Web Güvenliği

Tarihi

WORLD-WIDE-WEB

ARPANET

ETHERNET

ebay
Java
LYCOS
AOL.

iTunes
flickr
facebook
bing
tumblr.

?

INTERNET

FTP & TCP/IP

| 1969 | 1973 | 1976 | 1982 | 1990 | 1994 | 1995 | 1998 | 1999 | 2003 | 2004 | 2005 | 2007 | 2009 | 2010 | 2012 | 2014 |

Netscape
YAHOO!
amazon.com

Google
myspace.com
napster

WordPress
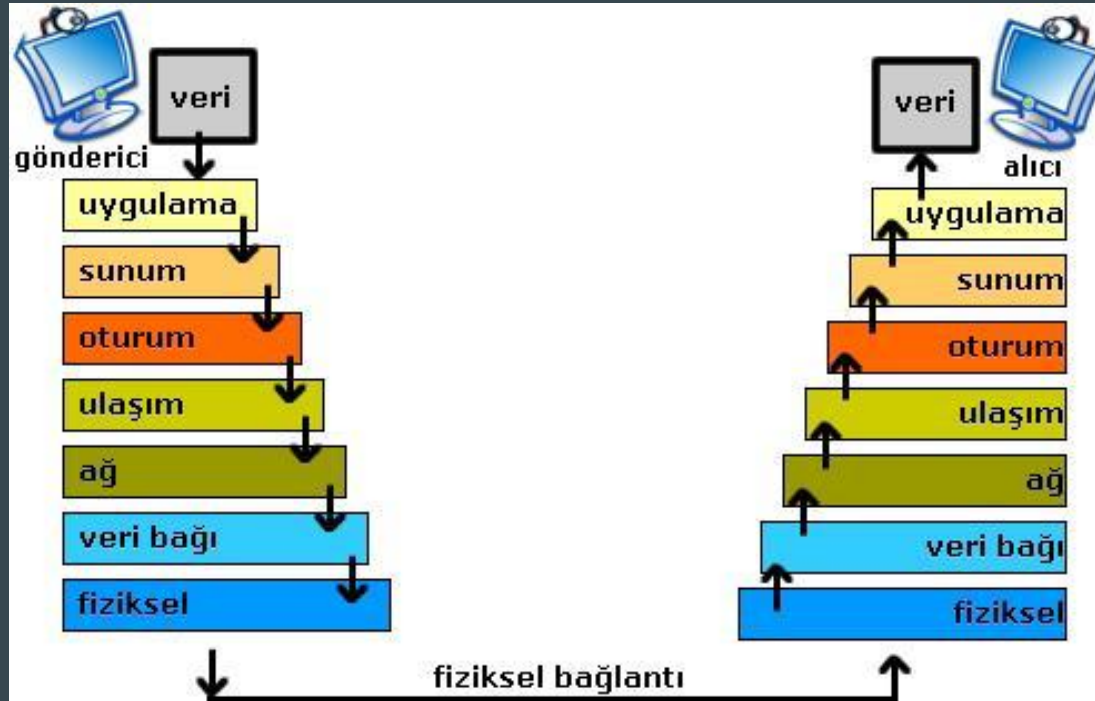Skype

YouTube
twitter

Pinterest
Instagram

?

Genel Kavramlar

1. OSI Modeli
2. TCP/IP
3. ISP (Internet Service Provider)
4. Server (Sunucu)
5. DNS (Domain Name Server)
6. Domain (Alan Adı)
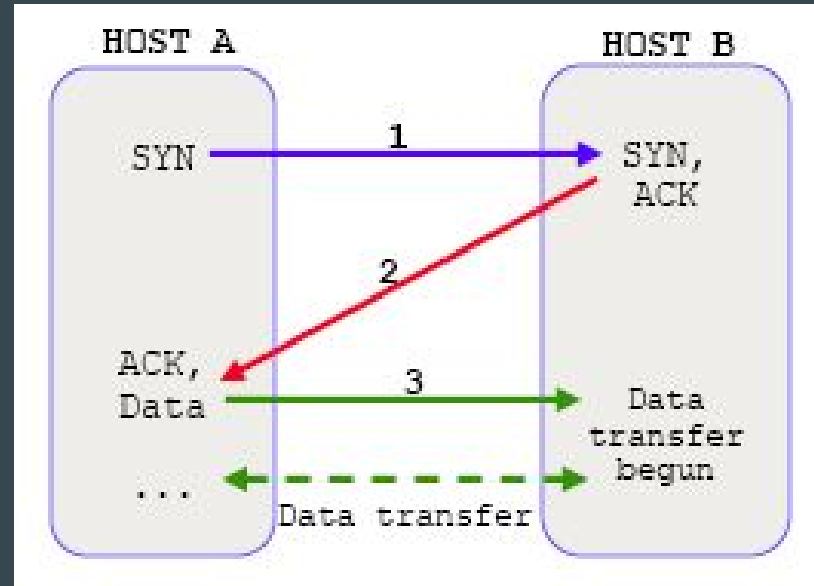7. HTTP / HTTPS
8. Request - Response

OSI Modeli

TCP/IP

3-Way Handshake

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255
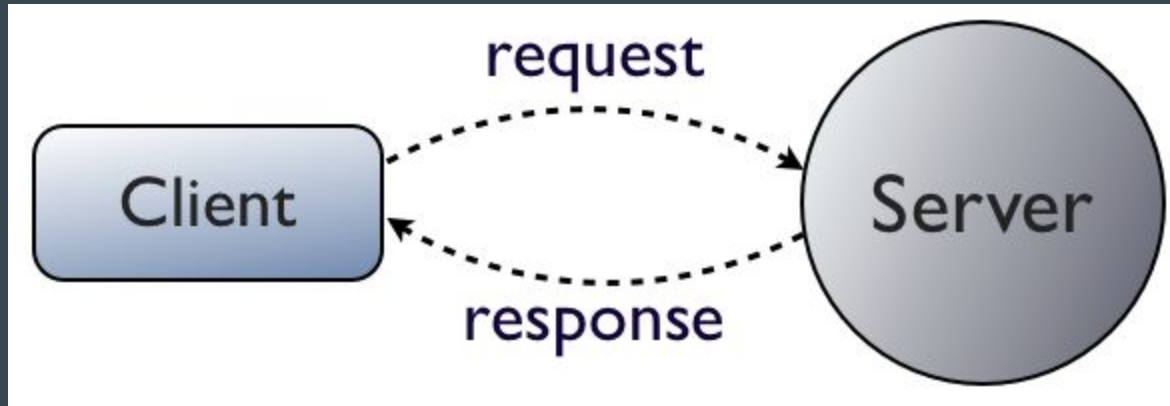
192.168.0.0 - 192.168.255.255

Domain Nedir?

HTTP

HTTP Methods

Method	Description
GET	Request to read a Web page
HEAD	Request to read a Web page's header
PUT	Request to store a Web page
POST	Append to a named resource (e.g., a Web page)
DELETE	Remove the Web page
TRACE	Echo the incoming request
CONNECT	Reserved for future use
OPTIONS	Query certain options

Status Codes

Error 404

Woops. Looks like this page doesn't exist.

HTTP Status Codes

Code	Description	Code	Description
200	OK	400	Bad Request
201	Created	401	Unauthorized
202	Accepted	403	Forbidden
301	Moved Permanently	404	Not Found
303	See Other	410	Gone
304	Not Modified	500	Internal Server Error
307	Temporary Redirect	503	Service Unavailable

Web Tabanlı Uygulamalar ve Teknolojiler

• • •

Teknolojiler, Frameworkler, Araçlar...

Open Source

...

Ortak Kod Havuzu (Github)
Proje temeli (boiler plate)
Kod blokları (npm)

UNIX?

OOH THAT OPEN SOURCE OS THAT I COPIED AND MADE TONS OF MONEY? COME AT ME BRO

quickmeme.com

Ortamına Göre Web Tabanlı Uygulama Gelistirme

• • •

Front-end ve Back-end
Client-side ve Server-side

BACK-END

FRONT-END

Front-end

•••

HTML, CSS, Javascript
ve Frameworkleri

```
91          <div class="resim"><img id="questionImage" src="img/jenerik/1.jpg" style="width:100%"/>
92          <div id="itemHolder"><img id="itemIcon" src=""/><div id="itemName"></div></div>
93          </div>
94     </div>
95
96     <div id="scroller" class="container">
97                <div id="questionText" class="soru"> <br> </div>
98                <div class="secenekler">
99                     <li id="c_1li" onclick="choice(1)" class="shadow-top"><img src="svg/blur2.svg"/> <span id="c_1"> 
100                    <li id="c_2li" onclick="choice(2)" class="shadow-top"><img src="svg/blur2.svg"/> <span id="c_2"> 
101                    <li id="c_3li" onclick="choice(3)" class="shadow-top"><img src="svg/blur2.svg"/> <span id="c_3"> 
102                    <li id="c_4li" onclick="choice(4)" class="shadow-top"><img src="svg/blur2.svg"/> <span id="c_4"> 
103                </div>
104
105          </div>
106     <div class="subheader">
107          <li class="share" onclick="shareCover()"><img src="svg/share.svg"/> Paylaş</li>
108          <li onclick="skipQuestion()"><img src="svg/forward.svg"/> Pas Geç</li>
109     </div>
110     </div>
111     <div id="login" style="width:100%;height:100%;">
112          <div class="header">
113                <div class="menu" onclick="switchBar()"><img src="svg/menu.svg"/></div>
114                <div class="logo">Stratera<b>Quiz</b></div>
115                <div class="right"><img src="svg/done.svg"/></div>
116          </div>
117          <div class="resim" style="background:url(img/bg_main.jpg); background-size:cover;width:100%;height:100%; background-po
118          </div>
```

```css
62  button {
63      background-image: -webkit-gradient(linear, 43% 0%, 43% 110%, color-stop(0, rgb(221, 221, 221)), color-stop(0.01, rgb(221, 22
64      background-image: -webkit-linear-gradient(-90deg, rgb(221, 221, 221) 0%, rgb(221, 221, 221) 1%, rgb(204, 204, 204) 4%, rgb(1
65      background-image: linear-gradient(180deg, rgb(221, 221, 221) 0%, rgb(221, 221, 221) 1%, rgb(204, 204, 204) 4%, rgb(170, 170,
66      width: auto;
67      height: auto;
68      border: rgb(153, 153, 153) 1px solid;
69      -webkit-border-radius: 50px;
70      border-radius: 50px;
71      margin: 5px;
72      padding: 17px;
73      font: normal 16px/120% "Intel Clear W", Arial, sans-serif;
74      color: rgb(84, 84, 84);
75      text-align: center;
76      text-shadow: 0px 1px 0px rgb(221, 221, 221);
77      margin-bottom: 15px;
78  }
79
80  button:focus {
81   background-image: -webkit-gradient(linear, 43% 0%, 43% 110%, color-stop(0, rgb(136,136,136)), color-stop(0.01, rgb(136,136,136
82      width: auto;
83      height: auto;
84      -webkit-border-radius: 50px;
85      border-radius: 50px;
86      margin: 5px;
87      padding: 17px;
88      font: normal 16px/120% "Intel Clear W", Arial, sans-serif;
89      color: rgb(238,238,238);
90      text-align: center;
```

```
82    function newQuestion() {
83        questionCounter++;
84      if(questionCounter == 10){ questionCounter = 1;
85       createInterstitial(); }
86      openCover();
87    var xhttp = new XMLHttpRequest();
88    var questionObj;
89    xhttp.onreadystatechange=function() {
90      if (xhttp.readyState == 4 && xhttp.status == 200) {
91        questionObj = JSON.parse(xhttp.responseText);
92
93                document.getElementById("itemHolder").style.display = "none";
94
95          var questionAskStyle = randomInt(1,3);
96          var questionStyle;
97          var theQuestionImage;
98          questionTypeReturn = questionObj.type;
99          if(questionObj.type==0){
100
101          questionStyle = questionObj.data1;
102          theQuestionImage = "img/jenerik/"+randomInt(1,12)+".jpg"; //changable
103
104          }else if(questionObj.type==1){
105
106          data1Split = questionObj.data1.split("|");
107          var champName = data1Split[0];
108          var champPerma;
```

Javascript Frameworkleri

● ● ●

jQuery, Backbone.js
Angular, React, Vue, Aurelia

DAYS WITHOUT NEW JAVASCRIPT FRAMEWORK
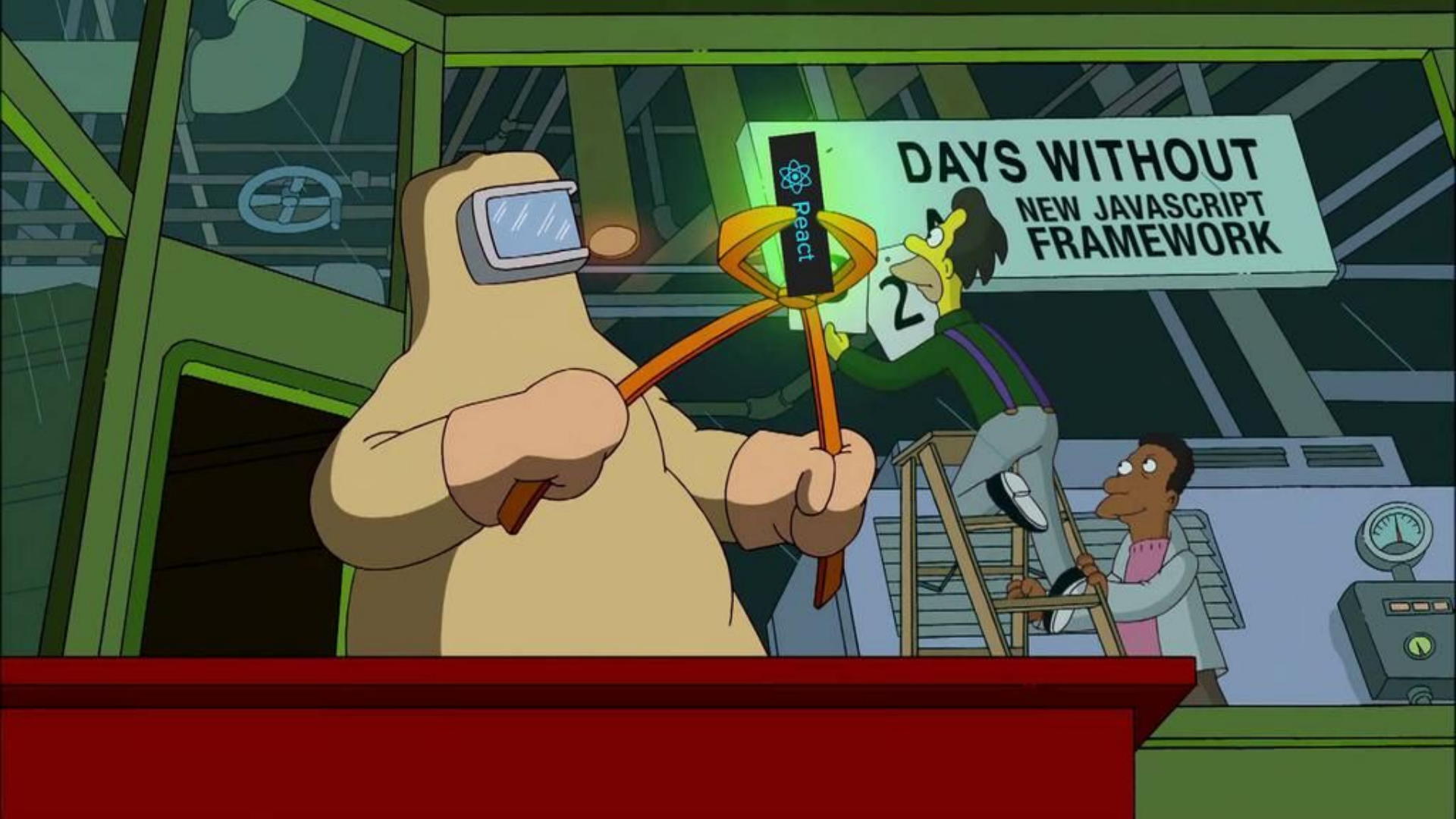
Back-end

...

PHP, Java, .NET, Ruby, Python, Perl, Node.js, Go...

PHP

Çok kullanan var!
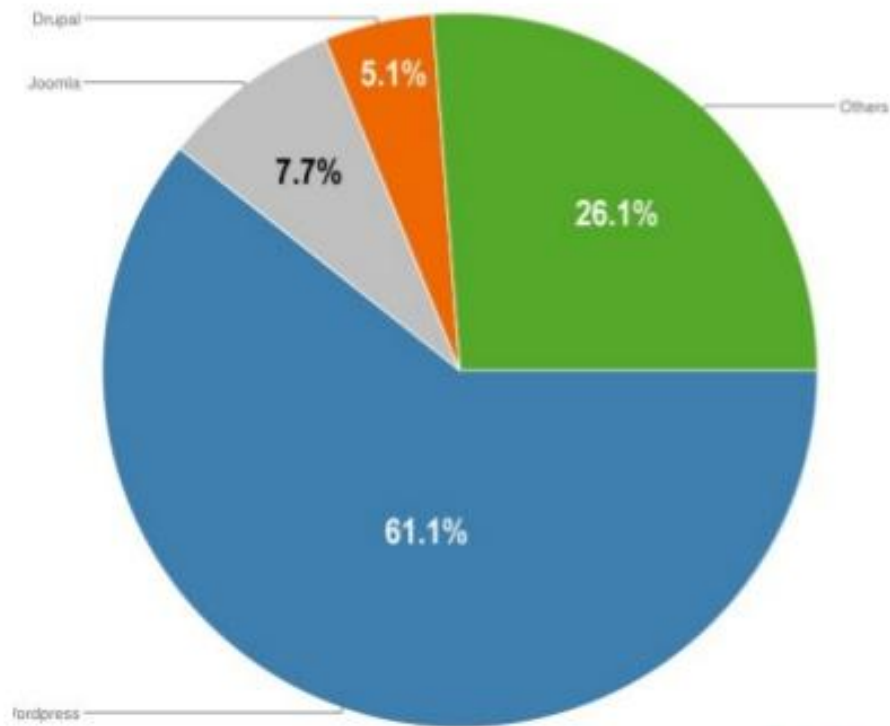
Full Stack?

...

Javascript FTW

Web Server

• • •

Apache, nginx, LiteSpeed
IIS, GWS

Apache Server Status for bhaskar-laptop

Server Version: Apache/2.2.16 (Unix) PHP/5.3.3 with Suhosin-Patch mod_ssl/2.2.16 OpenSSL/1.0.0a DAV/2
Server Built: Aug 17 2010 12:52:36

Current Time: Saturday, 02-Oct-2010 19:56:35 IST
Restart Time: Saturday, 02-Oct-2010 19:22:21 IST
Parent Server Generation: 1
Server uptime: 34 minutes 14 seconds
1 requests currently being processed, 5 idle workers

___W__...
....
....
....

Scoreboard Key:
"_" Waiting for Connection, "S" Starting up, "R" Reading Request,
"W" Sending Reply, "K" Keepalive (read), "D" DNS Lookup,
"C" Closing connection, "L" Logging, "G" Gracefully finishing,
"I" Idle cleanup of worker, "." Open slot with no current process

PID Key:
5727 in state: _ ,   5728 in state: _ ,   5729 in state: _
5730 in state: W ,   5731 in state: _ ,   5732 in state: _

To obtain a full report with current status information you need to use the ExtendedStatus On directive.

SSL/TLS Session Cache Status:

Apache/2.2.16 (Unix) PHP/5.3.3 with Suhosin-Patch mod_ssl/2.2.16 OpenSSL/1.0.0a DAV/2 Server at bhaskar-laptop Port 80

Commands: Use arrow keys to move, '?' for help, 'q' to quit, '<-' to go back.
 Arrow keys: Up and Down to move. Right to follow a link; Left to go back.
 H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
[bhaskar-laptop][0-$ Net {1*$ bash}   ][0.49 0.43 0.51][10/02 19:57]

Database

• • •

SQL - NoSQL
MySQL, MsSQL, PostgreSQL
MongoDB, Redis, Solr, Elastic

Server: localhost ▶ **Database: pakistanihaider** ▶ **Table: cv_skills**

Browse | Structure | SQL | Search | Insert | Export | Import | Operations

	Field	Type	Collation	Attributes	Null	Default	Extra	Action					
☐	**skill_id**	int(11)			No	None	auto_increment						
☐	**admin_id**	int(10)			No	None							
☐	**skill_name**	varchar(45)	latin1_swedish_ci		No	None							
☐	**skill_desc**	text	latin1_swedish_ci		Yes	NULL							
☐	**skill_rating**	varchar(10)	latin1_swedish_ci		Yes	NULL							
☐	**last_updated**	varchar(50)	latin1_swedish_ci		No	None							

↑_ **Check All / Uncheck All** _With selected:_

🖶 **Print view**   **Relation view**   **Propose table structure** ⓘ

Add [1] field(s) ⦿ At End of Table ○ At Beginning of Table ○ After [skill_id ▾] [Go]

+ Details...

🗔 Open new phpMyAdmin window

localhost/phpmyadmin/sql.php?db=pakistanihaider&table=cv_skills&token=b38531ede17d1a88b42a5e0a100b1c79&goto=tbl_structure.php&back=tbl_structure.php&session_max_rows=all&sql_query=SELECT+*+FROM+`cv_skills`+PROCEDURE+ANALYSE()

Database

pakistanihaider (8)

pakistanihaider (8)

- cv_adminlogin
- cv_education
- cv_language
- cv_portfolio
- cv_skills
- cv_user_profile
- cv_web_settings
- cv_work_exp

Rameez Hassan Mir 20:57

RELATIONAL DATABASE

Tech-Stack

• • •

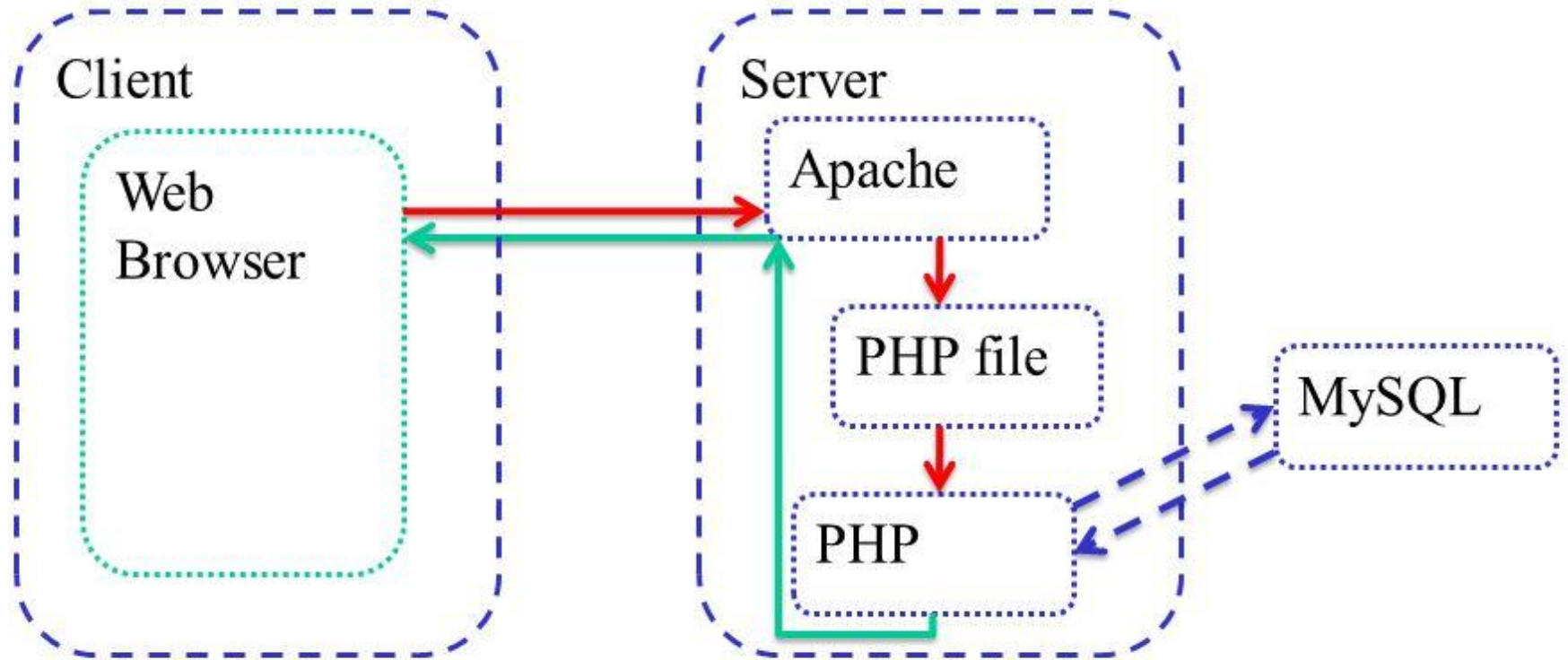Bir projede birlikte kullanılan teknolojiler bütünü.
LAMP - MEAN

LAMP

• • •

Linux, Apache, MySQL, PHP (Perl-Phyton)

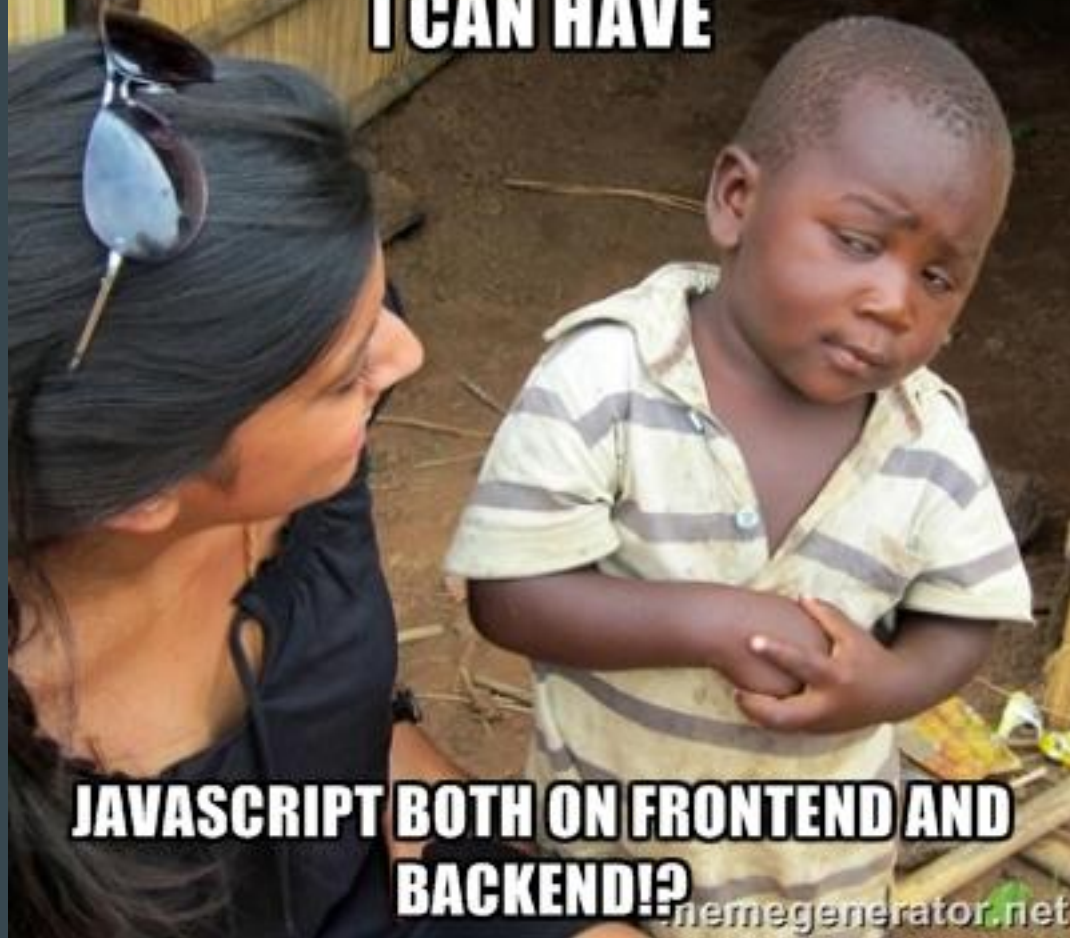This is often referred to as a LAMP (or WAMP) stack:
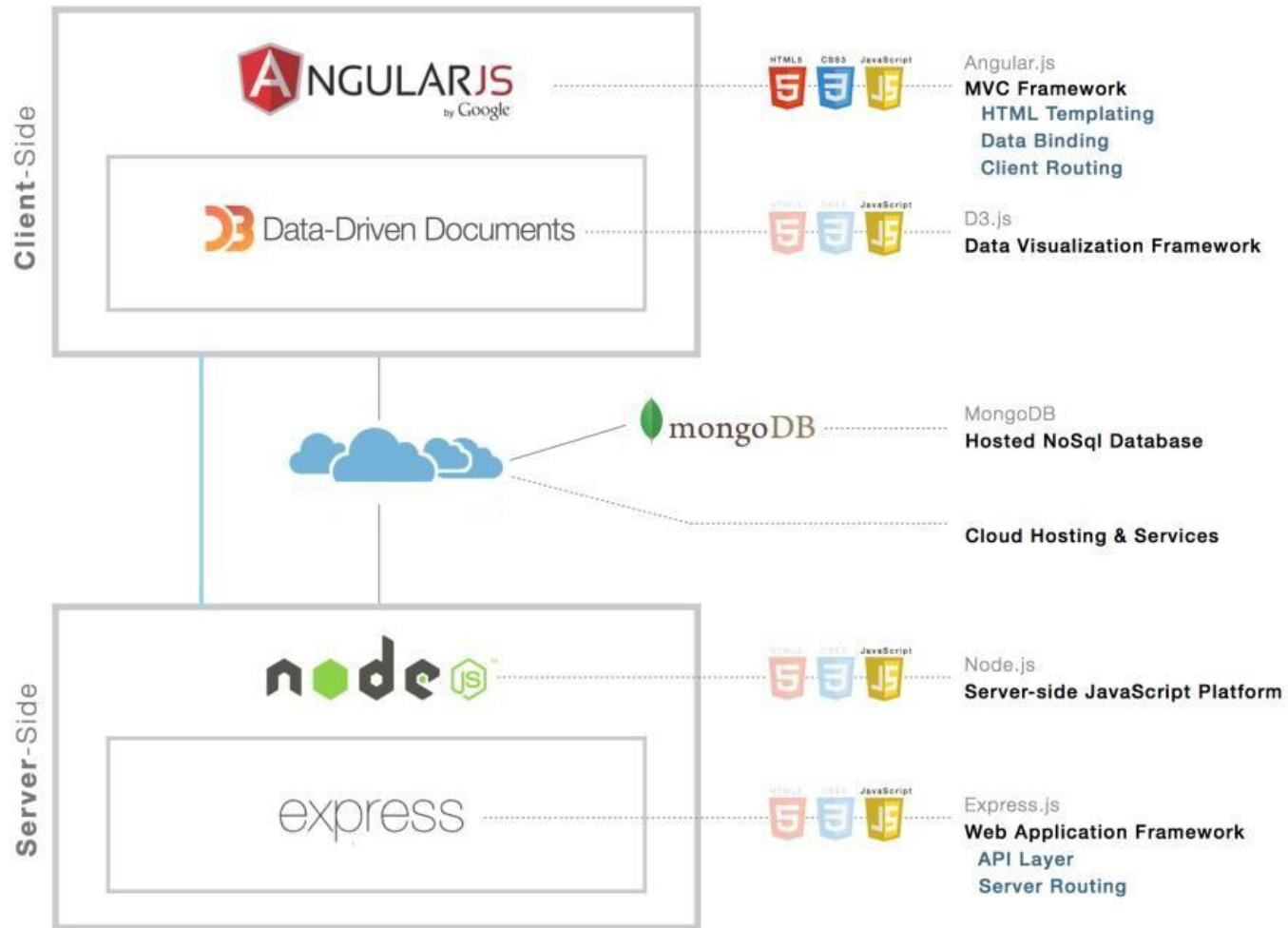**Linux (or Windows) Apache MySQL PHP**

MEAN

● ● ●

MongoDB, ExpressJS, AngularJS, NodeJS
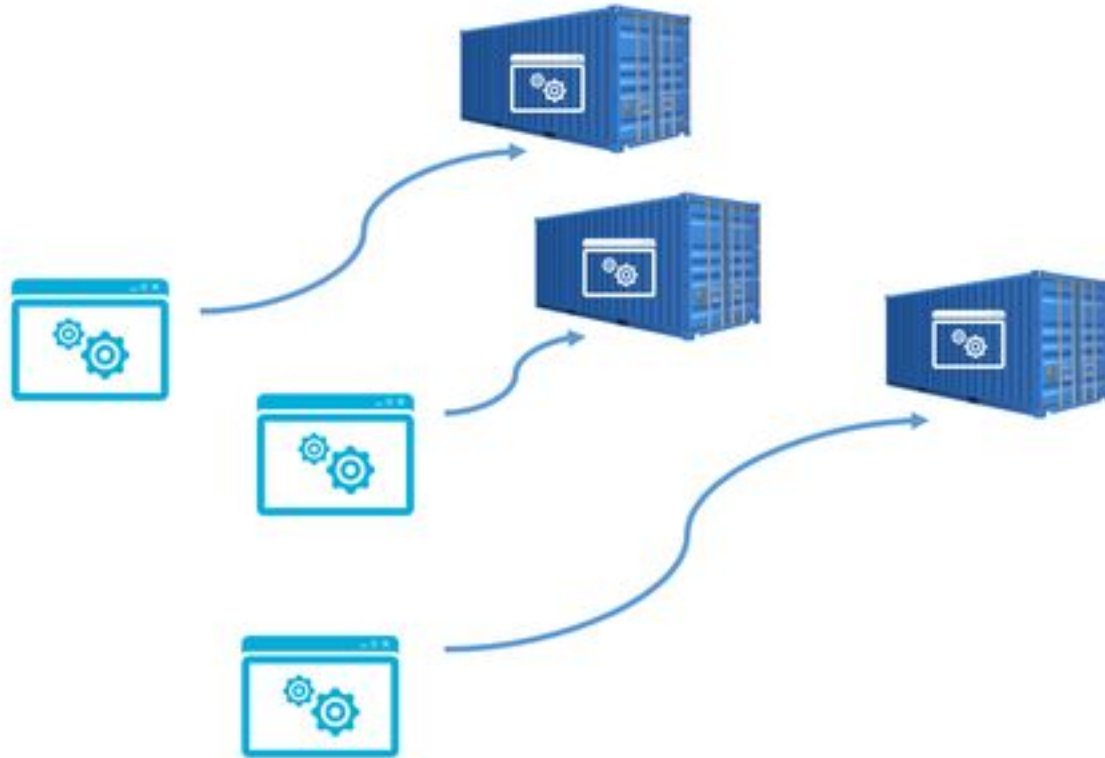(V8 Engine)

SO, WHAT YOU'RE SAYING IS THAT I CAN HAVE

JAVASCRIPT BOTH ON FRONTEND AND BACKEND!?

Client-Side

ANGULARJS by Google

HTML5 CSS3 JavaScript

Angular.js
MVC Framework
HTML Templating
Data Binding
Client Routing

D3 Data-Driven Documents

HTML5 CSS3 JavaScript

D3.js
Data Visualization Framework

Server-Side

mongoDB

MongoDB
Hosted NoSql Database

Cloud Hosting & Services

node js

HTML5 CSS3 JavaScript

Node.js
Server-side JavaScript Platform

express

HTML5 CSS3 JavaScript

Express.js
Web Application Framework
API Layer
Server Routing

Containerized Applications

LAMP is so yesterday!
...
MEAN is so tomorrow :(

LAMP

Good for:

APIs

Simple websites

e-Commerce

MEAN

Good for:

Tech-heavy start-ups

GUI-focused apps

Teams who know only Javascript

API

●●●

API tabanlı Web Uygulamaları
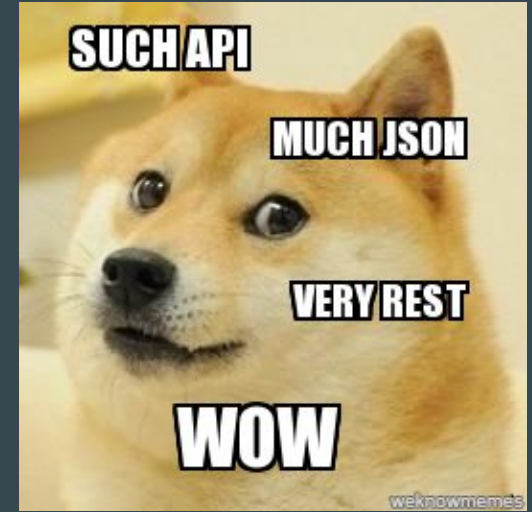SOAP, RESTful

MY API WOULD STAY UP

SOAP

●●●

Eski ve XML Kullanır
Enterprise Seviyesi
Windows, IIS, .NET

RESTful

• • •

Yeni ve JSON Kullanır
Open Source Teknolojiler Kullanır
PHP, Java, Javascript (Node, Angular..)

Photo Resources

- GET photos
- GET photos/search
- GET photos/:id
- GET photos/:id/comments
- GET photos/:id/votes
- PUT photos/:id
- POST photos
- POST photos/upload
- POST photos/:id/vote
- DELETE photos/:id/vote
- POST photos/:id/tags
- POST photos/:id/comments
- POST photos/:id/report
- DELETE photos/:id
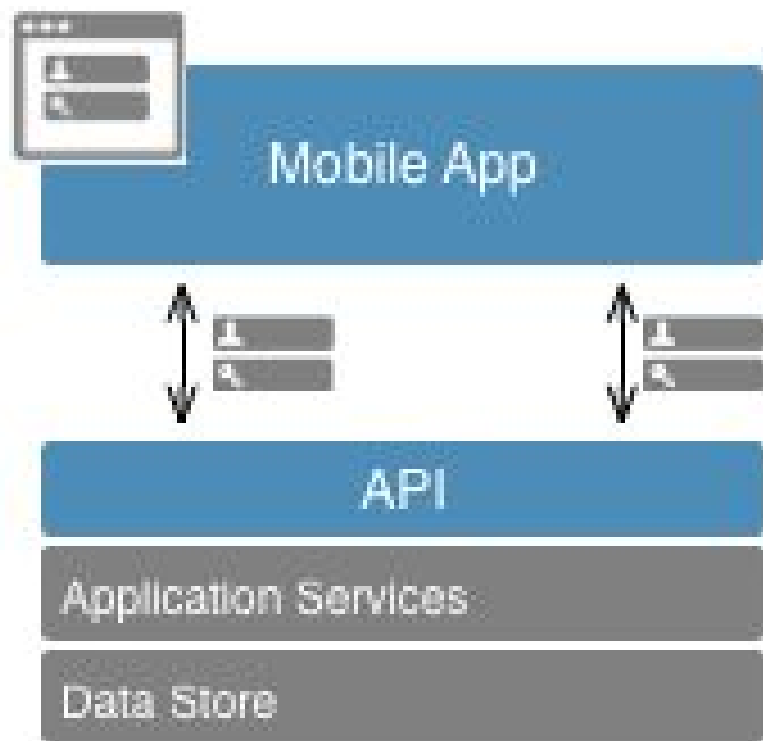- DELETE photos/:id/tags

Upload Method

- POST upload

500px

github.com/500px/api-documentation
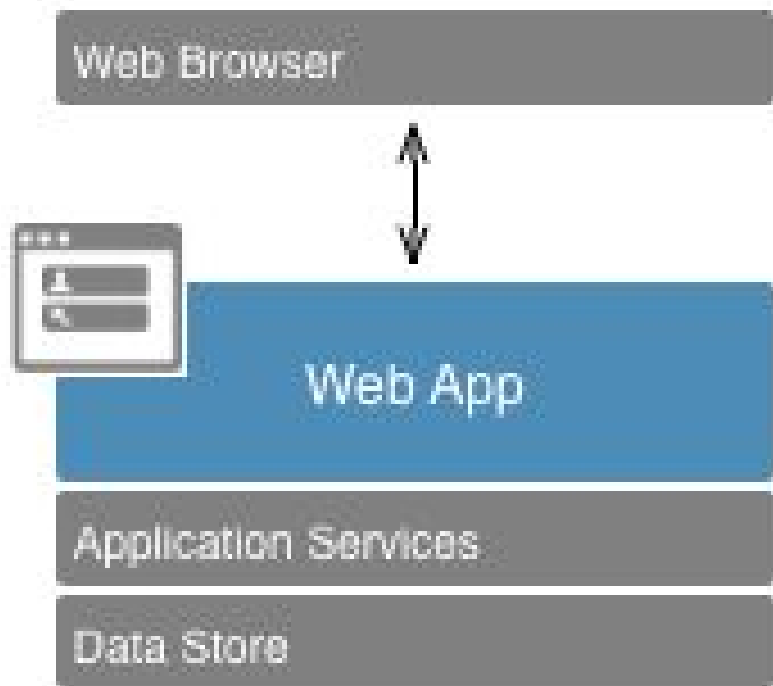
web app authentication points

mobile app authentication points