ICMC USP
SÃO CARLOS

GANESH

Segurança Web

Web

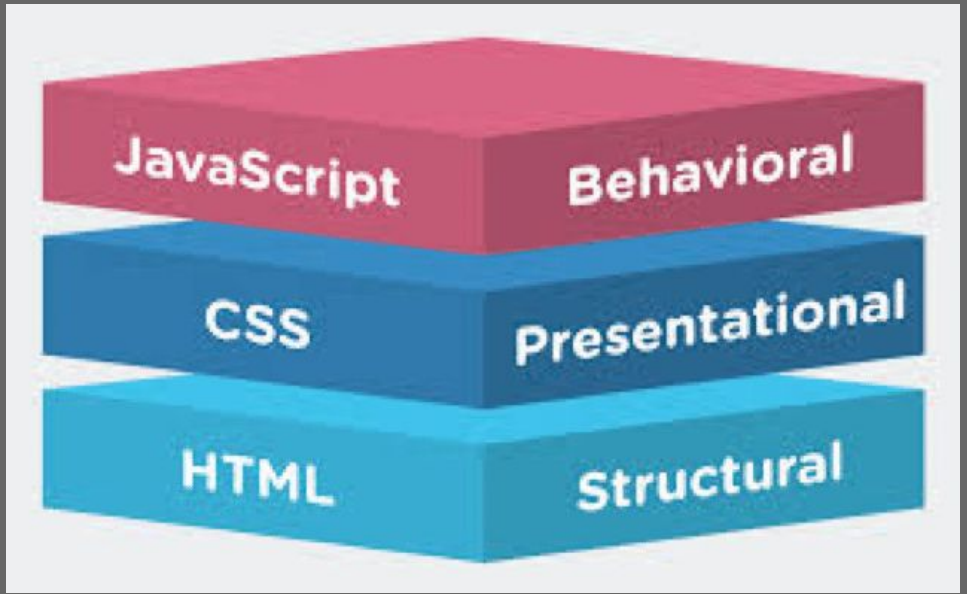
O que é?

Internet

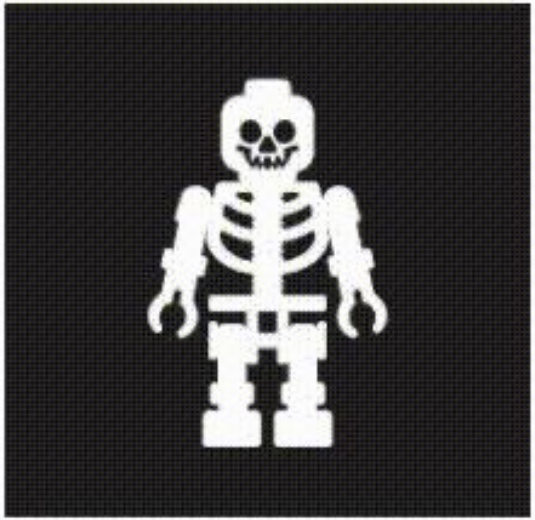
World Wide Web

A Página Web

- HTML - Hypertext Markup Language
- CSS - Cascading Style Sheets
- JavaScript - Não tem ligação com a linguagem Java!



HTML
structure

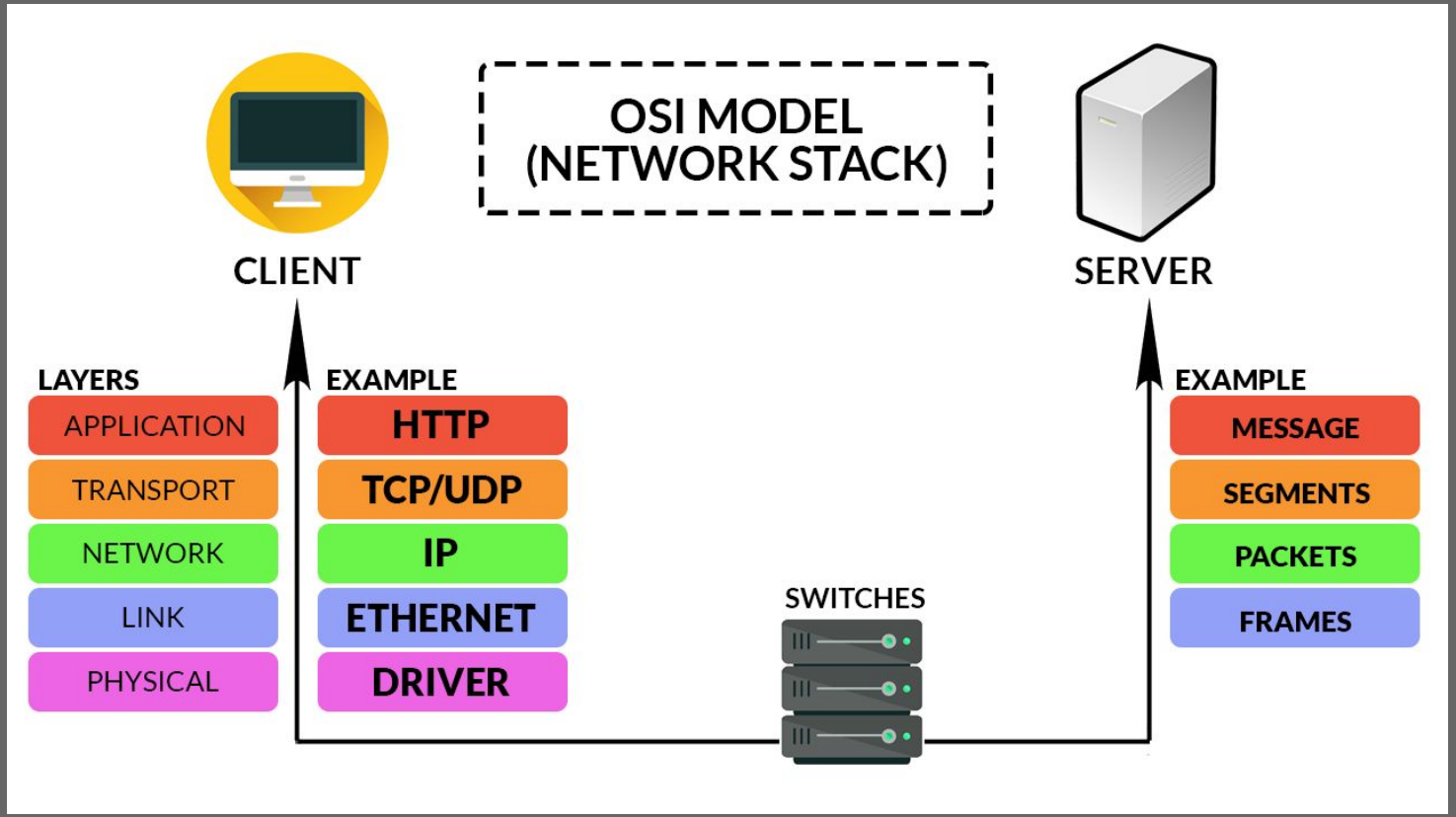


CSS
presentation/appearance

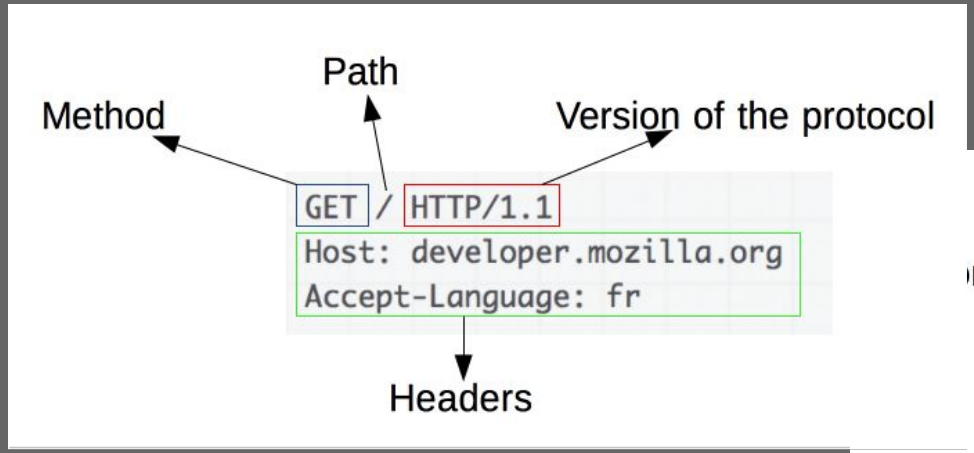
JavaScript
dynamism/action

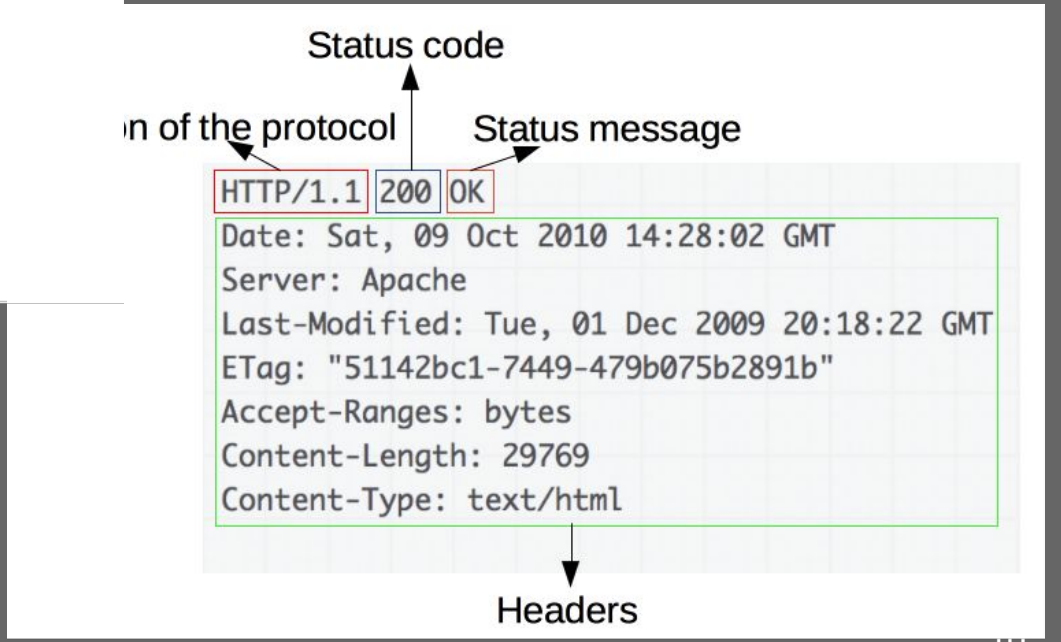
Hyper Text Transfer Protocol

Modelo OSI

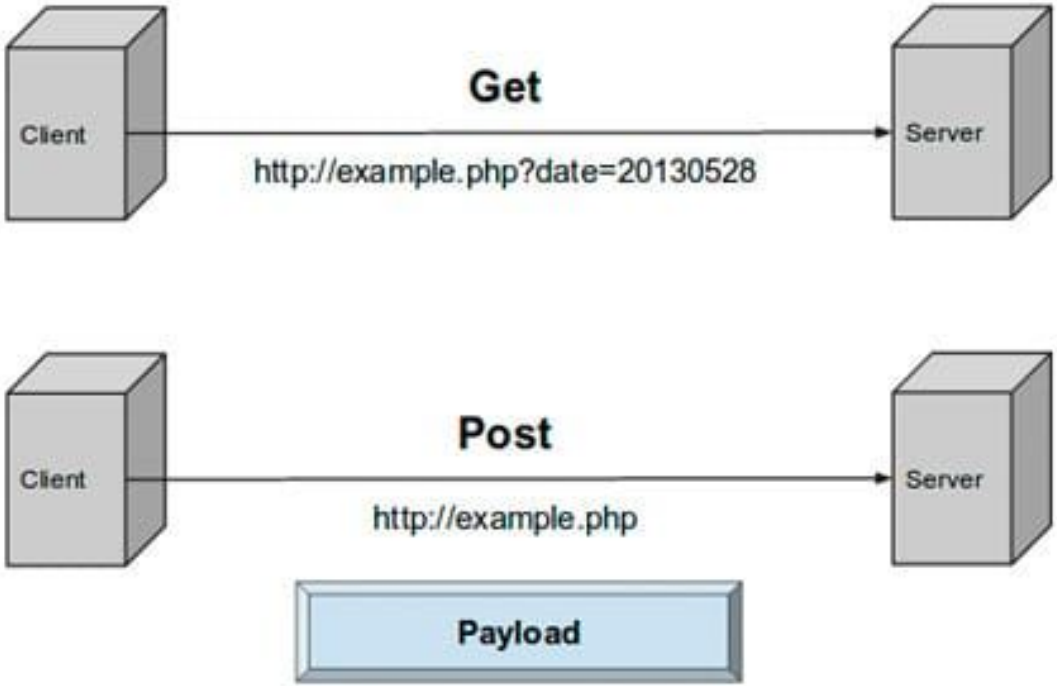

OSI MODEL
(NETWORK STACK)
CLIENT
SERVER
LAYERS
EXAMPLE
EXAMPLE
APPLICATION
TRANSPORT
NETWORK
LINK
PHYSICAL
HTTP
TCP/UDP
IP
ETHERNET
DRIVER
SWITCHES
MESSAGE
SEGMENTS
PACKETS
FRAMES

Mais sobre o HTTP





GET e POST


Client
Get
http://example.php?date=20130528
Server
Client
Post
http://example.php
Server
Payload
Form Data, JSON Strings, Query Parameters, View States, etc

O Navegador Web

Segurança Web

Open Web Application Security Project (OWASP)

OWASP Top 10


2017
OWASP
TOP
10
APPLICATION
SECURITY RISKS
A1
INJECTION
A2
BROKEN AUTHENTICATION
A3
SENSITIVE DATA EXPOSURE
A4
XML EXTERNAL ENTITIES (XXE)
A5
BROKEN ACCESS CONTROL
A6
SECURITY MISCONFIGURATION
A7
CROSS-SITE SCRIPTING (XSS)
A8
INSECURE DESERIALIZATION
A9
USING COMPONENTS WITH KNOWN VULNERABILITIES
A10
INSUFFICIENT LOGGING & MONITORING

SLQ Injection

Cross-site Scripting (XSS)

Demonstração

Alguns Materiais de Estudo

- https://portswigger.net/web-security
  - Bom para aprender conceitos, contém material teórico e exemplos práticos
- https://www.hackerone.com/blog/Hack-Learn-Earn-with-a-Free-E-Book
  - Livro com vulnerabilidades gerais exploradas em programas de bug bounty
- https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
  - Simulador de vulnerabilidades, explica o que é para fazer
- https://overthewire.org/wargames/natas/
  - Wargame, não possui dicas sobre os níveis
- HackTheBox - https://www.hackthebox.eu/
  - Simulação de ataques em ambientes reais
- https://developer.mozilla.org/en-US/docs/Learn
  - Material da Mozilla para aprender desenvolvimento Web
- https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
  - OWASP Top 10

GANESH

Grupo de Segurança da Informação
ICMC / USP - São Carlos, SP
http://ganesh.icmc.usp.br/
ganesh@icmc.usp.br
https://github.com/GANESH-ICMC

ICMC USP SÃO CARLOS

GANESH