

一次利用谷歌语法渗透公网弱目标实例

黑白之道 2019-08-11

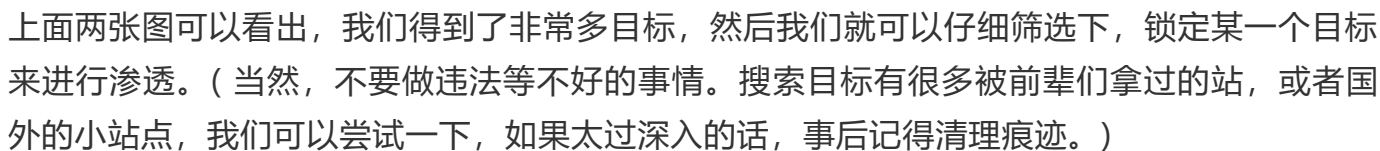


相信大家对谷歌语法都不陌生，这里不得不吐槽下我自己，虽然我很早就学习了一点谷歌语法，但从未进行过实践，然后时间久了也忘记了。有位朋友一直使用谷歌语法很有心得，终于在他的感染下我前几天又重新学习和研究了一下谷歌语法，发现是真的好用，感觉打开了新世界的大门。废话有点多了，接下来进入正题，利用谷歌语法最简单的一句，就可以得到许多公网的弱目标站点，轻轻松松就可以拿到一些webshell甚至服务器权限。

首先我们打开谷歌输入搜索语句：

index of / "phpinfo.php"
(或者inurl:/phpinfo.php)





我们随便打开一个目标来看一下：

Index of /

- [Parent Directory](#)
- [RuleConvert.php](#)
- [debugz.php](#)
- [newrules.txt](#)
- [phpinfo.php](#)
- [testmail.php](#)




基本上都是直接暴出目录，然后我们就可以来翻它的目录，来分析有没有可以利用的文件之类的。

然后两三分钟我就找出一个特别容易入侵的目标：

> ↺ 🏠 ⓘ 不安全 | ██████████ phpinfo.php

Hub - w11097...


PHP Version 5.0.4



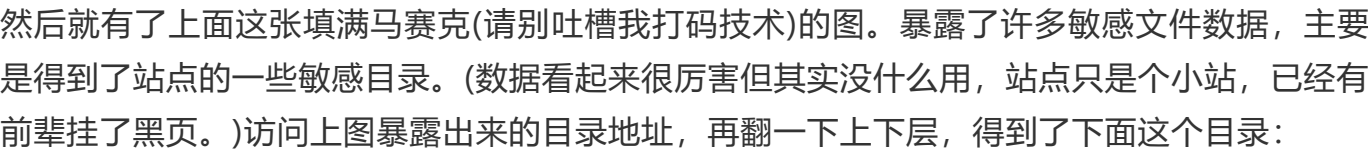
System	Windows NT MMDWEB 6.2 build 9200
Build Date	Mar 31 2005 02:44:34
Configure Command	██████████ /usr/sbin/apr-util snapshot-build" "--with-gu-sniareu
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows\php.ini
PHP API	20031224
PHP Extension	20041030
Zend Extension	220040412
Debug Build	no
Thread Safety	enabled
IPv6 Support	enabled
Registered PHP Streams	php, file, http, ftp, compress.zlib
Registered Stream Socket Transports	tcp, udp

This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.0.4-dev, Copyright (c) 1998-2004 Zend Technologies
















Powered By



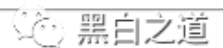
既然 phpinfo.php 在，那我就想它或许有其他敏感文件。那就直接用 site:www.xxxx.com来看下这个站的其他目录。



Index of /

Name	Last modified	Size	Description
 Parent Directory		-	
 DatePicker.js	23-Jul-2007 08:21	21K	
 notes/	22-Apr-2019 13:25	-	
 addFile.php.bak	01-Jun-2011 13:57	3.8K	
 edit.php	28-Feb-2011 14:49	971	
 edit.php.bak	28-Feb-2011 14:49	971	
 editor/	22-Apr-2019 13:25	-	
 files/	01-Aug-2019 19:12	-	
 images/	22-Apr-2019 13:25	-	
 insertFile.php	28-Feb-2011 15:18	1.2K	
 insertFile.php.bak	28-Feb-2011 15:18	1.2K	
 showCode.php	26-Oct-2011 09:08	3.0K	
 showCode.php.bak	26-Oct-2011 09:08	3.0K	
 showCode_zy.php	28-Feb-2011 16:01	1.7K	
 showCode_zy.php.bak	28-Feb-2011 16:01	1.7K	

Apache/2.0.54 (Win32) PHP/5.0.4 Server at t 80



然后我们打开addfile.php.bak这个文件，发现直接就是个上传文件点并告诉你上传后的路径：

← → ↻ 🏠 ⓘ 不安全 | www. .php.bak

🔍 97...

选择档案	<input type="button" value="选择文件"/> 未选择任何文件
文件中文名称	<input type="text"/>
文件时间	<input type="text" value="2019-08-01"/>
<input type="button" value="确定上传"/> <input type="button" value="查看发布给首页的代码"/>	

※注1: 请勿使用中文档名!!!

※注2: 档案上传后路径写法: 名称

※注3: News档案上传大小不得超过10MB

你上传了文件:

文件的 MIME 类型为:

上传文件大小(bytes):

黑白之道

直接上传一句话:

选择档案	<input type="button" value="选择文件"/> 1.php
文件中文名称	<input type="text" value="11111"/>
文件时间	<input type="text" value="2019-08-01"/>
<input type="button" value="确定上传"/> <input type="button" value="查看发布给首页的代码"/>	

※注1: 请勿使用中文档名!!!

※注2: 档案上传后路径写法: 当案名称

※注3: News档案上传大小不得超过10MB

你上传了文件:

文件的 MIME 类型为:

上传文件大小(bytes):

黑白之道

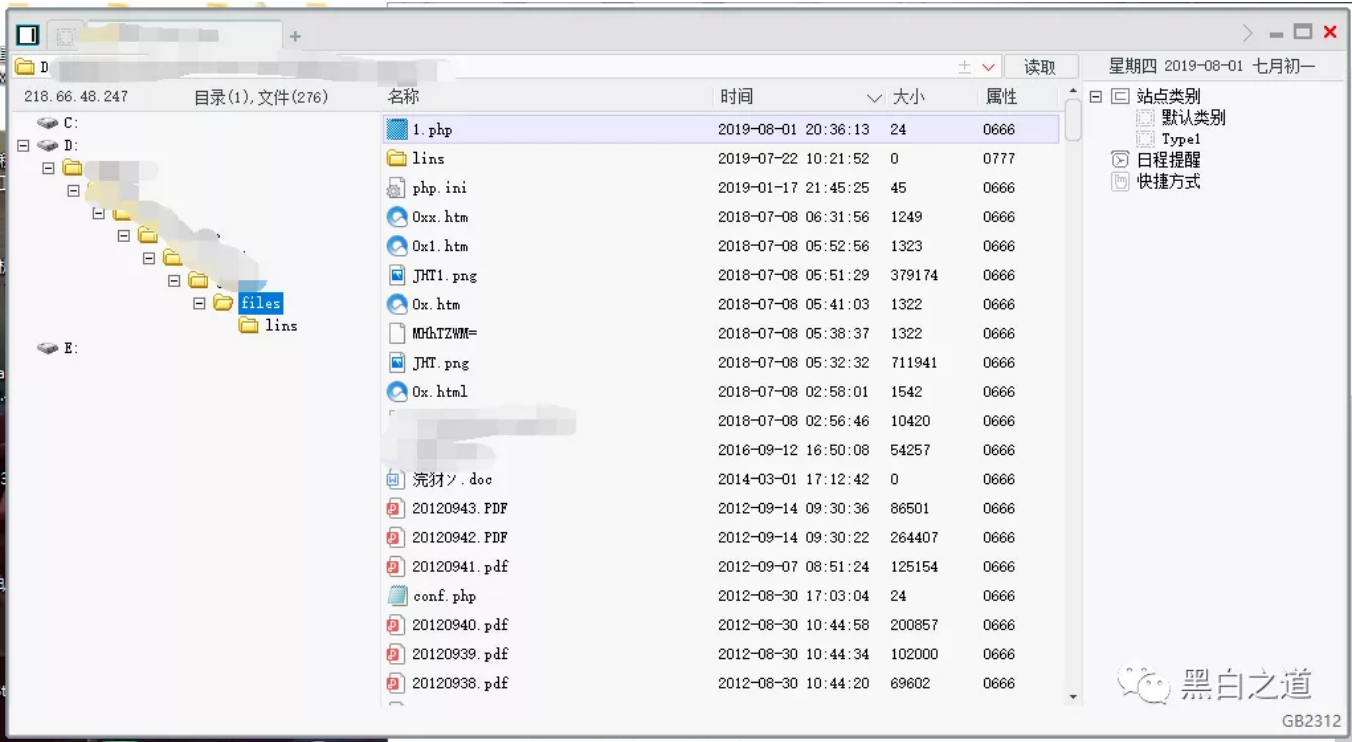
没有任何过滤, 上传成功。我们打开上传路径, 没有被杀。

Index of /

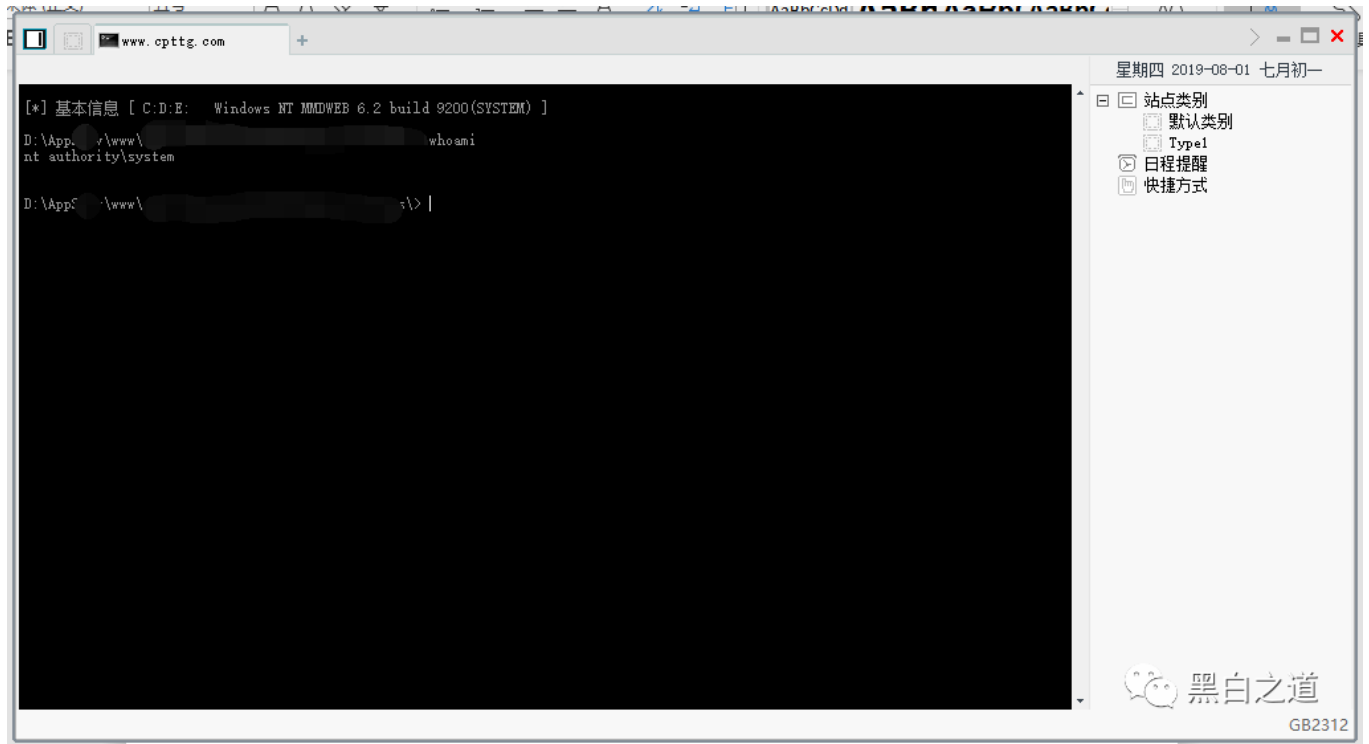
Name	Last modified	Size	Description
Parent Directory	-		
1.php	01-Aug-2019 20:36	24	
lins/	22-Jul-2019 10:21	-	
php.ini	17-Jan-2019 21:45	45	
Oxx.htm	08-Jul-2018 06:31	1.2K	
Ox1.htm	08-Jul-2018 05:52	1.3K	
JHT1.png	08-Jul-2018 05:51	370K	
Ox.htm	08-Jul-2018 05:41	1.3K	
MHhTZWM=	08-Jul-2018 05:38	1.3K	
JHT.png	08-Jul-2018 05:32	695K	
Ox.html	08-Jul-2018 02:58	1.5K	
307848656c6c2e6a7067	08-Jul-2018 02:56	10K	
[REDACTED]	12-Sep-2016 16:50	53K	
浣材ノ.doc	01-Mar-2014 17:12	0	
20120943.PDF	14-Sep-2012 09:30	84K	
20120942.PDF	14-Sep-2012 09:30	258K	
20120941.pdf	07-Sep-2012 08:51	122K	
conf.php	30-Aug-2012 17:03	24	
20120940 - 36	20-Aug-2012 10:44	102K	

黑白之道

直接菜刀连接，成功。



试试CMD，这个权限我就不多说了：



好了，这次分享就到这里结束。有没有发现想要wellshell非常简单？只要你有时间，使用最简单的谷歌语法就可以让你有无数的目标来进行练手。（当然不要做危险、违法的事情）。

所以我建议大家可以多学习一下谷歌语法，百度就可以搜到许多基础教程。其实语句就那么几句，但是套路是非常多的，主要靠你的脑洞。这次分享的只是谷歌语法的入门操作，可以说任何人看一下都能够学会，但是谷歌语法远不止如此，利用它能够做的事情非常多，需要大家多多去发掘。

最后给出一些比较基础和常见的语法，如果是初学者有兴趣可以尝试一下：

对公网的语法：

Index of /password

Index of / passwd

"index?of/" xxx?(mp3、 pdf)

"Index of /" password.txt

inurl:login

inurl:php?id=1

inurl:baidu.com

inurl:phpMyAdmin

inurl:ewebeditor

intitle:后台管理

intitle:后台管理 inurl:admin

对限定域名的语法：

site:xxxx.com

site:xxxx.com intext:管理

site:xxxx.com inurl:login

site:xxxx.com intitle:管理

site:xxxx.com intext:电话 //N个电话

site:a2.xxxx.com inurl:file(load)//上传点等

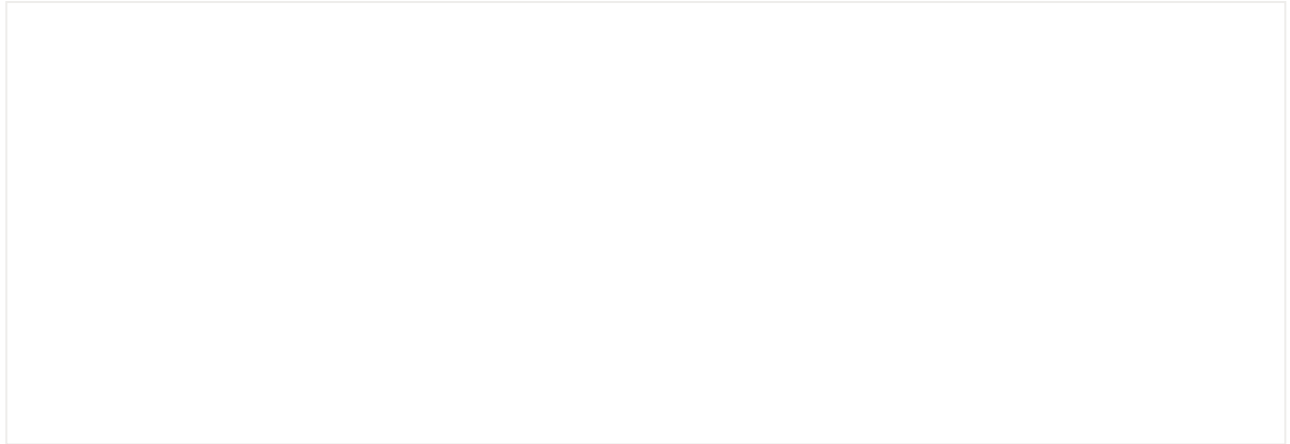
site:a2.xxxx.com intext:ftp://(地址、password等)

site:xxxx.com filetype: txt (doc docx xls xlsx等)

site:a2.xxxx.com filetype:asp(jsp php aspx等)//看看网站跑的什么脚本

site:xxxx.com intext:*@xxxx.com //得到邮件地址，还有邮箱的主人信息之类的

仅供学习研究使用，否则后果自负



[阅读原文](#)