漏洞及渗透练习平台

转载

小白白@ 于 2019-03-28 12:29:28 发布 3378 收藏 15

漏洞及渗透练习平台：

WebGoat漏洞练习环境

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

Damn Vulnerable Web Application(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

花式扫描器： 端口扫描器Nmap 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/lijiejie/subDomainsBrute

漏洞路由扫描器 https://github.com/jh00nbr/Routerhunter-2.0

迷你批量信息泄漏扫描脚本 https://github.com/lijiejie/BBScan

Waf类型检测工具 https://github.com/EnableSecurity/wafw00f

信息搜集工具 : 社工插件，可查找以email、phone、username的注册的所有网站账号信息 https://github.com/n0tr00t/Sreg

Github信息搜集，可实时扫描查询git最新上传有关邮箱账号密码信息 https://github.com/sea-god/gitscan

github Repo信息搜集工具 https://github.com/metac0rtex/GitHarvester

WEB： webshell大合集 https://github.com/tennc/webshell

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/hack_tools_for_me

XSS数据接收平台 https://github.com/firesunCN/BlueLotus_XSSReceiver

XSS与CSRF工具 https://github.com/evilcos/xssor

Short for command injection exploiter，web向命令注入检测工具 https://github.com/stasinopoulos/commix

数据库注入工具 https://github.com/sqlmapproject/sqlmap

Web代理，通过加载sqlmap api进行sqli实时检测 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/khalilbijjou/WAFNinja

http命令行客户端，可以从命令行构造发送各种http请求（类似于Curl） https://github.com/jkbrzt/httpie

浏览器调试利器 https://github.com/firebug/firebug

一款开源WAF https://github.com/SpiderLabs/ModSecurity

windows域渗透工具： windows渗透神器 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

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/htpwdScan

漏洞利用及攻击框架： msf https://github.com/rapid7/metasploit-framework

Poc调用框架，可加载Pocsuite,Tangscan，Beebeeto等 https://github.com/erevus-cn/pocscan

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

Beebeeto 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

Simple test for 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/byt3bl33d3r/MITMf

Inject code, jam wifi, and spy on wifi users https://github.com/DanMcInerney/LANs.py

可扩展的中间人代理工具 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，用于寻找程序和库然后收集他们的依赖关系，链接等信息 https://github.com/quarkslab/binmap

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（ Inject JavaScript to explore native apps on Windows, Mac, Linux, iOS and Android.）
https://github.com/frida/frida

隐写： 隐写检测工具 https://github.com/abeluck/stegdetect

各类安全资料: 域渗透教程 https://github.com/l3m0n/pentest_study

python security教程（原文链接http://www.primalsecurity.net/tutorials/python-tutorials/） https://github.com/smartFlash/pySecurity

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

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

《DO NOT FUCK WITH A HACKER》 https://github.com/citypw/DNFWAH

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

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-analysis

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/PythonVerbalExpressions

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

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/boltons

python爬虫系统 https://github.com/binux/pyspider

ctf向 python工具包 https://github.com/P1kachu/v0lt