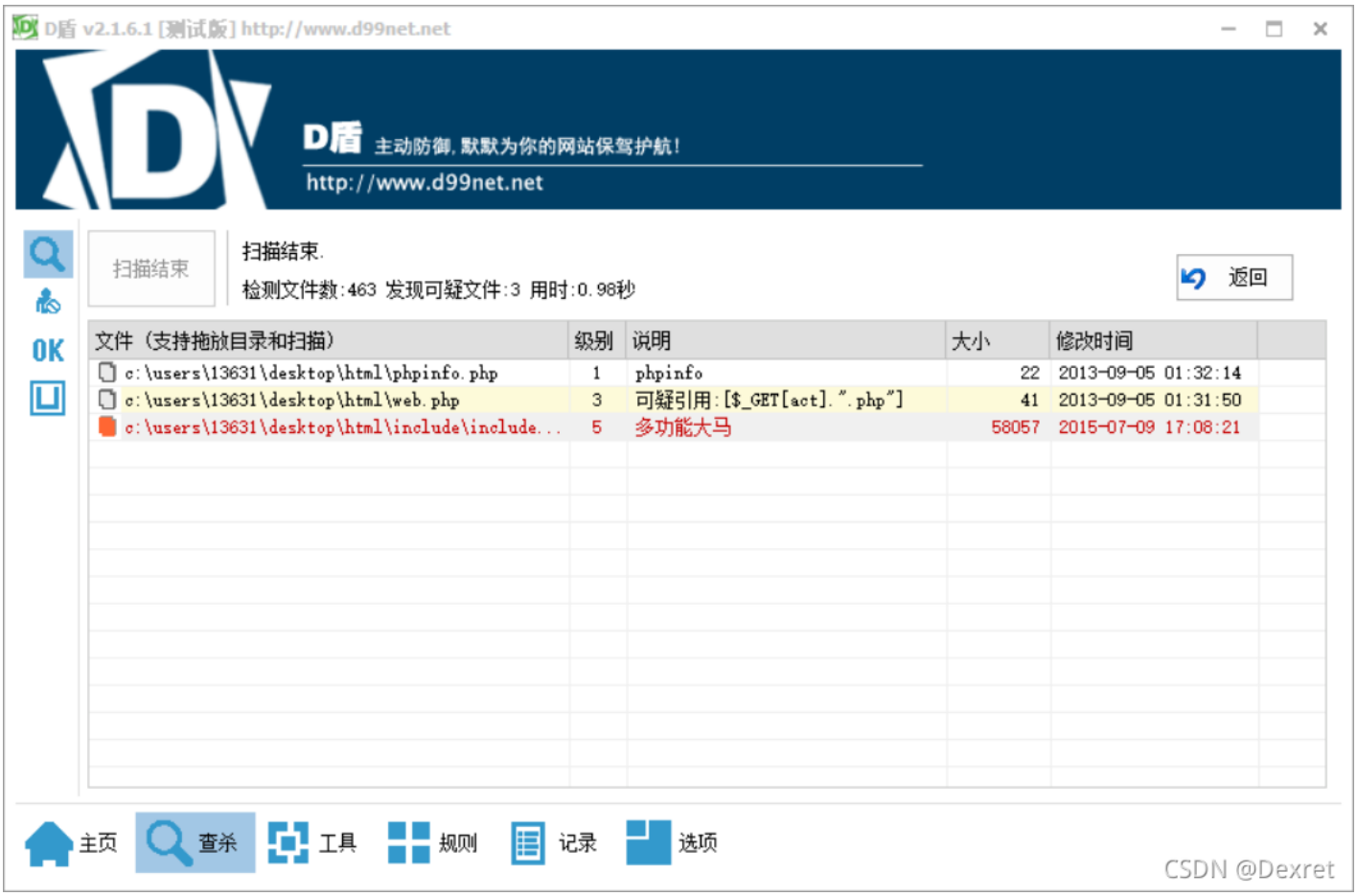
Buuctf 后门查杀

原创

Dexret 于 2021-11-18 20:56:43 发布 93 收藏
分类专栏： Buuctf Misc 文章标签： 安全 php

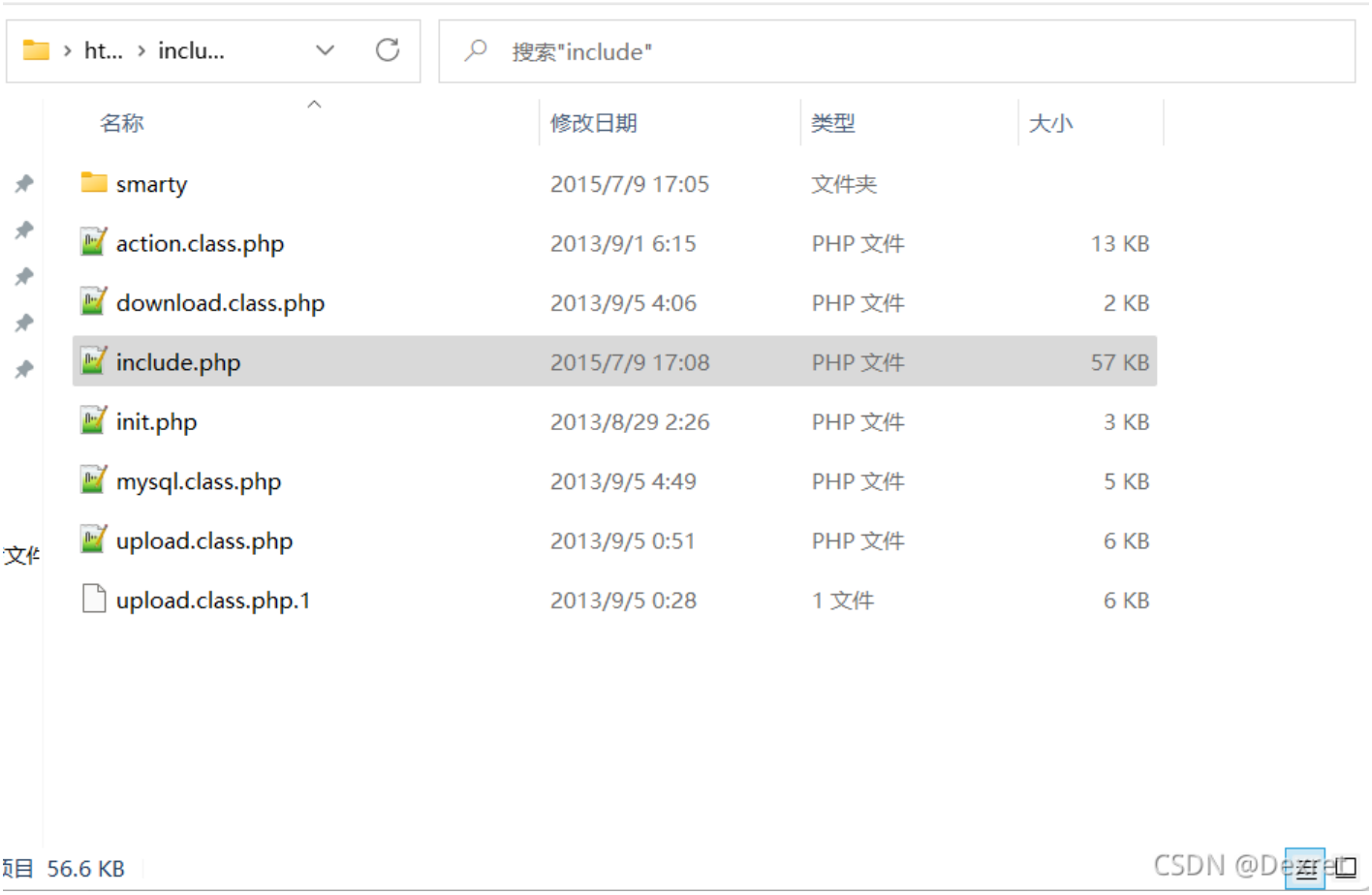
下载该文件，发现该文件为一个网站的源码，结合题意让我们找出该网站的webshell

既然是找webshell，那么直接用查杀软件D盾来扫描该网站源码



成功找到一个多功能大马，可以判断该木马为webshell

打开该目录下的网页源码include.php



对源码进行代码审计

```php
$P = $_POST;
unset($_POST);
/*====================== 程序配置 ======================*/

//echo encode_pass('angel');exit;
// 如果需要密码验证,请修改登陆密码,留空为不需要验证
$pass  = '6ac45fb83b3bc355c024f5034b947dd3'; //angel

//如您对 cookie 作用范围有特殊要求，或登录不正常，请修改下面变量，否则请保持默认
// cookie 前缀
$cookiepre = '';
// cookie 作用域
$cookiedomain = '';
// cookie 作用路径
$cookiepath = '/';
// cookie 有效期
$cookielife = 86400;

/*====================== 配置结束 ======================*/

$charsetdb = array(
```


发现一段md5，结合题意说flag为md5

可以判断该题的flag为：

```
flag{6ac45fb83b3bc355c024f5034b947dd3}
```