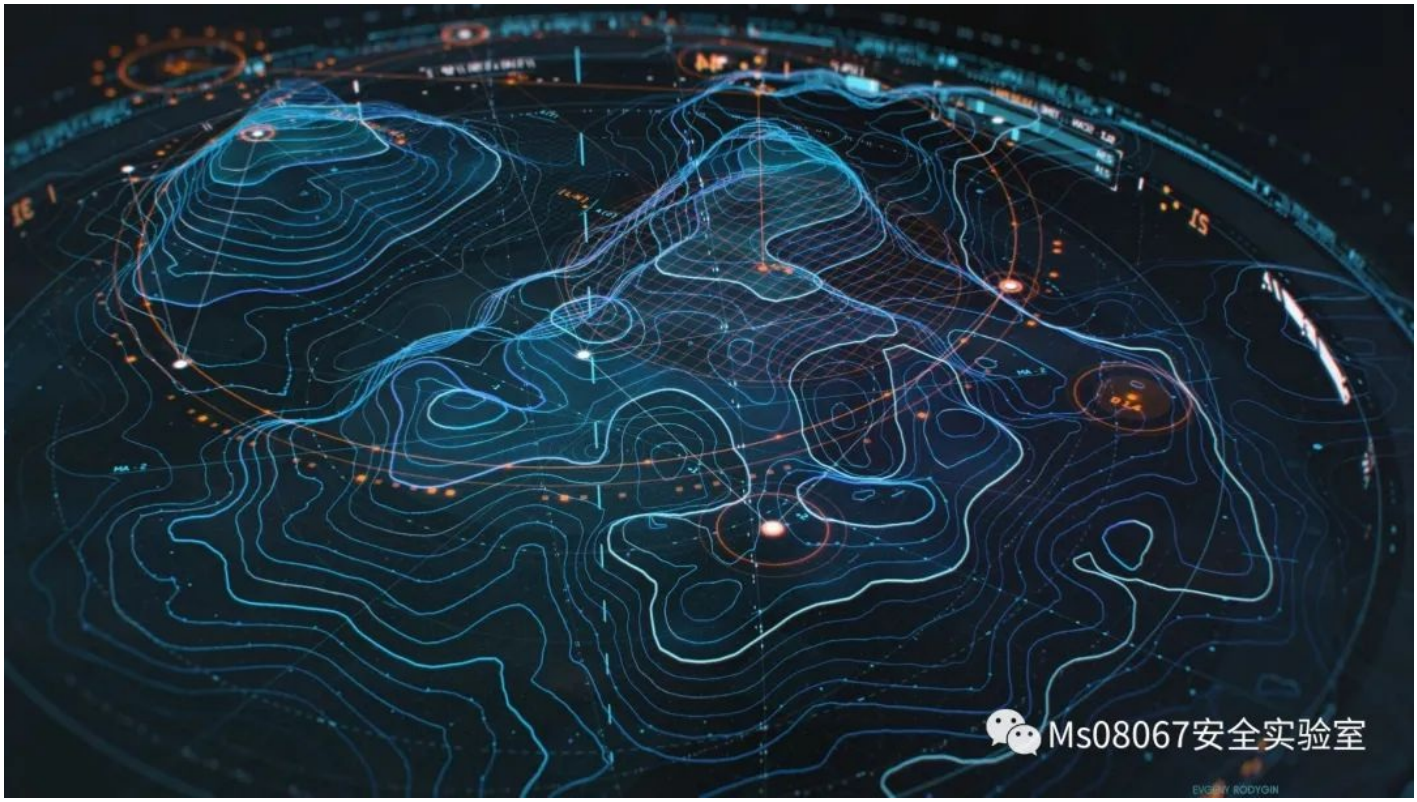
干货合辑！Ms08067安全实验室2020年度盘点

原创

Ms08067安全实验室 于 2021-01-03 09:00:00 发布 879 收藏 4

本文链接：https://blog.csdn.net/shuteer_xu/article/details/112167044

出品丨MS08067实验室（www.ms08067.com）



互联网承载着人类对虚拟世界的梦想，抬头仰望星辰大海，脚下仍是未知前路。

又是互相陪伴成长的一年！

好像2020的年终总结又迟到了

过去这一年，有人辛苦一点，

有人幸运一点，但我们都到了今天。

让我们一同憧憬美好的2021~

老样子，去年没学完的知识今年立个flag继续战！

最近的年度热词榜单、APP年度总结也都出来了~ 啊这...那也得蹭蹭最后一波热度！2020年度技术文干货递上~ 请注意查收！

Ms08067 年度关键词

干货/好文

是不是觉得那些奇怪的知识点又增加了？

想学的想看的，还没收藏的技术文都在这里~稳！

//

后浪~

快接好小编给你准备的这份干货宝典吧□□

安全攻防 关于数据安全的那些事

在互联网时代，数据安全与个人隐私受到了前所未有的挑战，各种新奇的攻击技术层出不穷。如何才能更好的保护我们的数据？可以从这几大块入手~

1

WEB安全攻防

《Web安全攻防》配套视频之SSRF漏洞及原理

《Web安全攻防》配套视频之文件后缀绕过攻击

《Web安全攻防》配套视频之文件类型绕过攻击

《Web安全攻防》配套视频之文件截断绕过攻击

《Web安全攻防》配套视频之竞争条件攻击

《Web安全攻防》配套视频之暴力破解

《Web安全攻防》配套视频之命令执行漏洞

《Web安全攻防》配套视频之逻辑漏洞挖掘

《Web安全攻防》配套视频之XXE漏洞攻击

《Web安全攻防》配套视频之XSS进阶

星球大战 | 渗透新鸟WEB安全零基础入门到进阶教程

2

内网安全攻防

《内网安全攻防》配套视频之安全域划分、域内权限解读

《内网安全攻防》配套视频之域环境搭建

《内网安全攻防》配套视频之通过防火墙m0n0wall构建内网各种环境

《内网安全攻防》配套视频之工作组信息收集

《内网安全攻防》配套视频之域内信息收集

《内网安全攻防》配套视频之定位域管理员

《内网安全攻防》配套视频之查找域管理进程

《内网安全攻防》配套视频之利用PS查询域内信息

《内网安全攻防》配套视频之bloodhound工具的使用

“内网安全攻防图书配套视频1.0"+“内网高级渗透技术2.0”

超级福利 |《内网安全攻防》官方配套视频 免费来袭

中秋国庆福利四连击 最后福利之内网高级渗透技术（高级提升）

我做“内网知识星球”一周年总结

3

python安全攻防

内部视频放送 |《Python安全攻防：渗透测试实战指南》知识星球

《Python安全攻防》配套视频之第一个python程序

《Python安全攻防:渗透测试实战指南》配套技术讲解

《Python安全攻防》配套视频之一步一步教你如何编写poc&exp脚本

新书介绍 |《Python安全攻防：渗透测试实战指南》出版进展及业界评论

想学二进制，成为逆向工程师？来看这里，超精华的指南与规划！

你准备好了吗？安卓逆向分析来啦~(福利返场)

4

kali安全攻防

《Kali Linux2020渗透测试指南》配套技术精讲

最后一天 |《Kali Linux2020 渗透测试指南》配套知 识星球福利

新书《Kali Linux2020 渗透测试指南》星球福利及最终目录&概要公布

5

二进制逆向入门

“0基础逆向”知识星球--2020年1月-3月授课内容归纳（文末有优惠券）

“二进制逆向星球”--一年授课内容汇总 + 新增课程目录（文末有福利）

星球大战 | 渗透新鸟WEB安全零基础入门到进阶教程

02

漏洞复现 那些年踩过的坑如何自愈

互联网世界充满了各种未知数~那些年踩过的坑得到的都是知识的升华。各种漏洞合辑；渗透测试跟实战分析！让你少走弯路！

1

漏洞复现

Joomla 3.4.6 RCE复现及分析

漏洞复现:CVE-2016-4437 Apache Shiro 反序列化

Jackson 反序列化远程代码执行漏洞复现

Windows全版本本地提权(CVE-2020-0787)

复现 | RCTF2020逆向cipher

漏洞复现 | CVE - 2020 - 5902踩坑记

漫谈-Weblogic-CVE-2020-2555

漫谈-Weblogic-CVE-2020-2551

漏洞复现 | CVE - 2017 - 5645

漏洞复现 | SaltStack认证绕过（CVE - 2020 - 11651）

CVE-2020-1472漏洞实战 深度剖析

自动化漏洞挖掘之初步构想

2

渗透测试一之内网篇

内网渗透（一）| 域渗透之SPN服务主体名称

内网渗透（二）| 域渗透之Kerberoast攻击

内网渗透（三）| AS-REP Roasting攻击

记一次有意思的文件上传

内网渗透（四）| 票据传递攻击

利用Metasploit 打入ThinkPHP内网

渗透测试业务逻辑测试汇总—专项篇

渗透测试业务逻辑测试汇总—通用篇

一张图告诉你，如何渗入企业内网

权限维持之打造不一样的映像劫持后门

看到日不下的站

【HTB系列】靶机Bitlab的渗透测试

3

渗透测试二之全局

HW弹药库之红队作战手册

Moriarty Corp靶场攻略

desc巧用及反引号 ` SQL注入——【61dctf】 inject writeup

手把手教你写JAVA反序列化的POC

WMI ——重写版

信息泄漏篇

我是怎么找到通用漏洞的

内网、域环境中的一些实用小技巧

如何查看域用户登录的计算机

通过计划任务实现持续性攻击

4

渗透实战

支付漏洞实战

APP | edxposed框架+trustmealredy模块抓包小程序

CMSEASY逻辑漏洞思路剖析

我是如何从传销成功进阶诈骗的（这是一篇励志的正能量文章）

一次稍显曲折的爆破经历

单引号双引号与poc的故事

WINHEX之从数据恢复到删盘跑路

一次有意思的代码审计(初学)

记一次面试题getshell

authing越权查看用户敏感信息

Mac风格的Windows

BeesCMS的SQL注入漏洞

后门技巧之使用网站关键字进行反连

使用Powershell对目标进行屏幕监控

利用Javascript做后门的利用方式

phpmyadmin getshell到提权

Linux下利用SUID提权

提权之DLL注入

使用Powershell对目标进行屏幕监控

MYSQl任意文件读取

XSS备忘录

如何在Google Web Toolkit环境下Getshell

Mysql报错注入之函数分析

干货合辑，一场关于星球学员头脑风暴

思维的碰撞衍生的是全新的思想收获~整合汇集了各种干货笔记及安全工具。结伴同行，必有我师焉...

1

星球学员分享

【学员笔记分享】汇编之EFLAGS寄存器中标志位

【分享】基于CloudFront的Web匿名代理池

【学员笔记分享】二进制逆向学习笔记：汇编之通用寄存器

【学员分享】基于sqlmap对DVWA靶场SQL注入进行破解

【学员分享】基于sql注入的sqli-lab靶场的手工注入

【学员分享】极客大挑战

“净网2020”打击网络色情，社工追踪变态色情狂

贷款诈骗 x 摸版0day + 实战预警脚本

通过编写python函数来一步步打造属于自己得渗透模块[提升工作效率]

对某大型网站的逻辑漏洞发现

从远程计算机获取WMI数据

Cobaltstrike去除特征

一文打尽 Linux/Windows端口复用实战

被“误伤”的后门文件

一文打尽端口复用 VS Haproxy端口复用

PowerShell5.X与WMI的集成 专题系列分享 第一部分

Windows域关系学习 全攻略

hackthebox 我的第一次

关于 MySQL 数据库空字符及弱类型的探讨

PHP反序列化笔记

Mr.Robot靶机 - 机器人先生

二进制逆向学习笔记：堆栈图解析汇编中函数调用的过程

【工控安全】从0~1学习PLC攻击

汇编指令大全第二篇{学习笔记}

C语言基础01--初见C语言

2

公益公开课

CDN Backfired | 清华大学DSN2020发表论文剖析（上）

国际安全学术会议DSN2020最佳论文奖 | “CDN 范围放大攻击”深入剖析（下）

视频 | 从零开始weblogic的反序列化漏洞

二进制安全入门公开课●限时￥1

做力所能及的事儿支持武汉●附《挖掘某最新cms漏洞》公开课录播

【精品公开课】90分钟之内入门SQL注入

【公益公开课】9.9元-90分钟之内入门SQL注入

1月1号晚8:00 JAVA漏洞分析与实战利用直播

3

安全工具

【福利】Cobalt Strike 4.0 官方教程笔记来了！

Cobalt Strike使用Cross C2上线Linux

Cobalt Strike 证书修改

firda学习

工具使用 | CobaltStrike上线Linux主机(CrossC2)

7大单兵武器库下载 | 渗透测试集成系统环境

自动化渗透测试工具包：APT2

sn0int - 半自动化 OSINT 框架和包管理器

THIS WONDERFUL LIFE

插播新书预告——JAVA代码安全审计

梦里寻她千百度 | 新书预告：JAVA代码安全审计

课程视频配合图书的整体结构主要从以下几个方面展开讲解：

1.Java代码审计预备知识

2.典型的Java Web漏洞剖析

3.Java EE开发框架安全审计

4.开源Java Web应用代码审计实战

5.“交互式应用程序安全测试”与“运行时应用自保护”等技术

6.Java安全编码规范

￥定价499元，人数超200人后，每新增100人，加价99元~~

新年福利：

前100位享受￥439元优惠价（名额有限还剩60个）

再附赠全书完整全套源码、工具及环境、配套的Docker镜像

官方网站：www.ms08067.com

Ms08067安全实验室

扫描下方二维码加入星球学习

加入后会邀请你进入内部微信群，内部微信群永久有效！

Java代码安全审计【Ms08067】

星主： 徐哥

知识星球

微信扫描预览星球详情

Ms08067安全实验室

内网攻防【Ms08067】

星主： 徐哥

知识星球

微信扫描预览星球详情

Ms08067安全实验室

2021 继续一起开心冲浪！