2018CSTC web2 writeup

转载

weixin_34198762 于 2018-05-14 09:47:00 发布 67 收藏
文章标签： php git javascript ViewUI
原文链接：https://yq.aliyun.com/articles/625462

全国网络空间安全技术大赛，比赛地址
http://cstc.xatu.edu.cn/

这次和小伙伴参加了线上初赛，再次被吊打，除了签到和这题Web2，连Web1就卡着一直没做出来/(ㄒoㄒ)/~~
题目地址：
http://117.34.116.192/

打开题目链接，首先会自动跳转到一个看似有文件包含的url界面

image.png

界面的内容是一个登陆页面

image.png

先尝试登陆页面的登陆功能，查看是否可能存在sql注入，结果发现这个登陆页面并没有和后端进行交互，登陆功能应该只是一个伪装
于是对疑似存在文件包含的url进行尝试，发现存在任意目录文件查看

```
117.34.116.192/index.php?file=/etc/passwd
```

image.png
心想题目不可能这么简单，果然在查看了许多可能的文件后，都没有发现flag的身影
这时候思路开始变化，尝试伪协议、包含web服务器日志、包含/proc/self/environ等,，但是都失败了，估计对访问权限做过控制
LFI、RFI思路可以参考https://blog.csdn.net/xysoul/article/details/45031675

尝试使用php、file、http等，服务端应该对file参数进行了检测

image.png
这里查看apache2的日志路径是默认的/var/log/apache2/error.log

image.png

但是包含后并没有内容，/proc/self/environ也同样没有内容返回

image.png
image.png
到这里卡了段时间（菜鸡的痛），无意间灵光一闪，随手一敲，发现这题还有个源码泄露。。。因为怕被ban，一直没起扫描器，不然源码泄露应该发现得早

```
http://117.34.116.192/.git/
```

image.png
拿起git源码泄露利用工具https://github.com/lijiejie/GitHack拿下源码
发现内容还有个upload.php

image.png

```
<?php
   function Administrator($value){
       if(empty($_COOKIE['in_adminid']) || empty($_COOKIE['in_adminexpire']) || $_COOKIE['in_adminexpire']
           return False;
       }
       setcookie("in_adminexpire",$_COOKIE['in_adminexpire'],time()+1800);
       if(!empty($_COOKIE['in_permission'])){
           $array=explode(",",$_COOKIE['in_permission']);
           $adminlogined=false;
           for($i=0;$i<count($array);$i++){
               if($array[$i]==$value){$adminlogined=true;}
           }
           if(!$adminlogined){
               return False;
           }
       }else{
           return False;
       }
       return true;
   }
   if (Administrator(2)){
       if(isset($_FILES['file'])){
           $filename = './img/img'.rand().'.jpg';
           move_uploaded_file($_FILES["file"]["tmp_name"],$filename);
           header('Refresh:3,url=index.php?file=upload.php');
           echo "Upload $filename Success!";
           die;
       }
   }else{
       header('Refresh:3,url=index.php?file=login.html');
       echo "Who are you!";
       die;
   }
?>
<!DOCTYPE html>
<html lang="zh-CN">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta name="description" content="">
    <meta name="author" content="">
    <link rel="icon" href="../../favicon.ico">
    <title>图床后台</title>
    <link href="https://cdn.bootcss.com/bootstrap/3.3.7/css/bootstrap.min.css" rel="stylesheet">
    <link href="starter-template.css" rel="stylesheet">
  </head>
  <body>
    <script src="https://cdn.bootcss.com/jquery/1.12.4/jquery.min.js"></script>
    <script src="https://cdn.bootcss.com/bootstrap/3.3.7/js/bootstrap.min.js"></script>
    <form class="form-horizontal" action="upload.php" method="post" enctype="multipart/form-data">
    <fieldset>
      <div id="legend" class="">
```

```
        <legend class="">添加图片</legend>
      </div>
    <div class="control-group">
          <!-- Text input-->
          <label class="control-label" for="input01">图片名</label>
          <div class="controls">
            <input placeholder="请输入Message标题" class="input-xlarge" type="text" name="title">
          </div>
        </div>

    <div class="control-group">
          <label class="control-label">附件</label>
          <!-- File Upload -->
          <div class="controls">
            <input class="input-file" id="file" type="file" name='file'>
          </div>
        </div>



    <div class="control-group">
          <label class="control-label">预览</label>
          <!-- Button -->
          <div class="controls">
            <button class="btn btn-success">Submit</button>
          </div>
        </div>

    </fieldset>
  </form>
  </body>
</html>
```

另外，打开index.php，不是熟悉的php代码，而是一个貌似加密过的文件

image.png

用记事本打开，看到了这里的关键词PM9SCREW，熟悉的php_screw加密
在之前的ctf比赛中出现过

image.png
暂时不管这个php_screw加密，首先对upload.php进行审计

```
function Administrator($value){
        if(empty($_COOKIE['in_adminid']) || empty($_COOKIE['in_adminexpire']) || $_COOKIE['in_adminexpire']
            return False;
        }
        setcookie("in_adminexpire",$_COOKIE['in_adminexpire'],time()+1800);
        if(!empty($_COOKIE['in_permission'])){
            $array=explode(",",$_COOKIE['in_permission']);
            $adminlogined=false;
            for($i=0;$i<count($array);$i++){
                if($array[$i]==$value){$adminlogined=true;}
            }
            if(!$adminlogined){
                return False;
            }
        }else{
            return False;
        }
        return true;
    }
```

函数Administrator中对cookie的内容进行了判断
需要cookie包含有in_adminid、in_adminexpire、in_adminname、in_adminpassword、in_permission字段
并且需要满足in_adminexpire等于(in_adminid、in_adminname、in_adminpassword、in_permission)字符串拼接后的MD5值
之后还需要in_permission中包含2

```
if (Administrator(2)){
        if(isset($_FILES['file'])){
            $filename = './img/img'.rand().'.jpg';
            move_uploaded_file($_FILES["file"]["tmp_name"],$filename);
            header('Refresh:3,url=index.php?file=upload.php');
            echo "Upload $filename Success!";
            die;
        }
    }else{
        header('Refresh:3,url=index.php?file=login.html');
        echo "Who are you!";
        die;
    }
```

当Administrator函数返回真值后，将会把上传的文件用move_uploaded_file函数拷贝到./img/下，并且通过随机数命名

这里很好绕过，可以直接上传一句话

image.png
再通过一开始看似无用的文件包含利用点，包含上传的jpg文件，即可RCE
ls发现当前目录下有f14g.php

image.png

查看f14g.php，发现和index.php一样，也是经过了php_screw的加密

image.png
接下来就是想办法把f14g.php的二进制内容获取下来之后
通过利用工具将其还原，这里参考http://wutongyu.info/about-php-screw-decode/
使用xxd命令拿下文件16进制表示

image.png

手动整理一下
image.png

使用xxd -r -ps将二进制流写进文件

```
echo 09504d39534352455709863e3cdeee36176f3d91ae7644268da98fda3f934ce958687055f21cfc4dad1303e3ccf373c2e34c33
```

完成后，可以利用工具直接解密

```
./decode ./f14g.php
```

最后得到flag

image.png

总结

文件上传配合文件包含使得RCE
git源码泄露
php_screw加密