

当网站服务器被入侵时，我们需要一款Webshell检测工具，来帮助我们发现webshell，进一步排查系统可能存在的安全漏洞。

本文推荐了10款Webshell检测工具，用于网站入侵排查。当然，目前市场上的很多主机安全产品也都提供这种WebShell检测能力，比如阿里云、青藤云、safedog等，本文暂不讨论。

## 1、D盾\_Web查杀

阿D出品，使用自行研发不分扩展名的代码分析引擎，能分析更为隐藏的WebShell后门行为。

兼容性：只提供Windows版本。

工具下载地址：[http://www.d99net.net/down/WebShellKill\\_V2.0.9.zip](http://www.d99net.net/down/WebShellKill_V2.0.9.zip)



## 2、百度WEBDIR+

下一代WebShell检测引擎，采用先进的动态监测技术，结合多种引擎零规则查杀。

兼容性：提供在线查杀木马，免费开放API支持批量检测。

在线查杀地址：<https://scanner.baidu.com/>

# 在线查杀木马

Q. 都可以上传什么类型的文件?

A. 我们支持的文件类型有 `php`, `phtml`, `inc`, `php3`, `php4`, `php5`, `war`, `jsp`, `jspx`, `asp`, `aspx`, `cer`, `cdx`, `asa`, `ashx`, `asmx`, `cfm`  
我们支持的压缩包有 `rar`, `zip`, `tar`, `xz`, `tbz`, `tgz`, `tbz2`, `bz2`, `gz`

Q. 这个服务是免费的吗?

A. 是的, 目前不收费, 也不限制上传数量

Q. WEBDIR+ 都会对文件做哪些操作?

A. 上传后的文件或者压缩包, 会经过WEBDIR+三种引擎的检测, 检测后文件会被立即删除, 全程无人工介入

Q. WEBDIR+ 是如何检测木马的?

A. 传统的正则表达式方式, 存在高误报、低查杀率的问题, WEBDIR+采用先进的动态监测技术, 结合多种引擎零规则查杀

→ **Drop files** to upload  
(or click)

请先点击上方区域选择文件

## 3、河马

专注webshell查杀研究, 拥有海量webshell样本和自主查杀技术, 采用传统特征+云端大数据双引擎的查杀技术。查杀速度快、精度高、误报低。

兼容性: 支持Windows、linux, 支持在线查杀。

官方网站: <https://www.shellpub.com/>



#### 4、Web Shell Detector

Webshell Detector具有“Webshell”签名数据库，可帮助识别高达99%的“Webshell”。

兼容性：提供php/python脚本，可跨平台，在线检测。

官方网站：<http://www.shelldetector.com/>

github项目地址：<https://github.com/emposha/PHP-Shell-Detector>

## Web Shell Detector v1.66 (PHP Version: 5.4.45)

Starting file scanner, please be patient file scanning can take some time.

Number of known shells in database is: 603

Files found: 12

File scan done, we have: 12 files to analyze

### Suspicious behavior found in: if.php

Full path:	if.php
Owner:	0
Permission:	0666
Last accessed:	07:33:51 06/04/2020
Last modified:	12:51:14 23/01/2018
MD5 hash:	1f276a4a127fa68e221c951db5212e16
Filesize:	166 B
suspicious functions used:	eval ( <a href="#">line:6</a> );
Fingerprint:	<b>Negative</b> (if wrong <a href="#">submit file for analyze</a> )

**Status:** 1 suspicious files found and 0 shells found. [Rescan and show suspicious files](#)

## 5、CloudWalker ( 牧云 )

一个可执行的命令行版本 Webshell 检测工具。目前，项目已停止更新。

兼容性，提供linux版本，Windows 暂不支持。

在线查杀demo：<https://webshellchop.chaitin.cn/>

github项目地址：<https://github.com/chaitin/cloudwalker>

```
Last login: Sat Sep 29 11:43:51 on tty000
cyrus@localhost ~/GoWebshellDetector/bin ? bin release ./detector -path ~/GoWebshellDetector/sample/test
```

# CloudWalker 1.0

2018/09/29 11:44:52 Detector started.

[+] 00000010 /Users/cyrus/GoWebshellDetector/sample/test/0ab6fd32.php	Risk:1
[+] 00000012 /Users/cyrus/GoWebshellDetector/sample/test/0c578edb.php	Risk:1
[+] 00000021 /Users/cyrus/GoWebshellDetector/sample/test/15c3629b.php	Risk:4
[+] 00000027 /Users/cyrus/GoWebshellDetector/sample/test/1af84356.php	Risk:1
[+] 00000032 /Users/cyrus/GoWebshellDetector/sample/test/1de39874.php	Risk:1
[+] 00000034 /Users/cyrus/GoWebshellDetector/sample/test/1eab02f4.php	Risk:1
[+] 00000040 /Users/cyrus/GoWebshellDetector/sample/test/29f763ed.php	Risk:1
[+] 00000041 /Users/cyrus/GoWebshellDetector/sample/test/2a85cfb0.php	Risk:4
[+] 00000043 /Users/cyrus/GoWebshellDetector/sample/test/2b7fc086.php	Risk:5
[+] 00000046 /Users/cyrus/GoWebshellDetector/sample/test/2ce169b7.php	Risk:4
[+] 00000074 /Users/cyrus/GoWebshellDetector/sample/test/43d689b5.php	Risk:5
[+] 00000077 /Users/cyrus/GoWebshellDetector/sample/test/4630e127.php	Risk:1
[+] 00000089 /Users/cyrus/GoWebshellDetector/sample/test/578b2c41.php	Risk:4
[+] 00000098 /Users/cyrus/GoWebshellDetector/sample/test/5ec46db2.php	Risk:5
[+] 00000111 /Users/cyrus/GoWebshellDetector/sample/test/69d4fe58.php	Risk:4
[+] 00000114 /Users/cyrus/GoWebshellDetector/sample/test/7240a53f.php	Risk:5
[+] 00000117 /Users/cyrus/GoWebshellDetector/sample/test/76805fa3.php	Risk:1
[+] 00000118 /Users/cyrus/GoWebshellDetector/sample/test/79d26e40.php	Risk:3
[+] 00000129 /Users/cyrus/GoWebshellDetector/sample/test/8c246f19.php	Risk:5
[+] 00000132 /Users/cyrus/GoWebshellDetector/sample/test/8ef364a7.php	Risk:4
[+] 00000133 /Users/cyrus/GoWebshellDetector/sample/test/8ef59b67.php	Risk:4
[+] 00000137 /Users/cyrus/GoWebshellDetector/sample/test/90b5f832.php	Risk:4
[+] 00000140 /Users/cyrus/GoWebshellDetector/sample/test/9abel705.php	Risk:4
[+] 00000147 /Users/cyrus/GoWebshellDetector/sample/test/a54bc389.php	Risk:1
[+] 00000153 /Users/cyrus/GoWebshellDetector/sample/test/ac1e0569.php	Risk:4
[+] 00000156 /Users/cyrus/GoWebshellDetector/sample/test/aedf0b57.php	Risk:5
[+] 00000157 /Users/cyrus/GoWebshellDetector/sample/test/b2381c76.php	Risk:1
[+] 00000178 /Users/cyrus/GoWebshellDetector/sample/test/c1972fa5.php	Risk:4
[+] 00000187 /Users/cyrus/GoWebshellDetector/sample/test/cd4b32e7.php	Risk:4
[+] 00000188 /Users/cyrus/GoWebshellDetector/sample/test/cd735fa0.php	Risk:5
[+] 00000189 /Users/cyrus/GoWebshellDetector/sample/test/cdb20365.php	Risk:1
[+] 00000195 /Users/cyrus/GoWebshellDetector/sample/test/d73f251a.php	Risk:4
[+] 00000205 /Users/cyrus/GoWebshellDetector/sample/test/de0837c2.php	Risk:4
[+] 00000212 /Users/cyrus/GoWebshellDetector/sample/test/e51376b8.php	Risk:5
[+] 00000215 /Users/cyrus/GoWebshellDetector/sample/test/e71a24d9.php	Risk:4
[+] 00000218 /Users/cyrus/GoWebshellDetector/sample/test/eab8f163.php	Risk:4
[+] 00000223 /Users/cyrus/GoWebshellDetector/sample/test/f3ca8061.php	Risk:1
[+] 00000227 /Users/cyrus/GoWebshellDetector/sample/test/f6bed102.php	Risk:3
[+] 00000231 /Users/cyrus/GoWebshellDetector/sample/test/fb3a7208.php	Risk:4
[+] 00000232 /Users/cyrus/GoWebshellDetector/sample/test/fc2a7b19.php	Risk:4

Testing fe0752dc.php / 40 risks / Runtime 22.50753517ss

2018/09/29 11:45:15 Risk (level1): 12

2018/09/29 11:45:15 Risk (level2): 0

2018/09/29 11:45:15 Risk (level3): 2

2018/09/29 11:45:15 Risk (level4): 18

2018/09/29 11:45:15 Risk (level5): 8

2018/09/29 11:45:15 Detector done (22.508249887s).

cyrus@localhost ~/GoWebshellDetector/bin ? bin release

## 6、Sangfor WebShellKill

Sangfor WebShellKill(网站后门检测工具)是一款web后门专杀工具，不仅支持webshell的扫描，同时还支持暗链的扫描。是一款融合了多重检测引擎的查杀工具。能更精准地检测出WEB网站已知和未知的后门文件。

兼容性：支持Windows、linux

工具下载地址：[http://edr.sangfor.com.cn/backdoor\\_detection.html](http://edr.sangfor.com.cn/backdoor_detection.html) (已停止访问)



## 7、深度学习模型检测PHP Webshell

一个深度学习PHP webshell查杀引擎demo，提供在线样本检测。

在线查杀地址：<http://webshell.cdxy.me/>

# Deep Learning model for PHP webshell detection

注：请求过于频繁会响应"429 Too Many Requests"，请控制在3QPS以内

Paste your php code here. Example: `<?php eval($_GET['shell'])?>`

Or upload sample with CURL:

```
`curl http://webshell.cdxy.me/api -F file=@webshell.php`
```

Or give it ALIAS:

```
`alias dwd='_a(){ curl http://webshell.cdxy.me/api -F file=@$1; }; _a'`  
`dwd webshell.php`
```

Submit

## 8、PHP Malware Finder

PHP-malware-finder 是一款优秀的检测webshell和恶意软件混淆代码的工具

兼容性：提供linux版本，Windows 暂不支持。

github项目地址：<https://github.com/jvoisin/php-malware-finder>

```
root@kali:~/php-malware-finder# yara -r ./php.yar ./webshell/
./php.yar(95): warning: $pr contains .* or .+, consider using .{,N} or .{1,N} with a reasonable value for N
DodgyPhp ./webshell//dama.php
NonPrintableChars ./webshell//phpdama.php
ObfuscatedPhp ./webshell//phpdama.php
DodgyPhp ./webshell//phpdama.php
DangerousPhp ./webshell//phpdama.php
SuspiciousEncoding ./webshell//phpdama.php
DodgyStrings ./webshell//phpdama.php
ObfuscatedPhp ./webshell//x.php
DodgyPhp ./webshell//x.php
DangerousPhp ./webshell//x.php
SuspiciousEncoding ./webshell//x.php
DodgyStrings ./webshell//x.php
```

## 9、findWebshell

这个项目是一款基于python开发的webshell检查工具，可以根据特征码匹配检查任意类型的webshell后门。

github项目地址：<https://github.com/he1m4n6a/findWebshell>

```
root@kali:~/findWebshell# python main.py -h
Usage: main.py [options]

Options:
  -h, --help                show this help message and exit
  -p PATH, --path=PATH      input web directory filepath
  -o OUTPUT, --output=OUTPUT
                             create a html report
  -e php|asp|aspx|jsp|all, --ext=php|asp|aspx|jsp|all
                             define what's file format to scan
```

## 10、在线webshell查杀工具

在线查杀地址：<http://tools.bugscaner.com/killwebshell/>

### 在线webshell查杀-灭绝师太版

请选择需要查杀的php文件或标准zip压缩包(允许上传最大2M):

Customize.jsp

Remove

Browse ...

正在检测中,你只管抽烟喝茶泡妞看小说,剩下的交给我吧!

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。

