**CrackMe Challenge** - MobileApp apk文件 GapkTool key:Andr0id\_ReVeRse\_C0mpl3t3

**UnpackMe Challenge** 脱壳peid 2012p4ck-Unp4cking-Unp4cked

**菜刀的保险箱** exe swf文件 用flash decomplier trillix破解 看按钮脚本 1231856318

**这是黑阔们经常干的事**：Windows\_CMD\_is\_useful!

**key就是** WeLc0m3\_2012

**UTF-7** 开头的“+”与末尾的“-” UTF编码 <meta http-equiv="content-type" content="text/html; charset=utf-7"> 换行代码 保存为html文件打开

iamutf7encoded

**JS Challenge** javascript 查看源代码 unescape解密 201211

**菜刀的相册** photo.asp?id=1 破+and 1=1 谷歌浏览器cookie编辑 photo.asp +id:-1 union select 1,password from admin (空格20%)

c00ki3inj3ct@2012

**CSS OR XSS** 直接看

**文件上传** 火狐插件firebug F12

**捡到银行卡** 523986

**你抓住了吗？** 设置内容设置java允许

**找找看看** 先下载图片winhex打开url解密得到,在源码中还有url解密

2qrytrnpymbKyQopOs2zPnDSvnOCvWLqQf1j4DSlJa51NV38HG749FcB5nCtnh

**只能上传图片哦** 修改图片后缀为phP

**谁是admin？？** 安装HackBar F9默认开启 输入<http://10.137.0.102/25/?ctf=php://input>，勾选Enable Post data 1181c1834012245d785120e3505ed169

**照猫画虎** 在地址栏输入<http://10.137.0.142/26/?id=ket1key1111:/1/1key> 0abd3587a3a633ca1300b554357ff03a

**排好队绕过去** sorry界面 地址栏加?uname[]=1&&passwd[]=2 117f8628f187c24bbe15febead3046fa

**这个地址好奇怪** 下载安装程序，选择curl for 32 bit 将程序解压，放到cmd里运行curl.exe，输入curl.exe –v <http://10.137.0.55/28/index.php> 1834012245d785120e3505ed169

**头都大了** F12 点击网络选项，选择/29/的这个文件，点击消息头，在响应头里找到“hereisflag”字段，b7bb30b3435f2e7c418b131f9e789f81

**不仅仅是个登录页面** <http://10.137.0.154/30/rebots.txt>

**浏览器的锅？？** 用burp 把User-Agent修改为opera浏览器的http请求头，Opera/9.80 (Windows NT 6.1; WOW64; U; zh-cn) Presto/2.10.229 Version/11.62

1bc50c66677667a56c3208e06cf64159

**我要出国！出国！** 用burp 修改Accept-Language为en-US,en;q=0.8 两次转发

d8016131a2724252b2419bf645aab221

**怎么回事，我是个flag** 下载火狐插件救援bug按F12打开firebug，选择cookies，新建 user 192.168.15.28 /35/ admin 记得勾时间旁边 刷新 flag{5d41402abc4b2a76b9719d911017c592}

**flag是什么呢** 在地址栏输入http://192.168.15.28/36/?password[]=1 flag{}

MSDJALSDJSDKSDSAASDJSKSKSKSKSKSKA

**这是一道简单的WEB** you\_are\_a\_good\_boy

**找呀找呀找不到** 在地址栏输入<http://192.168.15.28/37/?id=ture> 4c3cbcadf7b8a9ae2932afc00560a0d6

**爆破小组准备** 查看源码，发现提示1-255 用burp 随便提交一个查询，用burp抓取数据包 看到提交的key值，右键action将数据包发送到intruder进行爆破 进入intruder，选择payloads，将payload type设置成numbers 设置从1-255，步长为1 找到菜单栏的intruder，选择start attack 找到length不一样的值 找到这个界面，查看页面信息，得到flag

**如法炮制** 火狐附加组件下载HackBar，并启用 按F9调用，点击Enable Post data,下面输入id=sdpc1sdpc1111sdpc:/1/1sdpc

**这是一道简单的WEB** 在地址栏输入<http://10.137.0.35/41/?password[]=1>

44b552d856ba3dfb93a9e33229f0d540 you\_are\_a\_good\_boy

**绕绕绕** 火狐附加组件hackbar 点击Enable Post data URL：http://xxxxx/x/?name[]=1 下面password[]=2&id=admin

1kwnbf83sfe9d

**到底传什么值呢？** 在地址栏输入<http://10.137.0.20/43/?password[]=1> arrayagainb0ys

**整理一下你的发型** 按F12打开控制台，点击网络选项，在消息头里发现提示 检查文件 index\_hongya.php，输入地址栏<http://10.137.0.20/44/index\_hongya.php> 根据代码需要将admin用url编码编译一下，%61%64%6d%69%6e 加？user=admin 二次编码 <http://192.168.109.238/44/index_hongya.php?user=%2561%2564%256d%2569%256e>

cd70c87dab94375d1d11f3a5e70c4568

**我建议你放弃** e9f0c8f650be6119646732faf5a3cffc

**你确定你是管理员吗？** 安装并启用Hacker，Firebug F9 打开Hackber，通过post传递数组，username[]=1&password[]=0 不是administrator，F12打开firebug，修改cookies值 输入base64加密过的administrator，YWRtaW5pc3RyYXRvcg==

**红亚欢迎你** flag{2152fd8edc2e45df187ce5794bc72803}

**简单溢出** ?admin&user[]=123456789 1f18348f32c9a4694f16426798937ae2

**签到了** Welcome\_To\_CTF\_World

**30条命您配吗** haha\_u\_get\_30HP\_now

**bak** URL输入index.php.bak 63d0cea9d550e495fde1b81310951bd7

**bolanxian** URL输入index.php~ 8a3053357a2508363add4edb0cda8f2b

**use\_vim** URL输入.index.php.swo 912ec803b2ce49e4a541068d495ab570

**forgot\_someth** URL输入.svn/wc.db 6ded31434fc9a9472b24da4ecbd4a4db

**zhengze** 火狐浏览器，需要安装hackbar插件 勾选Post data,在弹出的文本框里输入解出的内容,点击执行Execute 网页输入http://60.10.10.21/198/index.php 下面id=hongyaahongyaaaaahongyaaa:/a/ahongya

**密码学**

**技术宅拯救世界** MD5加密 cp /Cardinal/YUI /home/kirito/local-memory/

**奇怪的文本** 下载之后 Base解码发现有个key文档 用hex打开问答 编辑转换base64-二进制 另存为rar

**用脑子想想** brainfuck网页破解部分

**rar** 需要密码 用爆破软件Archpr 打开软件设置一下，范围，一般加密都是大小写字母和数字。再设置一下长度four就是4位的，获得口令，输入密码

**爆吧** ARCHPR 长度4 base64+base32

**很多** rot13，rabbit，16进制解密

**Brainfuck2** brainfuck解密Ook to text 凯撒密码解密工具 偏移量13

**Brainfuck3** brain解密 escape解密

**双码** md5 base64 apples

**rot13** 移位密码

**excel** Advanced Office Password Recovery5.10 暴力破解 文档密码99999 打开

**套路** 转ascii 再莫斯 FLAGS0S

**恩五位** 0变a 1变b 培根密码 FQEEDNL

**不爆怎么做** 改改吧 ARCHPR爆破rar 解压 flag{where are you！}

**md5原理** md5为16进制得来，没有l，联想l改为1得flag admin

**32+32=** base64解码flag{e9708b278c79b230ca7d5e6925b0e079}

**code编码有很多** 进行unicode解码 flag{ebd668994f796e38c5164e09cf1c352b}

**看看都在其中** FLAG FF B ED FD F C BA E B C

**数字B** 使用rot13，再接base64解密 FlagIS6cvkrhFpVEHAK8Ap

**兔子兔子** rabbit解码 sImPle\_xUe\_yuan

**aes23333333** 密钥文件名 FLAG{five\_1s\_fun}

**word哎** 文档密码9919 显示隐藏文字 F\_L\_A0Ge{}ZHA\_1s 栅栏解码 11位 FLAG{ZHA\_1s\_\_0e}

**有点难** 文件ARCHPR的密钥9199 文档1AES解密 密钥9919 flag%7B6013221752df892237d0fc99fd8a328f%7D

**32** base32解密 flag{888e7b8b2d94aedbe6d0b7933c3506bf}

**什么编码** xxencode解码 flag{6a1ec673bfd3cf43bdb5d06e14f09707}

**uuuu** uuencode解码 flag{4e95cce551e20c81ea92b8f76c0ec8f5}

**uuuuuuuuuunnnnnnnnnn** unicode解码 flag{5be6f00e8b8722ef0c075bdb2b4d7001}

**再试试** quoted-printable编码 flag{40e4edc94b08e4d03d2df9e7ba76f10b}

**超级简单** rabbit解码 flag{97ff039a66796a89c9270109fe58a46d}

**aes知道吗** base64再aes flag{2dabe30552692f7f11d131e27a54c4e0}

**围起来** flag{\_Just\_4\_fun\_0.0\_}

**凯撒大帝的羊** 栅栏解密 字数5 flagisrcg1fdlw15woql

**rc？** 上面base64 下面rc4 flag{cc5ff8d6e7356e32076639ce07e4a7ee}

**Cipherception** always\_continue\_digging

**1\*1\*2** 先base64解密，再进行base32解密，再进行两次base64解密' flag{f614b0a347d7742ada84f7ac2ab42158}

**秘密电报** 培根密码解码 HONGYA

**小明丢失的明文** 用affine cipher flag{xiaoming\_mingwen}

**有趣的ISCC** 用winhex打开 unicode解密两次 flag{iscc is fun}

**重重蝶影** 多次base64 AES 与佛论禅+佛曰： 把我复制走

**animals** 直接rabbit 3b1c488411db6f1f2c676da7b6b8a5f9

**听说每个人都知道啥是base** base64两次 base32 base16 flag{33bcd42bd1c5576ddadcb0e501b525b9}

**Rail Fence Cipher** flag{d99516a57e4c90a59504b5ccgc3a83ec}

**jiami** JJEncode flag{7815696ecbf1c96e6894b779456d330e}

**都藏在数据里** wireshark导出http saveall 有个压缩文件 密码hongyakeji base64内容 flag{1d89dd312931e3444c6cd5c40c051e9e}

**暴力XX不可取** isccwearecoming

**凯撒是十三世** 凯撒密码解码 位移13 解得roqtp697t95j3对应键盘下方 flag：yougotme

**二战时期的密码** WELCOMECISRG

**我这密码忘了** 解两次base64 SK88WGLHBWJ1RMTK61D2X4C5CI7FI0TE

**IDC密码破解** 手机九键 GOODTEST

**KEYBORD** 键盘ORANGE

**被黑了** 摩斯密码JRQ058XMGC1I7PB4UNGA7BLNBCMS6YJ0

**多种办法解决** 文本里含jpg base64 base64转图片

**日常爆破系列2** 19491001

**日常爆破系列1** 无

**很普通的DISCO** flag{W0W\*funny}

**小明得到了什么** you\_are\_a\_good\_boy