

Bem Vindo!

diadetreinamento.com.br



Google Hacking



Julio C. Venturin

Sócio proprietário da empresa VK2, com experiência de dez anos em desenvolvimento web.

Formado em análise e desenvolvimento de sistemas pela FAE - Erechim.

vk2.com.br
[facebook/julio.venturin](https://facebook.com/julio.venturin)

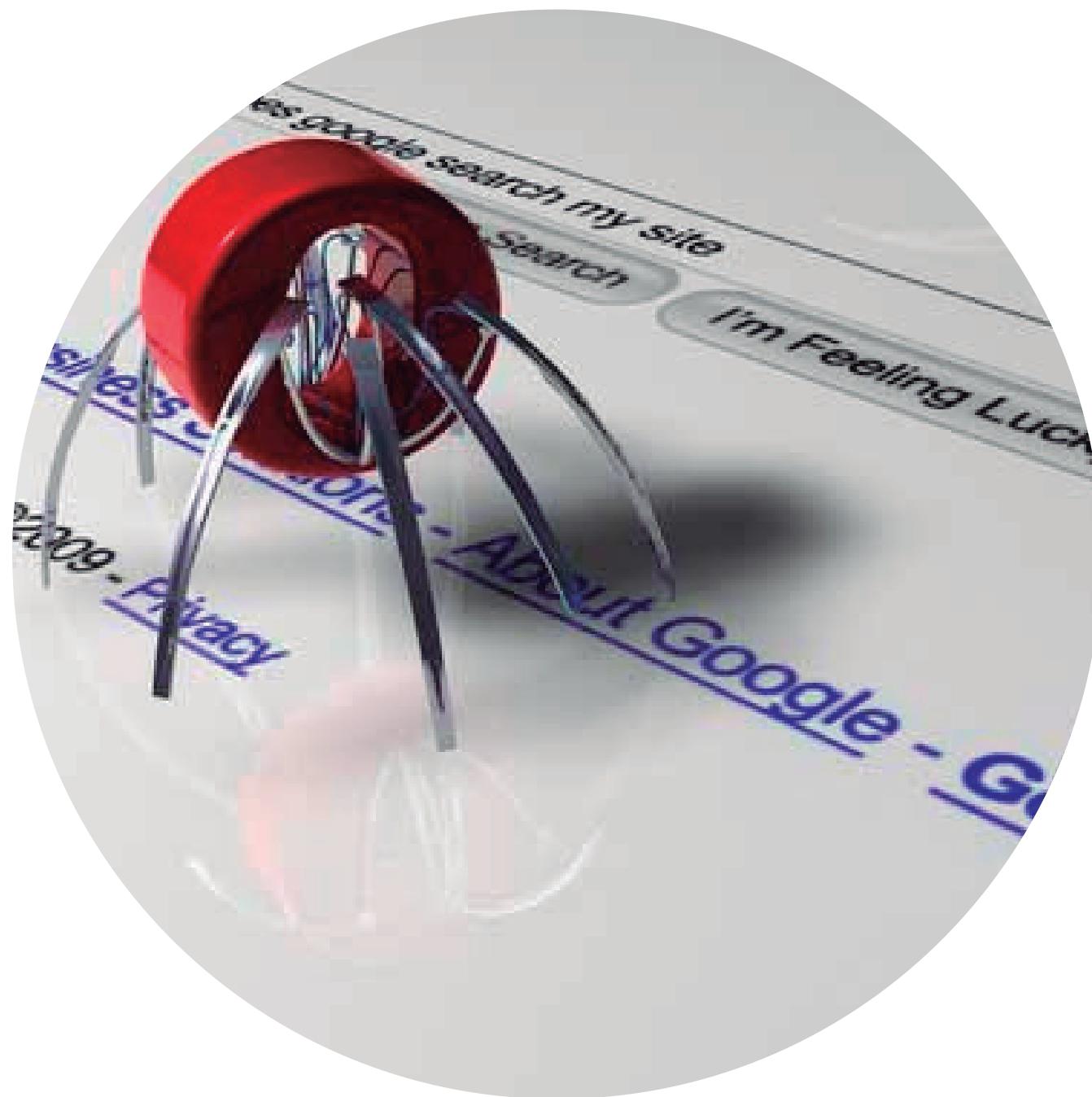
VAMOS COMEÇAR

Google Hacking

IMPORTANTE

**NÃO SAIA COPIANDO
ARQUIVOS E INFORMAÇÕES**

**VOCÊ PODE E VAI SER RESPONSABILIZADO POR PEGAR
INFORMAÇÕES DE TERCEIROS**



Como o google Funciona?

GOOGLEBOT, O ROBÔ DO GOOGLE

Googlebot é um aplicativo que percorre a internet em busca de conteúdo com o objetivo de indexar ou verificar alterações ocorridas desde a última "visita".

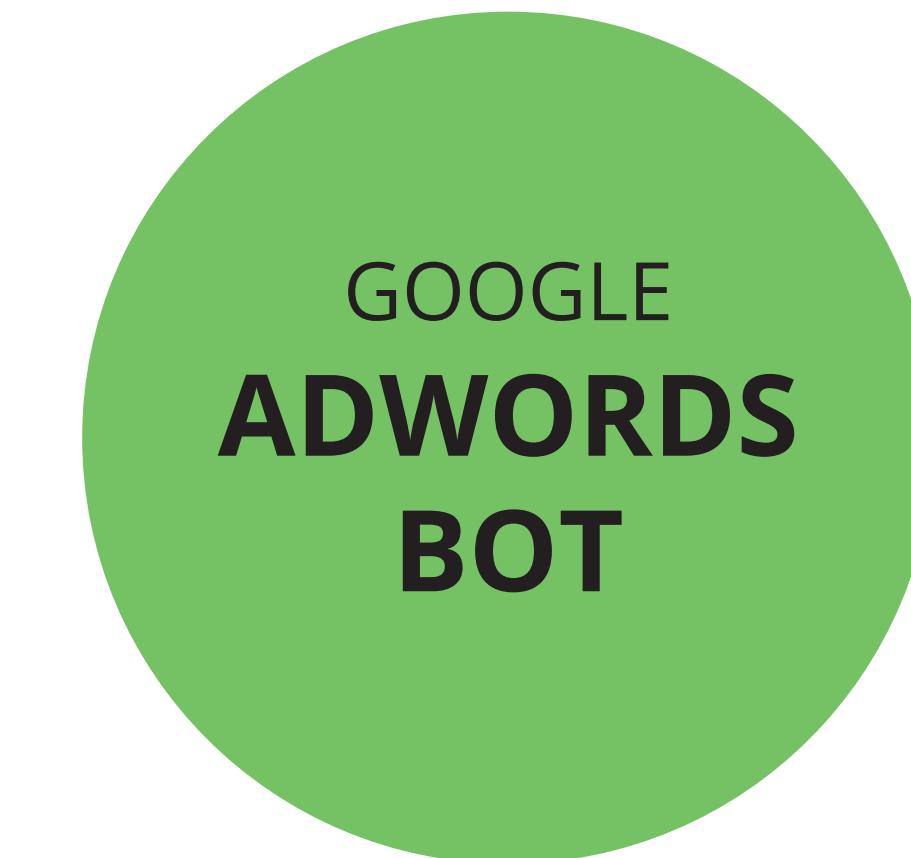
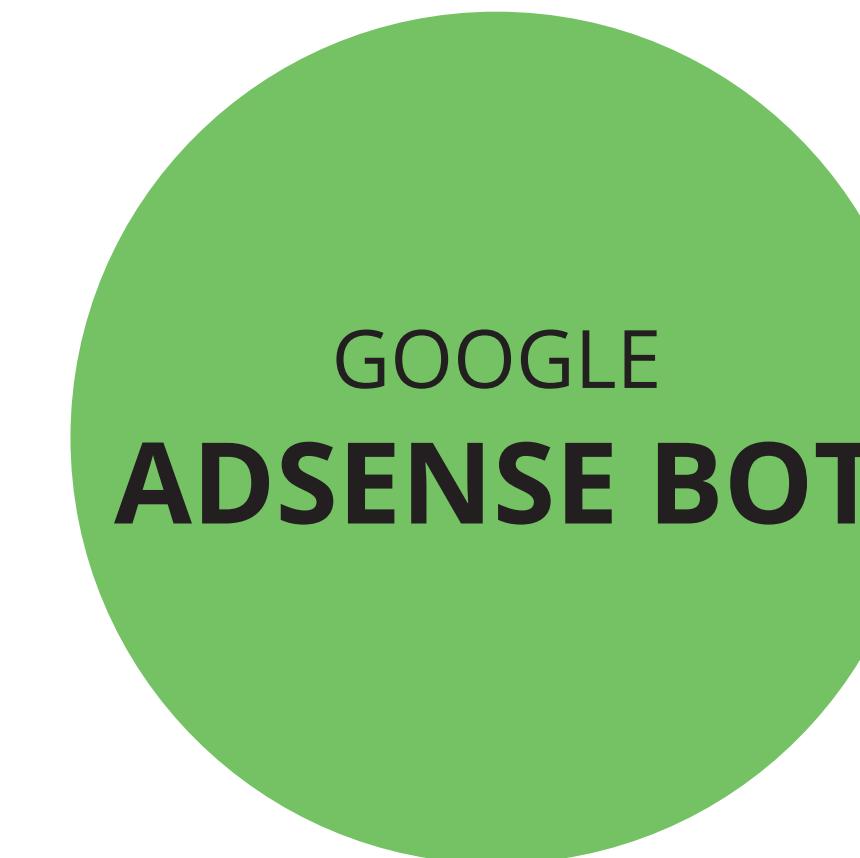
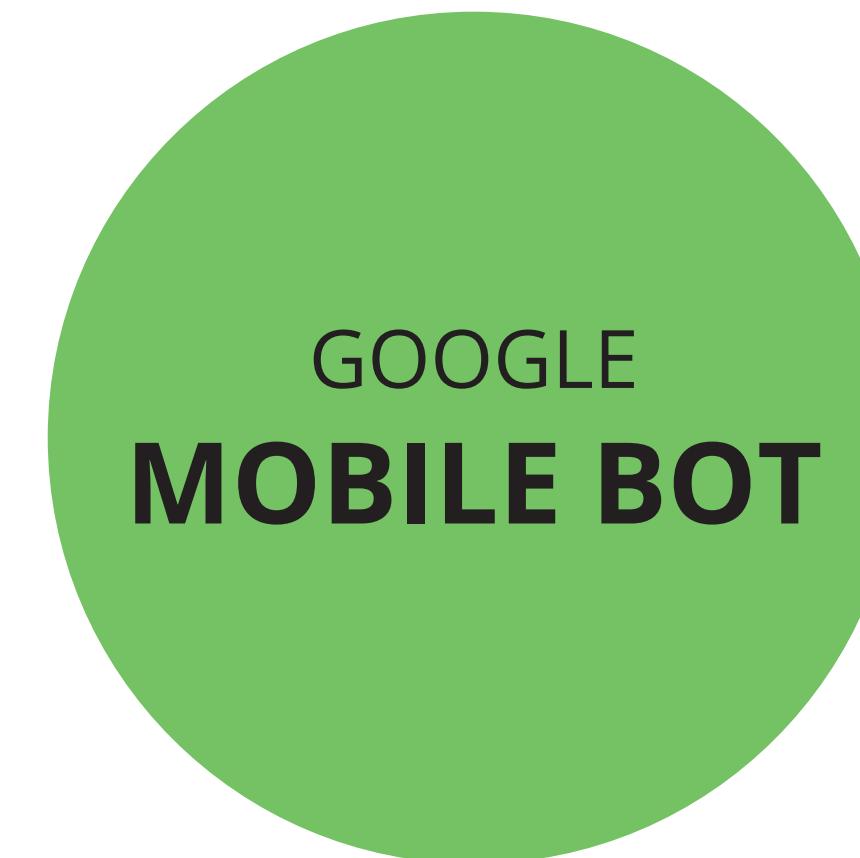
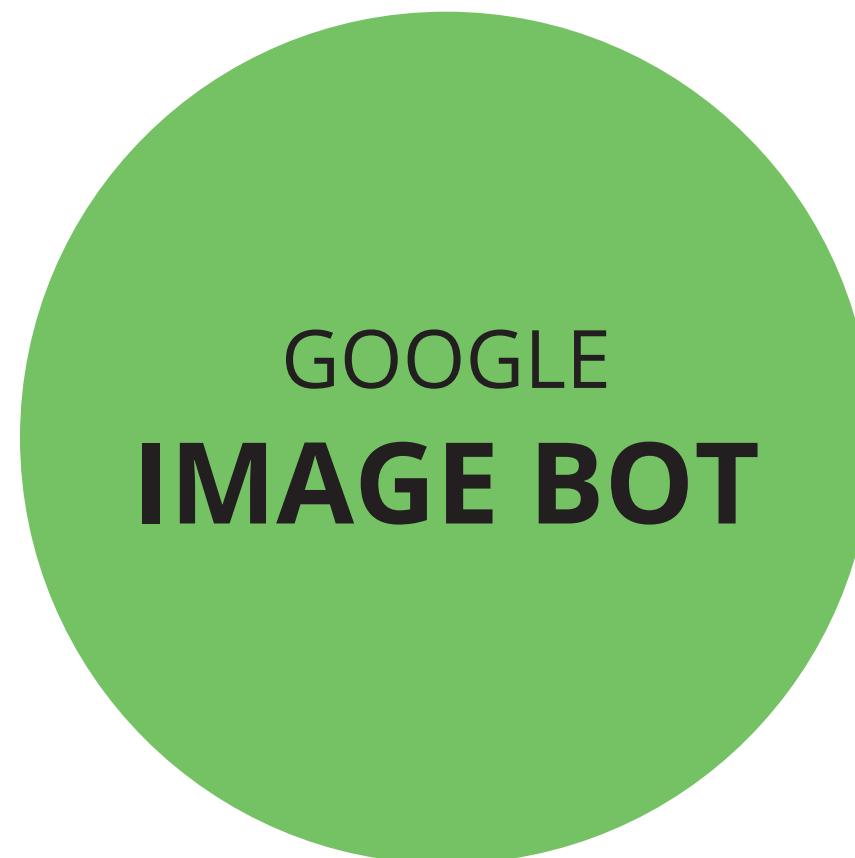
O SEU TRABALHO É LOCALIZAR PÁGINAS, MAPEAR SEUS LINKS, PRIORIZAR E ARMAZENAR AS INFORMAÇÕES.



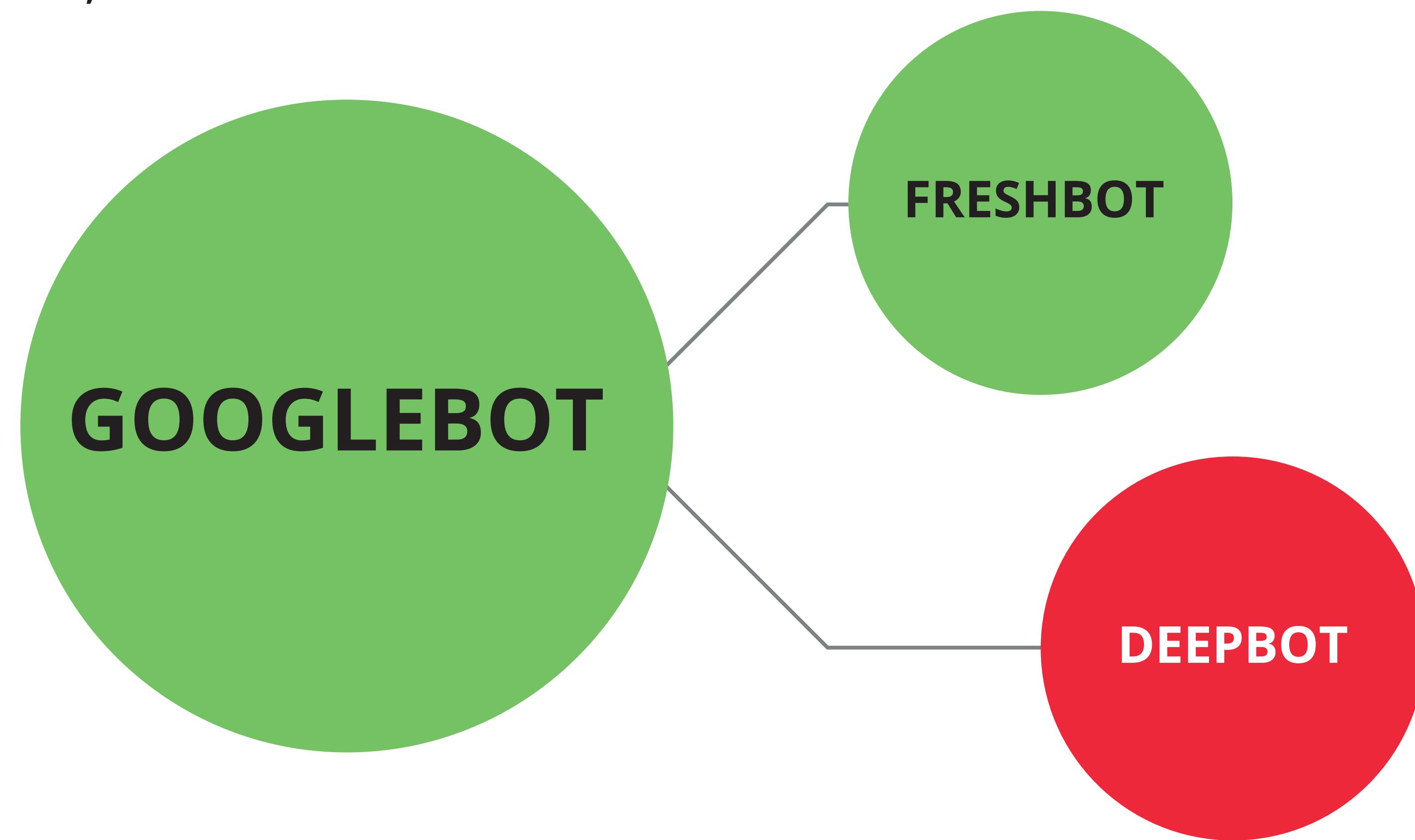
É SO ISSO?

GOOGLEBOTS, SÓ ACESSA
LINKS E OS INDEXA?

**EXISTEM VÁRIOS BOTS
DIFERENTES, ENTRE ELES:**



**EXISTEM VÁRIOS BOTS
DIFERENTES, ENTRE ELES:**



MAS E AÍ, O QUE É

GOOGLE HACKING

?

Google Hacking é a atividade de usar recursos de busca, visando atacar ou proteger melhor as informações de uma empresa. As informações disponíveis nos servidores web de uma empresa provavelmente estarão nas bases de dados do Google.

Um servidor mal configurado pode expor diversas informações da empresa no Google. Não é difícil conseguir acesso a arquivos de base de dados de sites através do Google.

O Google possui diversos recursos que podem ser utilizados durante um teste de invasão, e justamente por isso é considerada a melhor ferramenta para os hackers, pois permite acesso a todo e qualquer tipo de informação que se queira.

E AGORA

POR ONDE EU
COMEÇO?

OPERADORES DE BUSCA/PESQUISA

“Operadores de busca ou de pesquisa são palavras que podem ser adicionadas às pesquisas para ajudar a restringir os resultados.”

REF. SUPORTE.GOOGLE.COM.BR

OPERADORES booleanos	AÇÃO	DETALHE
AND	INCLUSÃO	Todos os termos ligados por AND (ou espaço) estão presentes no documento
OR	UNIÃO	Deve conter pelo menos umas das palavras que forem unidas por OR
	UNIÃO	Deve conter pelo menos umas das palavras que forem unidas por OR
-	EXCLUSÃO	Pesquisa determinado assunto, e exclui resultados que contenham - (subtração)
+	INCLUSÃO	Pesquisa determinado assunto, e adiciona resultados que contenham + (adição)
*	APROXIMADO	Substitui qualquer string de caráter importante permitindo ampliar os resultados.

COMANDOS AVANÇADOS

**intitle,
allintitle**

**inurl,
allinurl**

filetype

allintext

site

link

inanchor

daterange

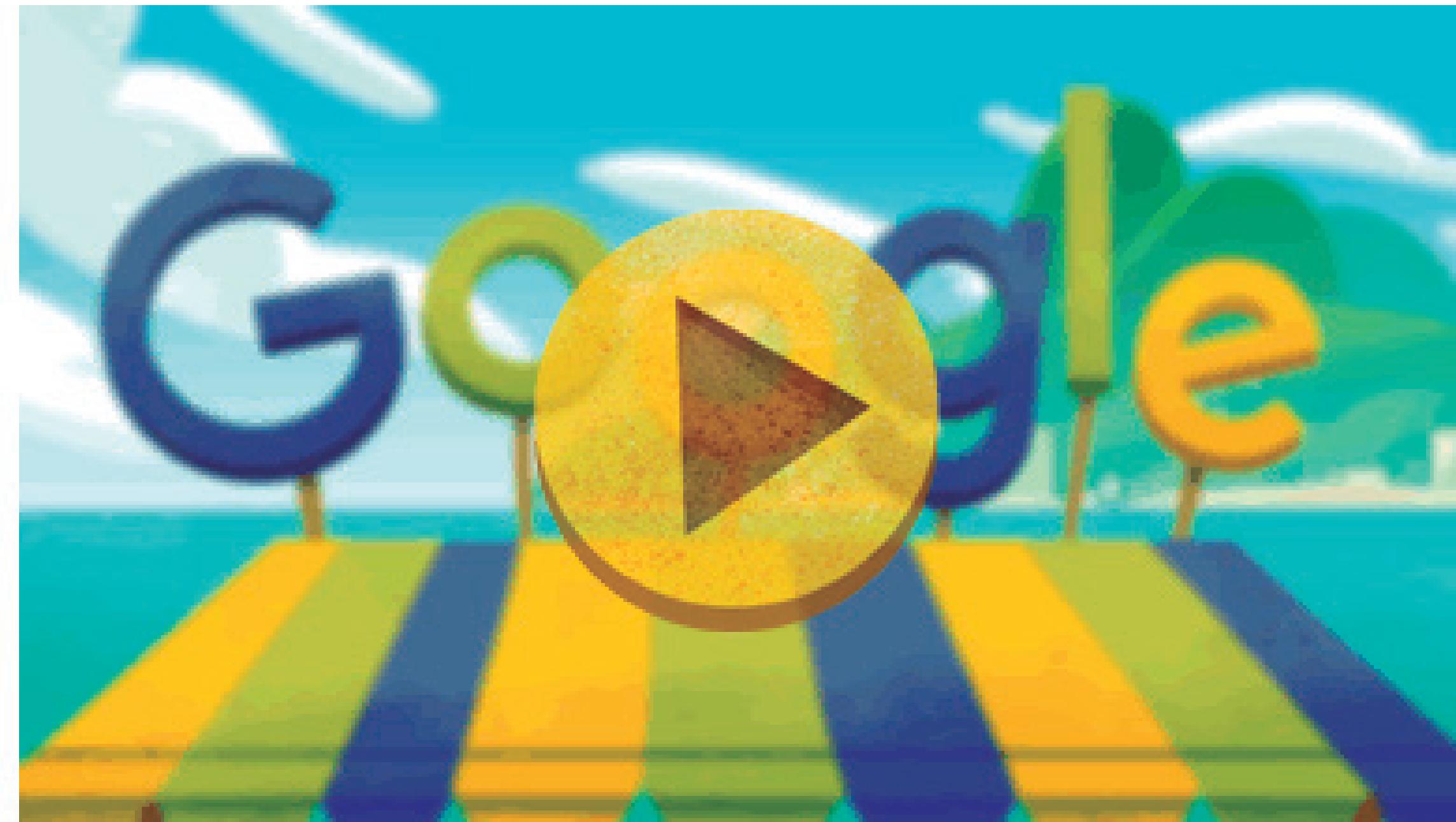
cache

info

MÃOS A OBRA

VAMOS HACKEAR

?



operador:**busca** operador:**busca** +operador:"**busca**"



Sem espaço

Um espaço para
adicionar mais
operadores

Utilize espaço antes de
usar um dos operadores
booleanos

Busca por arquivos de base de dados em sites do governo:

site:gov.br ext:SQL

Pesquisando sistemas que utilizem porta 8080:

inurl:8080 -intext:8080

Pesquisando sites com possíveis falhas:

allinurl:".php?site="

Pesquisando um arquivo .pdf de um assunto específico:

inurl:security filetype:pdf +intext:Linux

CONSTRUINDO SUA DORK

Uma dork é um conjunto de termos de busca que faz com que o Google reaja diretamente ao pesquisado, retornando resultados cada vez mais objetivos. Para construir sua Dork você primeiro deverá ter em mente o que deseja buscar.

MÃOS A OBRA

10 MIN PARA FAZER

UMA DORK

DOWNLOAD DAS

TABELAS DE OPERADORES

github.com/Diadetreinamento/GoogleHacking/tabela-operadores.pdf

JÁ SABEMOS CRIAR DORKS
MAS COMO VOU ME
DEFENDER?

01

NÃO MANTER ARQUIVOS IMPORTANTES ONLINE

A maneira mais eficiente e recomendada é **não manter** arquivos que possam conter senhas e ou informações relevantes em servidores de produção.

02

MANTER MEU SERVIDOR ATUALIZADO E CONFIGURADO

Manter e monitorar as permissões e restrições de acesso em meu servidor de produção.

Manter bloqueadas pastas de cache e relatórios.

03

CRIAR ARQUIVOS ROBOTS.TXT

Robots.txt é um arquivo que deve ser incluido no raiz do seu domínio com comandos para que o user agent (googlebot) não acesse uma URL específica. No entanto, ele pode ser usado para dar ao Google acesso a uma URL específica que seja um diretório secundário em um diretório principal bloqueado. Para tal use uma terceira palavra-chave, "Allow".

CONFIGURAÇÃO DE ARQUIVO ROBOTX.TXT

```
User-agent: *
Disallow: /administracao/
Disallow: /clientes/
Disallow: /cgi-bin/ #scripts e programas
Allow: /clientes/servicos.htm
```

Download do exemplo:

github.com/Diadetreinamento/GoogleHacking/robots.txt

OBRIGADO

Material em:

github.com/Diadetreinamento/GoogleHacking

vk2.com.br

facebook/**julio.venturin**

julio@vk2.com.br

e agora

“Partiu caçar pokémon”