CTF-比赛培训基础

原创

amingMM 于 2021-08-05 18:41:32 发布 151 收藏

https://www.bilibili.com/video/BV18Z4y1N7Ts?p=1

中国人民银行 THE PEOPLE'S BANK OF CHINA 金融业网络安全攻防比赛培训视频

1 CTF 介绍

目录
CONTENTS

CTF概览—概念

CTF（Capture The Flag）中文一般译作夺旗赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。

CTF概览—起源

CTF起源于1996年DEFCON全球黑客大会，以代替之前黑客们通过互相发起真实攻击进行技术比拼的方式。发展至今，已经成为全球范围网络安全圈流行的竞赛形式，2013年全球举办了超过五十场国际性CTF赛事。而DEFCON作为CTF赛制的发源地，DEFCON CTF也成为了目前全球最高技术水平和影响力的CTF竞赛，类似于CTF赛场中的“世界杯” 。

CTF竞赛模式

CTF竞赛流程

参赛团队之间通过进行攻防对抗、程序分析等形式，率先从主办方给出的比赛环境中得到一串具有一定格式的字符串或其他内容，并将其提交给主办方，从而夺得分数。为了方便称呼，我们把这样的内容称之为“Flag”。

单兵作战

理论、杂项、web、pwn、逆向等各种题目

综合靶场

团队形式，攻击相同环境的靶机
主要是web题型
只需攻击不用防御 针对同一个环境，越早拿到flag，获取的分数越高 一台靶机通常会有多个flag flag通常放在web根目录、桌面、C盘根目录、 C:\windows\system32、/、/tmp/、/home等

混战模式

参赛团队既是攻击者也是防御者
通常团队通过ssh管理靶机、只有web权限 flag每隔几分钟一轮，各队有自己的初始分数，flag被其他队拿到会被扣分，拿到其他 队的flag会加分 主办方会队每个队伍的服务进行check，check不过会被扣分，扣除的分数由服务check 正常的队伍均分。

CTF知识点

- Web
  - sql注入、xss、文件上传、包含漏洞、xxe、ssrf、命令执行、代码审计等等
- 破解题（Pwn）
  - 攻击远程服务器的服务
  - 会提供服务程序的二进制文件
  - 分析漏洞并写出exp
  - 栈溢出、堆溢出
  - 绕过保护机制（ASLR,NX等）
- 逆向（Reverse）
  - 逆向，破解程序的算法来得到程序中的flag
  - 对抗反调试、代码混淆等等
- 移动安全（Mobile）
  - 主要考察选手对安卓和ios系统的理解
- 杂项（Misc）

CTF知识点—杂项

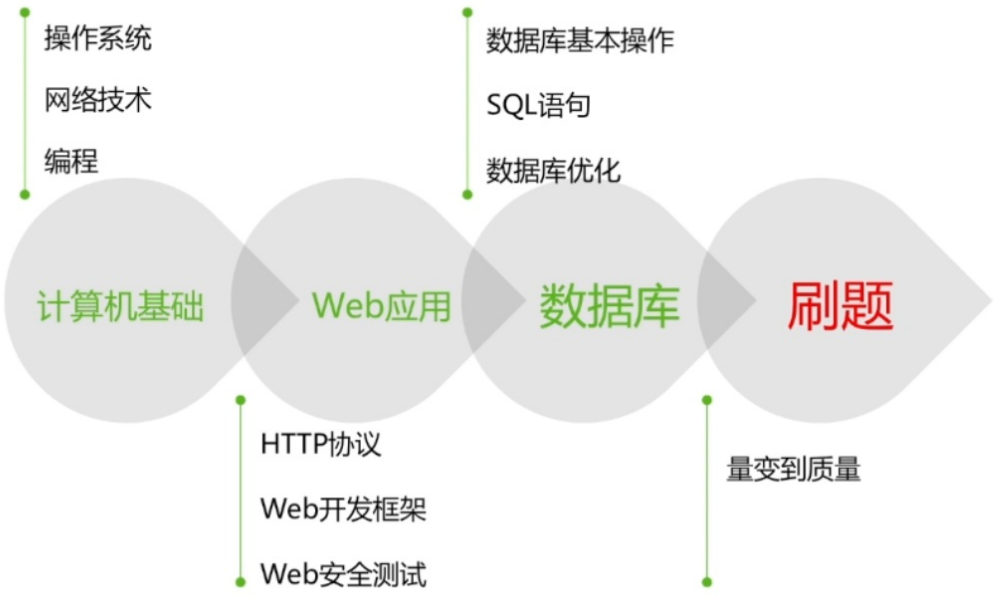
- 不属于上述类别或组合类别的题目统称为杂项
  - 取证
  - 编解码
  - 加解密
  - 隐写
  - 图片处理
  - 压缩包
  - 编程
  - ...

wireshark
古典密码 现代密码学
图片 视频 音频隐写
photoshop
攻击脚本

CTF学习攻略

Web  逆向

CTF学习攻略



writeup 官方 给的 解题思路

HTTP协议分析

02 HTTP协议结构

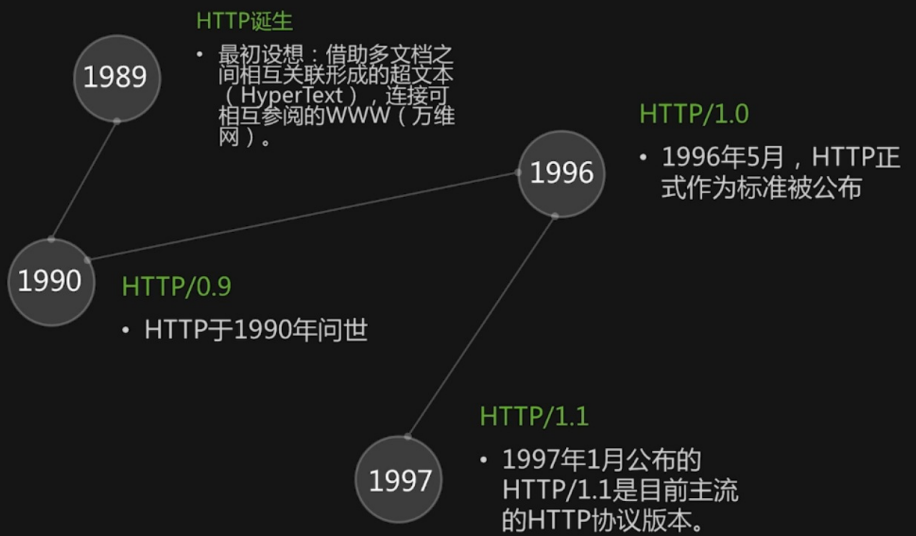
HTTP概念

超文本传输协议（HTTP，HyperText Transfer Protocol)是互联网上应用最为广泛的一种网络协议。所有的WWW文件都必须遵守这个标准。设计HTTP最初的目的是为了提供一种发布和接收HTML页面的方法。

HTTP协议和TCP/IP协议族内的其他众多的协议相同，用于客户端和服务器之间的通信。

web 基于 HTTP 通信

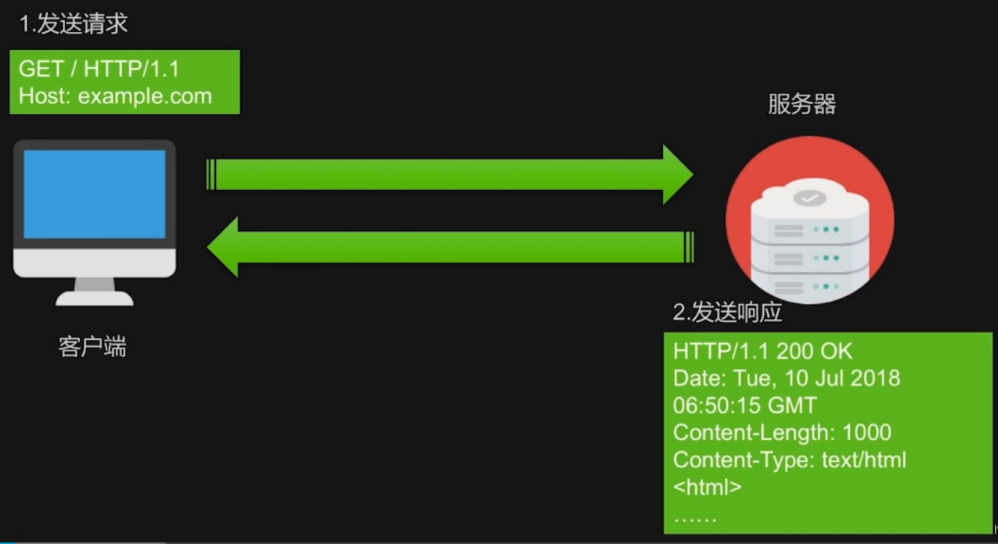
HTTP发展史



02

HTTP协议结构

HTTP通信过程



HTTP报文

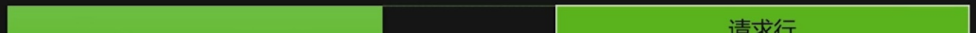
用于HTTP协议交互的信息被称为HTTP报文，请求端的HTTP报文叫做请求报文，响应端的叫做响应报文。HTTP报文是由多行（CR+LF作换行符）数据构成的字符串文本。

【报文首部】
服务器端或客户端需处理的请求或响应的内容及属性

【CR+LF】
CR(Carrige Return，回车符)和 LF(Line Feed，换行符)

【报文主体】
应被发送的数据

请求报文及响应报文的结构



HTTP请求报文

HTTP方法

- GET
  - 请求访问已被URI识别的资源。
- POST
  - 传输实体的主体。
- PUT
  - 传输文件
- HEAD
  - HEAD方法和GET方法一样，只是不返回报文主体部分。用于确认URI的有效性及资源更新的日期时间等。
- DELETE
  - 删除文件
- OPTIONS
  - 查询针对请求URI指定的资源支持的方法。
- TRACE
  - 让Web服务器端将之前的请求通信环回给客户端。

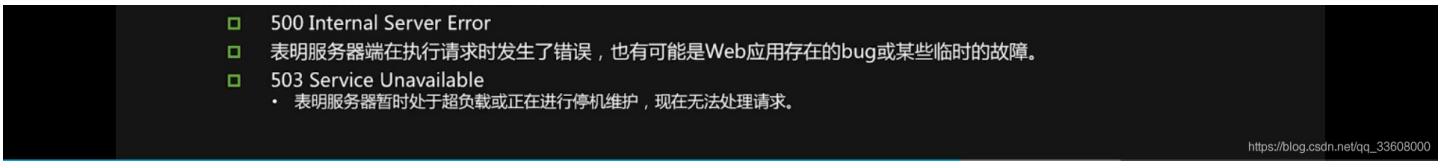
HTTP响应报文

HTTP状态码

- 1XX
  - 信息性状态码，接收的请求正在处理
- 2XX
  - 成功状态码，请求正常处理完毕
- 3XX
  - 重定向状态码，需要进行附加操作以完成请求
- 4XX
  - 客户端错误状态码，服务器无法处理请求
- 5XX
  - 服务器错误状态码，服务器处理请求出错

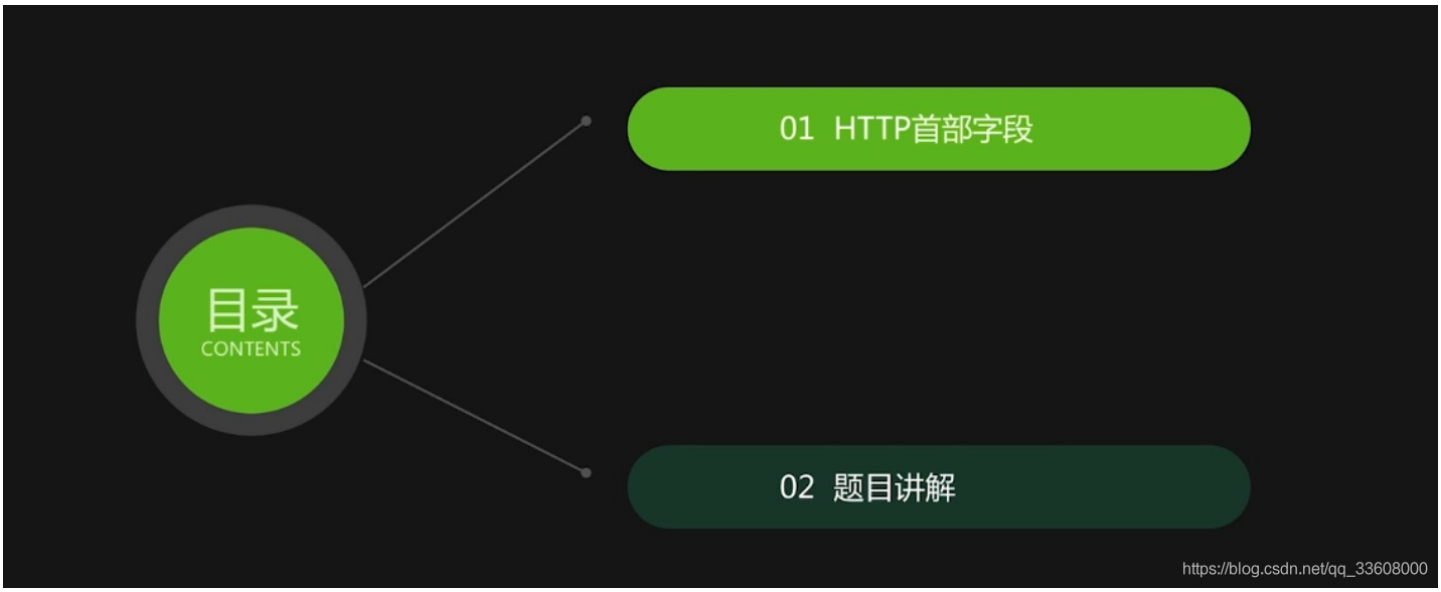
HTTP常见状态码

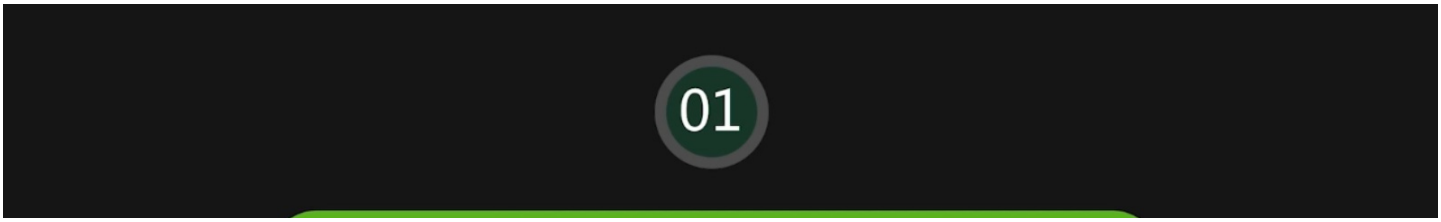
- 200 OK
  - 表示从客户端发来的请求在服务器端被正常处理了。
- 301 MOVED Permanently
  - 永久性重定向，表示请求的资源已被分配了新的URI，以后应使用资源现在所指的URI。
- 302 Found
  - 临时性重定向，表示请求的资源已被分配了新的URI，希望用户（本次）能使用新的URI访问。
- 304 Not Modified
  - 客户端发送附带条件的请求时，服务器端允许请求访问资源，但未满足条件的情况。304状态码返回时，不包含任何响应的主体部分。
- 400 Bad Request
  - 表示请求报文中存在语法错误，当错误发生时，需修改请求的内容后再次发送请求。
- 401 Unauthorized
  - 该状态码表示发送的请求需要有通过HTTP认证（BASIC、DIGEST认证）的认证信息。若之前已进行过1次请求，则表示用户认证失败。
- 403 Forbidden
  - 表明对请求资源的访问被服务器拒绝了。
- 404 Not Found
  - 表明服务器上无法找到请求的资源。

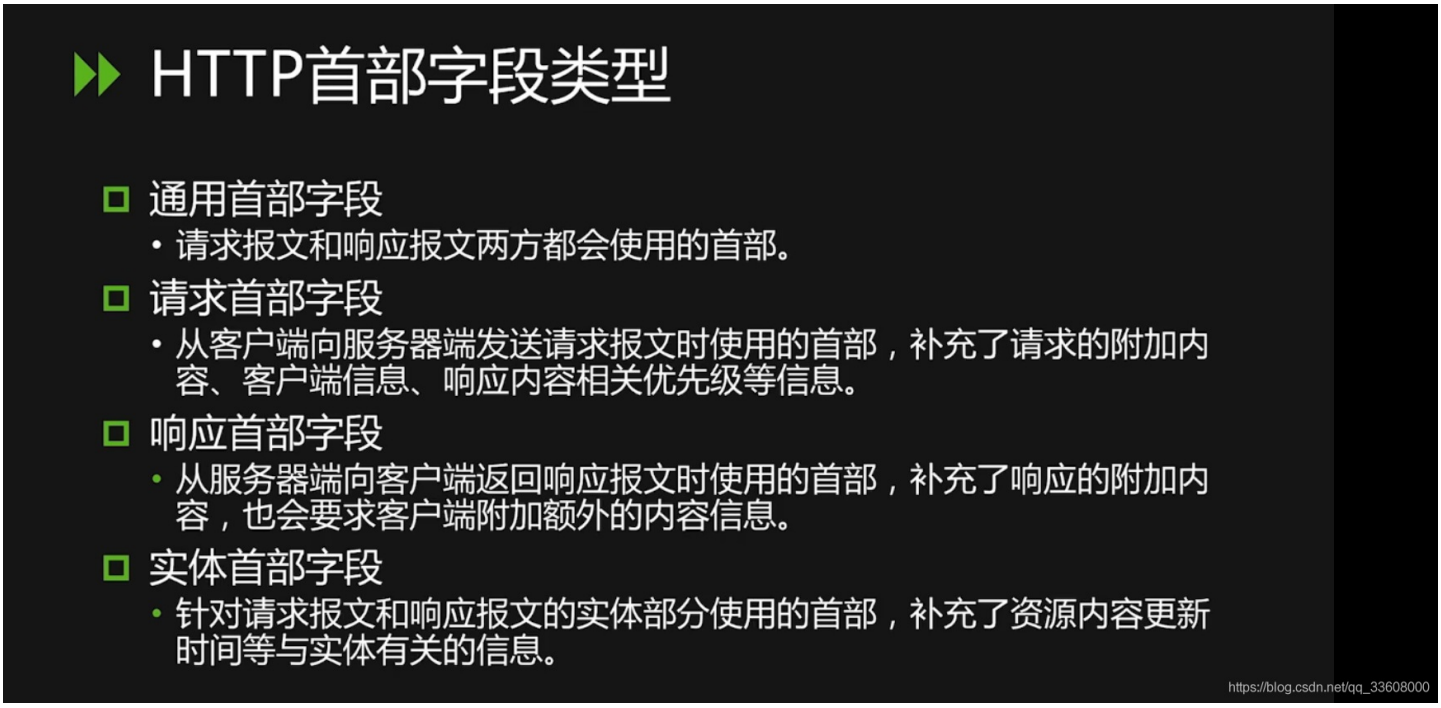


处理大量事务
提高可伸缩性

cookie 可管理状态







QQ 1274510382
Wechat JNZ_aming
商业联盟 QQ群538250800
技术搞事 QQ群599020441
纪年科技aming

网络安全 ,深度学习,嵌入式,机器强化,生物智能,生命科学。

叮叮叮：产品已上线 —>关注 官方-微信公众号——济南纪年信息科技有限公司
民生项目：商城加盟/娱乐交友/创业商圈/外包兼职开发-项目发布/
安全项目：态势感知防御系统/内网巡查系统
云服项目：动态扩容云主机/域名/弹性存储-数据库-云盘/API-Aleverthing
产品咨询/服务售后（同）

纸上得来终觉浅,绝知此事要躬行！！！

寻找志同道合伙伴创业中。。。抱团滴滴aming联系方式！！

#本文为广告系统自动投放广告

 # 如有侵权 删改 请速速联系我们

外包接单 程序代写

QQ群： 678653112

手机淘宝 扫描 淘宝店铺：