

IP发现:

```
root@kali ~  
└─ netdiscover -u 192.168.31.0/24  
  
Currently scanning: 192.168.31.0/16 | Screen View: Unique Hosts  
12 Captured ARP Req/Rep packets, from 4 hosts. Total size: 720  


| IP            | At MAC Address    | Count | Len | MAC Vendor / Hostname |
|---------------|-------------------|-------|-----|-----------------------|
| 192.168.128.1 | 00:50:56:c0:00:08 | 9     | 540 | VMware, Inc.          |
| 192.168.2.2   | 00:50:56:ec:67:db | 1     | 60  | VMware, Inc.          |
| 192.168.2.128 | 00:0c:29:cd:0b:2b | 1     | 60  | VMware, Inc.          |
| 192.168.2.254 | 00:50:56:f1:14:bf | 1     | 60  | VMware, Inc.          |


```

端口扫描:

```
root@kali ~  
└─ nmap -A -p- 192.168.2.128  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-21 07:02 CST  
Nmap scan report for 192.168.2.128  
Host is up (0.00040s latency).  
Not shown: 65533 filtered ports  
PORT      STATE SERVICE VERSION  
22/tcp    closed ssh  
80/tcp    open  http   Apache httpd  
|_ http-server-header: Apache  
|_ http-title: SpyderSec | Challenge  
MAC Address: 00:0C:29:CD:0B:2B (VMware)  
Device type: general purpose  
Running: Linux 2.6.X|3.X  
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3  
OS details: Linux 2.6.32 - 3.13  
Network Distance: 1 hop  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 0.40 ms 192.168.2.128  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 157.80 seconds  
root@kali ~
```

只开放了22和80端口。接下来，我在浏览器中打开此页面，访问web网页：



除了两张图片外，页面上没有任何主要内容。这些图像里面可能有隐藏信息，因此，我用exif工具读取图片信息。其中一个以“challenge”命名的图片里面有一些信息

exiftool Challenge.png



仔细观察后，我发现这些数据是十六进制的，需要把它们转换成可读形式

<http://string-functions.com/hex-string.aspx>

Hex to string converter

Enter the hexadecimal text to decode, and then click "Convert!":

35313a35333a34363a35373a36343a35383a33353a37313a36343a34353a36373a36613a34653
a37613a34393a33353a36333a33303a37383a34323a34663a33323a36373a33303a34613a3531
3a33643a3364

Convert!

The decoded string:

51:53:46:57:64:58:35:71:64:45:67:6a:4e:7a:49:35:63:30:78:42:4f:32:67:30:4a:51
:3d:3d?

发现还是十六进制字符串，还需要转换

Hex to string converter

Enter the hexadecimal text to decode, and then click "Convert!":

51534657645835716445676a4e7a4935633078424f3267304a513d3d?

Convert!

The decoded string:

QSFwdX5qdEgjNzI5c0xB02g0JQ==

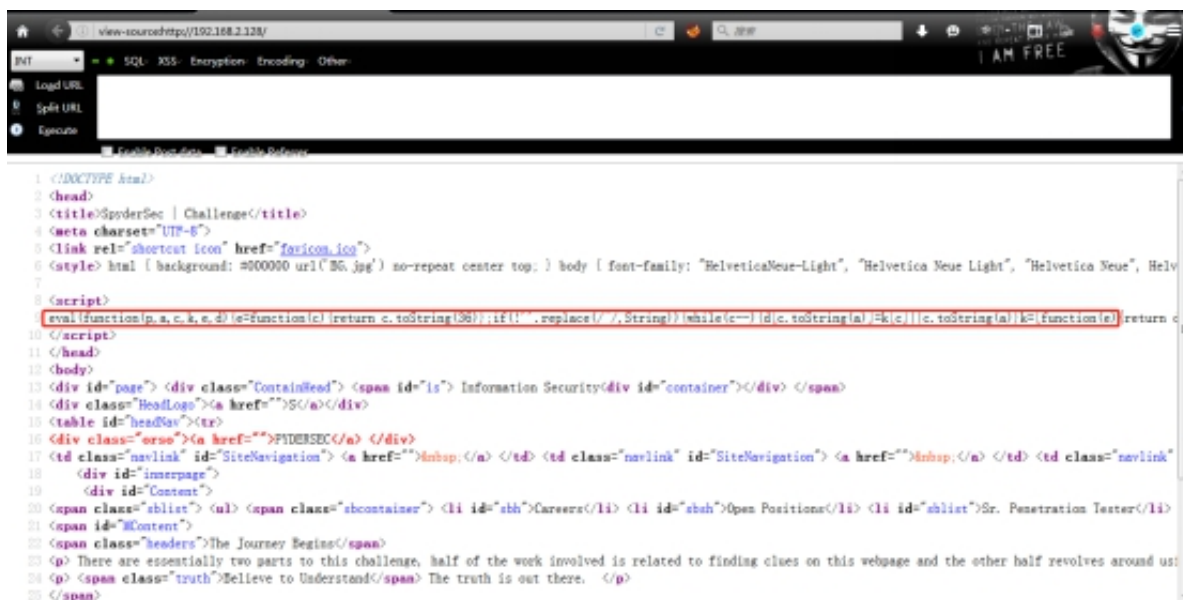
解密后是base64字符串，再次解密：

A!Vu~jtH#729sLA;h4%

```
root@kali ~  
└─> echo QSFwdX5qdEgjNzI5c0xB02g0JQ== | base64 -d  
A!Vu~jtH#729sLA;h4%#  
root@kali ~  
└─> 
```

这个字符串可能是密码或者目录，先记下来，后面可能用得着

现在我们看一下web页面的源代码



居然有eval函数，众所周知这是个危险函数，这段代码肯定有问题，我用javascript解包器解压这段代码

在线解压网站：<http://matthewfl.com/unPacker.html>

```
1 eval(function(p,a,c,k,e,d){e=function(c)
  {return
    c.toString(36)};if(!''.replace(/^/,String))
  {while(c--)
    {d[c.toString(a)]=k[c]||c.toString(a)}k=
    [function(e){return d[e]}};e=function()
    {return '\\w+'};c=1};while(c--){if(k[c])
```

```
{p=p.replace(new
RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}
('7:0:1:2:8:6:3:5:4:0:a:1:2:d:c:b:f:3:9:e',16
,16,'6c|65|72|27|75|6d|28|61|74|29|64|62|66|2
e|3b|69'.split('|'),0,{}))
```



把这些十六进制字符串再次解码:

www.string-functions.com

ONLINE STRING MANIPULATION TOOLS

Hex to string converter

Enter the hexadecimal text to decode, and then click "Convert!":

616c657428276d756c6465722e66626927283b

Convert!

The decoded string:
alert('mulder.fbi');

BRILLIANT

Which beaker fills first?

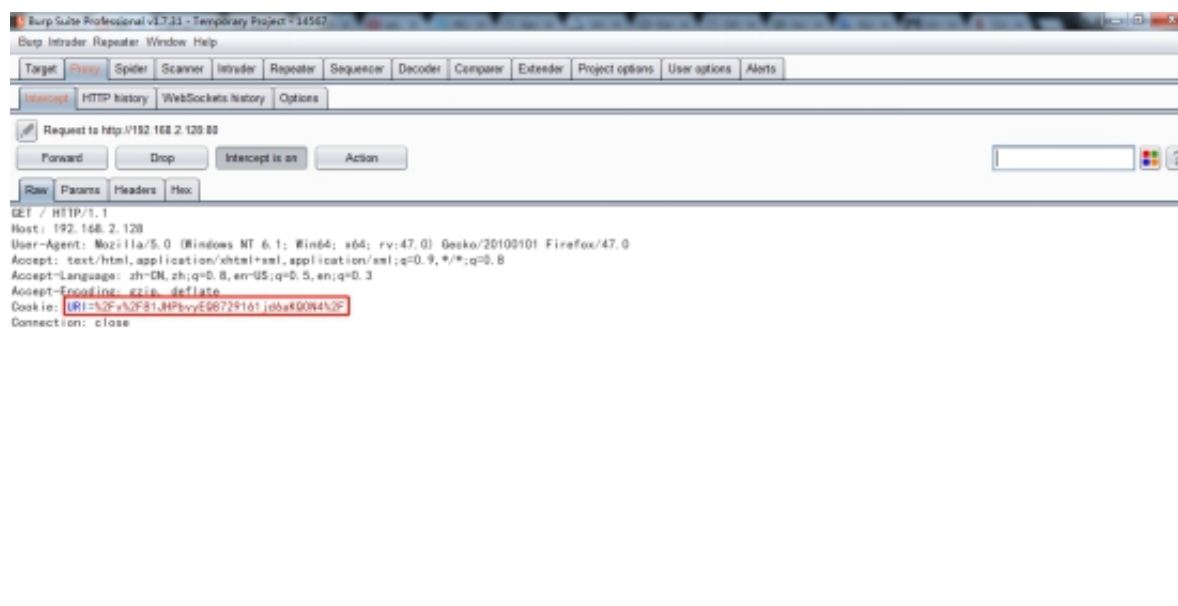


Physics has the answer.

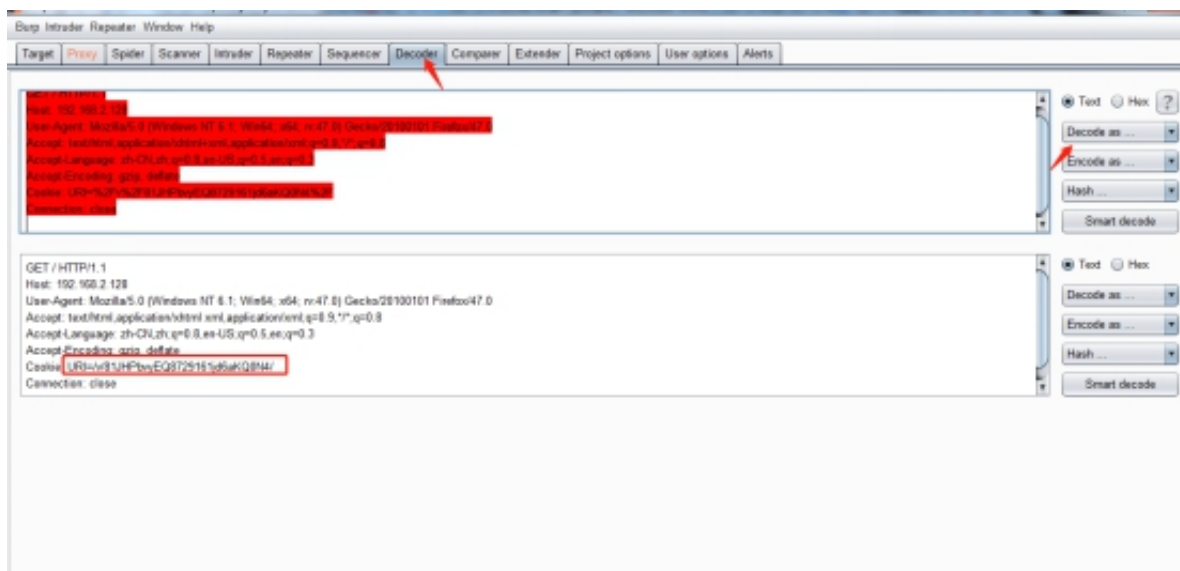
GET STARTED

转换后变成了`alert('mulder.fbi');`;

看到`alert`函数，就是和xss漏洞有关，用了很多方法都没有成功，我决定直接获取cookie，用burpsuit挂上代理获取cookie



Cookie 中发现一个url，后面这些应该是个路径，需要解码，发到decoder中解码：



URI=/v/81JHPbvyEQ8729161jd6aKQ0N4/在浏览器中访问这个路径：



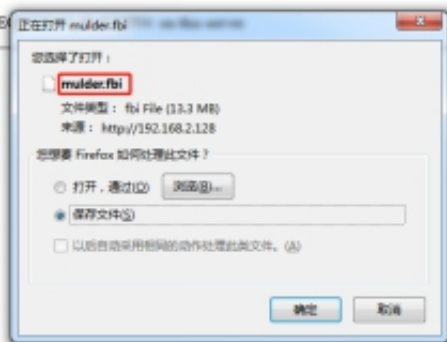
打开是 forbidden，记得之前解码那个：
`alert('mulder.fbi');`
里面的参数或许就是一个路径，访问试试：



Forbidden

You don't have permission to access /v/\$!JHPbvyEQ8729161jdbakQ0NA/mulder.fbi

Apache Server at 192.168.2.128 Port 80

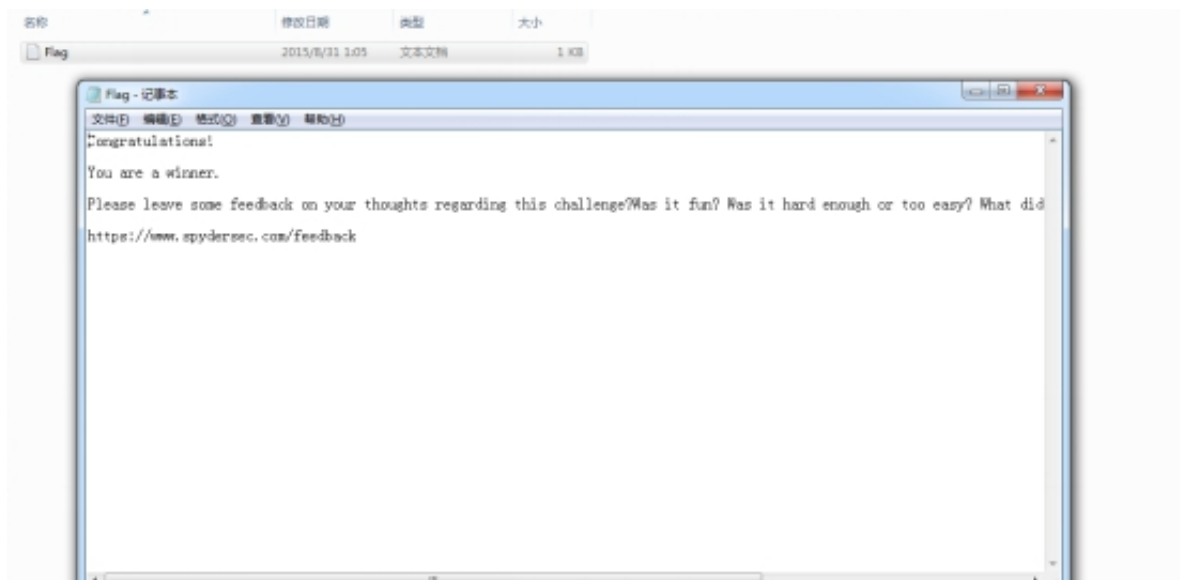
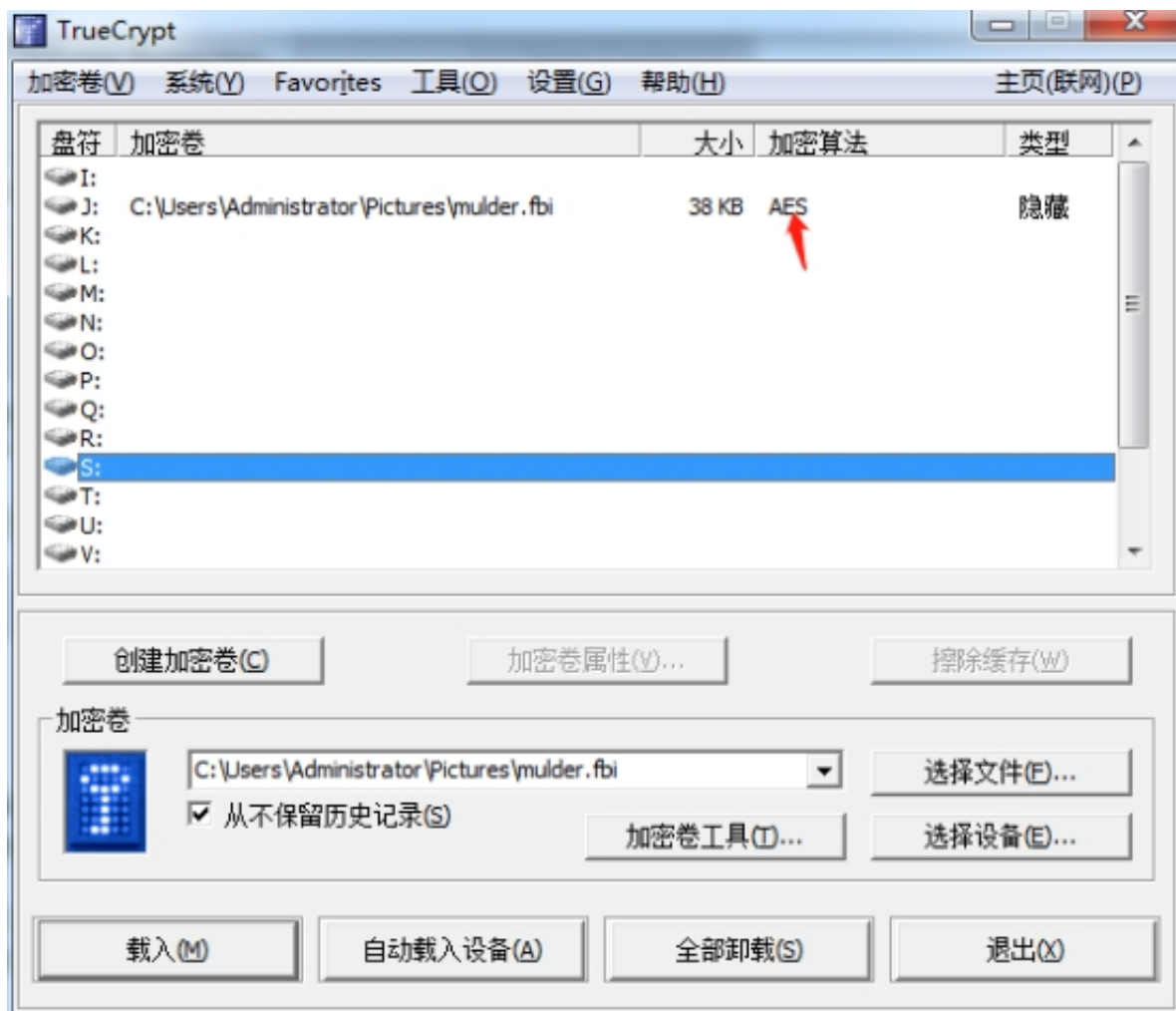


果然是一个文件，在kali中打开发现是一段音频，一脸懵逼
搜了一下发现是一个加密文件，使用truecrypt解密



需要输入密码，之前找到的字符串估计就是密码了

A!Vu~jtH#729sLA;h4%



解密成功，拿到flag:

1 Congratulations!

2

3 You are a winner.

4

5 Please leave some feedback on your thoughts regarding this challenge? Was it fun? Was it hard enough or too easy? What did you like or dislike, what could be done better?

总的来说，这个靶机并不难

|