

Web 安全启蒙

Vidar-Team 第五次培训

by E99p1ant🍆



Web 安全是啥呀？

前端后端学啥呀？

学长这题咋做呀？

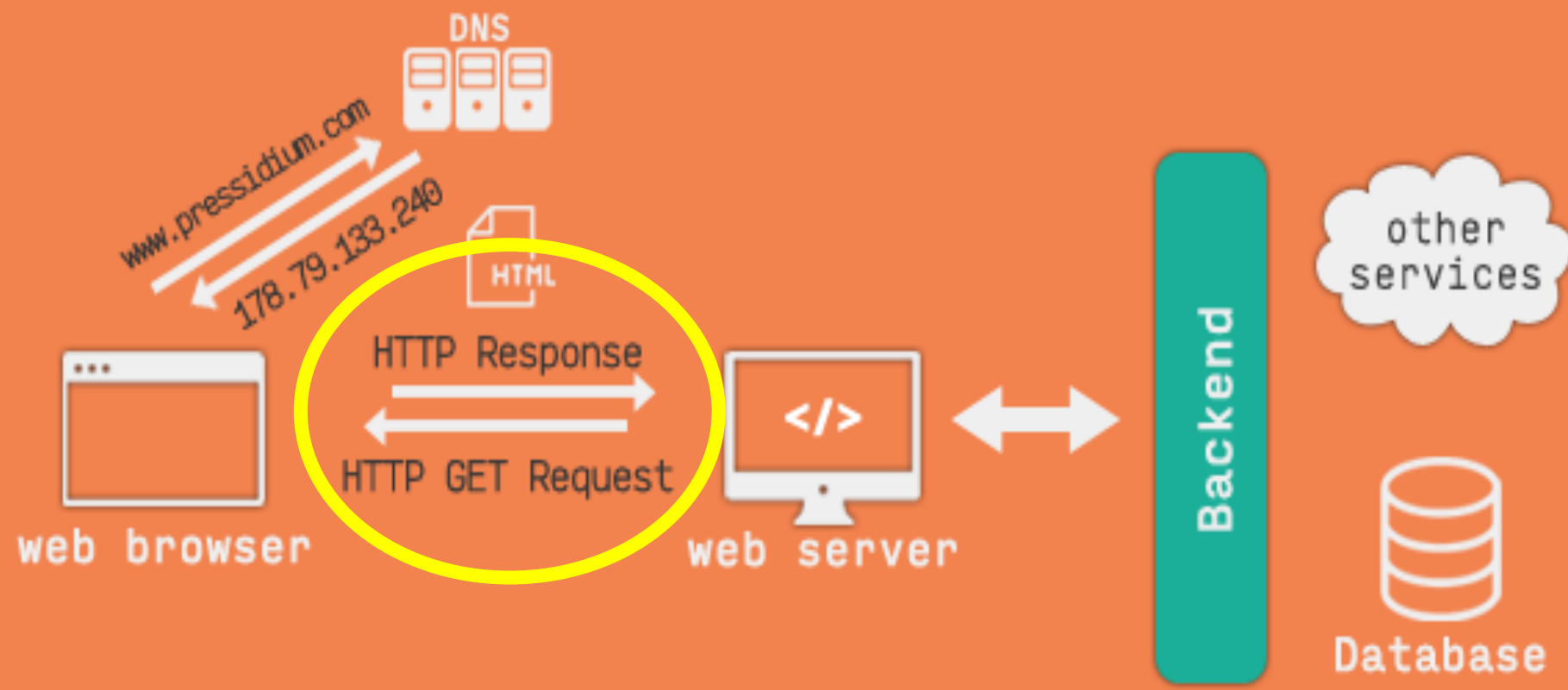
为什么要先学 HTTP 啊？



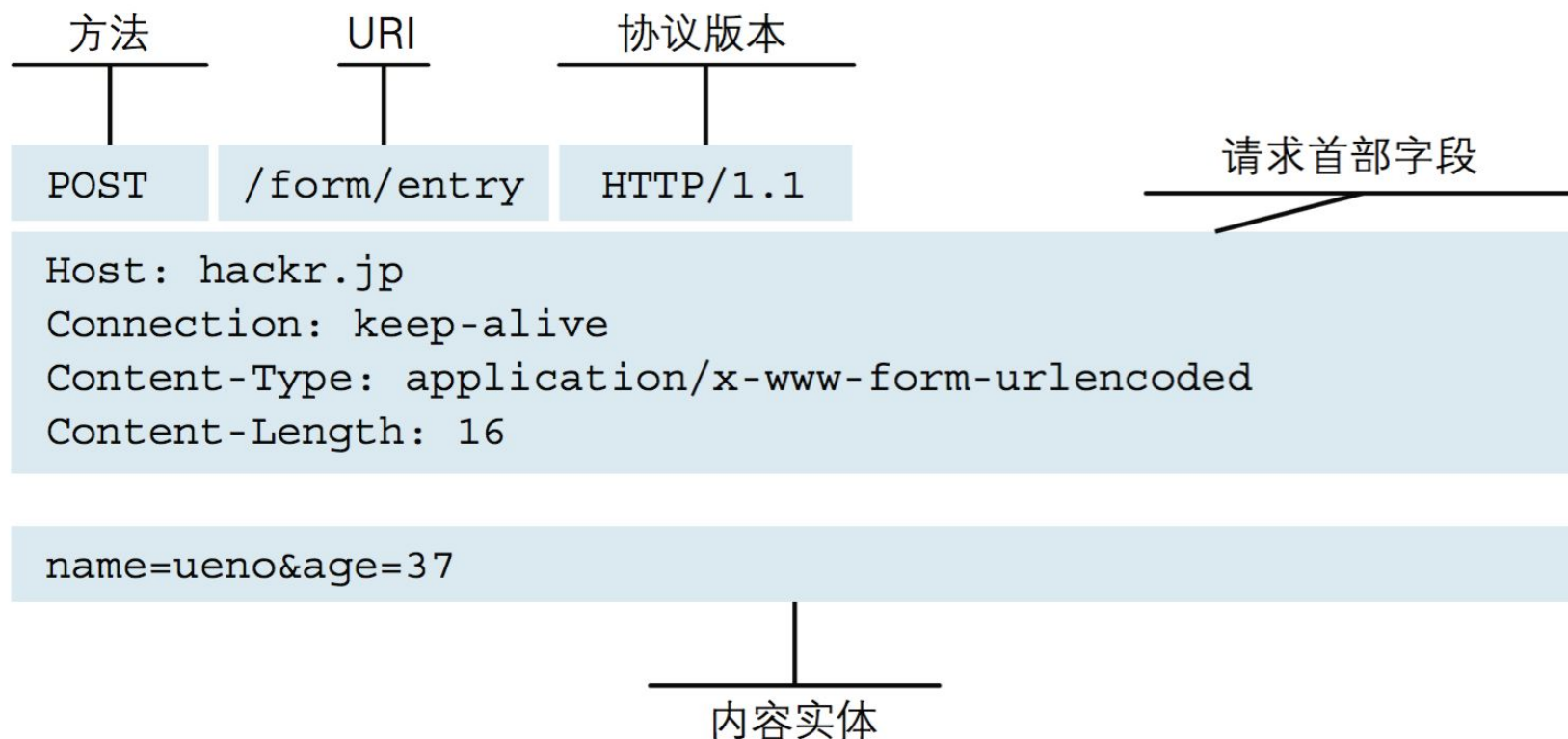
“Web 安全” 中的 Web 应用到底指的是什么？

Web 应用是如何运作的呢？





客户端请求



图：请求报文的构成

方法：GET/POST

.....

URI：请求资源的路径

内容实体：请求的参数

服务端响应

举例：

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 13 Jul 2000 05:46:53 GMT
Content-Length: 2291
Content-Type: text/html
Cache-control: private
```

<HTML>

<BODY>

.....

← 状态行

← 多个消息头 —

← 一个空行

← 实体内容 —

状态行用于描述服务器对请求的处理结果。

消息头用于描述服务器的基本信息，以及数据的描述，服务器通过这些数据的描述信息，可以通知客户端如何处理等一会儿它回送的数据。

代表服务器向客户端回送的数据

Tips: 状态码 Status Code

1**	Hold on
2**	Here you go
3**	Go away
4**	You fucked up
5**	I fucked up



VIDAR TEAM

服务端响应

举例：

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 13 Jul 2000 05:46:53 GMT
Content-Length: 2291
Content-Type: text/html
Cache-control: private
```

<HTML>

<BODY>

.....

← 状态行

← 多个消息头 —

← 一个空行

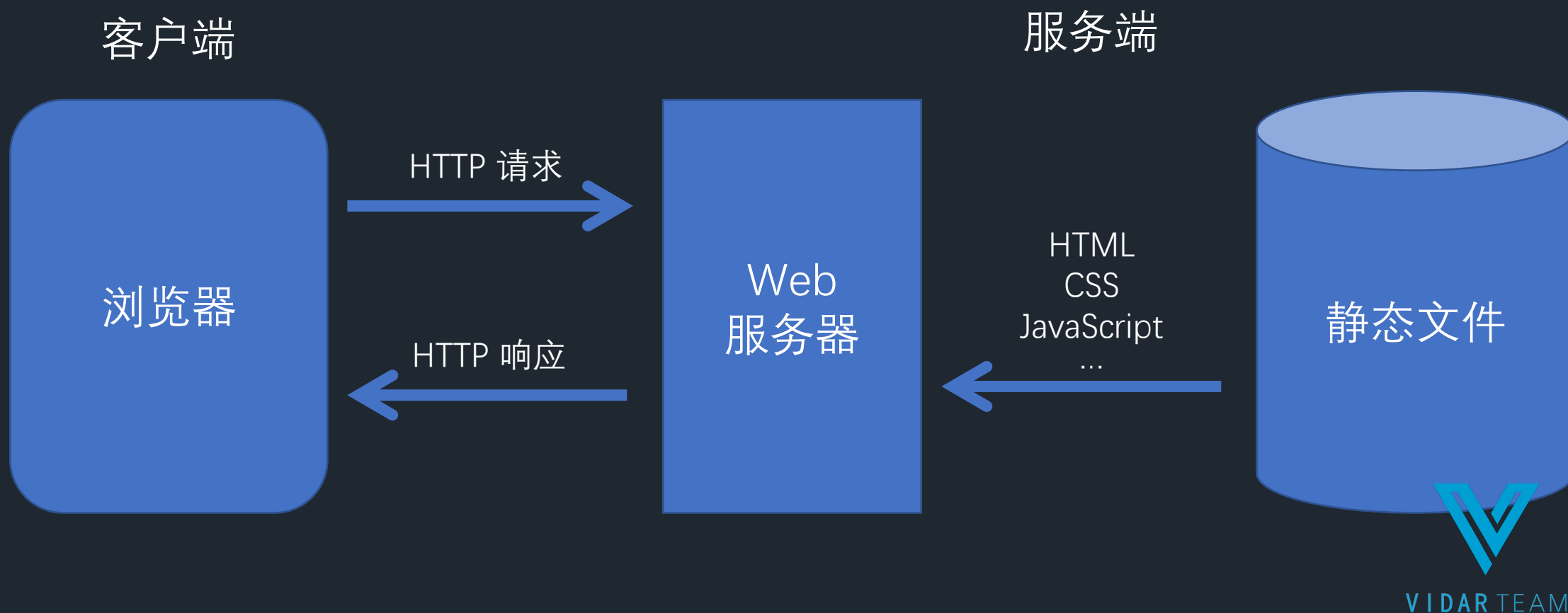
← 实体内容 —

状态行用于描述服务器对请求的处理结果。

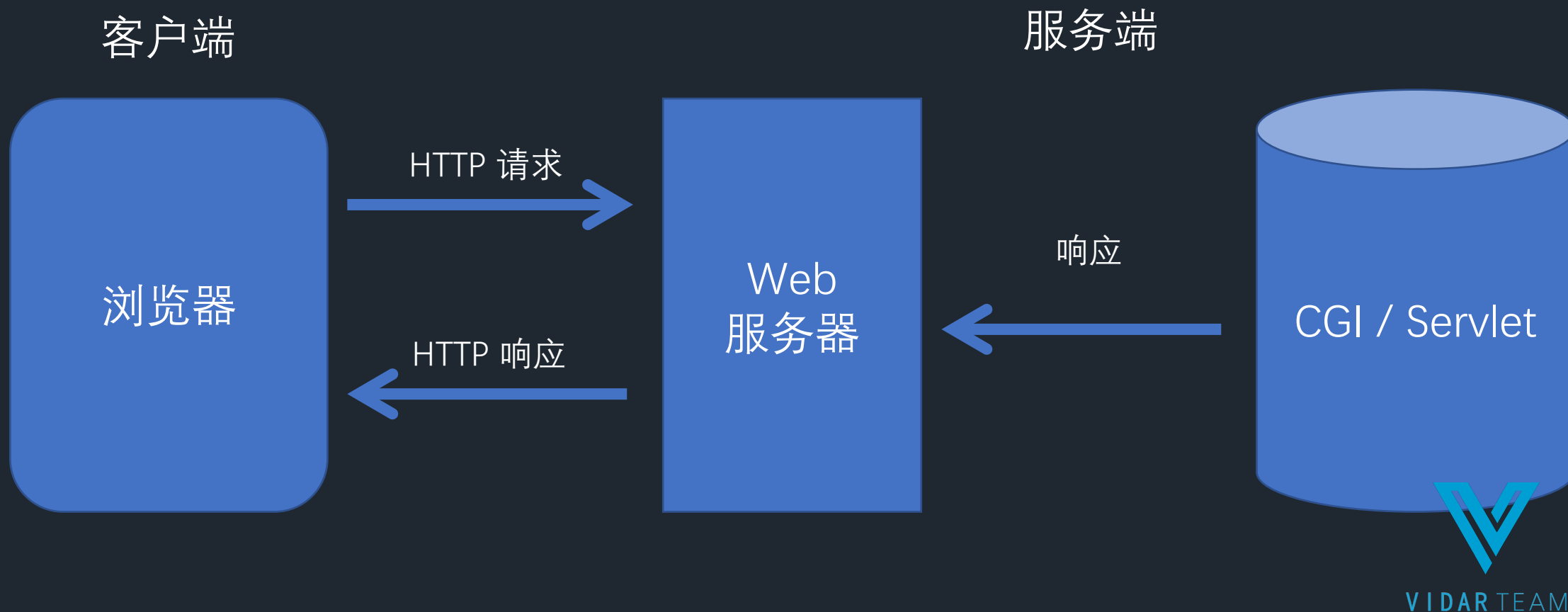
消息头用于描述服务器的基本信息，以及数据的描述，服务器通过这些数据的描述信息，可以通知客户端如何处理等一会儿它回送的数据。

代表服务器向客户端回送的数据

请求静态资源



请求动态资源





百度一下



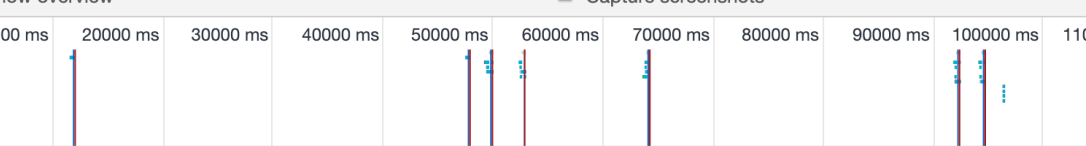
下载百度APP

有事搜一搜 没事看一看

Network

Filter ☒ Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other

☐ Use large request rows ☒ Group by frame
☒ Show overview ☐ Capture screenshots



Name	Status	Type	Initiator	Size	Time	Waterfall
www.baidu.com	200	doc...	Other	41.4 KB	94 ms	[Bar]
bd_logo1.png	200	png	(index)	8.0 KB	46 ms	[Bar]
bd_logo1.png?qua=high	200	png	(index)	8.0 KB	37 ms	[Bar]
baidu_jgylogo3.gif	200	gif	(index)	1016 B	46 ms	[Bar]
baidu_resultlogo@2.png	200	png	(index)	6.7 KB	46 ms	[Bar]
jquery-1.10.2.min_65682a2.js	200	script	(index)	32.7 KB	71 ms	[Bar]
zbios_x2_5869f49.png	200	png	(index)	24.4 KB	62 ms	[Bar]
icons_441e82f.png	200	png	(index)	17.4 KB	39 ms	[Bar]
all_async_search_99b3fbf.js	200	script	(index);720	86.5 KB	74 ms	[Bar]
every_cookie_mac_82990d4.js	(blocked...)	script	jquery-1.10.2...	0 B	3 ms	[Bar]
nu_instant_search_baaa58d.js	200	script	jquery-1.10.2...	5.8 KB	11 ms	[Bar]
quickdelete_33e3eb8.png	200	png	jquery-1.10.2...	1.3 KB	9 ms	[Bar]
swfobject_0178953.js	200	script	all_async se...	4.0 KB	12 ms	[Bar]
tu_77547af.js	200	script	all_async se...	5.8 KB	12 ms	[Bar]
voice_1672ed3.js	200	script	all_async se...	14.5 KB	19 ms	[Bar]
search-sug_d37baf2.js	200	script	all_async se...	11.3 KB	24 ms	[Bar]
soutu.css	200	styl...	jquery-1.10.2...	2.4 KB	9 ms	[Bar]
sugrec?prod=pc_his&from=pc_web&json=1&si...	200	xhr	jquery-1.10.2...	789 B	67 ms	[Bar]
camera_new_x2_fb6c085.png	200	png	jquery-1.10.2...	1.4 KB	12 ms	[Bar]
inject.js	200	script	content.js:65	1.5 KB	19 ms	[Bar]
ps_default.gif?t=1574853398501	200	gif	all_async se...	298 B	88 ms	[Bar]
ps_default.gif?t=1574853398501	200	gif	all_async se...	298 B	76 ms	[Bar]
ps_default.gif?t=1574853398501	200	gif	all_async se...	298 B	76 ms	[Bar]
ps_default.gif?t=1574853398501	200	gif	all_async se...	298 B	76 ms	[Bar]

24 / 25 requests | 276 KB / 276 KB transferred | 727 KB / 727 KB resources | Finish: 2.29 s | DOMContentLoaded: 406 ms | Load:

HTML (HyperText Markup Language 超文本标记语言)

```
<html>
  <head>
    <title></title>
  </head>
  <body>
  </body>
</html>
```

HTML 标签是由尖括号包围的关键词

HTML 标签通常是成对出现的

标签对中的第一个标签是开始标签，第二个标签是结束标签

标签通过嵌套、并列，形成父子、兄弟等关系

HTML (HyperText Markup Language 超文本标记语言)

```
<html>
  <head>
    <title>Hello World!</title>
  </head>
  <body>
    <h1>这是一号标题</h1>
    <h2>这是二号标题</h2>
    <h3>这是三号标题</h3>
    <p>这是一个段落</p>
    <!--
    这是个注释
    它下面是个二次元妹子的图片
    -->
    
    <!-- 换行 -->
    <br />
    这是个输入框
    <input name="输入框" type="text" />
    <button>这是个按钮</button>
  </body>
</html>
```

标签拥有属性，用来描述标签的一些额外信息

自闭和标签：如

CSS (Cascading Style Sheets 层叠样式表)

```
<link rel="stylesheet" href="index.css"/>
```

```
<style>
  body{
    text-align: center;
  }
  p{
    color: red;
  }
</style>
```

JavaScript

```
> window.outerWidth
```

```
< 1280
```

页面外部宽度

```
> window.outerHeight
```

```
< 680
```

页面外部高度

```
> window.location.href
```

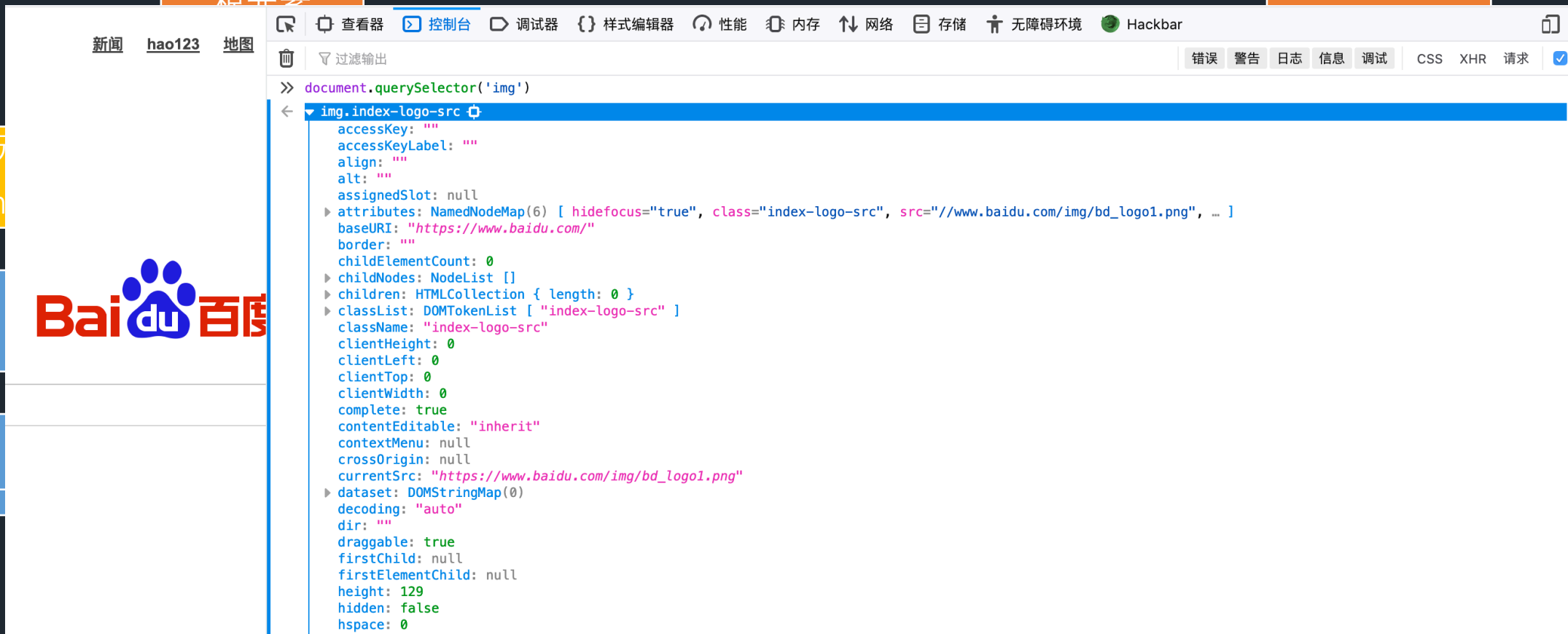
```
< "https://www.google.com/_/chrome/newtab?ie=UTF-8" 当前页面URL
```



VIDAR TEAM

JavaScript

相元素



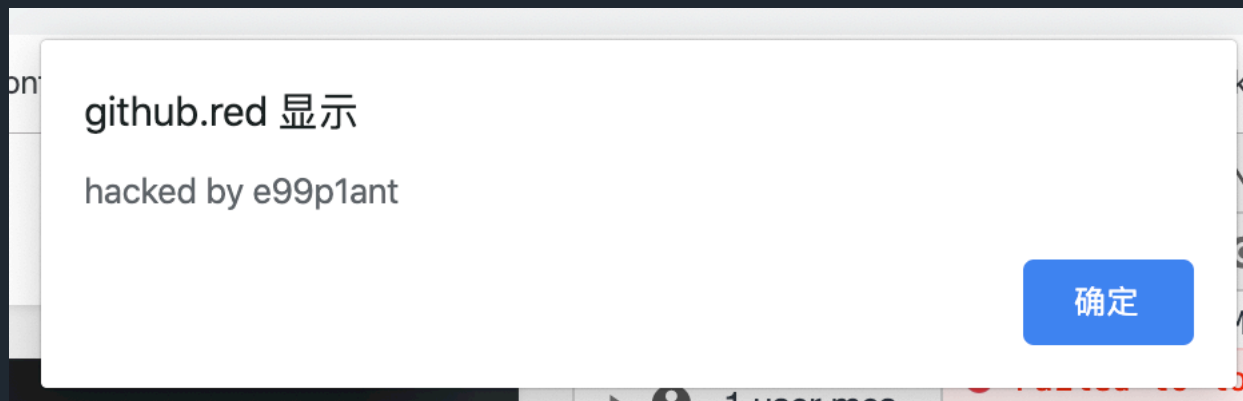
HTML -> DOM 树

JavaScript

```
<script>  
    // 内联 JS  
    console.log( 'e99p1ant' );  
</script>  
  
<script src="app.js"></script>
```

前端可能会出现哪些安全问题呢？

- 请求DNS服务器，查询域名对应的 IP
- 向服务器发送请求，接收服务器返回的数据
- 对返回的 HTML CSS JavaScript 进行加载和渲染



执行任意 JavaScript 代码：

窃取个人信息
盗取账号
伪造请求

...



XSS

Cross Site Scripting

跨站脚本攻击



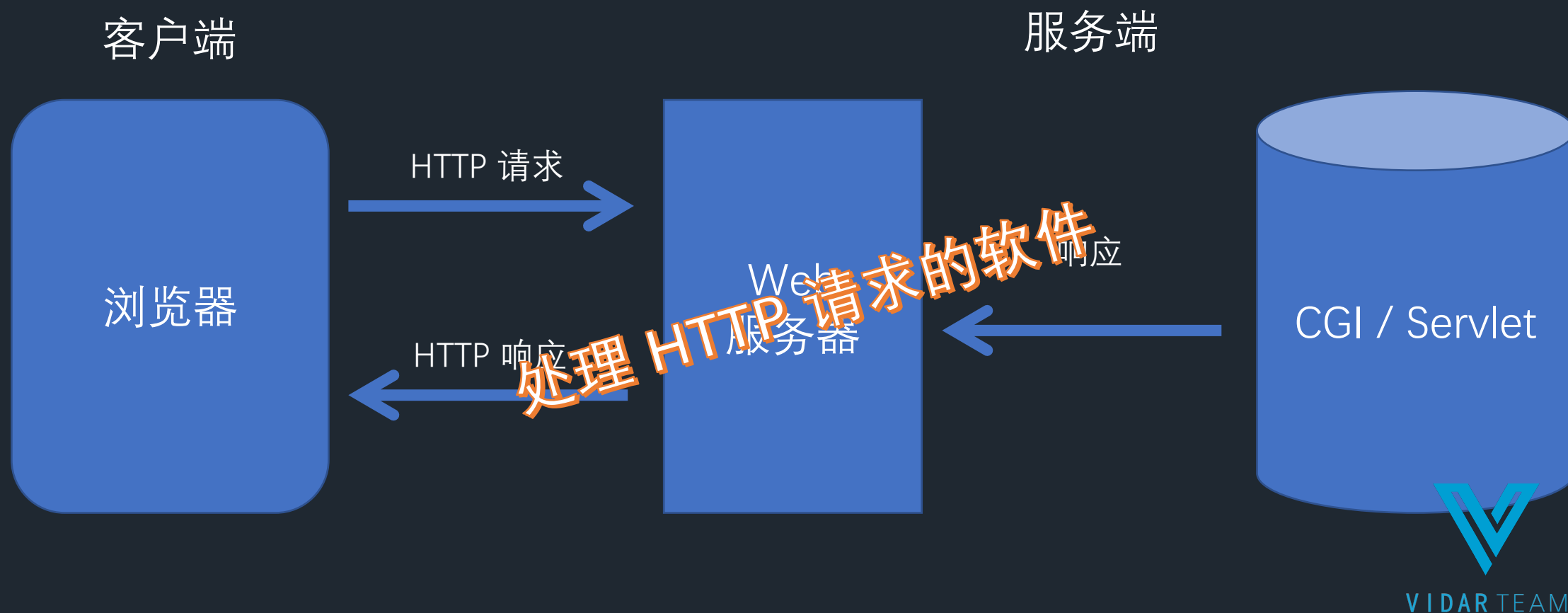
VIDAR TEAM

DEMO



VIDAR TEAM

后端呢……



Nginx、Apache (支持多平台)

IIS (Windows)

Tomcat (支持多平台, 一般用于Java Web项目)

5.配置Apache使其支持PHP

这篇笔记写的时间比较长了，不记得当时需不需要在Apache中配置组件支持PHP，如果你访问网站内的.php文件返回源码或下载文件，那么就需要配置组件。

需要在httpd.conf中添加以下代码，修改后重启Apache服务

```
LoadModule php5_module modules/libphp5.so
```

```
AddType application/x-httpd-php .php
```

```
AddType application/x-httpd-php-source .phps
```

如果我们能上传一个 .php 文件到服务器上？

a.jpg.xxx -> a.jpg.xxx

a.php.xxx -> a.php.xxx

文件解析漏洞

PHP – FastCGI

Python – uWSGI

CGI (电子工程术语)

 编辑

 本词条缺少名片图，补充相关内容使词条更完整，还能快速升级，赶紧来编辑吧！

 本词条由“科普中国”百科科学词条编写与应用工作项目 审核。

通用网关接口（**Common Gateway Interface/CGI**）是一种重要的互联网技术，可以让一个客户端，从网页浏览器向执行在网络服务器上的程序请求数据。**CGI描述了服务器和请求处理程序之间传输数据的一种标准。**

CGI / Servlet

SQL 注入

远程命令执行(RCE)

反序列化

跨站脚本攻击(XSS)

程序员为什么会被祭天??

未授权访问

弱口令

文件包含

目录遍历



讲一个大茄子🍆上网的小故事



VIDAR TEAM



访问某女装网站

请登录

e99p1ant

.....

登录

大茄子登录了自己的账号

来发布你的女装吧~

上传你的女装照!

选择文件 女装.JPG

上传

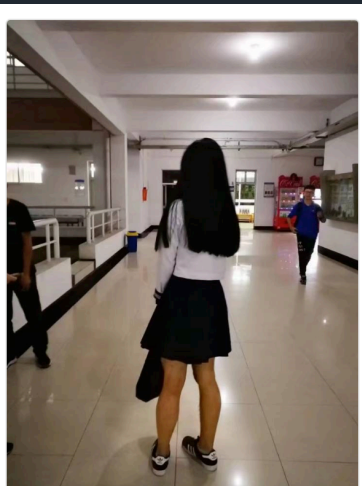
大茄子上传自己的女装照

C老板：好黑啊

摩尔桑：这根茄子他不

Y：还没我女装一半好看~

大茄子看了下大家的评论



删除

大茄子删除了照片



那python需要学到什么程度呢 还有就是这些学习的过程有没有什么检验自己的方法之类的

HTML CSS 基础 <https://www.w3cschool.cn/>

JS 基础：《JavaScript DOM编程基础》

JS 进阶：《JavaScript 语言精粹》

JS ES6语法特性: <https://github.com/bpesquet/thejsway>


PHP: 《PHP和MySQL Web开发》

<http://www.php.net> （正确食用方式：看完内容后，下面的评论也看一遍）

Python: 《Python从入门到实践》的入门部分

SQL、正则表达式 等等 资源非常多，自己找就好，最主要的是自己多用才能熟练。（不能手写SQL、正则表达式的都不是合格的Web狗）



A construction crane is silhouetted against a vibrant sunset sky filled with orange and yellow clouds. The crane's lattice structure and jib are prominent, extending from the bottom left towards the top right. The Chinese text is centered over the crane's jib.

万丈高楼平地起
勿以浮沙筑高台



VIDAR TEAM