2019年掘安杯writeup

原创

想吃小肥羊 于 2019-04-21 19:31:54 发布 415 收藏 1

文章标签： ctf 掘安杯

本文链接：https://blog.csdn.net/qq_41517934/article/details/89291007

一、下载下载

点开题目链接，看到“下载flag文件”，点击可下载flag.txt，但是却没有发现我们想要flag。

这时我们查看源码，发现有flag.php，于是尝试构造如下下载url，看是否存在可以下载的文件

url: `http://120.79.1.69:10002/?file=flag.php`

下载后的代码如下：

```php
<?php
header('Content-Type: text/html; charset=utf-8'); //网页编码
function encrypt($data, $key) {
 $key = md5 ( $key );
 $x = 0;
 $len = strlen ( $data );
 $l = strlen ( $key );
 for($i = 0; $i < $len; $i ++) {
  if ($x == $l) {
   $x = 0;
  }
  $char .= $key {$x};
  $x ++;
 }
 for($i = 0; $i < $len; $i ++) {
  $str .= chr ( ord ( $data {$i} ) + (ord ( $char {$i} )) % 256 );
 }
 return base64_encode ( $str );
}

function decrypt($data, $key) {
 $key = md5 ( $key );
 $x = 0;
 $data = base64_decode ( $data );
 $len = strlen ( $data );
 $l = strlen ( $key );
 for($i = 0; $i < $len; $i ++) {
  if ($x == $l) {
   $x = 0;
  }
  $char .= substr ( $key, $x, 1 );
  $x ++;
 }
 for($i = 0; $i < $len; $i ++) {
  if (ord ( substr ( $data, $i, 1 ) ) < ord ( substr ( $char, $i, 1 ) )) {
   $str .= chr ( (ord ( substr ( $data, $i, 1 ) ) + 256) - ord ( substr ( $char, $i, 1 ) ) );
  } else {
   $str .= chr ( ord ( substr ( $data, $i, 1 ) ) - ord ( substr ( $char, $i, 1 ) ) );
  }
 }
 return $str;
}

$key="MyCTF";
$flag="o6lziae0xtaqoqCtmWqcaZuZfrd5pbI=";//encrypt($flag,$key)

?>
```

通过观察代码，我们很容易发现，flag由encrypt函数加密了，但是代码中又提供了解密函数，所以我们可以稍作修改调用decrypt函数解密，运行代码之后就得到了flag：myCTF{cssohw456954GUEB}

```
43
44  $key="MyCTF";
45  $flag="o6lziae0xtaqoqCtmWqcaZuZfrd5pbI=";
46  echo decrypt($flag,$key)
47
48  ?>
```

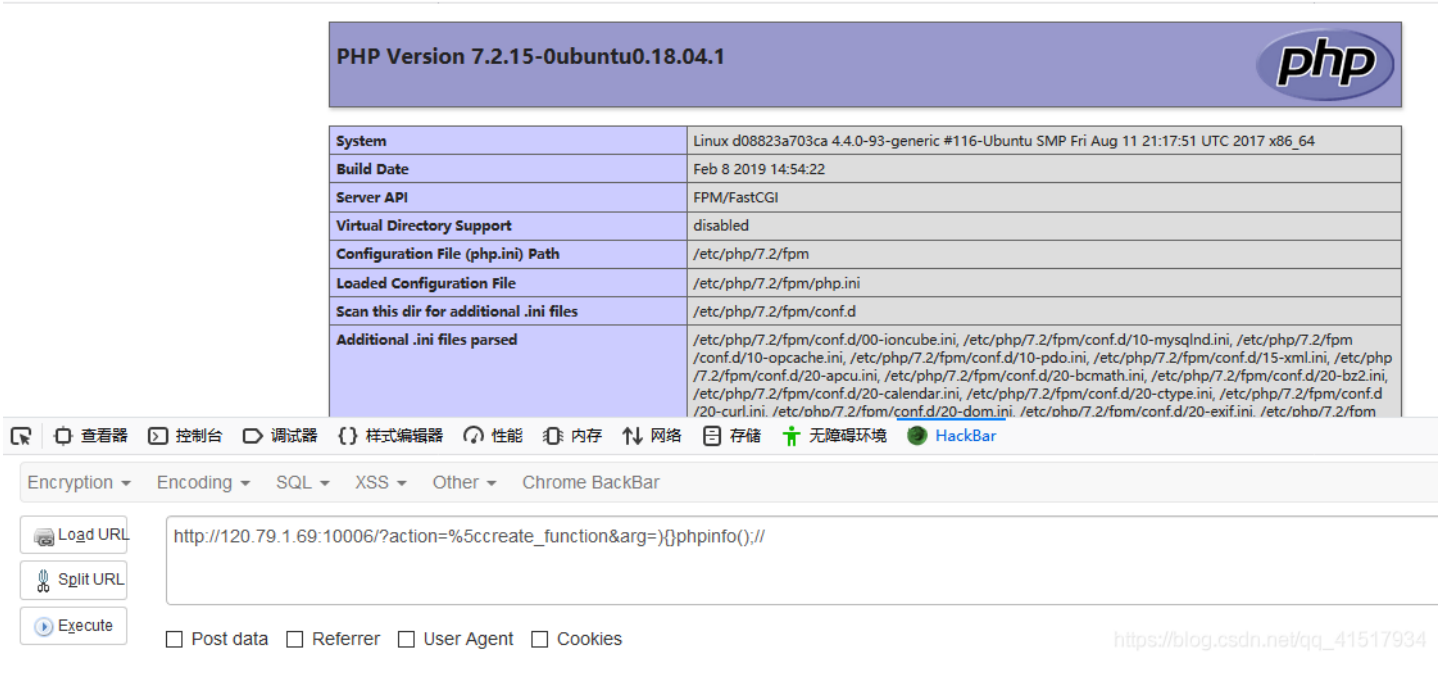
```
myCTF{cssohw456954GUEB}[Finished in 1.2s]
```


二、not_easy

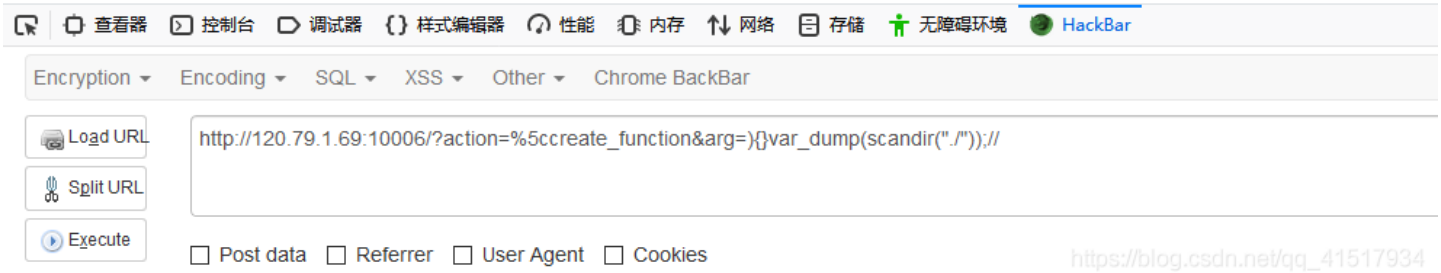
打开题目链接，得到以下代码：

```
<?php
error_reporting(0);
if(isset($_GET['action'])) {
    $action = $_GET['action'];
}

if(isset($_GET['action'])){
    $arg = $_GET['arg'];
}

if(preg_match('/^[a-z0-9_]*$/isD', $action)){
    show_source(__FILE__);
} else {
    $action($arg,'');
}
```

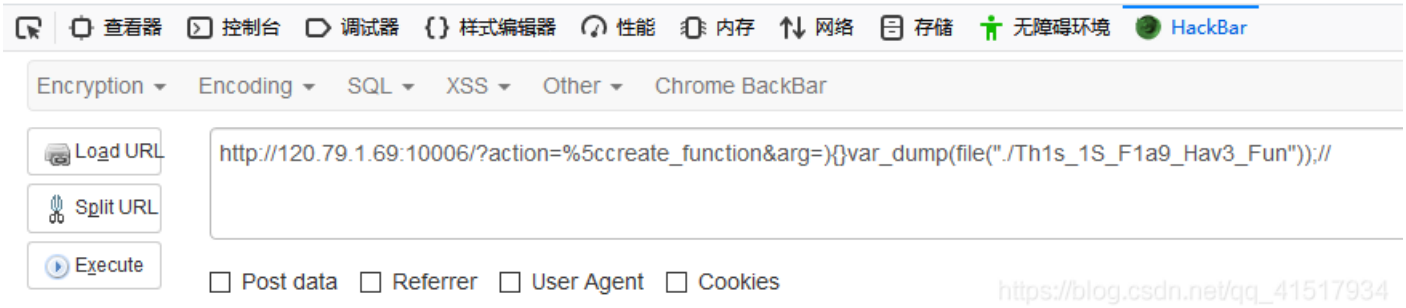
很明显这是一道create_function() 代码注入的题目，根据create_function()代码注入，需要绕过对$action参数的正则过滤，而在数字、字母和下划线都被过滤的情况下，可以考虑在开头或结尾插入字符来绕过正则。通过测试，发现在函数开头加字符“/”（%5c）可以绕过正则。知道了这个规律后我们就可以利用create_function() 代码注入执行命令了。



array(5) { [0]=> string(1) "." [1]=> string(2) ".." [2]=> string(21) "Th1s_1S_F1a9_Hav3_Fun" [3]=> string(9) "index.php" [4]=> string(6) "zx.php" }



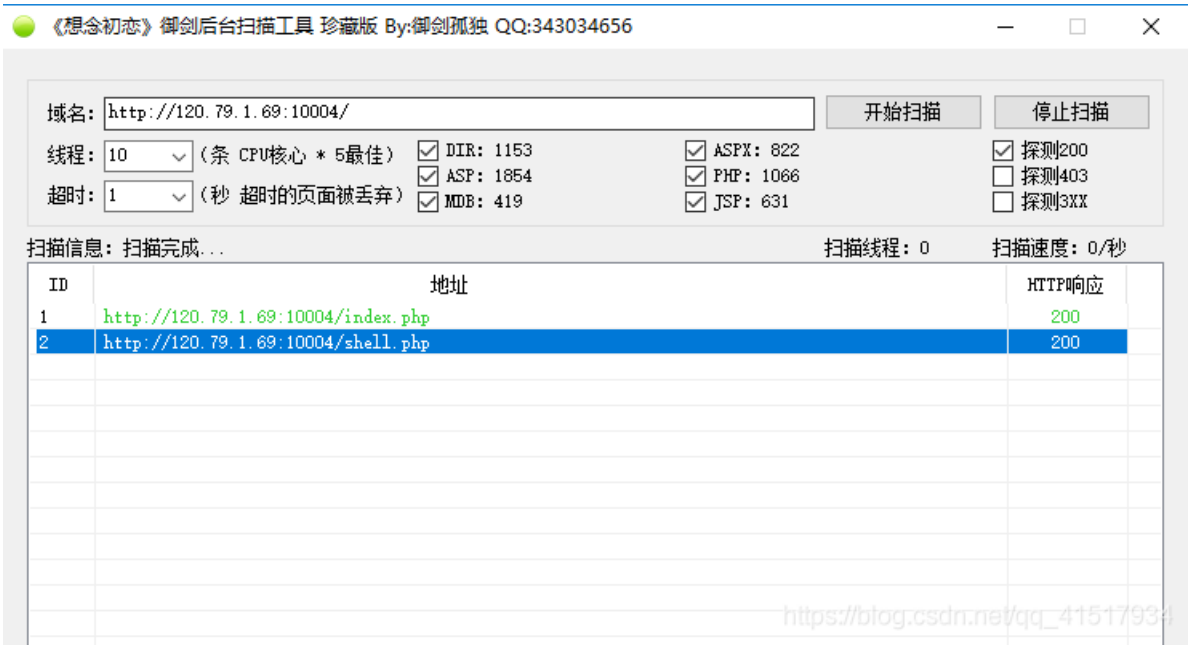
array(2) { [0]=> string(40) "jactf{c795359da56ae38ec9132eaad24733fc} " [1]=> string(1) " " }



最后我们得到了flag：jactf{c795359da56ae38ec9132eaad24733fc}

三、该网站已被黑

网站被黑有可能是存在黑客留下的webshell，可以先用御剑扫描下，果然发现了一个webshell。。。



之后用burp抓包暴力破解：

（1）在proxy->options中设置代理服务

（2）浏览器设置局域网

（3）proxy->intercept数据拦截

（4）后台输入密码登录，单击forward

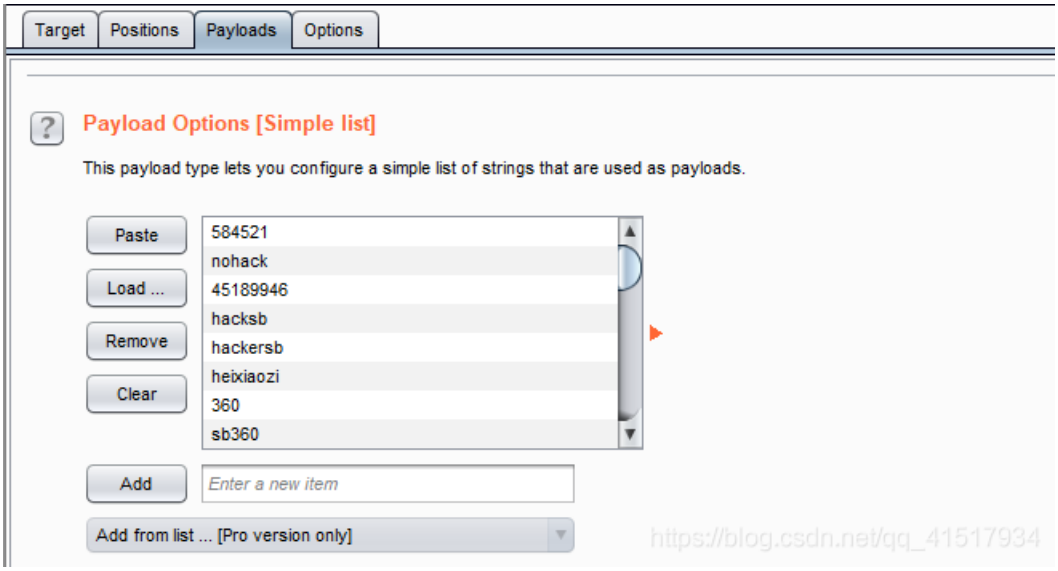
（5）action->send to intruder

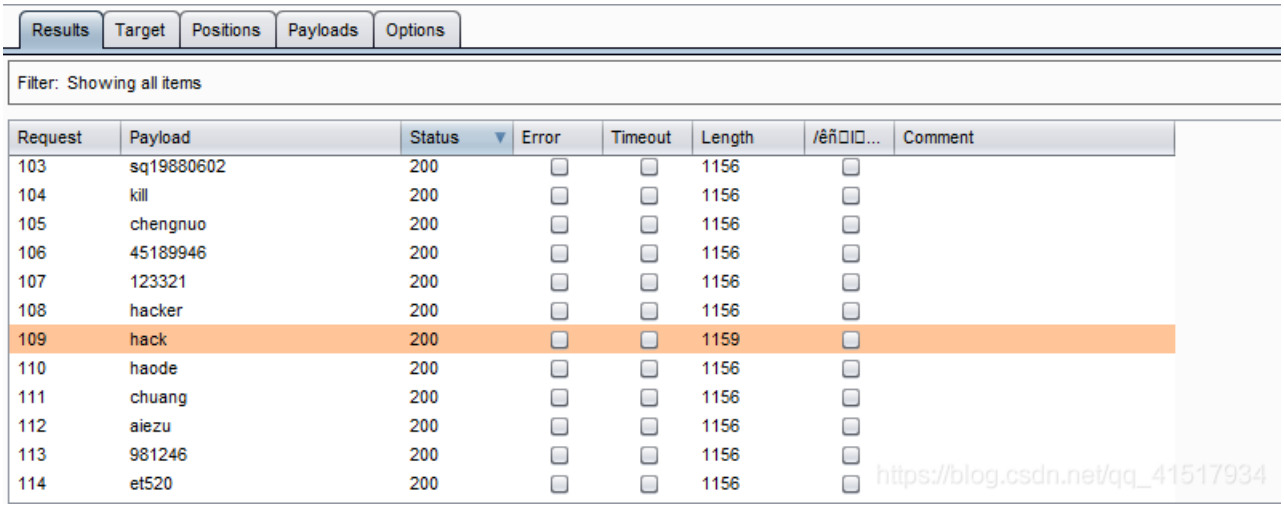
（6）点击clear,取消之前对已拦截数据的标记

（7）选中需要暴力破解的内容，点击add添加标记

（8）payloads->load，添加密码字典

（9）点击start attack开始暴力破解

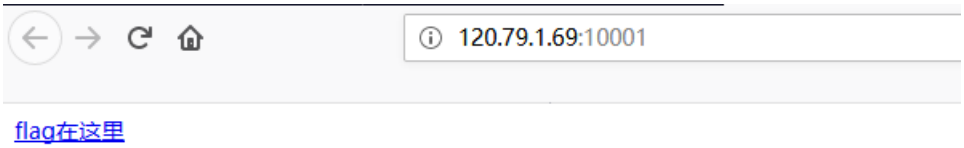




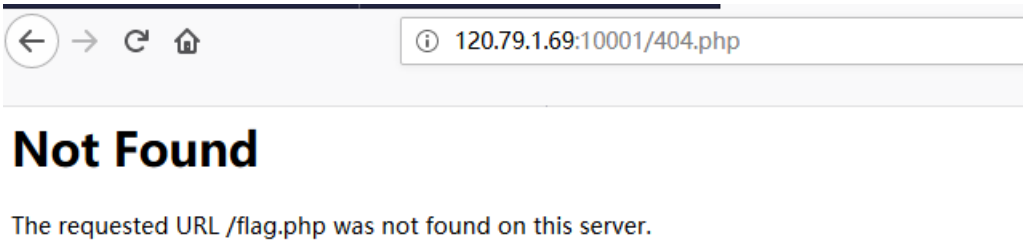
最后我们得到密码为hack，再次输入密码登录可得到Flag:jactf{DWDASFASCASFAFASFNKAS}

四、web签到

打开链接，题目如下：



点击“flag在这里”出现如下页面：



既然没有发现特别有用的信息，就用burpsuite抓包看看。抓包后，发现有一个flag.php文件进行302重定向了。

1219	http://120.79.1.69:10001	GET	/404.php	404	440	HTML	php	404 Not Found
1218	http://120.79.1.69:10001	GET	/flag.php	302	231	HTML	php	

点开flag.php的http头信息，发现了一个经过base64加密的flag

Connection: close
Flag: amFjdGZ7amFzYWZlMTEwcXdlYXNkenhjfQ==
location: 404.php
Content-Length: 0

经过base64解密后获得最终的flag。