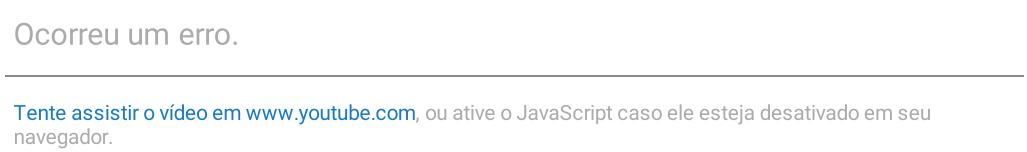
O que é Google Hacking? Técnicas + Conceitos

5 de junho de 20153 de novembro de 2015 / s0ph0s

O ***Google Hacking*** está cada dia mais conhecido através das técnicas que podemos utilizar para extrair informações através do buscador Google, tais como vulnerabilidades de serviços, aplicações ou até mesmo acesso de dispositivos eletrônico como webcams, câmeras de vigilância, impressoras remotas, servidores, informações de pessoas (RG, CPF, endereço,etc.). Acompanhe o tutorial abaixo que trará mais base de como são feita essas buscas e um vídeo para complementar o conhecimento.



O que é Google Hacking?

É uma técnica utilizada para buscar dados/informações em um determinado alvo, utilizando como base um buscador (como no caso o próprio Google). O Google por ser o maior buscador do mundo verifica o 'cache' dos sites e através dessas informações indexadas podemos fazer buscas por informações um tanto preciosas. Tais informações como diretórios abertos, arquivos de backups como de senhas e de banco de dados, e também pode nos permitir acessar dispositivos remotos devido a má configuração deles (câmeras privadas e públicas, babás eletrônicas, roteadores, webcams, entre outros). Para fazer essas buscar usamos *Dork* que utiliza o mecanismo do Google para filtrar melhor a informação a ser buscada, assim podemos encontrar possíveis vulnerabilidades a serem buscadas.

O que são Dorks?

São strings (conjunto de caracteres) que utilizamos para realizar as buscas filtrada no Google, assim podemos buscar a informação de um jeito mais eficaz. Vocês ouvirão falar muito delas em nossos tutoriais, porque para buscar falhas em determinado serviço (exemplo do apache, wordpress, joomla, sqli entre outros) podemos usar ela para facilitar a busca de nossos alvos.

Exemplo de uma Dork "*filetype: pdf*"

Entendendo o mecanismo de busca no Google

Agora abordaremos as forma de como fazer buscas utilizando o mecanismo de filtro do Google, as **sintaxes dos operadores** que podemos utilizar nos filtros de buscas, nada mais são estruturas usadas para criar *Dorks*.

- **intitle**

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

Exemplo de Dork “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**

Encontra texto em uma URL.

Exemplo de Dork “inurl: admin.php”

- **allinurl**

Funciona de maneira idêntica ao inurl mas de forma restritiva, exibindo resultados apenas em que todas as strings foram encontradas.

Exemplo de Dork “allinurl: login”

- **filetype**

Busca por um arquivo de determinado tipo (extensão) como pdf, txt, xls, entre outros.

Exemplo de Dork “filetype: pdf”

- ***intext***

Localiza uma string dentro do texto de uma página.

Exemplo de Dork “intext: @gmail”

- ***allintext***

Mesma função do intext, porém podemos encontrar esta string em qualquer lugar, exceto no title, URL e links.

Exemplo de Dork “allintext: pass”

- ***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”

Existem outros operadores que podemos usar para buscar como booleanos (como OR, NOT, AND..) e outros operadores lógicos como && , || as quais abordaremos no tutorial a frente.

Tipos de dorks para buscas

Segue exemplos abaixo de alguns tipos de dorks:

- **Buscando senhas em arquivos de Anotações/Banco de Dados/Servidores:**

intitle:”index of /” senhas.txt

filetype:txt + senha + com.br

filetype:txt intext:senha

intext: charset_test = email = default_persistent

inurl: / wwwboard / passwd.txt

filetype: log inurl: “password.log”

filetype: conf inurl: proftpd.conf-sample

filetype: bak inurl: “htaccess | passwd | shadow | htusers”

outlook filetype: pst

- **Buscando backup de configurações de CMSs,**

filetype: inurl sql: wp-conten t / Backup-*

intext:”~~Joomla1.txt” title:”Indexof /”

configuration.php_ “<?phpclass Jconfig{“

inurl:wp-config.old

inurl:configuration.php.bkp

- **Acesso a impressora remotas**

intitle:”Web Image Monitor” & inurl:”/mainframe.cgi”

- **Buscando câmeras/webcams disponíveis na internet:**

intitle:”Live View -AXIS 211″

inurl:”viewerframe?mode=motion“

inurl:”/control/userimage.html”

#inurl:”intitle:”sony network camera snc-m1″”

#inurl:”site:.viewnetcam.com -www.viewnetcam.com”

#Inurl:”intitle:”Toshiba Network Camera” user login”

#inurl:”intitle:”netcam live image”””

Existem diversas listas de dorks para cada tipo de serviço que explora vulnerabilidades diferentes, basta usar o próprio Google para achar to tipo de busca que deseja buscar. Lembrando que isso não é um invasão pois os dados estão aberto para acesso, mas a forma que você utiliza essa informação (seja para white/black hat) é o que vai determinar se é um delito ou não.