



COMO É FEITO UM SITE?

- Backend
- Front end:
 - HTML
 - CSS
 - Javascript

Pássaro é fotografado voando utilizando apenas a força da raiva, confira:



MAC E IP

- MAC: Número de fato do computador, não é colocado nos dados
- Internet Protocol:
 - Dinâmico (mas podemos mudar)
 - Ipv4
 - Ipv6: A diferença está em ser hexadecimal

PACKET

- Não é a unidade mínima de internet (este é o frame) mas é a unidade geral da internet
- Window size, destino, origem, flags
- Handshake



TCP

- Confiável
- Pesado
- É o mais usado em maior parte dos protocolos
- Possui uma numeração para garantir a ordem na mensagem

UDP

- Mais leve que o TCP mas menos confiavel
- Imagens, áudio entre outros

SUBNET

- É como a internet se comporta na maior parte do tempo
- ip addr show
- www.whatsmyrealip.com



PORTAS



- Um computador recebe várias mensagens ao mesmo tempo, fazendo com que tenhamos que entender onde vai cada mensagem
- 64000 portas
- Firewall

PROTOCOLOS MAIS COMUNS

- HTTP: Mais utilizado na internet, mas não confiável
- HTTPS: Mais seguro, possui uma encriptação assimétrica que é autenticada por outros sites
- FTP : File transfer protocol
- SSH: Secure shell, podemos controlar outro computador por meio dele, tomar cuidado com subnet



HEADERS

- Por meio deles podemos ver configurar questões básicas de comunicação
- HTTP:
 - GET
 - POST
 - DELETE

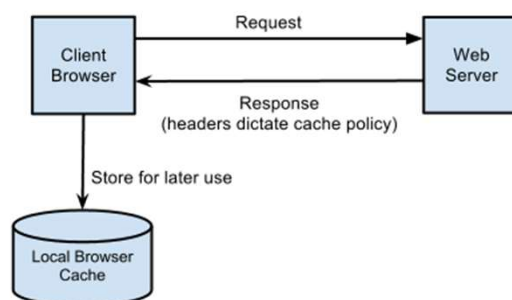
DNS

- Também chamado de nameserver
- Cloudflare
- Google
- DNS cache poisoning

MAIS ALGUNS TÓPICOS

CACHE

Método criado para reduzir pedidos mas carrega o navegador

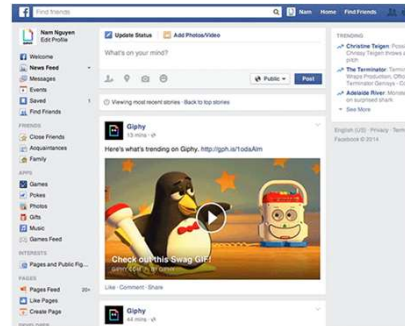


JAVASCRIPT REQUESTS

Orkut



Facebook



COOKIES

Por que precisamos deles?



GOOGLE DORKS

<https://www.exploit-db.com/google-hacking-database/>



EXPLOIT DATABASE

Home | Exploits | Shellcode | Papers | Google Hacking Database | Submit | Search

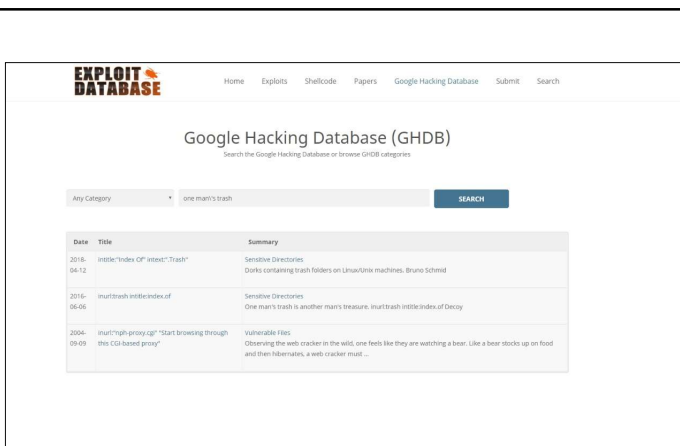
Google Hacking Database (GHDB)
Search the Google Hacking Database or browse GHDB categories

Any Category

Date	Title	Category
2018-11-06	"qprst"	Pages Containing Login Portals
2018-11-06	intext:publicarcade flttype.java	Files Containing Passwords
2018-11-06	intitle:"- Revision" + "subversion version"	Sensitive Directories
2018-11-06	index of / xan	Sensitive Directories
2018-11-06	inurl:"swagger-ui/index.html"	Various Online Devices
2018-11-02	intitle:veolia "Server Timer"	Web Server Detection
2018-11-01	intitle:"Sucuri Website Firewall - Access Denied"	Web Server Detection
2018-11-01	intext:"Powered by phpSQLiteCMS" intext:"phpSQLiteCMS - A simple & lightweight CMS"	Web Server Detection
2018-11-01	inurl:"phpSQLiteCMS/index.php"	Pages Containing Login Portals
2018-10-31	intitle:"SQLiteDatabase" + intext:"Welcome to SQLiteDatabase version "	Various Online Devices

Footholds (75)
Examples of queries that can help an attacker gain a foothold into a web server

Web Server Detection (113)
These links demonstrate Google's awesome ability to profile web servers.



EXPLOIT DATABASE

Home | Exploits | Shellcode | Papers | Google Hacking Database | Submit | Search

Google Hacking Database (GHDB)
Search the Google Hacking Database or browse GHDB categories

Any Category one man's trash

Date	Title	Summary
2018-04-12	intitle:"index of" intext:"Trash"	Sensitive Directories Dorks containing trash folders on Linux/Unix machines. Bruno Schmid
2016-06-06	inurl:trash intitle:index of	Sensitive Directories One man's trash is another man's treasure. Inurl:trash intitle:index of Decoy
2004-09-09	inurl:"high proxy.asp" "Start browsing through this CGI based proxy"	Vulnerable Files Observing the web crawler in the wild, one feels like they are watching a bear. Like a bear stocks up on food and then hibernates, a web crawler must ...

ONE MAN'S TRASH
Is another man's treasure