**X档案战队WRITEUP**

## 战队信息

战队名称：X档案战队

战队排名：5

## 解题情况

### 



示例的操作流程：

## 解题过程

### 题目序号 题目名称

### 操作内容：

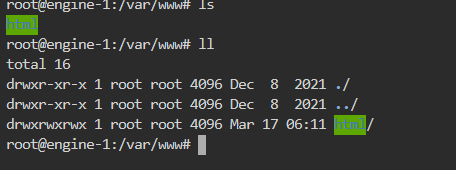
**SSRF:**

|  |
| --- |
| <?php  $blist = [array("localhost","@","127.","192.","10.","172.");](mailto:array(\"localhost\",\"@\",\"127.\",\"192.\",\"10.\",\"172.\");)  if(isset($\_GET['userInput']) && !is\_array($\_GET['userInput']) && in\_array($\_GET['userInput'], $blist)) {  //对传参做一个过滤而$blist就是过滤的内容，而且get进来的userInput不能是个数组  $curlVar = curl\_init();  curl\_setopt($curlVar, CURLOPT\_URL, $\_GET['userInput']);  curl\_setopt($curlVar, CURLOPT\_HEADER, 0);  curl\_exec($curlVar);  curl\_close($curlVar);  }  ?> |

**Photos:**

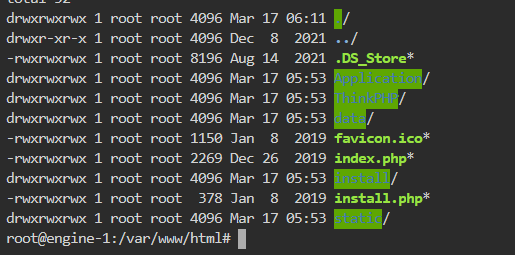
|  |
| --- |
| config.php如下 主要修改了黑名单列表变成白名单列表  <?php  $config=Array(  'WList' => ['jpg','png','jpeg','gif'],  'htmlPath' => 'static/html/',  'uploadDir' => 'static/img/gallery/',  'set\_error\_handler' => 'noError',  'set\_exception\_handler' => 'noError',  'register\_shutdown\_function' => 'noError'  ); **index.ph**p如下 新增内容如下：  1.获取图片内容  $bfile = file\_get\_contents($\_FILES['files']['tmp\_name'][0]);  2.查看是否有非法字符串包含在内  if (!in\_array($ext, $config['WList'])) {  echo "请上传图片!";  return ;  }  <?php  include('config.php');  set\_error\_handler($config['set\_error\_handler']);  set\_exception\_handler($config['set\_error\_handler']);  // register\_shutdown\_function($config['set\_error\_handler']);  if(!empty($\_FILES)){  uploadFile();  }else if(isset($\_GET['upload'])){  show('upload.html');  }else{  show('index.html');  }  function uploadFile(){  global $config;  $bfile = file\_get\_contents($\_FILES['files']['tmp\_name'][0]);  try{  // print\_r($\_FILES);  $chack = ;  if($chack){  echo "请上传图片!";  return ;  }  $uploaddir=isset($config['uploadDir'])?$config['uploadDir']:'static/img/gallery/';    $filename=basename($\_FILES['files']['name']['0']);  $ext=pathinfo($filename, PATHINFO\_EXTENSION);  if (!in\_array($ext, $config['WList'])) {  echo "请上传图片!";  return ;  }  // foreach($config['blackList'] as $b){  // if(strtolower($ext)!=$b){  // }  // }  list($width, $height) = getimagesize($\_FILES['files']['tmp\_name'][0]);  $image\_p = imagecreatetruecolor($width, $height);  $image = imagecreatefrompng($\_FILES['files']['tmp\_name'][0]);  imagecopyresampled($image\_p, $image, 0, 0, 0, 0, $width, $height, $width, $width);  imagepng($image\_p, $uploaddir.$filename);  echo "上传成功，审核通过后将会展示您的图片！";  return ;  }catch (Throwable $t){  echo "上传失败！";  echo $t;  return;  }  }  function show($html){  global $config;  echo file\_get\_contents($config['htmlPath'].$html);  }  function noError(){  echo "上传失败！";  exit();  } |

### 74fix操作内容：

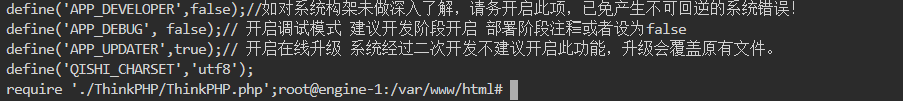
登录服务器发现html目录拥有777权限，随即怀疑可能是权限过高

导致html下的static静态文件也有执行php文件的权限，所以将html目录递归修改为755

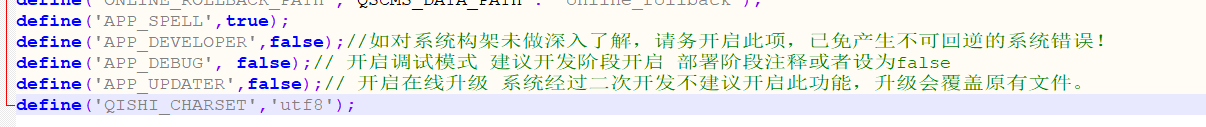
权限



又发现index.php存在 define('APP\_UPDATER',true);// 开启在线升级 系统经过二次开发不建议开启此功能，升级会覆盖原有文件。



该在线升级开启也存在风险，故将define('APP\_UPDATER',true);修改为define('APP\_UPDATER',false);



总结：将index.php文件改写，递归修改html目录权限。

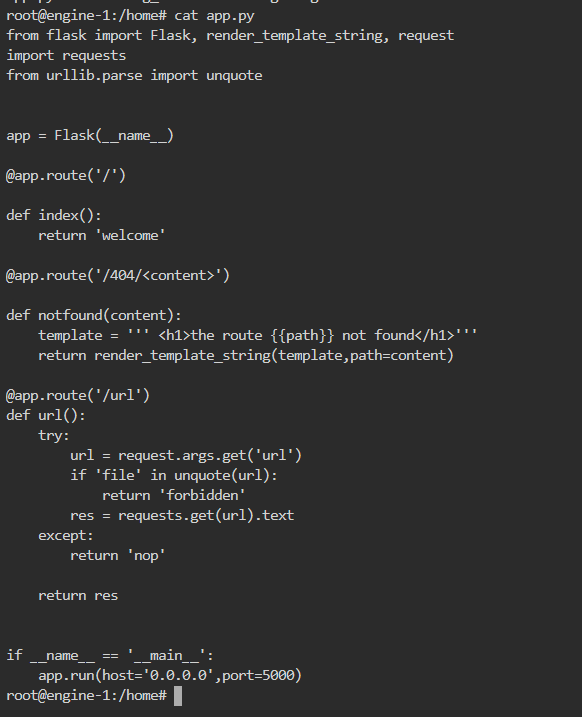
|  |
| --- |
| **update.sh**  #! /bin/sh  mv file1 /var/www/html/index.php  chmod -R 755 /var/www/html  **file1**  <?php  // 应用入口文件  if(version\_compare(PHP\_VERSION,'5.3.0','<')) die('require PHP > 5.3.0 !');  if (!is\_file('./data/install.lock')) {  header('Location: ./install.php');  exit;  }  define('QSCMS\_PRE', 'qs\_');  // 定义应用名称  define('APP\_NAME','Application');  // 定义应用目录  define('APP\_PATH','./Application/');  /\* 数据目录\*/  define('QSCMS\_DATA\_PATH', './data/');  /\*项目自定义类库\*/  define('QSCMSLIB\_PATH', APP\_PATH . 'Common/qscmslib/');  define('QSCMS\_APPAPI\_PATH', APP\_PATH . 'Appapi/Install/');  /\* 数据库备份存放目录\*/  define('DATABASE\_BACKUP\_PATH', QSCMS\_DATA\_PATH . 'backup/database/');  /\* 模板备份存放目录\*/  define('TPL\_BACKUP\_PATH', QSCMS\_DATA\_PATH . 'backup/tpl/');  /\* 缓存目录\*/  define('RUNTIME\_PATH', QSCMS\_DATA\_PATH . 'Runtime/');  /\* SESSION目录\*/  define('SESSION\_PATH', realpath(rtrim(dirname(\_\_FILE\_\_), '/\\') . DIRECTORY\_SEPARATOR . 'data' . DIRECTORY\_SEPARATOR . 'session'));  /\* COOKIE目录\*/  define('COOKIE\_SAVE\_PATH', QSCMS\_DATA\_PATH . 'cookie/');  /\* HTML静态文件目录\*/  define('HTML\_PATH', QSCMS\_DATA\_PATH . 'html/');  /\* 伪静态文件目录\*/  define('REWRITE\_PATH', QSCMS\_DATA\_PATH . 'rewrite/');  /\* 计划任务日志目录\*/  define('CRON\_LOG\_PATH', QSCMS\_DATA\_PATH . 'cron\_log/');  /\* SQL逾时日志目录\*/  define('SQL\_LOG\_PATH', QSCMS\_DATA\_PATH . 'sqllog/');  /\* 招聘效果统计数据缓存目录\*/  define('STATISTICS\_PATH', QSCMS\_DATA\_PATH . 'statistics/');  /\*MOBILE配置文件路径\*/  define('MOBILE\_CONFIG\_PATH', APP\_PATH . 'Mobile/Conf/');  /\*home配置文件路径\*/  define('HOME\_CONFIG\_PATH', APP\_PATH . 'Home/Conf/');  define('ONLINE\_UPDATER\_PATH', QSCMS\_DATA\_PATH . 'online\_updater');  define('ONLINE\_ROLLBACK\_PATH', QSCMS\_DATA\_PATH . 'online\_rollback');  define('APP\_SPELL',true);  define('APP\_DEVELOPER',false);//如对系统构架未做深入了解，请务开启此项，已免产生不可回逆的系统错误！  define('APP\_DEBUG', false);// 开启调试模式 建议开发阶段开启 部署阶段注释或者设为false  define('APP\_UPDATER',false);// 开启在线升级 系统经过二次开发不建议开启此功能，升级会覆盖原有文件。  define('QISHI\_CHARSET','utf8'); |

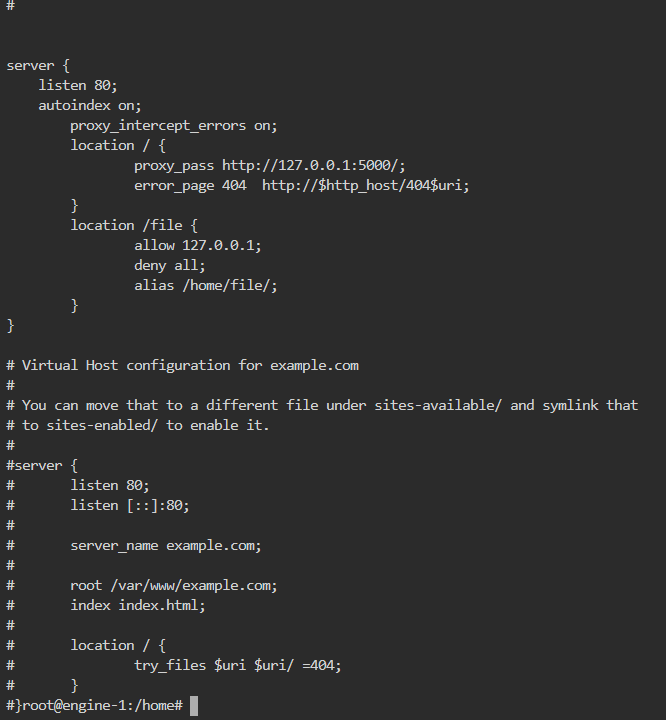
### aaaagent

### 操作内容：

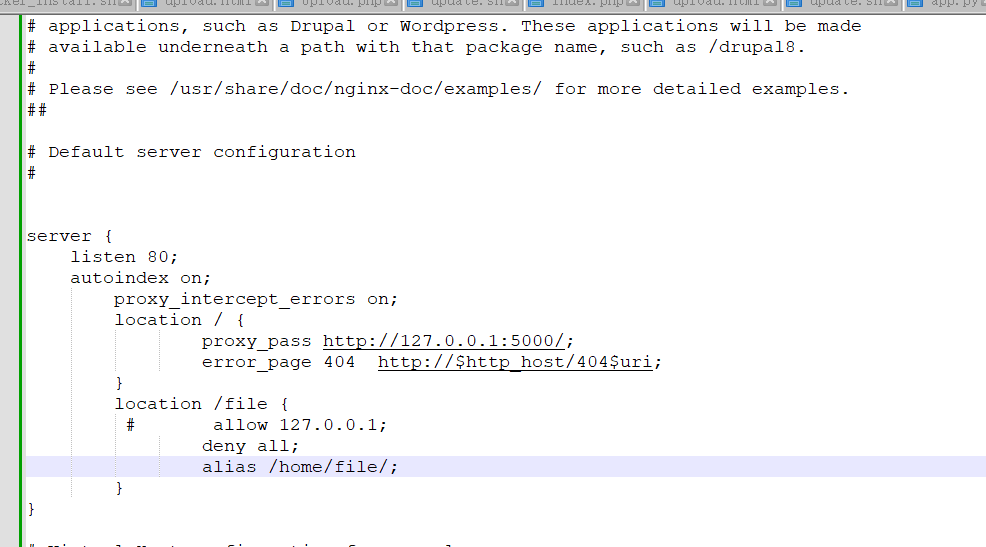
分析python代码和nginx配置，发现可能存在如下代理利用：

http://eci-2zea6nnim10n6ojijb4h.cloudeci1.ichunqiu.com/url?url=http://127.0.0.1/file/，该代码可能绕过仅允许本地访问/home/file文件夹，所以采取修改nginx配置的方式。





注释掉 /etc/nginx/sites-enabled/default 文件中的allow 127.0.0.1，拒绝所有访问/file路径请求即可。



### 如该题使用自己编写的脚本代码请详细写出，不允许截图

|  |
| --- |
| **update.sh**  mv file2 /etc/nginx/sites-enabled/default  chmod 644 /etc/nginx/sites-enabled/default  **file2**  **##**  **# You should look at the following URL's in order to grasp a solid understanding**  **# of Nginx configuration files in order to fully unleash the power of Nginx.**  **# https://www.nginx.com/resources/wiki/start/**  **# https://www.nginx.com/resources/wiki/start/topics/tutorials/config\_pitfalls/**  **# https://wiki.debian.org/Nginx/DirectoryStructure**  **#**  **# In most cases, administrators will remove this file from sites-enabled/ and**  **# leave it as reference inside of sites-available where it will continue to be**  **# updated by the nginx packaging team.**  **#**  **# This file will automatically load configuration files provided by other**  **# applications, such as Drupal or Wordpress. These applications will be made**  **# available underneath a path with that package name, such as /drupal8.**  **#**  **# Please see /usr/share/doc/nginx-doc/examples/ for more detailed examples.**  **##**  **# Default server configuration**  **#**  **server {**  **listen 80;**  **autoindex on;**  **proxy\_intercept\_errors on;**  **location / {**  **proxy\_pass http://127.0.0.1:5000/;**  **error\_page 404 http://$http\_host/404$uri;**  **}**  **location /file {**  **# allow 127.0.0.1;**  **deny all;**  **alias /home/file/;**  **}**  **}**  **# Virtual Host configuration for example.com**  **#**  **# You can move that to a different file under sites-available/ and symlink that**  **# to sites-enabled/ to enable it.**  **#**  **#server {**  **# listen 80;**  **# listen [::]:80;**  **#**  **# server\_name example.com;**  **#**  **# root /var/www/example.com;**  **# index index.html;**  **#**  **# location / {**  **# try\_files $uri $uri/ =404;**  **# }** |