

渗透测试工具

原创

[aweiname2008](#) 已于 2022-02-21 14:01:28 修改 3271 收藏 3

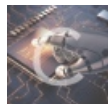
分类专栏: [渗透测试](#) 文章标签: [渗透测试](#)

于 2021-11-20 14:10:49 首次发布

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/aweiname2008/article/details/121438783>

版权



[渗透测试](#) 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

漏洞及渗透练习平台:

WebGoat漏洞练习平台:

<https://github.com/WebGoat/WebGoat>

webgoat-legacy漏洞练习平台:

<https://github.com/WebGoat/WebGoat-Legacy>

zuldirl漏洞练习平台:

<https://github.com/710leo/ZVulDrill>

vulapps漏洞练习平台:

<https://github.com/Medicean/VulApps>

dwa漏洞练习平台:

<https://github.com/RandomStorm/DVWA>

数据库注入练习平台:

<https://github.com/Audi-1/sqli-labs>

用node编写的漏洞练习平台, like OWASP Node Goat:

<https://github.com/cr0hn/vulnerable-node>

Ruby编写的一款工具, 生成含漏洞的虚拟机:

<https://github.com/cliffe/secgen>

花式扫描器:

Nmap端口扫描器:

<https://github.com/nmap/nmap>

本地网络扫描器:

<https://github.com/SkyLined/LocalNetworkScanner>

子域名扫描器:

<https://github.com/lijejie/subDomainsBrute>

<https://github.com/aboul3la/Sublist3r>

<https://github.com/TheRook/subbrute>

<https://github.com/infosec-au/altdns>

linux漏洞扫描:

<https://github.com/future-architect/vuls>

基于端口扫描以及关联CVE:

<https://github.com/m0nad/HellRaiser>

漏洞路由扫描器:

<https://github.com/jh00nbr/Routerhunter-2.0>

送你惊喜信自泄漏扫描脚本。

https://github.com/lijiejie/BBScan

Waf类型检测工具:

https://github.com/EnableSecurity/wafw00f

服务器端口弱口令扫描器:

https://github.com/wilson9x1/fenghuangscanner_v3

Fox-scan扫描器:

https://github.com/fengxuangit/Fox-scan/

信息搜集工具:

社工收集器:

https://github.com/n0tr00t/Sreg

Github信息搜集:

https://github.com/sea-god/gitscan

github Repo信息搜集工具:

https://github.com/metac0rtex/GitHarvester

信息探测及扫描工具:

https://github.com/darryllane/Bluto

内部网络信息扫描器:

https://github.com/sowish/LNScan

远程桌面登录扫描器:

https://github.com/linuz/Sticky-Keys-Slayer

网络基础设施渗透工具

https://github.com/SECFORCE/sparta

SNMAP密码破解:

https://github.com/SECFORCE/SNMP-Brute

WEB:

webshell大合集:

https://github.com/tennc/webshell

免杀webshell生成脚本:

https://github.com/yzddmr6/webshell-venom

渗透以及web攻击脚本:

https://github.com/brianwrf/hackUtils

web渗透小工具大合集:

https://github.com/rootphantomer/hacktoolsfor_me

XSS数据接收平台:

https://github.com/firesunCN/BlueLotus_XSSReceiver

XSS与CSRF工具:

https://github.com/evilcos/xssor

xss多功能扫描器:

https://github.com/shawarkhanethicalhacker/BruteXSS

web漏洞扫描器:

https://github.com/andresriancho/w3af

WEB漏洞扫描器:

https://github.com/sullo/nikto

渗透常用小工具包:

https://github.com/leonteale/pentestpackage

web目录扫描器:

https://github.com/maurosoria/dirsearch

web向命令注入检测工具:

https://github.com/stasinopoulos/commix

自动化SQL注入检查工具:

<https://github.com/epinna/tplmap>

SSL扫描器:

<https://github.com/rbsec/ssllscan>

安全工具集合:

<https://github.com/codejanus/ToolSuite>

apache日志分析器:

<https://github.com/mthbernares/ARTLAS>

php代码审计工具:

<https://github.com/pwnsdx/BadCode>

web指纹识别扫描:

<https://github.com/urbanadventurer/whatweb>

检查网站恶意攻击:

<https://github.com/ciscococsirt/malspider>

wordpress漏洞扫描器:

<https://github.com/wpscanteam/wpscan>

固件漏洞扫描器:

https://github.com/misterch0c/firminator_backend

数据库注入工具

<https://github.com/sqlmapproject/sqlmap>

Web代理:

<https://github.com/zt2/sqli-hunter>

新版中国菜刀:

<https://github.com/Chora10/Cknife>

git泄露利用EXP:

<https://github.com/lijiejie/GitHack>

浏览器攻击框架:

<https://github.com/beefproject/beef>

自动化绕过WAF脚本:

<https://github.com/khalibijou/WAFNinja>

<https://github.com/owtf/wafbypasser>

一款开源WAF:

<https://github.com/SpiderLabs/ModSecurity>

http命令行客户端:

<https://github.com/jkbrzt/httpie>

浏览器调试利器:

<https://github.com/firebug/firebug>

DISCUZ漏洞扫描器:

<https://github.com/code-scan/dzscan>

自动化代码审计工具

<https://github.com/wufeifei/cobra>

浏览器攻击框架:

<https://github.com/julienbedard/browsersploit>

tomcat自动后门部署:

<https://github.com/mgeeky/tomcatWarDeployer>

网络空间指纹扫描器:

<https://github.com/nanshihui/Scan-T>

burpsuit之J2EE扫描插件:

<https://github.com/ilmila/J2EEScan>

windows域渗透工具:

获取明文及哈希:

<https://github.com/gentilkiwi/mimikatz>

Powershell渗透库合集:

<https://github.com/PowerShellMafia/PowerSploit>

Powershell tools合集:

<https://github.com/clymb3r/PowerShell>

powershell的mimikittenz:

<https://github.com/putterpanda/mimikittenz>

域渗透教程:

https://github.com/l3m0n/pentest_study

Fuzz:

Web向Fuzz工具

<https://github.com/xmendez/wfuzz>

HTTP暴力破解, 撞库攻击脚本

<https://github.com/lijiejie/httpwdScan>

漏洞利用及攻击框架:

msf框架:

<https://github.com/rapid7/metasploit-framework>

pocsscan攻击框架:

<https://github.com/erevus-cn/pocscan>

Pocsuite攻击框架:

<https://github.com/knownsec/Pocsuite>

Beebeeto攻击框架:

<https://github.com/n0tr00t/Beebeeto-framework>

漏洞POC&EXP:

ExploitDB官方git版本:

<https://github.com/offensive-security/exploit-database>

php漏洞代码分析:

<https://github.com/80vul/phpcodz>

CVE-2016-2107:

<https://github.com/FiloSottile/CVE-2016-2107>

CVE-2015-7547 POC:

<https://github.com/fjserna/CVE-2015-7547>

JAVA反序列化POC生成工具:

<https://github.com/frohoff/ysoserial>

JAVA反序列化EXP:

<https://github.com/foxglovesec/JavaUnserializeExploits>

Jenkins CommonCollections EXP:

<https://github.com/CaledoniaProject/jenkins-cli-exploit>

CVE-2015-2426 EXP (windows内核提权):

<https://github.com/Vlad902/hacking-team-windows-kernel-lpe>

use docker to show web attack(PHP本地文件包含结合phpinfo getshell 以及ssrf结合curl的利用演示):

<https://github.com/hxer/vulnapp>

php7缓存覆写漏洞Demo及相关工具:

<https://github.com/GoSecure/php7-opcache-override>

XcodeGhost木马样本:

<https://github.com/XcodeGhostSource/XcodeGhost>

中间人攻击及钓鱼

中间人攻击框架:

<https://github.com/secretsquirrel/the-backdoor-factory>

<https://github.com/secretsquirrel/BDFProxy>

<https://github.com/42h122d2r/MTM4>

<https://github.com/DylanD33d3r/lanlani>

Inject code, jam wifi, and spy on wifi users:

<https://github.com/DanMcInerney/LANs.py>

中间人代理工具:

<https://github.com/intrepidusgroup/mallory>

wifi钓鱼:

<https://github.com/sophron/wifiphisher>

密码破解:

密码破解工具:

<https://github.com/shinnok/johnny>

本地存储的各类密码提取利器:

<https://github.com/AlessandroZ/LaZagne>

二进制及代码分析工具:

二进制分析工具

<https://github.com/devttys0/binwalk>

系统扫描器

<https://github.com/quarkslab/binmap>

rp:

<https://github.com/0vercl0k/rp>

Windows Exploit Development工具

<https://github.com/lillypad/badger>

二进制静态分析工具 (python):

<https://github.com/bdcht/amoco>

Python Exploit Development Assistance for GDB:

<https://github.com/longld/peda>

对BillGates Linux Botnet系木马活动的监控工具

<https://github.com/ValdikSS/billgates-botnet-tracker>

木马配置参数提取工具:

<https://github.com/kevthehermit/RATDecoders>

Shellphish编写的二进制分析工具 (CTF向):

<https://github.com/angr/angr>

针对python的静态代码分析工具:

<https://github.com/yinwang0/pysonar2>

一个自动化的脚本 (shell) 分析工具, 用来给出警告和建议:

<https://github.com/koalaman/shellcheck>

基于AST变换的简易Javascript反混淆辅助工具:

<https://github.com/ChiChou/etacsufbo>

EXP编写框架及工具:

二进制EXP编写工具:

<https://github.com/t00sh/rop-tool>

CTF Pwn 类题目脚本编写框架:

<https://github.com/Gallopsled/pwntools>

an easy-to-use io library for pwning development:

<https://github.com/zTrix/zio>

跨平台注入工具:

<https://github.com/frida/frida>

哈希长度扩展攻击EXP:

<https://github.com/citronneur/rdpy>

隐写:

隐写检测工具

<https://github.com/abeluck/stegdetect>

各类安全资料:

data_hacking合集:

https://github.com/ClickSecurity/data_hacking

mobile-security-wiki:

<https://github.com/exploitprotocol/mobile-security-wiki>

书籍《reverse-engineering-for-beginners》:

<https://github.com/veficos/reverse-engineering-for-beginners>

一些信息安全标准及设备配置:

https://github.com/luyg24/IT_security

APT相关笔记:

<https://github.com/kbandla/APTnotes>

Kcon资料:

<https://github.com/knownsec/KCon>

《DO NOT FUCK WITH A HACKER》:

<https://github.com/citypw/DNFVAH>

各类安全脑洞图:

<https://github.com/phiith0n/Mind-Map>

信息安全流程图:

<https://github.com/SecWiki/sec-chart/tree/294d7c1ff1eba297fa892dda08f3c05e90ed1428>

各类CTF资源

近年ctf writeup大全:

<https://github.com/ctfs/write-ups-2016>

<https://github.com/ctfs/write-ups-2015>

<https://github.com/ctfs/write-ups-2014>

fbctf竞赛平台Demo:

<https://github.com/facebook/fbctf>

ctf Resources:

<https://github.com/ctfs/resources>

ctf及黑客资源合集:

<https://github.com/bt3gl/My-Gray-Hacker-Resources>

ctf和安全工具大合集:

<https://github.com/zardus/ctf-tools>

ctf向 python工具包

<https://github.com/P1kachu/v0lt>

各类编程资源:

大礼包（什么都有）:

<https://github.com/bayandin/awesome-awesomeness>

bash-handbook:

<https://github.com/denysdovhan/bash-handbook>

python资源大全:

<https://github.com/jobbole/awesome-python-cn>

git学习资料:

<https://github.com/xirong/my-git>

安卓开源代码解析

<https://github.com/android-cn/android-open-project>

python框架, 库, 资源大合集:

<https://github.com/vinta/awesome-python>

JS 正则表达式库（用于简化构造复杂的JS正则表达式）:

<https://github.com/VerbalExpressions/JSVerbalExpressions>

Python:

python 正则表达式库（用于简化构造复杂的python正则表达式）：

<https://github.com/VerbalExpressions/>

python任务管理以及命令执行库：

<https://github.com/pyinvoke/invoke>

python exe打包库：

<https://github.com/pyinstaller/pyinstaller>

Veil-Evasion免杀项目：

<https://github.com/Veil-Framework/Veil-Evasion>

py3 爬虫框架：

<https://github.com/orf/cyborg>

一个提供底层接口数据包编程和网络协议支持的python库：

<https://github.com/CoreSecurity/impacket>

python requests 库：

<https://github.com/kennethreitz/requests>

python 实用工具合集：

<https://github.com/mahmoud/boltions>

python爬虫系统：

<https://github.com/binux/pyspider>

福利：

微信自动抢红包动态库

<https://github.com/east520/AutoGetRedEnv>

微信抢红包插件（安卓版）

<https://github.com/geeeeeeeek/WeChatLuckyMoney>

hardsed神器：

<https://github.com/yangyangwithgnu/hardseed>

甲方安全工程师生存指南

web索引及日志搜索工具：

<https://github.com/thomaspatzke/WASE>

开源日志采集器：

<https://github.com/wgliang/logcool>

扫描CS结构的web debugger

<https://github.com/Kozea/wdb>

恢复sqlite数据库删除注册信息：

<https://github.com/aramosf/recoversqlite/>

gps欺骗检测工具：

<https://github.com/zxsecurity/gpsnitch>

应急处置响应框架：

<https://github.com/biggiesmallAG/nightHawkResponse>

web安全开发指南：

<https://github.com/FallibleInc/security-guide-for-developers>

各个知名厂商漏洞测试报告模板：

<https://github.com/juliocesarfort/public-pentesting-reports>

linux下恶意代码检测包：

<https://github.com/rfxn/linux-malware-detect>

操作系统运行指标可视化框架：

<https://github.com/facebook/osquery>

恶意代码分析系统：

<https://github.com/cuckoosandbox/cuckoo>

定期搜索及存储web应用：

<https://github.com/Netflix/Scumblr>

事件响应框架

事件响应框架:

<https://github.com/google/grr>

综合主机监控检测平台:

<https://github.com/ossec/ossec-hids>

分布式实时数字取证系统:

<https://github.com/mozilla/mig>

Microsoft & Unix 文件系统及硬盘取证工具:

<https://github.com/sleuthkit/sleuthkit>

蜜罐:

SSH蜜罐:

<https://github.com/desaster/kippo>

蜜罐集合资源:

<https://github.com/paralax/awesome-honeypots>

kippo进阶版蜜罐:

<https://github.com/micheloosterhof/cowrie>

SMTP 蜜罐:

<https://github.com/awhitehatter/mailoney>

web应用程序蜜罐:

<https://github.com/mushorg/glastopf>

数据库蜜罐:

<https://github.com/jordan-wright/elasticshoney>

web蜜罐:

<https://github.com/atiger77/Dionaea>

远控:

用gmail充当C&C服务器的后门

<https://github.com/byt3bl33d3r/gcat>

开源的远控:

<https://github.com/UbbeLoL/uRAT>

c#远控:

<https://github.com/hussein-aitlahcen/BlackHole>