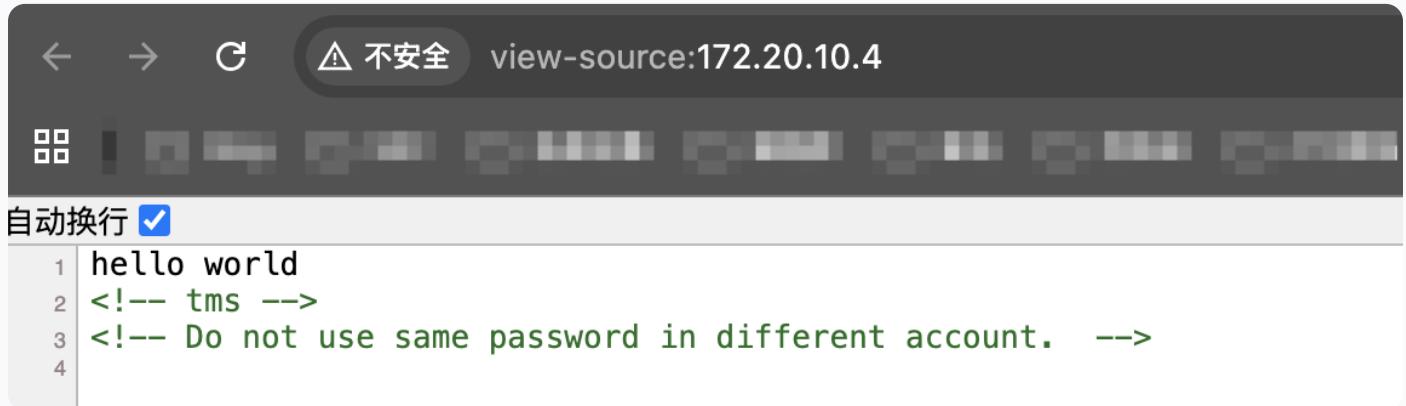


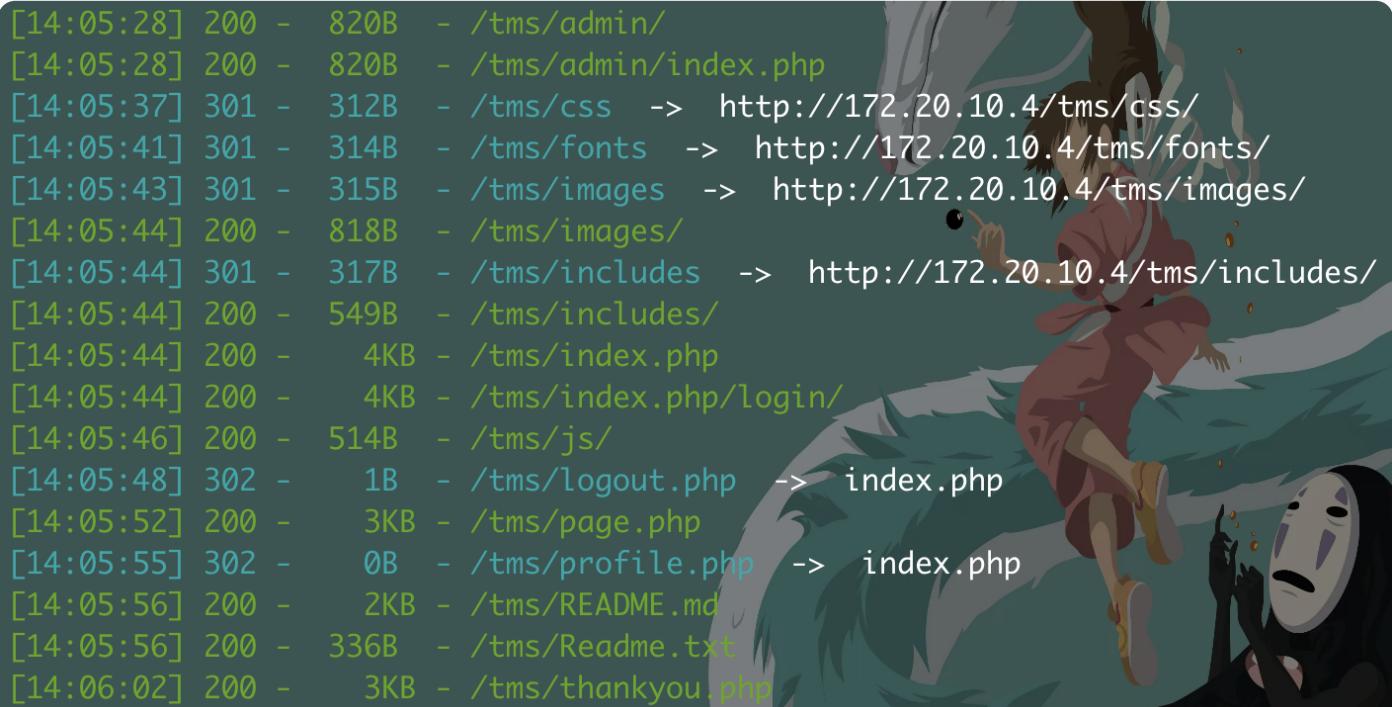
信息收集

查看源码



```
1 hello world
2 <!-- tms -->
3 <!-- Do not use same password in different account. -->
4
```

目录扫描



```
[14:05:28] 200 - 820B - /tms/admin/
[14:05:28] 200 - 820B - /tms/admin/index.php
[14:05:37] 301 - 312B - /tms/css -> http://172.20.10.4/tms/css/
[14:05:41] 301 - 314B - /tms/fonts -> http://172.20.10.4/tms/fonts/
[14:05:43] 301 - 315B - /tms/images -> http://172.20.10.4/tms/images/
[14:05:44] 200 - 818B - /tms/images/
[14:05:44] 301 - 317B - /tms/includes -> http://172.20.10.4/tms/includes/
[14:05:44] 200 - 549B - /tms/includes/
[14:05:44] 200 - 4KB - /tms/index.php
[14:05:44] 200 - 4KB - /tms/index.php/login/
[14:05:46] 200 - 514B - /tms/js/
[14:05:48] 302 - 1B - /tms/logout.php -> index.php
[14:05:52] 200 - 3KB - /tms/page.php
[14:05:55] 302 - 0B - /tms/profile.php -> index.php
[14:05:56] 200 - 2KB - /tms/README.md
[14:05:56] 200 - 336B - /tms/Readme.txt
[14:06:02] 200 - 3KB - /tms/thankyou.php
```

README.md

```
← → C △ 不安全 172.20.10.4/tms/README.md ⌂ ☆  
# Tourism-Management-System  
  
_____  
Installation Steps(Configuration)  
_____  
1. Download and Unzip file on your local system.  
2.Copy tms folder and tms folder inside root directory (for xampp xampp/htdocs, for wamp wamp/www, for lamp var/www/html)  
  
_____  
Database Configuration  
  
Open phpmyadmin  
Create Database tms  
Import database tms.sql (available inside zip package)Open Your browser put inside browser ↗  
http://localhost/tms  
  
//////////\|||||  
Login Details for admin :  
Open Your browser put inside browser ↗ http://localhost/tms/admin  
  
Username : admin  
  
Password : Test@123  
  
//////////\|||||  
  
Login Details for user:  
Open Your browser put inside browser ↗ http://localhost/tms/  
  
Username : anuj@gmail.com  
  
Password : Test@123  
  
|||||||  
  
_____  
Screen Short  
![Screenshot 2022-03-08 at 8 03 04 PM](https://user-images.githubusercontent.com/54598380/157259105-06bf9333-74a6-434c-9c75-f409957e7a8a.png)  
![Screenshot 2022-03-08 at 8 02 31 PM](https://user-images.githubusercontent.com/54598380/157259124-6b5dc12a-5fca-420e-9dca-e26ab1234718.png)  
![Screenshot 2022-03-08 at 8 02 23 PM](https://user-images.githubusercontent.com/54598380/157259131-7739c156-e542-4e23-8f32-63e8d356e602.png)  
![Screenshot 2022-03-08 at 8 02 13 PM](https://user-images.githubusercontent.com/54598380/157259136-bf10adaf-c641-4743-8cc1-fc6a2414d4d4.png)  
![Screenshot 2022-03-08 at 8 07 26 PM](https://user-images.githubusercontent.com/54598380/157259740-70228ad8-0b42-4c97-99a8-e678954076ac.png)  
![Screenshot 2022-03-08 at 8 07 35 PM](https://user-images.githubusercontent.com/54598380/157259746-a37391f8-405d-41ec-a07b-be540f60e6f4.png)
```

Readme.txt

```
← → C △ 不安全 172.20.10.4/tms/Readme.txt ⌂ ☆  
  
Installation Steps(Configuration)  
1. Download and Unzip file on your local system.  
2.Copy tms folder and tms folder inside root directory (for xampp xampp/htdocs, for wamp wamp/www, for lamp var/www/html)  
  
Database Configuration  
  
Open phpmyadmin  
Create Database tms  
Import database tms.sql (available inside zip package)  
Open Your browser put inside browser "http://localhost/tms"  
  
Login Details for admin :  
Open Your browser put inside browser "http://localhost/tms/admin"  
Username : admin  
Password : Test@123  
  
Login Details for user:  
Open Your browser put inside browser "http://localhost/tms/"  
Username : anuj@gmail.com  
Password : Test@123
```

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: 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](#)

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

[Q IP查询](#) [Q 域名查询](#) [■ HASH解密](#) [■ MD5加密](#) [◀ 字符串转换](#)

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