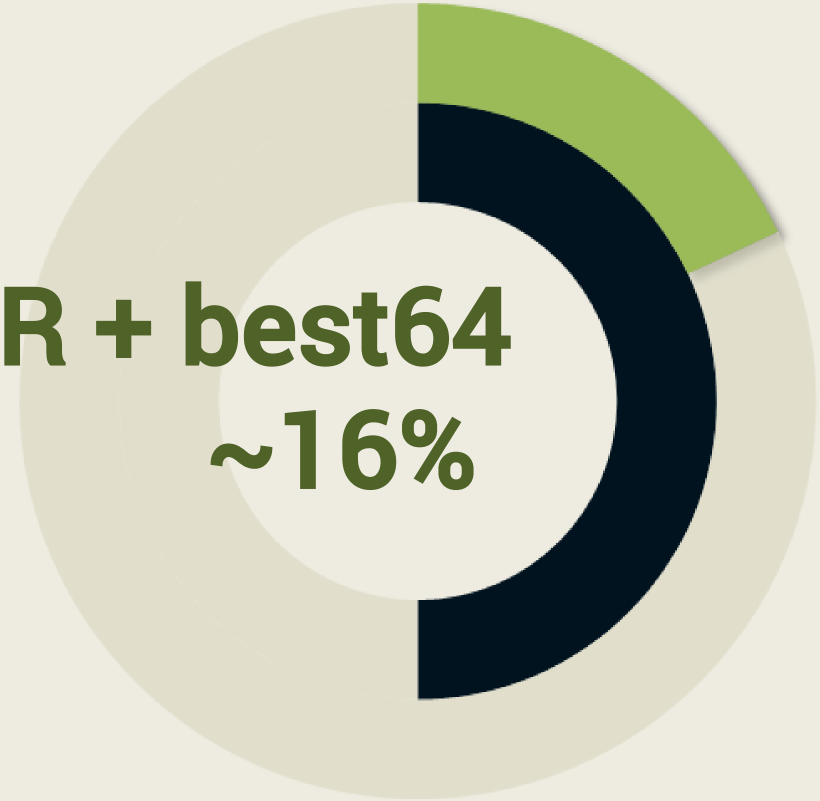
Hashcat with best64.rule

Considering whole new dumps

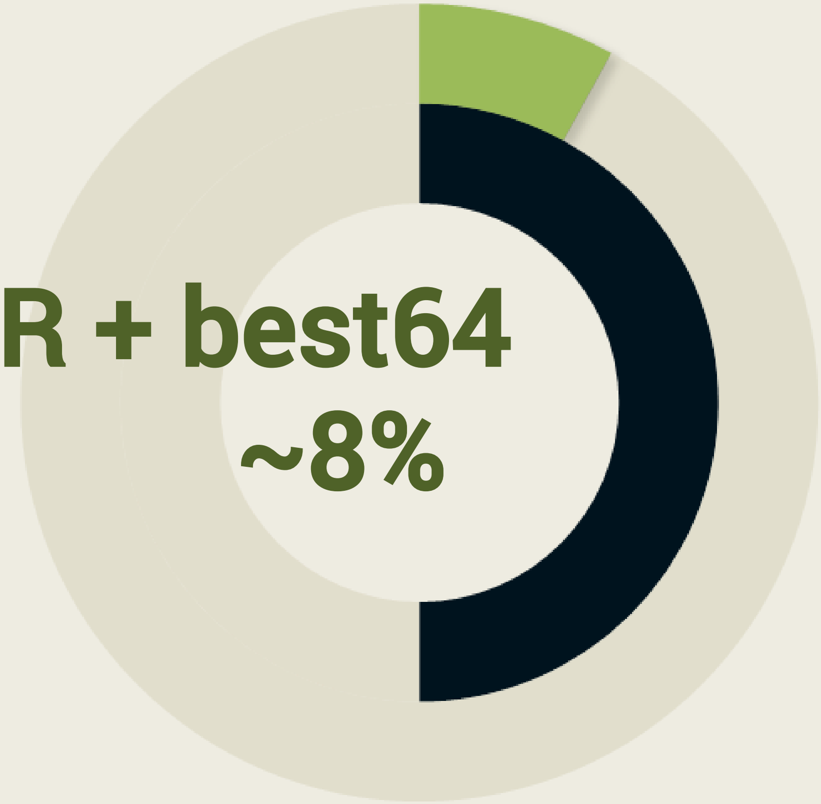
no password policy



8 alphanum
(uppercase + lowercase)

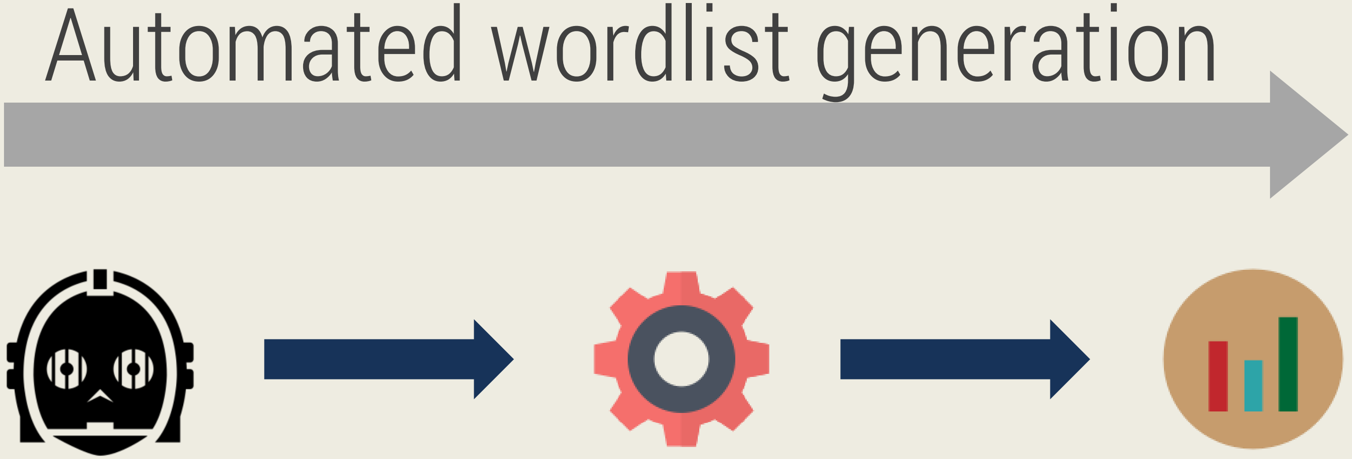


6 alphanum + special
(uppercase + lowercase)



The Future
NEXT EXIT

improve pastebot



Automated wordlist generation

pastebot

Dumpmon

Parsing data

CrackEngine

White Chappel

JtR

Hashcat

Wordlists

Pipal

Tag cloud

distributed approach

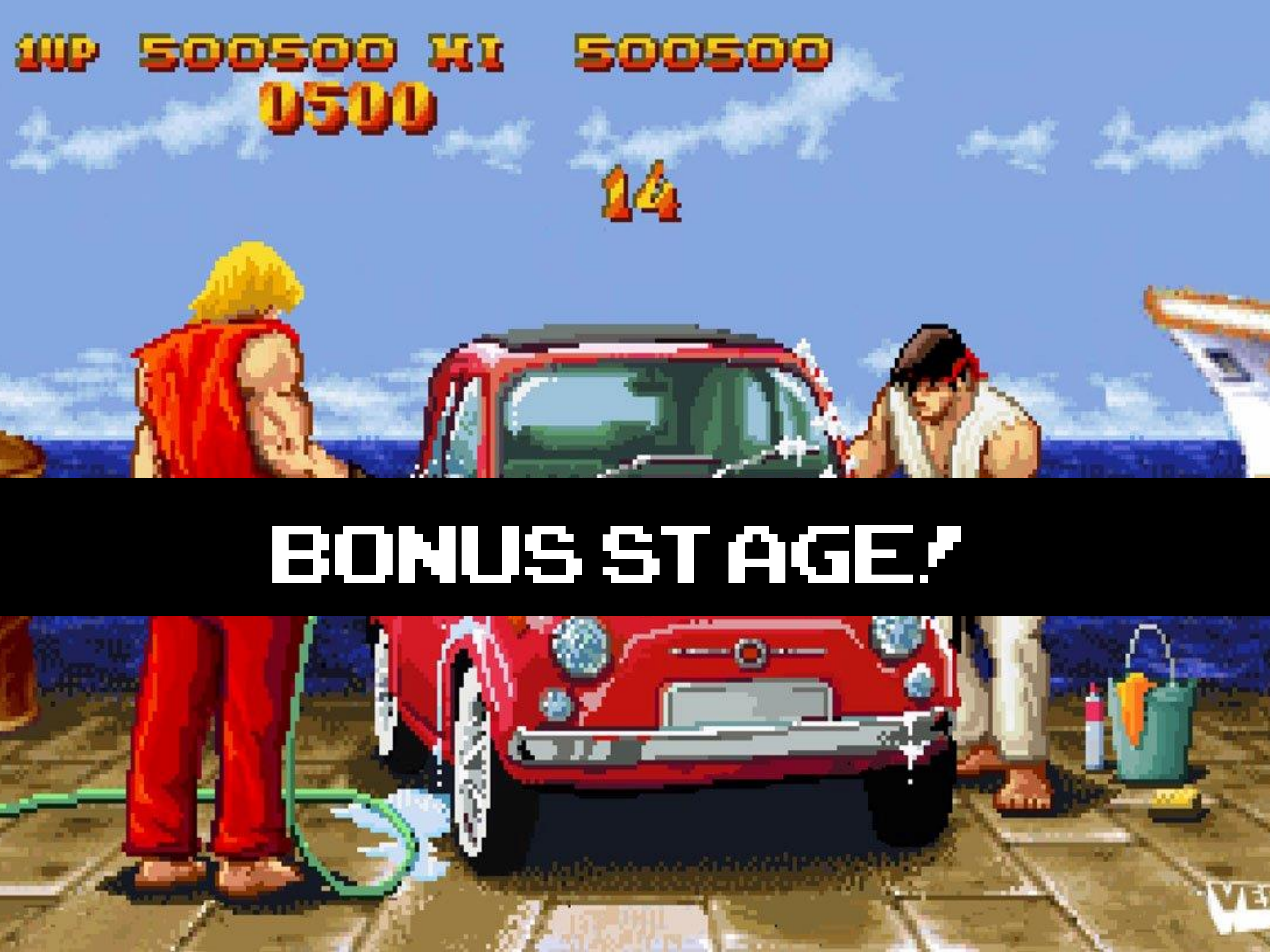
CrackEngine

Collaborative

Multiple nodes

Auto deploy Instances

(really) Long-term future



BONUS STAGE!

Sorry, folks!

Makes a lot more sense in Portuguese

porondequerqueeuvalevovocenoolhar

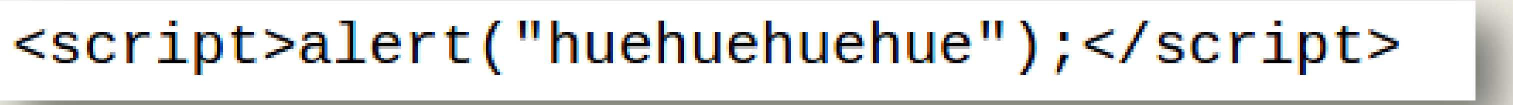
euamomeusfilhos

Em um dump pornográfico

vemnimimqueeutoqueto

Em um dump .gov

ninguemdescobreminhasenhamano



```
<script>alert("huehuehuehue");</script>
```

Thank You!

daniel@codalabs.net

@0xc0da

codalabs.net

/0xc0da