



安恒明鉴网站恶意代码检测系统云端登录地址为: <u>https://moedu.websaas.cn</u>

# 登录账户自行注册,注册后待管理员审核后即可使用(管理员最晚1天内会审核完毕),有问题可发邮件联系aqtb@moe.edu.cn

🗲 🛈 ณ https://183.131.1.166:6688/webshell/login	😻 🐹 🥝 🧕	Q. 百度 <ctrl+k></ctrl+k>	☆自Ⅰ	▶ ⋒
网站恶意代码检测系统    首页				
B B B B B B B B B B B B B B		用户登录 <sup>用户名</sup> huizhou 磁码 6pcp6 还没有账号?	<b>、<b>P</b>6 立即注册</b>	





#### 成功登录后点击左侧菜单栏中的"引擎下载选项"

♥ 概述 - 网站恶意代码检测系统 ×	+		
🗲 🛈 🖍 https://183.131.1.166:6688	8/webshell/overview	マ 器 C	☆ 自 ∔ 余
网站恶意代码检测系统	概述		(@)
■ 概述	Home / 概述		
<ul> <li>         ・ 引擎下载         <ul> <li></li></ul></li></ul>	未登录客户端工具	未扫描	0时0分0秒
☑ 深度分析结果	您最近一次登入IP为	最近一次扫描时间	最近一次扫描用时
Ⅰ 人工审核结果			
◆ 管理 >	0 威胁列表总数	0 家度分析确认数	0 人工审核确认数
	风险趋势		最近被篡改文件时间 TOP5







🖉 🦁 网站恶意代码检测系统 - 首页 🗙 🔪		
( i 🔒 https://183.131.1.166:668	webshell/download 🛛 😵 C 🛞 🤇 百度 < Ctrl+K > 🟠 自 🖡 🏠	9
网站恶意代码检测系统	概述	huizh
■ 概述	Home / 引擎下载	
▶ 引擎下载		
▲ 威胁列表	引擎下载	
☑ 深度分析结果	Windows Linux	
■ 人工审核结果	引擎下载	
◆管理 >	hgind Downlood 時間 Downlood 解 2000 中国 企業 (************************************	





# 下载后的压缩包文件 进入引擎文件夹, 启动恶意代码检测客户端 Cp.W/sSieanir au 文件解压 CpWsScan

₹ ► CpWsScan ►				
) 工具(T) 帮助(H)				
▼ 共享 ▼ 新建文件夹				
名称	修改日期	类型	大小	
🖟 logs	2017/9/28 10:18	文件夹		
📄 config.json	2017/8/8 12:59	JSON 文件	1 KB	
🛃 CpWsScan	2017/9/28 10:47	快捷方式	1 KB	
🚳 php7ts.dll	2017/8/3 13:27	应用程序扩展	4,582 KB	
Ø policy.xml	2017/7/31 15:44	HTML 文档	49 KB	
📰 settings.ini	2017/8/14 15:02	配置设置	1 KB	
🥃 update.exe	2017/8/14 9:20	应用程序	3,498 KB	
	2017/8/11 17:37	JSON 文件	1 KB	
🥥 wsclient.exe	2017/8/14 17:15	应用程序	3,928 KB	
sengine.exe	2017/8/14 12:33	应用程序	2,387 KB	
wsscanner.exe	2017/8/14 14:15	应用程序	10,240 KB	



## 第3步,运行查杀引擎进行扫描 WINDOWS查杀引擎使用说明

#### 输入用户名和密码登录查杀引擎



# 第3步,运行查杀引擎进行扫描







## 第3步,运行查杀引擎进行扫描 WINDOWS查杀引擎使用说明

#### 进入查杀过程,扫描完成后,扫描引擎会将可疑文件上传到云端,便于进一步深度检测和人工审核

◎明鉴◎网站	恶意代码	8检测工具			
扫描位置: C:\Users\xue	\Desktop\y	un\php 建议将网	示:为避免影响业务系 网站目录拷贝到其他 <b>朋</b>	系统的正 员务器上	
	: 45 [	■ 成肪文件: 39 (○)	发现威胁: 39 🕔 已用时	间: <mark>00:00</mark> :1	0
扫描对象	类型	描述	特征	危险等级	修改时间
C:\Users\xue\Desktop'	РНР	异常内容	create_function{ base64_d	紧急	2017-04-19 07:32:18
C:\Users\xue\Desktop'	PHP	异常内容:可疑的危险函数	exec	中危	2017-04-19 07:32:18
C:\Users\xue\Desktop'	РНР	异常内容:可疑的危险函数	shell_exec	中危	2017-04-19 07:32:18
C:\Users\xue\Desktop'	PHP	异常内容:PHP常见一句ì	eval{ gzinflate( }	紧急	2017-04-19 07:32:18
C:\Users\xue\Desktop'	РНР	异常内容	create_function{ gzinflate(	紧急	2017-04-19 07:32:18
C:\Users\xue\Desktop'	РНР	异常内容:可疑的危险函数	exec	中危	2017-04-19 07:32:18
C:\Users\xue\Desktop'	РНР	异常内容:PHP常见一句ì	eval{ gzinflate( }	紧急	2017-04-19 07:32:18
C:\Users\xue\Desktop'	РНР	异常内容:PHP常见一句ì	eval{ gzinflate( }	紧急	2017-04-19 07:32:18
C:\Users\xue\Desktop'	РНР	异常内容	create_function{ gzinflate(	紧急	2017-04-19 07:32:18
C·\LIsers\xue\Deskton'	РНР	县堂内容	create function{ gzinflate(	医争	2017-04-19 07:32:18

当前版本:v2.0.1.0

Powered By Dbappsecurity Ltd.



## 第3步,运行查杀引擎进行扫描 Linux查杀引擎使用说明

- 步骤一:到平台上下载linux客户端wsscaner.zip
- 步骤二:将wsscaner.zip上传到linux服务器上任意路径,我这里放在/home下
- 步骤三: cd /home
  - unzip wsscaner.zip
  - cd wsscaner
  - chmod 755 wsscanner
  - ./wsscanner

## **第3步,运行查杀引擎进行扫描** Linux查杀引擎使用说明



步骤四:执行以上命令后,跳出下面的界面,输入平台的用户名密码

步骤五:验证成功后,输入网站程序所在的路径(要扫描的路径),按回车执行

步骤六:自动执行扫描,进入扫描过程,等待完成后按ctrl+x退出

「提示─── |:按ctrl+x键退出程序

「统计信息─── |扫描对象数:1

发现威胁数:0 扫描用时:00:00:00

扫描: 扫描结束

100%

## 风险提示:为避免影响业务系统的正 常运行,建议将网站目录拷贝到其他 服务器上进行扫描操作



### **DBAPP** 安恒信息

#### 安恒明鉴网站恶意代码检测系统云端登录地址为: <u>https://moedu.websaas.cn</u>

🗲 🛈 🐔 https://183.131.1.166:6688/webshell/login	🦁 🗱 🖸	8	<b>Q</b> 百度 <ctrl+k></ctrl+k>	☆自	÷	î î
网站恶意代码检测系统						
B			用户登录 <sup>用户名</sup> huizhou 密码 •••• 验证码 6pcp6 还没有账号?	<b>срб</b> 立即注册		

# 第4步,登录网站恶意代码检测系统查看扫描结果 查看威胁列表



#### 点击左侧菜单栏的"威胁列表"查看扫描结果

网站恶意代码检测系统	概	怸										🥘 admin ~
● 概述	Ho	ome	/ 威胆	警告按钮	<b>同以讲行</b> 下畫	均扫描	动象文	件、杳	看详情、	提交深	度分析	f、提交人
≛ 引擎下载		篡改E	日期:	「 宙 校	删除笙撮作	ч I I I I I I I I I I I I I I I I I I I		扫描时间:	нинк			
◇ 威胁列表		开始	时间	「日心く」	加川小丁工和编制			开始时间		至	结束时间	
☑ 深度分析结果		深度分	分析:		人工审核:	文件来源: 不限		关键字: ▼ 「高级神索·1#前标	<del>。 #米</del> 刑#文性夕			
		-1 PK			, The second sec	1 14		· [IPI%(3C3C4)"+12	2", <del>2</del> .", <b>2</b> ."		$\mathbf{i}$	
◎ 待审核列表			深度分	析 🖻 人工审核	▲上传文件							• 2 ≧ ≣.
□ 数据展示	Г	_		CEAL					签订口台		112 <del>-1</del>	
			-	所属甲位  ▼	扫描灯家    ₹	特征数	类型  ♥	又1午米源 ♥	暴仪日期  ▼	扫描町目 ♥	次念 -	操作口
		+		杭州安恒	make2.php	1	PHP	云检测	2017-04-19 07:32:18	2017-08-16 17:47:39	… 深度分析 … 人工检测	
		+		杭州安恒	dev_core.php	2	PHP	云检测	2017-04-19 07:32:18	2017-08-16 17:47:39	… 深度分析 … 人工检测	2 🗉 2 🖻 🕯
		+		杭州安恒	b374k-2.6.php	2	PHP	云检测	2017-04-19 07:32:18	2017-08-16 17:47:39	深度分析 人工检测	1 2 2 1
		+		杭州安恒	b374k-2.8.source.php	5	PHP	云检测	2017-04-19	2017-08-16 17:47:39	深度分析 人工检测	2 🗉 🛛 🖻 👔
		+		杭州安恒	b374k-2.5.source.php	4	PHP	云检测	2017-04-19 07:32:18	2017-08-16 17:47:39	深度分析 人工检测	* • • •
		+		杭州安恒	b374k-2.6.source.php	2	PHP	云检测	2017-04-19 07:32:18	2017-08-16 17:47:39	… 深度分析 … 人工检测	1 2 2 1
		+		杭州安恒	b374k-2.4.php	15	PHP	云检测	2017-04-19 07:32:18	2017-08-16 17:47:39	深度分析 人工检测	± = 2 ē i
		+		杭州安恒	b374k-3.2.3.php	8	PHP	云检测	2017-04-19 07:32:18	2017-08-16 17:47:39	深度分析 人工检测	1 2 2 1
		+		杭州安恒	b374k-2.2.php	12	PHP	云检测	2017-04-19	2017-08-16	深度分析 人工检测	1 2 2 1

# **第4步,登录网站恶意代码检测系统查看扫描结果** 手动上传可疑文件



**DB** ΔP

网站恶意代码检测系统	概述												🥘 xue1 ~
■ 概述	Home / 威胁列表												
➡ 引擎下载	篡改日期:				扫描时间:								
∽ 威胁列表	开始时间	至结束时间			开始时间				至结束时	间			
☑ 深度分析结果	深度分析:	人工审核:	文件来源:		关键字:								
➡ 人工审核结果		▼ 小限	▼ 11限	•	[高级搜索:]#单位	2#类型#文件名						( 4 単)	间 ,
<b>夺</b> 管理 >	☑ 深度分析	<b>こ</b> 上传文件 よ 导出报告	■ 删除								C	<b>C</b> 3	:≡ -
	□ 扫描对象		特征数	类型 🔶	文件来源	篡改日期	\$ ž	日描时间	♦  状态	♦ 操作项			
				没有	找到匹配的记录								

## 第4步,登录网站恶意代码检测系统查看扫描结果 扫描结果查询



### 可通过篡改日期、扫描时间、深度分析、人工审核、危害等级和关键字查询检测结果

Hom	ne /	/ <del></del>	检测										
篡改日期: 开始时间 至 结束时间							扫描明	时间:	结束时间	≠ R+1间			
深不	开始时间     王 结束时间       深度分析:     人工审核:     危害等级:       不限     不限     请选择								Q 查询				
	<ul> <li>☑ 深度分析</li> <li>亘 人工审核</li> <li>■ 删除</li> <li>● ① ② ③ Ⅲ ▼</li> </ul>												
			单位  🍦	扫描对象	特征数	类 🝦	描述  🍦	篡改日期    🍦	扫描时间	状态	操作项		
+	•		杭州	Class_Dzl_Fso.asp	1	ASP	异常内容:使用 了FSO的 CreateTextFil e OpenTextF	2017-05-04 10:40:39	2017-06-07 13:22:22	… 深度分 析 … 人工检	* = 2 9 •		

## 如需获得更多操作指引请详阅"安恒明鉴恶意代码检测系统用户手册"

