

# Pentest com Kali Linux





**Instrutor: Vitor Mazuco**

**<http://facebook.com/vitormazuco>**

**Email: [vitor.mazuco@gmail.com](mailto:vitor.mazuco@gmail.com)**

**WebSite: <http://vmzsolutions.com.br>**



## Entendendo o mecanismo de busca no Google

Vamos ver as forma de como fazer buscas usando o mecanismo de filtro do Google, as sintaxes dos operadores que temos a permissão de utilizar nos filtros de buscas, nada mais são estruturas usadas para criar os nossos Dorks.



intitle

## Intitle

Faz a busca no conteúdo do título [tag title] da página.

Exemplo: “intitle: senhas”.



## Allintitle

Ele quebra a regra do exemplo acima, dizendo ao Google que todas as palavras que seguem devem ser encontradas no title da página (mais restrito).

Exemplo de Dork: “allintitle:admin”



**inurl**

**inurl**

Encontra texto em uma URL.

Exemplo de Dork: “inurl:admin.php”



allinurl

## allinurl

É quase igual ao inurl mas de forma mais restritiva, exibindo resultados apenas em que todas as *strings* foram encontradas.

Exemplo de Dork: “allinurl: login”



**filetype**

## **filetype**

Ele procura por um arquivo de determinado tipo (extensão): pdf, txt, xls, etc.

Exemplo de Dork: “filetype: pdf”



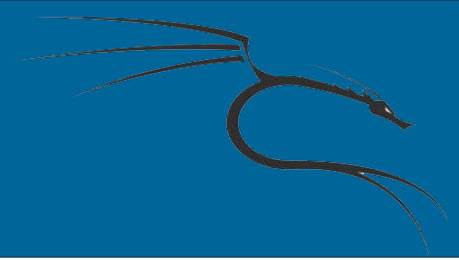


**intext**

**intext**

Procura uma string dentro do texto de uma página.

Exemplo de Dork: “intext: @yahoo”



## allintext

Parecido com o *intext*, porém podemos achar esta string em qualquer lugar, exceto no title, URL e links.

Exemplo de Dork: “allintext: pass”

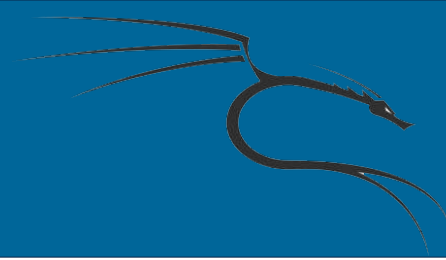


site

## site

Direciona a pesquisa para o conteúdo de um determinado site, como exemplos de domínio gov,com,br, entre outros.

Exemplo de Dork “site:com.br”



## site

Existem outros comandos que podemos usar para buscar como booleanos (entre eles o OR, NOT, AND) e outros operadores lógicos como: '&&' e '||'.