Day24　WEB漏洞–文件上传之WAF绕过及安全修复

24.1 上传参数名解析

明确哪些东西能修改?

- Content-Disposition:一般可更改
- name:表单参数值,不能更改
- filename:文件名,可以更改
- Content-Type:文件MIME，视情况更改

24.2 常见绕过方法

1. 数据溢出-防匹配(xxx...)　:就是在关键点前面写入大量的无用数据来干扰对后面主要数据的检测
2. 符号变异-防匹配('　"；)：有的检测可能是基于单引号和双引号来获取数据，可以修改单引号或双引号的位置或增加删除单双引号来干扰waf
3. 数据截断-防匹配(%00;　换行)：
4. 重复数据-防匹配(参数多次)

```
#Payload :
大量垃圾数据缓冲溢出(Ccontent-Disposition,filename等)

#单引号、双引号、分号
filename=x.php
filename="x.php
```

```
filename='x.php
filename="a.jpg;.php";

# %00、换行
filename="a.php%00.jpg"
filename="Content-Disposition : form-data;name="upload_file" ; x.php"
filename="x.jpg" ; filename="x.jpg" ; . . . ..filename="x.php";
filename=
"
x
.
p
h
p
"
;

```

借助白名单，在filename内写入前面的一些数据，最后再写入x.php，程序判定filename时发现有前面的数据就放行，遇到x.php后发现没有变量接收，然后放弃检测，但最后x.php上传给了filename

24.3 文件上传安全修复方案

```
后端验证:采用服务端验证模式后缀检测:
基于黑名单，白名单过滤MIME检测:
基于上传自带类型检测
内容检测:文件头，完整性检测

自带函数过滤:参考uploadlabs函数
自定义函数过滤:function check_file(){ }
WAF防护产品:宝塔,云盾,安全公司产品等
```

语言	可解析后缀
asp/aspx	asp,aspx,asa,asax,ascx,ashx,asmx,cer,aSp,aSpx,aSa,aSax,aScx,aShx,aSmx,cEr
php	php,php5,php4,php3,php2,pHp,pHp5,pHp4,pHp3,pHp2,html,htm,phtml,pht,Html,Htm,pHtml
jsp	jsp,jspa,jspx,jsw,jsv,jspf,jtml,jSp,jSpx,jSpa,jSw,jSv,jSpf,jHtml

- Windows下文件名不区分大小写，Linux下文件名区分大写欧西
- Windows下ADS流特性，导致上传文件xxx.php::$DATA = xxx.php
- Windows下文件名结尾加入`.`,`空格`,`<`,`·>`,`>>>`,`0x81-0xff`等字符，最终生成的文件均被windows忽略。

资源:

```
https://github.com/fuzzdb-project/fuzzdb
https://github.com/TheKingOfDuck/fuzzDicts
```