WEB 专题课三

文件上传 && 渗透

godspeed 2022-07-08

目录

- 文件上传漏洞—— 40分钟 休息5分钟
- 渗透测试——40分钟 休息5分
- 信息收集 \ 40分钟 休息5分
- 外网打点 /

一、文件上传漏洞的原理

- 程序员在对用户文件上传部分的控制不足或者存在处理缺陷
  - 用户可以越过其本身权限向服务器上上传可执行的动态脚本文件。
  - 这里上传的文件可以是木马，病毒，恶意脚本或者WebShell等。
- 文件上传 本身没有问题，有问题的是文件上传后，服务器怎么处理、解释文件。如果服务器的处理逻辑做的不够安全，则会导致严重的后果。

1.1 webshell

WebShell就是以asp、php、jsp等网页文件形式存在的一种命令执行环境，也可以将其称之为一种网页后门。攻击者在入侵了一个网站后，通常会将这些asp或php后门文件与网站服务器web目录下正常的网页文件混在一起，然后使用浏览器来访问这些后门，得到一个命令执行环境，以达到控制网站服务器的目的（可以上传下载或者修改文件，操作数据库，执行任意命令等）。WebShell后门隐蔽较性高，可以轻松穿越防火墙，访问WebShell时不会留下系统日志，只会在网站的web日志中留下一些数据请求记录

实践：我手上有个webshell

http://150.158.58.29:10007/webshell.php

- webshell能干啥？浏览器演示
- 教大家用python写与webshell进行交互

介绍简单的php函数

- 执行命令
  - system,passthru
  - eval
- 文件读
  - file_get_contents("/etc/passwd")
  - highlight_file
  - show_source
- 文件写
  - file_put_contents

介绍常用的php函数

- 当前目录 && 列目录
  - getcwd
  - scandir
- 编码
  - base64_encode && base64_decode
- 打印
  - var_dump 含长度信息
  - print_r 可读性较高
  - echo 不能打印array

进阶一点的 不做要求

- get_cfg_var('disable_functions')

  > “ Gets the value of a PHP configuration option ”

- get_defined_functions()

  > “ Returns an array of all defined functions ”

- getallheaders()

  > “ Fetch all HTTP request headers ”

php的标签

`<?php phpinfo(); ?>` 一直支持

`<?=phpinfo();` 支持 5.4以上都支持 5.4以下默认不支持

`<? phpinfo(); ?>` 开短标签才支持

`<script language="php">phpinfo();</script>` 7开始不支持

`<% phpinfo(); %>` php5开启asp_tags on才支持 7不支持 asp_tags也被删了

1.2 哪些语言写的网站容易受到危害

- php
- asp
- jsp

相对而言，如下代码写的网站，不太容易受到文件上传的影响

- nodejs
- python
- go

1.3 文件上传校验

- 前端校验——不安全，可被绕过
  - 调用js函数来检查上传文件的扩展名。当用户在客户端选择文件点击上传的时候，客户端还没有向服务器发送任何消息，就对本地文件进行检测来判断是否是可以上传的类型，这种方式称为前台脚本检测扩展名

1.3 文件上传校验

- 后端校验
  - 文件头content-type字段校验（image/gif）
  - 文件内容头校验（GIF89a、\x89PNG、\xFF\xD8\xFF）
  - 后缀名黑名单校验
  - 后缀名白名单校验
  - 自定义正则校验
  - 函数校验

1.3 文件上传校验


文件上传
客户端
JS校验
服务端
检查后缀
白名单
黑名单
.htaccess
apache服务器的配置文件，解析某个后缀为php脚本
.user.ini
不管是什么中间件，以fastcgi运行的php，都受影响
MIME伪造
00截断
古老的nginx
php版本低于5.3，选项GPC为关闭状态时
特殊可解析后缀
需要特定的配置，如php7，php5
::$DATA绕过
windows
中间件解析漏洞
apache、iis
过滤
双写绕过
检查内容
文件头检查
调用函数
getimagesize
exif_imagetype
二次渲染
代码逻辑
条件竞争

1.4 练习题

前端： http://150.158.58.29:10007/ctf1.php
Content-Type: http://150.158.58.29:10007/ctf2.php
支持了额外的后缀： http://150.158.58.29:10007/ctf3.php
单次过滤： http://150.158.58.29:10007/ctf4.php
调用api判断文件类型： http://150.158.58.29:10007/ctf5.php
前面这些上课时实践
条件竞争，留作业,上课演示一下： http://150.158.58.29:10007/ctf6.php

时间如有多：
[文件包含]buuoj练习题1: https://buuoj.cn/challenges#BUU UPLOAD COURSE 1

二、渗透

2.1 学渗透 先学法律 刑法285条

- 违反国家规定，侵入**国家事务、国防建设、尖端科学技术领域**的计算机信息系统的，处三年以下有期徒刑或者拘役。
- 违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段
  - 获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。【刑法修正案七】

2.1 学渗透 先学法律 刑法285条

- 提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。【刑法修正案七】

2.2 渗透案例一

张三15岁，热衷于网络黑客技术，经常在谷歌搜索目标练习武艺，希望小有所成后能够报效祖国，某日张三正常googlehack，无意又找到了一个好下手的目标，于是施展了一套广播体操，注入、种马、提权、漫游内网一气呵成，但进去后张三懵逼了，首先全英文不说，反正都看不懂，但是张三玩过红警，里面有许多类似红警的卫星图片，此时张三才知道他进入了A国军事服务器，当时出于害怕，观摩了一会便离开下线了。

2.3 案件分析

- 通过googlehack这样的查询语句，可以简单发现网站存在的漏洞，这样的行为，可以定性为犯罪预备，即为犯罪准备工具、制造条件的行为。
- 依照我国刑法规定，对于预备犯，可以比照既遂犯从轻、减轻处罚或者免除处罚。在实务中，如果不是案发后对本机做取证工作，单纯googlehack行为很难被发现，如果没有后续的违法动作，仅针对此行为一般也不予处罚。

2.3 案件分析

关于SQL注入和上传ASP这样的行为，可以认定为非法侵入计算机信息系统的手段，对于主观上是出于好奇、逞能、报复等都不影响对该罪的法律定性。但是本罪侵犯的客体是国家重要领域和要害部门的计算机信息系统安全，本案中，张三入侵的可能是军事，是否属于犯罪客体应当由省级以上负责计算机信息系统安全保护管理工作的部门检验确认（对此很多办案机关也存在主观臆断），如果是则可以被认定为非法侵入计算机信息系统罪，依照刑法第二百八十五条违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

2.3 案件分析

- 对于侵入后在内网浏览服务器的数据库或源码等内容，这样的行为在法律上可以证实张三非法侵入行为的**既遂**，可以依照计算机信息系统内容的重要程度和张三浏览的具体情况来判断最终的量刑。
- 很多时候，行为人使用各种武艺，都不能渗透成功，这样的行为如何定性呢，首先法律规定本罪为行为犯，即只要实施这样的行为即可构成犯罪，但是因为武艺不够或者其它客观因素，不能侵入成功，则应当构成未遂，对于未遂犯，可以比照既遂犯从轻或者减轻处罚。这里要提醒大家的是，没有可以免除处罚这么一法律规定。

2.3 案件分析

- 最后，张三案发时只有15周岁，只对刑法规定的强奸、故意杀人等八类案件负刑事责任，所以张三未达到本案中应负刑事责任的年龄，因此张三完全不用担心被查水表。
- 延伸一下，如果张三入侵的是其它计算机信息系统，比如某公司，且仅有入侵行为，则不能构成本罪。是否构成犯罪或者构成其它犯罪，应当分析张三入侵后的行为或结果。

2.4 什么是渗透?

以安全为基本原则，通过攻击者以及防御者的角度去分析目标所存在的安全隐患以及脆弱性，以保护系统安全为最终目标。

2.5 有合法的渗透吗?

- 护网行动
  - 公安部牵头、用以评估企事业单位的网络安全的活动
  - 公安部会组织攻防两方，进攻方会在一周～一月内对防守方发动网络攻击，检测出防守方（企事业单位）存在的安全漏洞。通过与进攻方的对抗，企事业单位网络、系统以及设备等的安全能力会大大提高。
  - "护网行动"是国家应对网络安全问题所做的重要布局之一。"护网行动"从2016年开始，随着我国对网络安全的重视，涉及单位不断扩大，越来越多的单位都加入到护网行动中，网络安全对抗演练越来越贴近实际情况。

2.5 有合法的渗透吗?

护网一般按照行政级别分为国家级护网、省级护网、市级护网；除此之外，还有一些行业对于网络安全的要求比较高，因此也会在行业内部展开护网行动，比如金融行业。

2.5 有合法的渗透吗?

- SRC（各个公司的应急响应中心）
  - 白帽子在指定范围的网站里挖掘漏洞
  - 提交至SRC评级，一般可分为无影响、低危、中危、高危、严重等级别
  - SRC提交至内部修复
  - 给予白帽子赏金
- 原则：
  - 不破坏、点到为止
- hackerone

2.5 有合法的渗透吗?

在企业中，一般要拿到对方的授权书，才可以开始渗透，一般会包括如下内容：

- 时间
- 范围
- 参与人员
- 规则

三、渗透的流程

- 确定目标
- 信息收集
- 漏洞探测
- 漏洞利用
- 内网转发
- 内网渗透
- 痕迹清除
- 撰写渗透测试报告

文本

考虑到内容敏感性，故删去部分内容 :)

基础作业

zjusec.com

- War of tomcat 【外网打点，自学完成——tomcat部署war包】 20分
- php include 自学完成——php文件包含 [20分]
- 大乌龟找妈妈 30分
- 上课讲的条件竞争 burp截一下图就行[30分]
  写一下思路即可，做过的再做一遍

挑战作业：

- [.htaccess && php的奇怪标签] https://buuoj.cn/challenges#[GXYCTF2019]BabyUpload

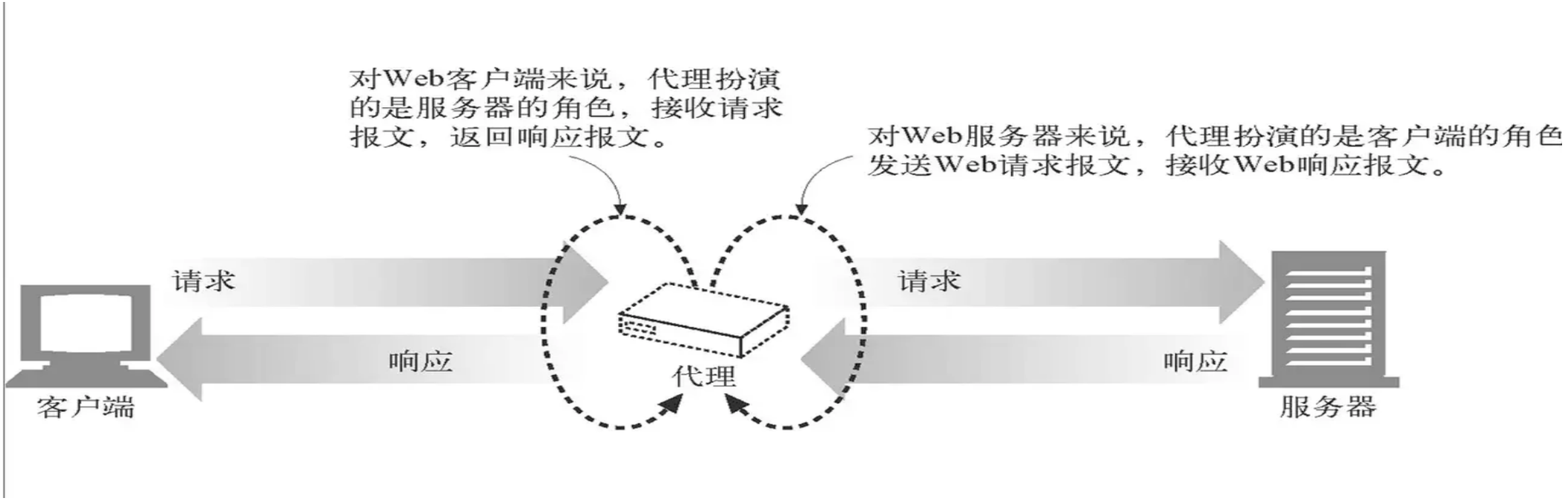
后面内容课上不讲 有兴趣自己看看

题外话：代理的类型

- http代理
- https代理
- SOCKS代理
  - socks4 支持tcp
  - socks4a 比4多一点点功能
  - socks5 支持tcp和udp

题外话：代理的类型——HTTP代理

(一)普通代理



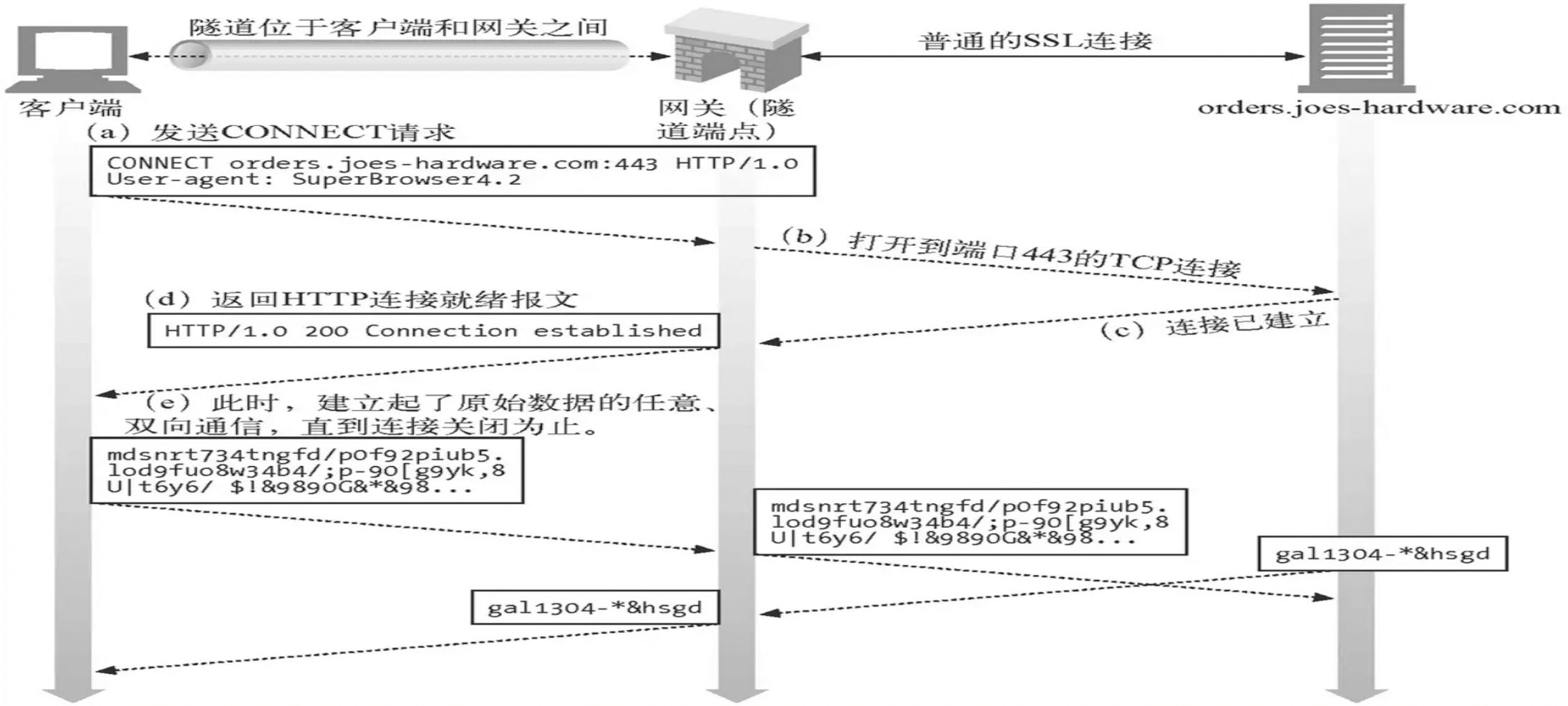
——HTTP 权威指南

题外话：代理的类型——HTTP代理

(二)隧道代理

HTTP 客户端通过 CONNECT 方法请求隧道代理创建一条到达任意目的服务器和端口的 TCP 连接，并对客户端和服务器之间的后继数据进行盲转发。

题外话：代理的类型——HTTP代理——(二)隧道代理



题外话：HTTP代理——小结

普通代理例子：

> 假如你现在要和某一个客户约个会议，于是跟秘书说:"打电话给XX客户，下午17:00约个会议"。
> 于是秘书拿起电话打过去，跟XX客户说："下午17:00约个会议"。
> 然后XX客户回答说："OK"。
> 这时秘书挂了电话，然后跟你说："OK"。

题外话：HTTP代理——小结

隧道代理例子：
假如你现在要和某一个客户约个会议，于是跟秘书说："打电话给XX客户"。——发起CONNECT请求
于是秘书拿起电话打过去，接通之后，把电话给你。——建立隧道完毕
你跟XX客户说："下午17:00约个会议"。——通信
然后XX客户回答说："OK"。——通信
然后XX客户挂了电话后，秘书也从你手上拿走了电话挂掉。——关闭隧道