

建站之星(sitestar)后台两处上传漏洞

南部漂泊

采集关键词: `inurl:index.php?_m=frontpage`

前言:

(2017-6-8)看了 t00ls 的 zip 包含更多的 php 文件, 来上传 getshell 的漏洞, 测试失败, 有点生气啊, 就自己研究了一下 cms, 所以有了下面的 0day, 挖掘到了任意文件。

漏洞描述:

建站之星(sitestar)后台两处上传漏洞:

1】 banner 滚动条编辑-单图片-content-type 造成任意文件上传、

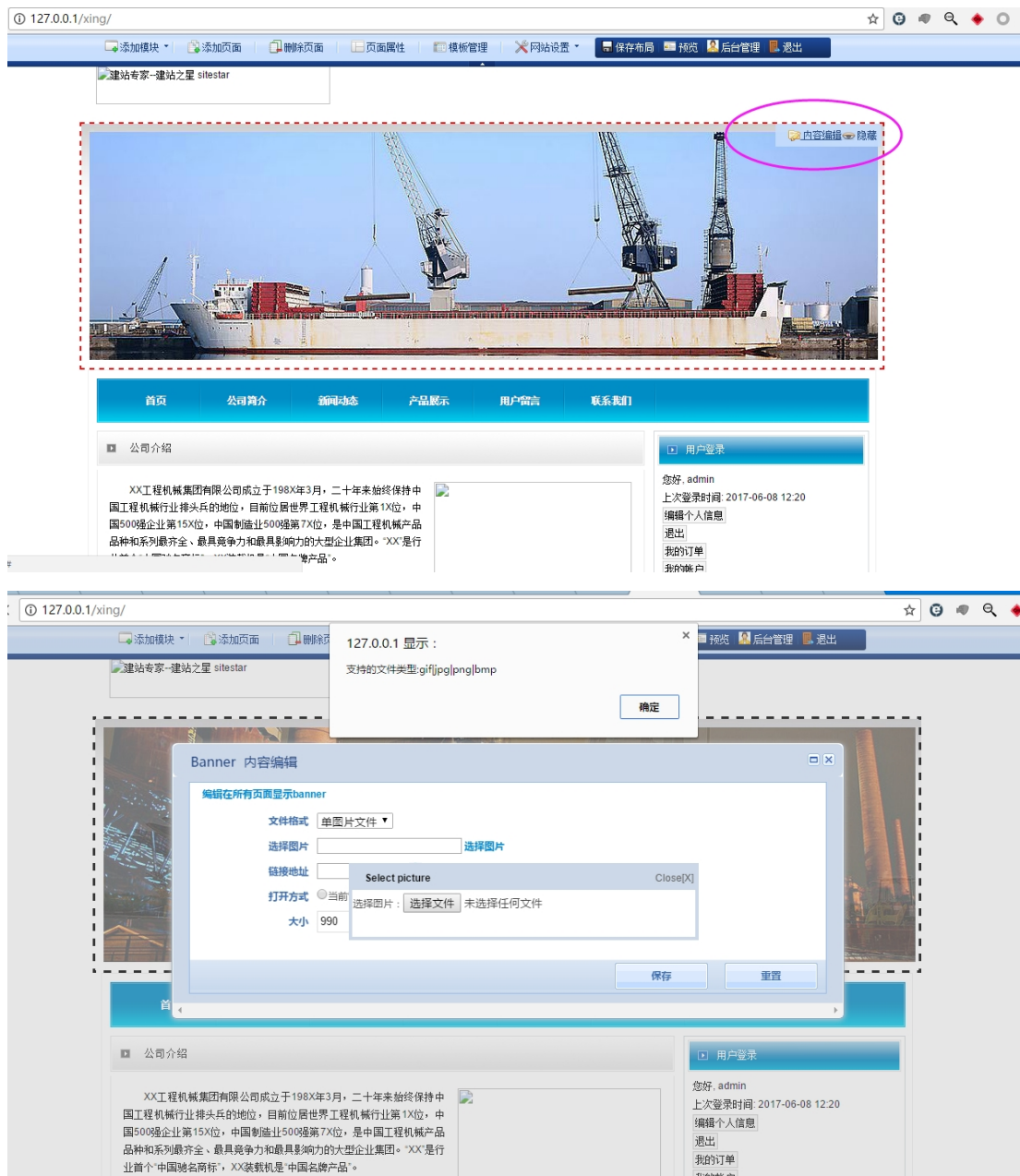
2】 后台的产品管理-编辑更多图片-上传可突破

`inurl:index.php?_m=frontpage`

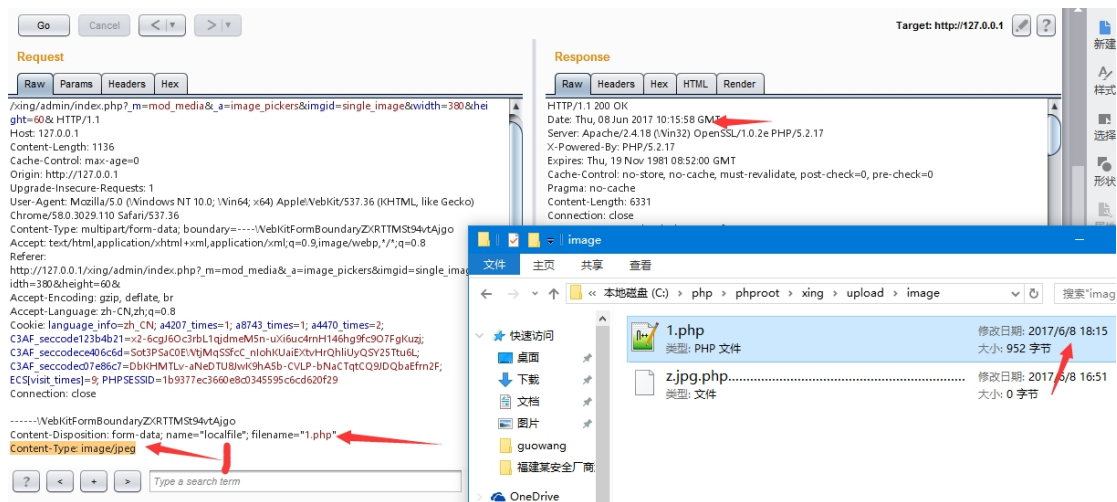
漏洞详情:

1】 banner 滚动条编辑-单图片任意文件上传、

管理员对前台的 banner 滚动条编辑-选择单图片上传, 直接上传 php 会提示不允许上传, **burp 抓包, 修改报文中的 Content-Type 为: Content-Type: image/jpeg, 造成任意文件上传**



直接开启 burp 抓包，修改如下：



2】后台的产品管理上传可突破

后台选择-产品管理，选择一个产品更改：



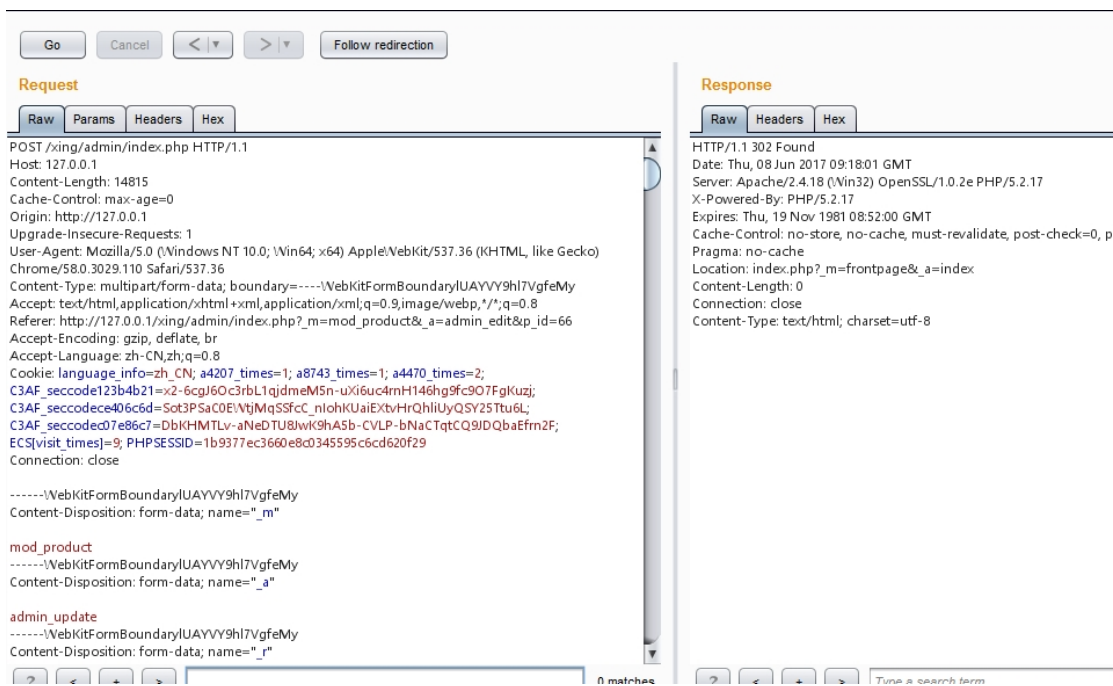
打开了其中的一个产品：



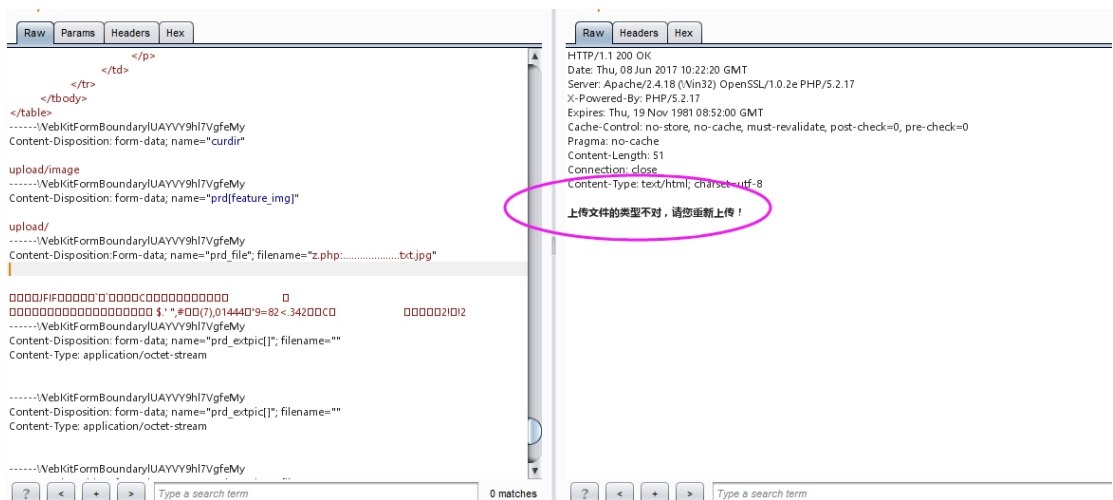
往下拉，选择更多图片：



选择一个本地图片，然后保存-同时抓包：

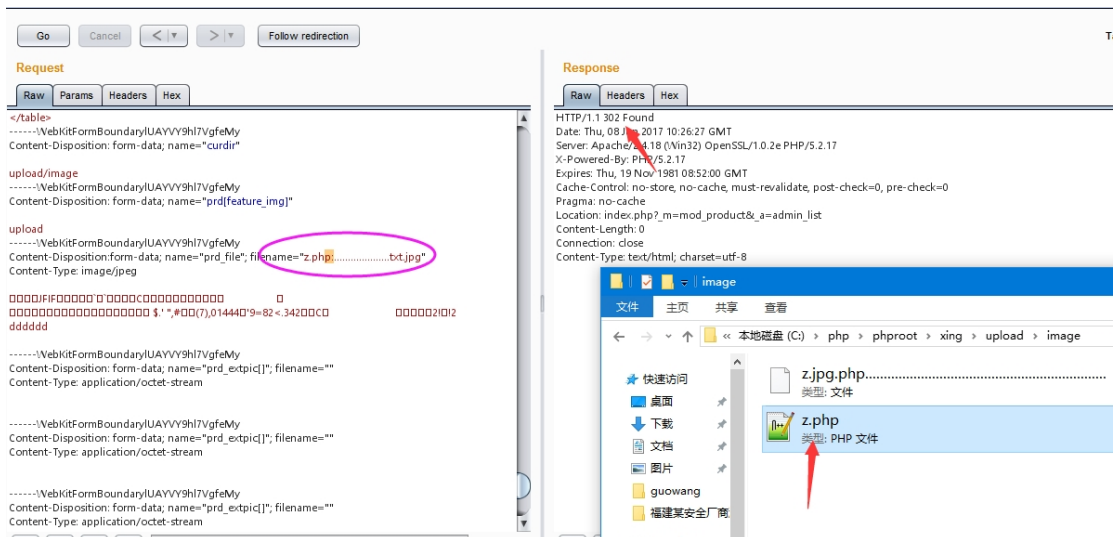


同样开始修改数据包，保持 Content-Type 为：Content-Type: image/jpeg，这是前提条件，这时候，若是删除 Content-Type 会显示如下，文件类型有误：

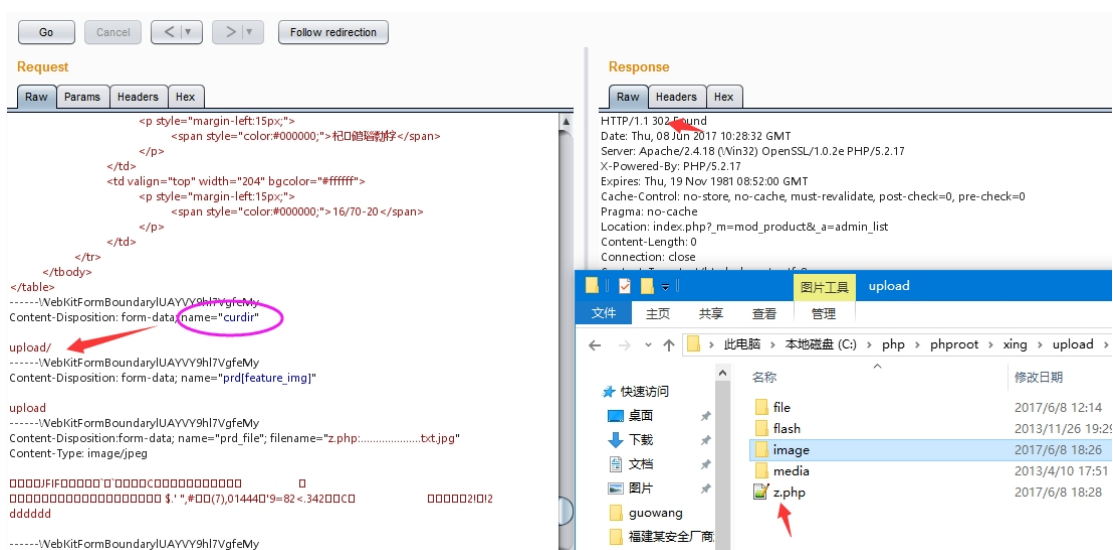


所以保持 content-type:，直接突破：

修改文件名为：2.php:.....jpg，注意冒号的位置，会生成不同的文件的，绕过：



同样这里产生了一个跨目录漏洞，本来我互联网找了一个站点测试的，当时 image 不解析，所以就尝试找跨目录漏洞，然后就诞生了。



如下，互联网测试的站点，getshell:

← → ↻

www. .com/upload/xxxx.php?

6

/home/ /wwwroot/

本地硬盘

网站根目录

本程序目录

信息操作

上传文件

基本信息

系统信息

执行PHP脚本

授权工具

执行SQL执行

MYSQL操作

MYSQL提权

Serv-U提权

执行命令

反弹提权

文件下载

端口扫描

批量操作




















批量挂马清马

批量替换内容

批量搜索文件

地址: /root 转到

新建文件 新建目录 文件 未选择任何文件 上传

上级目录	操作	文件属性
 include	改名 删除 打包	0700
 model	改名 删除 打包	0700
 template	改名 删除 打包	0700
 upload	改名 删除 打包	0700
 data	改名 删除 打包	0700
 script	改名 删除 打包	0700
 naviga	改名 删除 打包	0700
 m-ter	改名 删除 打包	0700
 insta	改名 删除 打包	0700
 local	改名 删除 打包	0700
 sql	改名 删除 打包	0700
 mo	改名 删除 打包	0700
 cad	改名 删除 打包	0700
 adn	改名 删除 打包	0700
 view	改名 删除 打包	0700
 libr	改名 删除 打包	0700
 flite	改名 删除 打包	0700
 onlinepay	改名 删除 打包	0700
 i	改名 删除 打包	0700