Bootcamp Java 04/11/22

falhas do http 1.1

hol - head of line blocking (não poder fazer mais de uma requisição por vez)

http 2.0

ele traz uma multiplexação, trazendo mais de uma requisição com um mapeamento melhor com as streams.

priorização de recursos utilizando pesos, dando uma ordem de relevância.

formato geral de uma requisição http

Interface gráfica do usuário, Aplicativo, Word

Descrição gerada automaticamente

Interface gráfica do usuário

Descrição gerada automaticamente

dentro do http 2.0 ele pode reutilizar o header. caso ele seja igual para mais de uma requisição

Push

envia tudo que precisa sem esperar a requisição do cliente

Uma imagem contendo Texto

Descrição gerada automaticamente

esse push não é habilitado por default

Características http 2.0

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Servidores / Sistemas de aplicação

servidores interessantes

* apache
* nginx
* xampp

Apache

datado de 1995

contribuição com a www (world wide web)

opensource e gratuitio

mantido pela apache software foundation

Caracterísitcas

* modular, dinâmico e carregável
* multiple request processing
* altamente escalável ( +10,000 conexões simultâneas)
* lida com arquivos estáticos, index, auto-indexing e negociação de conteúdo
* tls/ssl via open SSl ou wolfSSL
* servidores virtuais com endereços baseados em ip ou nome
* compatibilidade com IPV6
* suporte a versão 2.0 do http
* proxy reverso, websocket

XAMPP

pacote /ambiente

apache server

mariaDB

interpretadores scripts - PHP/pearl

OpenSSL, phpMyAdmin, mediaWki, Joo mla, Wordpress

o xampp é voltado para teste e desenvolvimento, não possui acesso a internet

NGINIX

servidor lançado em 2004

* web server
* proxy reverson
* load balancer
* mail proxy
* http cache

Recursos

* + 10,00 conexões
* lida com arquivos estáticos, index, auto-index
* proxy reverso
* load balance
* tls/ ssl com sni via openSSL
* suporte a http 2.0
* compativel com IPV
* fastCGI, SCHI, uWSGI com cache
* suporte a gRCP (v 1.13.10)
* servires virtuais baseados em ip e nome
* webSocket desde 1.3.13
* url rewriting and redirection

Como ocorre a comunicação cliente/servidor

usando a ferramenta wireshark (muito utilizada em redes)

Conceitos básicos da segurança da informação

criptografia por chave

Mapeia o texto legível para texto ilegível, meio que bloqueando o conteúdo.

assimétrica

Uma imagem contendo Interface gráfica do usuário

Descrição gerada automaticamente

Simétrica

Uma imagem contendo Texto

Descrição gerada automaticamente

Cifra de cesar

substituição da letra pela k-ésima do alfabeto, rotatividade do alfabeto

k=1,26

Diagrama

Descrição gerada automaticamente

no caso do b a 3ª posição a frente é o E

Cifra de blocos

Interface gráfica do usuário, Texto, Aplicativo, chat ou mensagem de texto

Descrição gerada automaticamente

Cifra de fluxo

Uma imagem contendo Linha do tempo

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

certificado digital

certificação de chave pública

entidade certificadora

verificamos através da chave, ao gerar o certificado damos dados a certificadora e ela gera nossa certificação digital

ela verifica a identidade e emite os certificados, mantendo vínculo entre a chave e a entididade

padrões de autoridades certificadoras

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

Protocolo SSL

* segurança para conexões TCP
* confidencialidade
* integridade
* autenticidade end-point

Importância do SSL

cenário de ataque passivo: listening. verificando informações

cenário de ataque ativo: modificar informações dentro da request

usando o https prejudica os hacker, os impossibilitando de modificar as requests

ele permite a confidencialidade e a segurança dos dados

Operação do SSL

fases

handshake, key derivation e data transfer

Handshake

conexão de 3 vias tcp

Diagrama

Descrição gerada automaticamente

verificação de autenticidade.

Diagrama

Descrição gerada automaticamente

a certificação gera uma chave pública

que cria a master secret key

essa ms é usada somente na sessão atual

Verificação da chave ms

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

transferencia efetiva dos dados

record + mac devem ser enviados

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

ao fazer isso é enviado record +mac para o meu usuário

HTTP + SSL

Segurança na comunicação HTTP

over Tcp

verificação da autenticidade por certificados digitais na porta 443

há sites que não utilizam, porém sofrem com os riscos

LGPD

Lei geral da proteção de dados

promulgado em 2018

entrou em vigor em agosto de 2020

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

O que a lei protege

* dados de identificação dos usuários
* dados sensíveis

religião etnia,

* define o tratamento dos dados
* livre consentimento
* direito do titular das informações
* sanções aos que descumpres as regras

Com a LGPD foi criada a ANPD (agência nacional de proteção de dados)

* zelar pela proteção dos dados
* elaboração de diretrizes para politica nacional de proteção
* promover conhecimento das normas
* editar regulamentos
* realizar auditorias