

广东省强网杯2015 writeup

原创

[atestprofile](#) 于 2015-12-13 02:04:24 发布 9581 收藏 1

分类专栏: [CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/ganliuzhuo/article/details/50280057>

版权



[CTF 专栏收录该内容](#)

0 篇文章 0 订阅

订阅专栏

第一次参加这么正式的安全比赛, 拖了有点久, 现在把比赛时候的一些想法和思路记录下来。

从web狗的角度来看资格赛关于web的题目不算是很难, pwn和re的题就不评论了。

1.常用的管理员密码:

试了好几个, 最后提交admin通过

2.单身狗:

二维码的一部分被doge挡住了, 直接修复下然后扫一下即可得出flag, 送分题

3.回旋13踢:

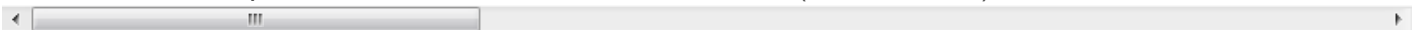
ROT13

4.奇怪的数据库:

其实也就是把ANSI转成了UNICODE, lake2在“ASP数据库插马小议”中讨论过, 转回ANSI即可

5.跳来跳去:

页面跳得快, 用Burp Suite截包可以看到cookie始终为同一个值(test2的md5值), 尝试用常用的账号进行MD5加密



6.万国码:

把给的unicode转成中文

7.小苹果:

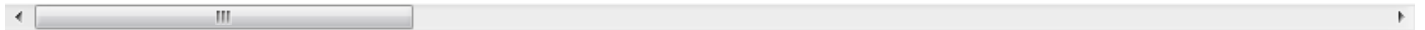
SilentEye直接decode

8.眼前:

strings工具输出到txt后搜索flag

9.又一个后台:

从页面的form表单可以拼凑出<http://123.59.54.182:4943/index.php?username=admin&pass=hackmeplease>, 这



后台: 832857ad8b88.php

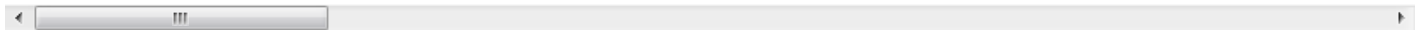
进去后页面有一个post的id参数, 尝试sql注入, 直接丢sqlmap里跑并把flag表里的数据dump出来即可。

10.正确的密码:

md5密文里不可能出现l, 去掉

11.致敬经典:

这道题一开始给了张凯撒电影里的人物截图, 还真有点误导性, 找了很多相关这个人物的资料也没发现有什么线



12.来看一下flag的格式:

开场热身题, 直接交flag即可

13.大黑阔:

从给的pcap包里把图片提取出来, 是一张中国地图。

题目提示是黑阔在聊天, 从数据里可以找出几段话

```
[{'content':'how about wangsicong 100?\n','stime':'15:41:36'}]\n\n[{'content':'how about wangsicong 100?','stime':'15:41:52'}]\n\n[{'content':'guominlaogong ','stime':'15:42:05'}]\n\n[{'content':'lol...','stime':'15:42:10'}]\n\ncontent=what is 100?&\n\n[{'content':'his family has alot of building..you know..','stime':'15:42:44'}]\n\n[{'content':'ok','stime':'15:43:44'}]\n\n[{'content':'upload to me','stime':'15:43:49'}]\n\n[{'content':'yes','stime':'15:44:24'}]\n\n[{'content':'well! ','stime':'15:44:35'}]
```

王思聪，100，这两个关键词很重要，过度百度万达100看看会返回什么结果，结果发现第100家万达在昆明，在

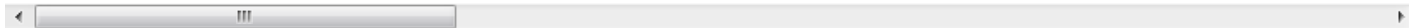


再处理一下看看



14. 爆破:

给出了一个压缩包，解开后有一个readme.txt，还有一个有密码的Desktop.zip，这个加密的包里还有一个readme



```
Strange... had a false hit.
Ta-daaaaa! key0=df96dc88, key1=b432ddfd, key2=df4b9e93
Probabilistic test succeeded for 24 bytes.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Strange... had a false hit.
Stage 2 completed. Starting zipdecrypt on Sun Nov 29 13:21:46 2015
Decrypting answer/key.txt (93cc3c98bac382a9443cc4e7)... OK!
Decrypting readme.txt (03cb26263c718c55931e15e6)... OK!
Finished on Sun Nov 29 13:21:46 2015
ganliuzhuodeMacBook-Pro:6005400ffa8ecd5053ab56d0f868d198 ganliuzhuo$ ls
Desktop.zip  plaintext.zip  readme.txt  result.zip
```

15. 女神在哪儿：

我自己觉得吧，最坑的就是这道题了==，而且还是500分的题，简直是压倒性的题目啊，脑洞不小.....

从给出的聊天截图里可以得出以下结论：

1.电视当时应该是在播浙江卫视，真的要吐槽女神的手机像素如此低，简直就是马赛克拼出来的==，还有女神说



新闻深一度：新闻深一度20150921



和聊天截图里的一模一样，可以判定女神在浙江

2.wifi名为qthjfsbg，按大家一般的尿性，应该是个拼音的首字母组成的，七天酒店订的wifi不是这个ssid，那就从



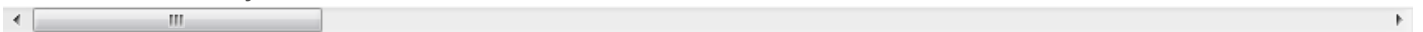
3.记录里说附件有山，有湖，还有点偏，出去洗剪吹也才15块。地方应该在不是那么繁荣的地方而且附件可能有



瞬间排名就从30上升到了第2

16.小心猪圈：

base64解出：God job:57656C6C20646F6E653A4A35584759364A414E3558474B4944544F52535841494442.



发现字母都没超过F，其实一开始尝试变成图片像素的角度去考虑的，结果发现好像构成不了一张图。

从base16的角度来看

```
>>> base64.b16decode(str)
b'Me ll done:J5KGV6JANSXGKI DTORSXA I DB05QXS0S RGI 4XKVRT JJU G I SCNONMU QUT QMI ZDK6 SPNU 4U
UYL0I I3UK3LJOBRU24BTMLJTQ5 DCGJ4HGVLJGF2VEU3Y CNGP04DMMU DWA5 DEI 4YXMY SHGU 4UE3JZGBSG
2ML2MZIT2PI -'
```

既然都有了base64和base16，那就试下base32

```
>>> str="J5KGV6JANSXGKI DTORSXA I DB05QXS0S RGI 4XKVRT JJU G I SCNONMU QUT QMI ZDK6 SPNU 4U
UYL0I I3UK3LJOBRU24BTMLJTQ5 DCGJ4HGVLJGF2VEU3Y CNGP04DMMU DWA5 DEI 4YXMY SHGU 4UE3JZGBSG2ML
2MZIT2PI -"
>>> base64.b32decode(str)
b'On ly one step away:Q29uZ3JhdHU sYXRpb25zOm9 janB7entpcmp3bW8tb2xsa i1ubMx3LMpveGk
tdG1vb05ybm90dnizfQ--'
```

最后再来个base64

```
>>> base64.b64decode(str)
b'Congratulations:ocjpb(zkirjumo-01lj-nmlw-joxi-tmolnrnotvms)'
```

说好的Only one step呢= =

在这里卡了好久，凯撒试过也没得出结果，最后队友提起题目是猪圈，然后找到猪圈密码图进行字母变换才得出



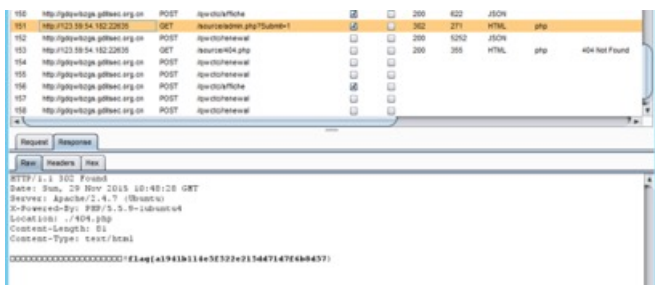
17.找彩蛋:

先看源码

```
源代码

<?php
include('conf/eq.php');
if(isset($_GET['Submit'])){
    header('Location: ../404.php');
    echo $secret;
}
?>
```

构造请求并截图



到了决赛是采用了AWD形式来进行

每台防护机上有4个web网站分别为dedecms,phpok,phpoa,Discuz!

不能上外网，不允许带资料和私带工具。

最后通过3个漏洞顺利拿了高校组第一的成绩。