Penetration_Testing_POC-About 渗透测试有关的POC、EXP、脚本、提权、小工具等

原创

github导航师 于 2020-09-10 00:06:12 发布 3532 收藏 29
分类专栏： 网络安全 文章标签： 安全漏洞 thinkphp cms

Penetration_Testing_POC

搜集有关渗透测试中用到的POC、脚本、工具、文章等姿势分享，作为笔记吧，欢迎补充。

请善用搜索[Ctrl+F]查找

IOT Device&Mobile Phone

- 天翼创维awifi路由器存在多处未授权访问漏洞
- 华为WS331a产品管理页面存在CSRF漏洞
- CVE-2019-16313 蜂网互联企业级路由器v4.31密码泄露漏洞
- D-Link路由器RCE漏洞
- CVE-2019-13051-Pi-Hole路由端去广告软件的命令注入&权限提升
- D-Link DIR-859-RCE UnAutenticated (CVE-2019–17621)
- Huawei HG255 Directory Traversal[目录穿越]|本地备份文件
- D-Link Devices - Unauthenticated Remote Command Execution in ssdpcgi (Metasploit)CVE-2019-20215(Metasploit)
- 从 Interfaces.d 到 RCE：Mozilla WebThings IoT 网关漏洞挖掘
- 小米系列路由器远程命令执行漏洞（CVE-2019-18370，CVE-2019-18371）
- Intelbras Wireless N 150Mbps WRN240 - Authentication Bypass (Config Upload-未经验证即可替换固件)
- cve-2020-8634&cve-2020-8635|Wing FTP Server 6.2.3权限提升漏洞发现分析复现过程|Wing FTP Server 6.2.5权限提升
- CVE-2020-9374-TP LINK TL-WR849N - RCE
- CVE-2020-12753-LG 智能手机任意代码执行漏洞
- CVE-2020-12695-UPnP 安全漏洞
- 79款 Netgear 路由器遭远程接管0day
- dlink-dir610-exploits-Exploits for CVE-2020-9376 and CVE-2020-9377

Web APP

- 致远OA_A8_getshell_0day
- Couch through 2.0存在路径泄露漏洞
- Cobub Razor 0.7.2存在跨站请求伪造漏洞
- joyplus-cms 1.6.0存在CSRF漏洞可增加管理员账户
- MiniCMS 1.10存在CSRF漏洞可增加管理员账户
- Z-Blog 1.5.1.1740存在XSS漏洞
- YzmCMS 3.6存在XSS漏洞
- Cobub Razor 0.7.2越权增加管理员账户
- Cobub Razor 0.8.0存在SQL注入漏洞
- Cobub Razor 0.8.0存在物理路径泄露漏洞
- 五指CMS 4.1.0存在CSRF漏洞可增加管理员账户
- DomainMod的XSS集合
- GreenCMS v2.3.0603存在CSRF漏洞可获取webshell&增加管理员账户
- yii2-statemachine v2.x.x存在XSS漏洞
- maccms_v10存在CSRF漏洞可增加任意账号
- LFCMS 3.7.0存在CSRF漏洞可添加任意用户账户或任意管理员账户
- Finecms_v5.4存在CSRF漏洞可修改管理员账户密码
- Amazon Kindle Fire HD (3rd Generation)内核驱动拒绝服务漏洞
- Metinfo-6.1.2版本存在XSS漏洞&SQL注入漏洞
- Hucart cms v5.7.4 CSRF漏洞可任意增加管理员账号
- indexhibit cms v2.1.5 直接编辑php文件getshell
- S-CMS企业建站系统PHP版v3.0后台存在CSRF可添加管理员权限账号
- S-CMS PHP v3.0存在SQL注入漏洞
- MetInfoCMS 5.X版本GETSHELL漏洞合集
- discuz ml RCE 漏洞检测工具
- thinkphp5框架缺陷导致远程代码执行
- FineCMS_v5.0.8两处getshell
- Struts2_045漏洞批量检测|搜索引擎采集扫描
- thinkphp5命令执行
- typecho反序列化漏洞
- CVE-2019-10173 Xstream 1.4.10版本远程代码执行
- IIS/CVE-2017-7269-Echo-PoC
- CVE-2019-15107 Webmin RCE
- thinkphp5 rce漏洞检测工具
- thinkphp5_RCE合集
- thinkphp3.X-thinkphp5.x
- 关于ThinkPHP框架的历史漏洞分析集合
- CVE-2019-11510
- Redis(<=5.0.5) RCE
- Redis 4.x/5.x RCE（主从复制导致RCE）
- 生成Redis恶意模块so文件配合主从复制RCE达到命令执行|相关文章
- RedisWriteFile-通过 `Redis` 主从写出无损文件，可用于 `Windows` 平台下写出无损的 `EXE`、`DLL`、 `LNK` 和 `Linux` 下的 `OS` 等二进制文件
- WeblogicScanLot系列，Weblogic漏洞批量检测工具
- jboss_CVE-2017-12149
- Wordpress的拒绝服务（DoS）-CVE-2018-6389
- Webmin Remote Code Execution (authenticated)-CVE-2019-15642

- CVE-2019-16131 OKLite v1.2.25 任意文件上传漏洞
- CVE-2019-16132 OKLite v1.2.25 存在任意文件删除漏洞
- CVE-2019-16309 FlameCMS 3.3.5 后台登录处存在sql注入漏洞
- CVE-2019-16314 indexhibit cms v2.1.5 存在重装并导致getshell
- 泛微OA管理系统RCE漏洞利用脚本
- CVE-2019-16759 vBulletin 5.x 0day pre-auth RCE exploit
- zentao-getshell 禅道8.2 - 9.2.1前台Getshell
- 泛微 e-cology OA 前台SQL注入漏洞
- Joomla-3.4.6-RCE
- Easy File Sharing Web Server 7.2 - GET 缓冲区溢出 (SEH)
- 构建ASMX绕过限制WAF达到命令执行(适用于ASP.NET环境)
- CVE-2019-17662-ThinVNC 1.0b1 - Authentication Bypass
- CVE-2019-16278andCVE-2019-16279-about-nostromo-nhttpd
- CVE-2019-11043-PHP远程代码执行漏
- ThinkCMF漏洞全集和
- CVE-2019-7609-kibana低于6.6.0未授权远程代码命令执行
- ecologyExp.jar-泛微ecology OA系统数据库配置文件读取
- freeFTP1.0.8-'PASS'远程缓冲区溢出
- rConfig v3.9.2 RCE漏洞
- apache_solr_rce
- CVE-2019-7580 thinkcmf-5.0.190111后台任意文件写入导致的代码执行
- Apache Flink任意Jar包上传导致远程代码执行
- 用于检测JSON接口令牌安全性测试
- cve-2019-17424 nipper-ng_0.11.10-Remote_Buffer_Overflow远程缓冲区溢出附PoC
- CVE-2019-12409_Apache_Solr RCE
- Shiro RCE (Padding Oracle Attack)
- CVE-2019-19634-class.upload.php <= 2.0.4任意文件上传
- Apache Solr RCE via Velocity Template Injection
- CVE-2019-10758-mongo-express before 0.54.0 is vulnerable to Remote Code Execution
- CVE-2019-2107-Android播放视频-RCE-POC(Android 7.0版本，7.1.1版本，7.1.2版本，8.0版本，8.1版本，9.0版本)
- CVE-2019-19844-Django重置密码漏洞(受影响版本:Django master branch,Django 3.0,Django 2.2,Django 1.11)
- CVE-2019-17556-unsafe-deserialization-in-apache-olingo(Apache Olingo反序列化漏洞，影响: 4.0.0版本至4.6.0版本)
- ZZCMS201910 SQL Injections
- WDJACMS1.5.2模板注入漏洞
- CVE-2019-19781-Remote Code Execution Exploit for Citrix Application Delivery Controller and Citrix Gateway
- CVE-2019-19781.nse---use Nmap check Citrix ADC Remote Code Execution
- Mysql Client 任意文件读取攻击链拓展
- CVE-2020-5504-phpMyAdmin注入(需要登录)
- CVE-2020-5509-Car Rental Project 1.0版本中存在远程代码执行漏洞
- CryptoAPI PoC CVE-2020-0601|另一个PoC for CVE-2020-0601
- New Weblogic RCE (CVE-2020-2546、CVE-2020-2551) CVE-2020-2546|WebLogic WLS核心组件RCE分析（CVE-2020-2551）|CVE-2020-2551-Weblogic IIOP 反序列化EXP
- CVE-2020-5398 - RFD(Reflected File Download) Attack for Spring MVC
- PHPOK v5.3&v5.4getshell | phpok V5.4.137前台getshell分析 | PHPOK 4.7从注入到getshell
- thinkphp6 session 任意文件创建漏洞复现 含POC --- 原文在漏洞推送公众号上
- ThinkPHP 6.x反序列化POP链（一）|原文链接
- ThinkPHP 6.x反序列化POP链（二）|原文链接
- ThinkPHP 6.x反序列化POP链（三）|原文链接
- WordPress InfiniteWP - Client Authentication Bypass (Metasploit)

- 【Linux提权/RCE】OpenSMTPD 6.4.0 < 6.6.1 - Local Privilege Escalation + Remote Code Execution
- CVE-2020-7471-django1.11-1.11.282.2-2.2.103.0-3.0.3 StringAgg(delimiter)使用了不安全的数据会造成SQL注入漏洞环境和POC
- CVE-2019-17564 : Apache Dubbo反序列化漏洞
- CVE-2019-2725(CNVD-C-2019-48814、WebLogic wls9-async)
- YzmCMS 5.4 后台getshell
- 关于Ghostcat(幽灵猫CVE-2020-1938漏洞)：CNVD-2020-10487(CVE-2020-1938), tomcat ajp 文件读取漏洞poc|Java版本POC|Tomcat-Ajp协议文件读取漏洞|又一个python版本CVE-2020-1938漏洞检测|CVE-2020-1938-漏洞复现环境及EXP
- CVE-2020-8840：Jackson-databind远程命令执行漏洞（或影响fastjson）
- CVE-2020-8813-Cacti v1.2.8 RCE远程代码执行 EXP以及分析（需要认证/或开启访客即可不需要登录）(一款Linux是基于PHP,MySQL,SNMP及RRDTool开发的网络流量监测图形分析工具)|EXP|CVE-2020-8813MSF利用脚本
- CVE-2020-7246-PHP项目管理系统qdPM< 9.1 RCE
- CVE-2020-9547：FasterXML/jackson-databind 远程代码执行漏洞
- CVE-2020-9548：FasterXML/jackson-databind 远程代码执行漏洞
- Apache ActiveMQ 5.11.1目录遍历/ Shell上传
- CVE-2020-2555：WebLogic RCE漏洞POC|CVE-2020-2555-Weblogic com.tangosol.util.extractor.ReflectionExtractor RCE
- CVE-2020-1947-Apache ShardingSphere UI YAML解析远程代码执行漏洞
- CVE-2020-0554：phpMyAdmin后台SQL注入
- 泛微E-Mobile Ognl 表达式注入|表达式注入.pdf
- 通达OA RCE漏洞|通达OAv11.6版本RCE复现分析+EXP-EXP下载
- CVE-2020-10673-jackson-databind JNDI注入导致远程代码执行
- CVE-2020-10199、CVE-2020-10204漏洞一键检测工具，图形化界面（Sonatype Nexus <3.21.1）
- CVE-2020-2555-Oracle Coherence 反序列化漏洞|分析文章
- cve-2020-5260-Git凭证泄露漏洞
- 通达OA前台任意用户伪造登录漏洞批量检测
- CVE-2020-11890 JoomlaRCE <3.9.17 远程命令执行漏洞(需要有效的账号密码)
- CVE-2020-10238【JoomlaRCE <= 3.9.15 远程命令执行漏洞(需要有效的账号密码)】&CVE-2020-10239【JoomlaRCE 3.7.0 to 3.9.15 远程命令执行漏洞(需要有效的账号密码)】
- CVE-2020-2546，CVE-2020-2915 CVE-2020-2801 CVE-2020-2798 CVE-2020-2883 CVE-2020-2884 CVE-2020-2950 WebLogic T3 payload exploit poc python3|CVE-2020-2883-Weblogic coherence.jar RCE|WebLogic-Shiro-shell-WebLogic利用CVE-2020-2883打Shiro rememberMe反序列化漏洞，一键注册filter内存shell
- tongda_oa_rce-通达oa 越权登录+文件上传getshell
- CVE-2020-11651-SaltStack Proof of Concept【认证绕过RCE漏洞】|CVE-2020-11651&&CVE-2020-11652 EXP
- showdoc的api_page存在任意文件上传getshell
- Fastjson <= 1.2.47 远程命令执行漏洞利用工具及方法
- SpringBoot_Actuator_RCE
- jizhicms(极致CMS)v1.7.1代码审计-任意文件上传getshell+sql注入+反射XSS
- CVE-2020-9484：Apache Tomcat Session 反序列化代码执行漏洞|CVE-2020-9484：Apache Tomcat 反序列化RCE漏洞的分析和利用
- PHPOK 最新版漏洞组合拳 GETSHELL
- Apache Kylin 3.0.1命令注入漏洞
- weblogic T3 collections java InvokerTransformer Transformer InvokerTransformer weblogic.jndi.WLInitialContextFactory
- CVE-2020-5410 Spring Cloud Config目录穿越漏洞
- NewZhan CMS 全版本 SQL注入（0day）
- 盲注 or 联合？记一次遇见的奇葩注入点之SEMCMS3.9（0day）
- 从PbootCMS(2.0.3&2.0.7前台RCE+2.0.8后台RCE)审计到某狗绕过
- CVE-2020-1948 : Apache Dubbo 远程代码执行漏洞
- CVE-2020-5902-F5 BIG-IP 远程代代码执行（RCE）&任意文件包含读取|CVE-2020-5902又一EXP加测试docker文件
- CVE-2020-8193-Citrix未授权访问任意文件读取
- 通读审计之天目MVC_T框架带Home版(temmokumvc)_v2.01

- CVE-2020-14645-WebLogic 远程代码执行漏洞|Weblogic_CVE-2020-14645
- CVE-2020-6287-SAP NetWeaver AS JAVA 授权问题漏洞-创建用户EXP|SAP_RECON-PoC for CVE-2020-6287, CVE-2020-6286 (SAP RECON vulnerability)
- CVE-2018-1000861, CVE-2019-1003005 and CVE-2019-1003029-jenkins-rce
- CVE-2020-3452：Cisco ASA/FTD 任意文件读取漏洞
- 74CMS_v5.0.1后台RCE分析
- CVE-2020-8163 - Remote code execution of user-provided local names in Rails
- 【0day RCE】Horde Groupware Webmail Edition RCE
- pulse-gosecure-rce-Tool to test for existence of CVE-2020-8218
- Exploit for Pulse Connect Secure SSL VPN arbitrary file read vulnerability (CVE-2019-11510)
- Zblog默认Theme_csrf+储存xss+getshell

提权辅助相关

- windows-kernel-exploits Windows平台提权漏洞集合
- windows 溢出提权小记/本地保存了一份+Linux&Windows提取脑图
- Windows常见持久控制脑图
- CVE-2019-0803 Win32k漏洞提权工具
- 脏牛Linux提权漏洞
- 远控免杀从入门到实践之白名单（113个）|远控免杀从入门到实践之白名单（113个）总结篇.pdf
- Linux提权-CVE-2019-13272 A linux kernel Local Root Privilege Escalation vulnerability with PTRACE_TRACEME
- Linux权限提升辅助一键检测工具
- 将powershell脚本直接注入到进程中执行来绕过对powershell.exe的限制
- CVE-2020-2696 – Local privilege escalation via CDE dtsession
- CVE-2020-0683-利用Windows MSI “Installer service”提权
- Linux sudo提权辅助工具—查找sudo权限配置漏洞
- Windows提权-CVE-2020-0668：Windows Service Tracing本地提权漏洞
- Linux提取-Linux kernel XFRM UAF poc (3.x - 5.x kernels)2020年1月前没打补丁可测试
- linux-kernel-exploits Linux平台提权漏洞集合
- Linux提权辅助检测Perl脚本|Linux提权辅助检测bash脚本
- CVE-2020-0796 - Windows SMBv3 LPE exploit #SMBGhost|【Windows提取】Windows SMBv3 LPE exploit 已编译版.exe|SMBGhost_RCE_PoC-远程代码执行EXP|Windows_SMBv3_RCE_CVE-2020-0796漏洞复现
- getAV---windows杀软进程对比工具单文件版
- 【Windows提权工具】Windows 7 to Windows 10 / Server 2019|搭配CS的修改版可上线system权限的session
- 【Windows提权工具】SweetPotato修改版，用于webshell下执行命令|本地编译好的版本|点击下载或右键另存为|SweetPotato_webshell下执行命令版.pdf
- 【bypass UAC】Windows 8.1 and 10 UAC bypass abusing WinSxS in "dccw.exe"
- 【Windows提权】CVE-2018-8120 Exploit for Win2003 Win2008 WinXP Win7
- 【Windows提权 Windows 10&Server 2019】PrintSpoofer-Abusing Impersonation Privileges on Windows 10 and Server 2019|配合文章食用-pipePotato复现|Windows 权限提升 BadPotato-已经在Windows 2012-2019 8-10 全补丁测试成功
- 【Windows提权】Windows 下的提权大合集
- 【Windows提权】-CVE-2020-1048 | PrintDemon本地提权漏洞-漏洞影响自1996年以来发布(Windows NT 4)的所有Windows版本
- 【Windows bypass UAC】UACME-一种集成了60多种Bypass UAC的方法
- CVE-2020–1088： Windows wersvc.dll 任意文件删除本地提权漏洞分析
- 【Windows提权】CVE-2019-0863-Windows中错误报告机制导致的提权-EXP
- 【Windows提权】CVE-2020-1066-EXP
- 【Windows提权】CVE-2020-0787-EXP-ALL-WINDOWS-VERSION-适用于Windows所有版本的提权EXP
- 【Windows提权】CVE-2020-1054-Win32k提权漏洞Poc|CVE-2020-1054-POC
- 【Linux提权】对Linux提权的简单总结

- 【Windows提权】wesng-Windows提权辅助脚本
- 【Windows提权】dazzleUP是一款用来帮助渗透测试人员进行权限提升的工具，可以在window系统中查找脆弱面进行攻击。工具包括两部分检查内容，exploit检查和错误配置检查。

PC

- 微软RDP远程代码执行漏洞（CVE-2019-0708）
- CVE-2019-0708-python版
- MS17-010-微软永恒之蓝漏洞
- macOS-Kernel-Exploit
- CVE-2019-1388 UAC提权 (nt authority\system)
- CVE-2019-1405和CVE-2019-1322：通过组合漏洞进行权限提升 Microsoft Windows 10 Build 1803 < 1903 - 'COMahawk' Local Privilege Escalation
- CVE-2019-11708
- Telegram(macOS v4.9.155353) 代码执行漏洞
- Remote Desktop Gateway RCE bugs CVE-2020-0609 & CVE-2020-0610
- Microsoft SharePoint - Deserialization Remote Code Execution
- CVE-2020-0728-Windows Modules Installer Service 信息泄露漏洞
- CVE-2020-0618: 微软 SQL Server Reporting Services远程代码执行（RCE）漏洞|GitHub验证POC(其实前文的分析文章也有)
- CVE-2020-0767Microsoft ChakraCore脚本引擎【Edge浏览器中的一个开源的ChakraJavaScript脚本引擎的核心部分】安全漏洞
- CVE-2020-0688：微软EXCHANGE服务的远程代码执行漏洞|CVE-2020-0688_EXP---另一个漏洞检测利用脚本|又一个cve-2020-0688利用脚本|Exploit and detect tools for CVE-2020-0688
- CVE-2020-0674: Internet Explorer远程代码执行漏洞检测
- CVE-2020-8794: OpenSMTPD 远程命令执行漏洞
- Linux平台-CVE-2020-8597: PPPD 远程代码执行漏洞
- Windows-CVE-2020-0796：疑似微软SMBv3协议“蠕虫级”漏洞|相关讨论|CVE-2020–0796检测与修复|又一个CVE-2020-0796的检测工具-可导致目标系统崩溃重启
- SMBGhost_RCE_PoC（CVE-2020-0796）
- WinRAR 代码执行漏洞 (CVE-2018-20250)-POC|相关文章|全网筛查 WinRAR 代码执行漏洞 (CVE-2018-20250)
- windows10相关漏洞EXP&POC
- shiro rce 反序列 命令执行 一键工具
- CVE-2019-1458-Win32k中的特权提升漏洞【shell可用-Windows提取】
- CVE-2019-1253-Windows权限提升漏洞-AppXSvc任意文件安全描述符覆盖EoP的另一种poc|CVE-2019-1253
- BypassAV【免杀】Cobalt Strike插件，用于快速生成免杀的可执行文件
- CVE-2020-0674：Internet Explorer UAF 漏洞exp【在64位的win7测试了IE 8, 9, 10, and 11】
- SMBGhost_AutomateExploitation-SMBGhost (CVE-2020-0796) Automate Exploitation and Detection
- MS Windows OLE 远程代码执行漏洞(CVE-2020-1281)
- CVE-2020-1350-Windows的DNS服务器RCE检测的powershell脚本|CVE-2020-1350-DoS
- CVE-2020-1362-Microsoft Windows WalletService权限提升漏洞
- CVE-2020-10713-GRUB2 本地代码执行漏洞
- CVE-2020-1313-Microsoft Windows Update Orchestrator Service权限提升漏洞，可用于Windows提权操作，支持新版的Windows server 2004
- CVE-2020-1337-exploit-Windows 7/8/10上Print Spooler组件漏洞修复后的绕过|cve-2020-1337-poc

tools-小工具集版本合

- java环境下任意文件下载情况自动化读取源码的小工具
- Linux SSH登录日志清除/伪造
- python2的socks代理
- dede_burp_admin_path-dedecms后台路径爆破(Windows环境)

- PHP 7.1-7.3 disable_functions bypass
- 一个各种方式突破Disable_functions达到命令执行的shell
- 【PHP】bypass disable_functions via LD_PRELOA (no need /usr/sbin/sendmail)
- 另一个bypass PHP的disable_functions
- cmd下查询3389远程桌面端口
- 伪装成企业微信名片的钓鱼代码
- vbulletin5-rce利用工具(批量检测/getshell)/保存了一份源码:vbulletin5-rce.py
- CVE-2017-12615
- 通过Shodan和favicon icon发现真实IP地址
- Cobalt_Strike扩展插件
- Windows命令行cmd的空格替换
- 绕过disable_function汇总
- WAF Bypass
- 命令注入总结
- 隐藏wifi-ssid获取 · theKingOfNight's Blog
- crt.sh证书/域名收集
- TP漏洞集合利用工具py3版本-来自奇安信大佬Lucifer1993
- Python2编写的struts2漏洞全版本检测和利用工具-来自奇安信大佬Lucifer1993
- sqlmap_bypass_D盾_tamper
- sqlmap_bypass_安全狗_tamper
- sqlmap_bypass_空格替换成换行符-某企业建站程序过滤_tamper
- sqlmap_bypass_云锁_tamper
- masscan+nmap扫描脚本
- PHP解密扩展
- linux信息收集/应急响应/常见后门检测脚本
- RdpThief-从远程桌面客户端提取明文凭据辅助工具
- 使用powershell或CMD直接运行命令反弹shell
- FTP/SSH/SNMP/MSSQL/MYSQL/PostGreSQL/REDIS/ElasticSearch/MONGODB弱口令检测
- GitHack-.git泄露利用脚本
- GitHacker---比GitHack更好用的git泄露利用脚本
- SVN源代码泄露全版本Dump源码
- 多进程批量网站备份文件扫描
- Empire|相关文章:后渗透测试神器Empire详解
- FOFA Pro view 是一款FOFA Pro 资产展示浏览器插件，目前兼容 Chrome、Firefox、Opera
- Zoomeye Tools-一款利用Zoomeye 获取有关当前网页IP地址的各种信息(需要登录)
- 360 0Kee-Team 的 crawlergo动态爬虫 结合 长亭XRAY扫描器的被动扫描功能
- 内网神器Xerosploit-娱乐性质(端口扫描|DoS攻击|HTML代码注入|JavaScript代码注入|下载拦截和替换|嗅探攻击|DNS欺骗|图片替换|Web页面篡改|Drifnet)
- 一个包含php,java,python,C#等各种语言版本的XXE漏洞Demo
- 内网常见渗透工具包
- 从内存中加载 SHELLCODE bypass AV查杀|twitter示例
- 流量转发工具-pingtunnel是把tcp/udp/sock5流量伪装成icmp流量进行转发的工具
- 内网渗透-创建Windows用户(当net net1 等常见命令被过滤时,一个文件执行直接添加一个管理员【需要shell具有管理员权限!】|adduser使用方法 |【windows】绕过杀软添加管理员用户的两种方法|【windows】使用vbs脚本添加管理员用户
- pypykatz-通过python3实现完整的Mimikatz功能(python3.6+)
- 【windows】Bypassing AV via in-memory PE execution-通过在内存中加载多次XOR后的payload来bypass杀软|作者自建gitlab地址
- wafw00f-帮助你快速识别web应用是否使用何种WAF(扫描之前很有用)
- Linux提取其他用户密码的工具(需要root权限)

- apache2_BackdoorMod-apache后门模块
- 对密码已保存在 Windwos 系统上的部分程序进行解析,包括：Navicat,TeamViewer,FileZilla,WinSCP,Xmangager系列产品（Xshell,Xftp)
- 一个简单探测jboss漏洞的工具
- 一款lcx在golang下的实现-适合内网代理流量到公网,比如阿里云的机器代理到你的公网机器
- Cobalt Strike Aggressor 插件包
- Erebus-Cobalt Strike后渗透测试插件,包括了信息收集、权限获取、密码获取、痕迹清除等等常见的脚本插件
- cobaltstrike后渗透插件，偏向内网常用工具（目前包含1.定位域管理员2.信息收集(采用ADfind)3.权限维持(增加了万能密码,以及白银票据)4.内网扫描(nbtscan(linux/windows通用))5.dump数据库hash(支持mysql/mssql(快速获取数据库的hash值))）
- IP/IP段资产扫描-->扫描开放端口识别运行服务部署网站-->自动化整理扫描结果-->输出可视化报表+整理结果
- A script to scan for unsecured Laravel .env files
- Struts2漏洞扫描Golang版-【特点:单文件、全平台支持、可在webshell下使用】
- Shiro<=1.2.4反序列化，一键检测工具|Apache shiro <= 1.2.4 rememberMe 反序列化漏洞利用工具
- weblogicScanner-完整weblogic 漏洞扫描工具修复版
- GitHub敏感信息泄露监控
- Java安全相关的漏洞和技术demo
- 在线扫描-网站基础信息获取|旁站|端口扫描|信息泄露
- bayonet是一款src资产管理系统，从子域名、端口服务、漏洞、爬虫等一体化的资产管理系统
- 内网渗透中常用的c#程序整合成cs脚本，直接内存加载
- 【漏洞库】又一个各种漏洞poc、Exp的收集或编写
- 【内网代理】内网渗透代理转发利器reGeorg|**相关文章:**配置reGeorg+Proxifier渗透内网|reGeorg+Proxifier实现内网sock5代理|内网渗透之reGeorg+Proxifier|reGeorg+Proxifier使用
- 【内网代理】Neo-reGeorg重构的reGeorg
- 【内网代理】Tunna-通过http隧道将TCP流量代理出来
- 【内网代理】proxy.php-单文件版的php代理
- 【内网代理】pivotnacci-通过HTTP隧道将TCP流量代理出来或进去
- 【内网代理】毒刺(pystinger)通过webshell实现**内网SOCK4代理,端口映射**.|pystinger.zip-下载
- 【内网代理】php-proxy-app-一款代理访问网站的工具
- get_Team_Pass-获取目标机器上的teamviewerID和密码(你需要具有有效的目标机器账号密码且目标机器445端口可以被访问(开放445端口))
- chromepass-获取chrome保存的账号密码/cookies-nirsoft出品在win10+chrome 80测试OK|SharpChrome-基于.NET 2.0的开源获取chrome保存过的账号密码/cookies/history|ChromePasswords-开源获取chrome密码/cookies工具
- java-jdwp远程调试利用|相关文章:jdwp远程调试与安全
- 社会工程学密码生成器，是一个利用个人信息生成密码的工具
- 云业CMS(yunyecms)的多处SQL注入审计分析|原文地址|官网下载地址|sqlmap_yunyecms_front_sqli_tamp.py
- www.flash.cn 的钓鱼页，中文+英文
- 织梦dedecms全版本漏洞扫描
- CVE、CMS、中间件漏洞检测利用合集 Since 2019-9-15
- Dirble -快速目录扫描和爬取工具【比dirsearch和dirb更快】
- RedRabbit - Red Team PowerShell脚本
- Pentest Tools Framework - 渗透测试工具集-适用于Linux系统
- 白鹿社工字典生成器，灵活与易用兼顾。
- NodeJsScan-一款转为Nodejs进行静态代码扫描开发的工具
- 一款国人根据poison ivy重写的远控
- NoXss-可配合burpsuite批量检测XSS
- fofa 采集脚本
- java web 压缩文件 安全 漏洞
- 可以自定义规则的密码字典生成器,支持图形界面
- dump lass 工具(绕过/干掉卡巴斯基)|loader.zip下载

- GO语言版本的mimikatz-编译后免杀
- CVE-2019-0708-批量检测扫描工具
- dump lsass的工具|又一个dump lsass的工具
- Cobalt Strike插件 - RDP日志取证&清除
- xencrypt-一款利用powershell来加密并采用Gzip/DEFLATE来绕过杀软的工具
- SessionGopher-一款采用powershell来解密Windows机器上保存的session文件，例如： WinSCP, PuTTY, SuperPuTTY, FileZilla, and Microsoft Remote Desktop，支持远程加载和本地加载使用
- CVE-2020-0796 Local Privilege Escalation POC-python版本|CVE-2020-0796 Remote Code Execution POC
- Windows杀软在线对比辅助
- 递归式寻找域名和api
- mssqli-duet-用于mssql的sql注入脚本,使用RID爆破,从Active Directory环境中提取域用户
- 【Android脱壳】之一键提取APP敏感信息
- Shiro系列漏洞检测GUI版本-ShiroExploit GUI版本
- 通过phpinfo获取cookie突破httponly
- phpstudy RCE 利用工具 windows GUI版本
- WebAliveScan-根据端口快速扫描存活的WEB
- 扫描可写目录.aspx
- PC客户端（C-S架构）渗透测试
- wsltools-web扫描辅助python库
- struts2_check-用于识别目标网站是否采用Struts2框架开发的工具
- sharpmimi.exe-免杀版mimikatz
- thinkPHP代码执行批量检测工具
- pypykatz-用纯Python实现的Mimikatz
- Flux-Keylogger-具有Web面板的现代Javascript键盘记录器
- JSINFO-SCAN-递归式寻找域名和api
- FrameScan-GUI 一款python3和Pyqt编写的具有图形化界面的cms漏洞检测框架
- SRC资产信息聚合网站
- Spring Boot Actuator未授权访问【XXE、RCE】单/多目标检测
- JNDI注入利用工具【Fastjson、Jackson 等相关漏洞】
- 各种反弹shell的语句集合页面
- 解密weblogic AES或DES加密方法
- 使用 sshLooterC 抓取 SSH 密码|相关文章|本地版本
- redis-rogue-server-Redis 4.x/5.x RCE
- ew-内网穿透(跨平台)
- xray-weblisten-ui-一款基于GO语言写的Xray 被动扫描管理
- SQLEXP-SQL 注入利用工具，存在waf的情况下自定义编写tamper脚本 dump数据
- SRC资产在线管理系统 - Shots
- luject：可以将动态库静态注入到指定应用程序包的工具，目前支持Android/iPhonsOS/Windows/macOS/Linux|相关文章
- CursedChrome：Chrome扩展植入程序，可将受害Chrome浏览器转变为功能齐全的HTTP代理，使你能够以受害人身份浏览网站
- pivotnacci：通过HTTP隧道进行Socks连接
- PHPFuck-一款适用于php7以上版本的代码混淆|[PHPFuck在线版本
- 冰蝎 bypass open_basedir 的马
- goproxy heroku 一键部署套装，把heroku变为免费的http(s)\socks5代理
- 自己收集整理的端口、子域、账号密码、其他杂七杂八字典，用于自己使用
- xFTP6密码解密
- Mars-战神TideSec出品的WDScanner的重写一款综合的漏洞扫描,资产发现/变更,域名监控/子域名挖掘,Awvs扫描,POC检测,web指纹探测、端口指纹探测、CDN探测、操作系统指纹探测、泛解析探测、WAF探测、敏感信息检测等等工具
- Shellcode Compiler：用于生成Windows 和 Linux平台的shellcode工具

- BadDNS 是一款使用 Rust 开发的使用公共 DNS 服务器进行多层子域名探测的极速工具
- 【Android脱壳】XServer是一个用于对方法进行分析的Xposed插件|相关文章：Xposed+XServer无需脱壳抓取加密包|使用xserver对某应用进行不脱壳抓加密包
- masscan_to_nmap-基于masscan和nmap的快速端口扫描和指纹识别工具
- Evilreg -使用Windows注册表文件的反向Shell (.Reg)
- Shecodject工具使用python注入shellcode bypass 火絨,360,windows defender
- Malleable-C2-Profiles-Cobalt Strike的C2隐藏配置文件相关|渗透利器Cobalt Strike - 第2篇 APT级的全面免杀与企业纵深防御体系的对抗
- AutoRemove-自动卸载360
- ligolo：用于渗透时反向隧道连接工具
- RMIScout: Java RMI爆破工具
- 【Android脱壳】FRIDA-DEXDump-【使用Frida来进行Android脱壳】
- Donut-Shellcode生成工具
- JSP-Webshells集合【2020最新bypass某云检测可用】
- one-scan-多合一网站指纹扫描器，轻松获取网站的 IP / DNS 服务商 / 子域名 / HTTPS 证书 / WHOIS / 开发框架 / WAF 等信息
- ServerScan一款使用Golang开发的高并发网络扫描、服务探测工具。
- 域渗透-Windows hash dump之secretsdump.py|相关文章
- WindowsVulnScan：基于主机的漏洞扫描工【类似windows-exp-suggester】
- 基于实战沉淀下的各种弱口令字典
- SpoofWeb：一键部署HTTPS钓鱼站
- VpsEnvInstall：一键部署VPS渗透环境
- tangalanga：Zoom会议扫描工具
- 碎遮SZhe_Scan Web漏洞扫描器，基于python Flask框架，对输入的域名/IP进行全面的信息搜集，漏洞扫描，可自主添加POC
- Taie-RedTeam-OS-泰阿安全实验室-基于XUbuntu私人订制的红蓝对抗渗透操作系统
- naiveproxy-一款用C语言编写类似于trojan的代理工具
- BrowserGhost-一个抓取浏览器密码的工具，后续会添加更多功能
- GatherInfo-渗透测试信息搜集/内网渗透信息搜集
- EvilPDF：一款把恶意文件嵌入在 PDF 中的工具
- SatanSword-红队综合渗透框架，支持web指纹识别、漏洞PoC检测、批量web信息和端口信息查询、路径扫描、批量JS查找子域名、使用google headless、协程支持、完整的日志回溯
- Get-WeChat-DB-获取目标机器的微信数据库和密钥
- ThinkphpRCE-支持代理IP池的批量检测Thinkphp漏洞或者日志泄露的py3脚本
- fakelogonscreen-伪造（Windows）系统登录页面,截获密码
- WMIHACKER-仅135端口免杀横向移动|使用方法以及介绍|横向移动工具WMIHACKER|原文链接
- cloud-ranges-部分公有云IP地址范围
- sqltools_ch-sqltools2.0汉化增强版
- railgun-poc_1.0.1.7-多功能端口扫描/爆破/漏洞利用/编码转换等|railgun作者更新到GitHub了，目前是1.2.8版本 | railgun-v1.2.8.zip-存档
- dede_funcookie.php-DEDECMS伪随机漏洞分析 (三) 碰撞点(爆破，伪造管理员cookie登陆后台getshell
- WAScan-一款功能强大的Web应用程序扫描工具【基于python开发的命令行扫描器】
- Peinject_dll-CS插件之另类持久化方法-PE感染
- MSSQL_BackDoor-摆脱MSSMS和 Navicat 调用执行 sp_cmdExec
- xShock-一款针对Shellshock漏洞的利用工具【例如低版本cgi的默认配置页面进行利用】
- tini-tools-针对红蓝对抗各个场景使用的小工具-【主要是Java写的工具】【目前有phpstudy.jar和域名转IP工具.jar】
- code6-码小六是一款 GitHub 代码泄露监控系统，通过定期扫描 GitHub 发现代码泄露行为
- taowu-cobalt-strike-适用于cobalt strike3.x与cobalt strike4.x的插件
- Weblogic-scan-Weblogic 漏洞批量扫描工具
- revp：反向HTTP代理，支持Linux，Windows和macOS

- fofa2Xray-一款联合fofa与xray的自动化批量扫描工具,使用Golang编写，适用于windows与linux
- CasExp-Apereo CAS 反序列化利用工具
- C_Shot-shellcode远程加载器|相关文章
- dz_ml_rce.py-Discuz! ml RCE漏洞利用工具
- Redis未授权访问漏洞利用工具
- Shiro 回显利用工具|相关文章
- GetIPinfo-用于寻找多网卡主机方便内网跨网段渗透避免瞎打找不到核心网
- Layer子域名挖掘机-Layer5.0 SAINTSEC
- cve_2020_14644.jar-Weblogic 远程命令执行漏洞（CVE-2020-14644）回显利用工具
- TechNet-Gallery-PowerShell武器库|Powershell ebserver：PowerShell实现的Web服务器，无需IIS，支持PowerShell命令执行、脚本执行、上传、下载等功能|PS2EXE-GUI：将PowerShell脚本转换为EXE文件
- spybrowse：窃取指定浏览器的配置文件
- FavFreak：执行基于favicon.ico的侦察
- gorailgun_v1.0.7-集漏洞端口扫描利用于一体的工具
- 【shell管理工具】Godzilla-哥斯拉|AntSword-蚁剑|Behinder-冰蝎
- 由python编写打包的Linux下自动巡检工具|源处
- 【内网探测】SharpNetCheck-批量检测机器是否有出网权限，可在dnslog中回显内网ip地址和计算机名，可实现内网中的快速定位可出网机器
- fofa搜索增强版-使用fofa的url+cookies即可自动下载所有结果
- SharpBlock-A method of bypassing EDR's active projection DLL's by preventing entry point exection|相关文章
- bypasswaf-云锁数字型注入tamper/安全狗的延时、布尔、union注入绕过tamper
- 通达OA 2017 版本SQL注入脚本
- t14m4t：一款封装了THC-Hydra和Nmap的自动化爆破工具
- ksubdomain：一款基于无状态子域名爆破工具
- smuggler-一款用python3编写的http请求走私验证测试工具
- Fuzz_dic：又一个类型全面的参数和字典收集项目
- PentesterSpecialDict-该项目对 [fuzzDicts | fuzzdb | Dict] 等其他网上字典开源项目进行整合精简化和去重处理
- PowerUpSQL：为攻击SQLServer而设计的具有攻击性的PowerShell脚本|利用PowerUpSQL攻击SQL Server实例
- adbsploit-一个基于Python3和ADB的安卓设备漏洞利用和管理工具
- monsoon-一个用Go语言编写的目录扫描工具，类似于dirsearch
- 【Android脱壳】Youpk-又一款基于ART的主动调用的脱壳机
- 【webshell免杀】php免杀D盾webshell生成工具
- Steganographer-一款能够帮助你在图片中隐藏文件或数据的Python隐写工具
- AV_Evasion_Tool:掩日 - 免杀执行器生成工具
- GODNSLOG-河马师傅（河马webshell检测作者）基于go语言开发的一款DNSLOG工具，支持docker一键部署

文章/书籍/教程相关

- windwos权限维持系列12篇PDF
- Linux 权限维持之进程注入(需要关闭ptrace) | 在不使用ptrace的情况下，将共享库（即任意代码）注入实时Linux进程中。(不需要关闭ptrace)|[总结]Linux权限维持-原文地址
- 44139-mysql-udf-exploitation
- emlog CMS的代码审计_越权到后台getshell
- PHPOK 5.3 最新版前台注入
- PHPOK 5.3 最新版前台无限制注入（二）
- Thinkphp5 RCE总结
- rConfig v3.9.2 RCE漏洞分析
- weiphp5.0 cms审计之exp表达式注入
- zzzphp1.7.4&1.7.5到处都是sql注入
- FCKeditor文件上传漏洞及利用-File-Upload-Vulnerability-in-FCKEditor

- zzcms 2019 版本代码审计
- 利用SQLmap 结合 OOB 技术实现音速盲注
- 特权提升技术总结之Windows文件服务内核篇(主要是在webshell命令行执行各种命令搜集信息)|(项目留存PDF版本)
- WellCMS 2.0 Beta3 后台任意文件上传
- 国外详细的CTF分析总结文章(2014-2017年)
- 这是一篇“不一样”的真实渗透测试案例分析文章-从discuz的后台getshell到绕过卡巴斯基获取域控管理员密码|原文地址
- 表达式注入.pdf
- WordPress ThemeREX Addons 插件安全漏洞深度分析
- 通达OA文件包含&文件上传漏洞分析
- 高级SQL注入：混淆和绕过
- 权限维持及后门持久化技巧总结
- Windows常见的持久化后门汇总
- Linux常见的持久化后门汇总
- CobaltStrike4.0用户手册_中文翻译_3
- Cobaltstrike 4.0之 我自己给我自己颁发license.pdf
- Cobalt Strike 4.0 更新内容介绍
- Cobal_Strike_自定义OneLiner
- cobalt strike 快速上手 [一]
- Cobalt strike3.0使用手册
- Cobalt_Strike_Spear_Phish_CS邮件钓鱼制作
- Remote NTLM relaying through CS
- 渗透测试神器Cobalt Strike使用教程
- Cobalt Strike的teamserver在Windows上快速启动脚本
- ThinkPHP v6.0.0_6.0.1 任意文件操作漏洞分析
- Django_CVE-2020-9402_Geo_SQL注入分析
- CVE-2020-10189_Zoho_ManageEngine_Desktop_Central_10反序列化远程代码执行
- 安全狗SQL注入WAF绕过
- 通过将JavaScript隐藏在PNG图片中，绕过CSP
- 通达OA任意文件上传_文件包含GetShell
- 文件上传Bypass安全狗4.0
- SQL注入Bypass安全狗4.0
- 通过正则类SQL注入防御的绕过技巧
- MYSQL_SQL_BYPASS_WIKI-mysql注入,bypass的一些心得
- bypass云锁注入测试
- 360webscan.php_bypass
- think3.2.3_sql注入分析
- UEditor SSRF DNS Rebinding
- PHP代码审计分段讲解
- 京东SRC小课堂系列文章
- windows权限提升的多种方式|Privilege_Escalation_in_Windows_for_OSCP
- bypass CSP|Content-Security-Policy(CSP)Bypass_Techniques
- 个人维护的安全知识框架,内容偏向于web
- PAM劫持SSH密码
- 零组资料文库-(需要邀请注册)
- redis未授权个人总结-Mature
- NTLM中继攻击的新方法
- PbootCMS审计
- De1CTF2020系列文章

- xss-demo-超级简单版本的XSS练习demo
- 空指针-Base_on_windows_Writeup--最新版DZ3.4实战渗透
- 入门KKCMS代码审计
- SpringBoot 相关漏洞学习资料，利用方法和技巧合集，黑盒安全评估 checklist
- 文件上传突破waf总结
- 极致CMS（以下简称_JIZHICMS）的一次审计-SQL注入+储存行XSS+逻辑漏洞|原文地址
- 代码审计之DTCMS_V5.0后台漏洞两枚
- 快速判断sql注入点是否支持load_file
- 文件上传内容检测绕过
- Fastjson_=1.2.47反序列化远程代码执行漏洞复现
- 【Android脱壳】_腾讯加固动态脱壳（上篇）
- 【Android脱壳】腾讯加固动态脱壳（下篇）
- 【Android脱壳】记一次frida实战——对某视频APP的脱壳、hook破解、模拟抓包、协议分析一条龙服务
- 【Android抓包】记一次APP测试的爬坑经历.pdf
- 完整的内网域渗透-暗月培训之项目六
- Android APP渗透测试方法大全
- App安全检测指南-V1.0
- 借github上韩国师傅的一个源码实例再次理解.htaccess的功效
- Pentest_Note-渗透Tips，总结了渗透测试常用的工具方法
- 红蓝对抗之Windows内网渗透-腾讯SRC出品
- 远程提取Windows中的系统凭证
- 绕过AMSI执行powershell脚本|AmsiScanBufferBypass-相关项目
- 踩坑记录-Redis(Windows)的getshell
- Cobal_Strike踩坑记录-DNS Beacon
- windows下隐藏webshell的方法
- DEDECMS伪随机漏洞分析 (三) 碰撞点(爆破，伪造管理员cookie登陆后台getshell
- 针对宝塔的RASP及其disable_functions的绕过
- 渗透基础WMI学习笔记
- 【海洋CMS】SeaCMS_v10.1代码审计实战
- 红队攻防实践：闲谈Webshell在实战中的应用
- 红队攻防实践：unicode进行webshell免杀的思考
- php无eval后门
- 【代码审计】ThinkPhp6任意文件写入
- YzmCMS代码审计
- BadUSB简单免杀一秒上线CobaltStrike
- BasUSB实现后台静默执行上线CobaltStrike
- 手把手带你制作一个X谁谁上线的BadUSB|近源渗透-BadUsb-原文地址
- 一文学会Web_Service漏洞挖掘
- 唯快不破的分块传输绕WAF
- Unicode的规范化相关漏洞挖掘思路实操
- 换一种姿势挖掘任意用户密码重置漏洞-利用不规范化的Unicode编码加burp挖掘
- 全方面绕过安全狗2
- 冰蝎——从入门到魔改
- 冰蝎——从入门到魔改(续)
- 技术分享_ 内网渗透手动学习实践
- 权限维持之打造不一样的映像劫持后门
- Jboss漏洞利用总结
- Java RMI服务远程命令执行利用|小天之天的测试工具-attackRMI.jar

- PbootCMS任意代码执行(从v1.0.1到v2.0.9)的前世今生
- 实战绕过双重waf(玄武盾+程序自身过滤)结合编写sqlmap的tamper获取数据
- OneThink前台注入分析
- 记一次从源代码泄漏到后台(微擎cms)获取webshell的过程
- Android抓包—关于抓包的碎碎念-看雪论坛-Android板块ChenSem|原文地址
- CVE-2020-15778-Openssh-SCP命令注入漏洞复现报告
- bolt_cms_V3.7.0_xss和远程代码执行漏洞
- 关于Cobalt_Strike检测方法与去特征的思考
- 代码审计_PHPCMS_V9前台RCE挖掘分析
- 【免杀】C++免杀项目推荐-附件下载|原文地址
- 利用图片隐写术来远程动态加载shellcode|原文地址
- [后渗透]Mimikatz使用大全|原文地址
- 渗透测试XiaoCms之自力更生代码审计-后台数据库备份SQL注入到getshell|原文地址
- HW礼盒：深信服edr RCE，天融信dlp unauth和通达OA v11.6版本RCE
- [0day]通达 OA v11.7 后台 SQL 注入到 RCE-原文地址
- wordpress 评论插件 wpDiscuz 任意文件上传漏洞分析
- Gopher协议使用总结-原文地址
- sqlmap使用总结|【实战技巧】sqlmap不为人知的骚操作-原文地址|记一份SQLmap 使用手册小结（一）|记一份SQLmap 使用手册小结（二）
- mac上Parallels Desktop安装kali linux 2020.2a并安装好Parallels Tools+Google拼音输入法
- 通达OA v11.5 多枚0day漏洞复现|续集 _ 再发通达OA多枚0day-原文地址
- POSCMS(20200821)_任意 SQL 语句执行（需要登录后台）-原文地址|POSCMS v3.2.0漏洞复现(getshell+前台SQL注入)-原文地址
- 多线程+二分法的巧用——通达OA 2017 SQL盲注-原文地址
- 宝塔面板webshell隐藏小技巧-原文地址
- 配合隐写术远程动态加载 shellcode|原文地址
- MySQL蜜罐获取攻击者微信ID-原文地址
- 蓝天采集器 v2.3.1 后台getshell（需要管理员权限）
- 实战-从社工客服拿到密码登录后台加SQL注入绕过安全狗写入webshell到提权进内网漫游-原文地址
- 0day安全_软件漏洞分析技术(第二版)
- 安恒信息《渗透攻击红队百科全书》
- lcx端口转发(详解)
- php_bugs-PHP代码审计分段讲解
- 深信服edr终端检测响应平台（<3.2.21）代码审计挖掘（RCE）-原文地址
- 深信服edr终端检测响应平台（<3.2.21）代码审计挖掘（权限绕过）-原文地址
- Hook梦幻旅途之Frida
- 简单的源码免杀过av
- duomicms代码审计