

# 目录

前言	1.1
渗透测试概述	1.2
渗透测试和攻击	1.2.1
网络攻击和防御	1.2.1.1
渗透测试手段	1.3
Web前端	1.3.1
代码注入类	1.3.1.1
XSS跨站脚本	1.3.1.1.1
CSRF跨站请求伪造	1.3.1.1.2
后端	1.3.2
SQL注入	1.3.2.1
RCE远程代码执行	1.3.2.2
SSRF服务端请求伪造	1.3.2.3
CORS跨域资源共享	1.3.2.4
越权访问	1.3.2.5
后端语言	1.3.2.6
Java	1.3.2.6.1
JAVA反序列化	1.3.2.6.1.1
struts2	1.3.2.6.1.2
文件	1.3.3
文件包含	1.3.3.1
文件上传	1.3.3.2
目录浏览	1.3.3.3
任意文件读取和下载	1.3.3.4
XML文件	1.3.3.5
XXE	1.3.3.5.1
渗透测试工具	1.4
漏洞扫描类	1.4.1
Metasploit	1.4.1.1
AppScan	1.4.1.2
AWVS	1.4.1.3
Burp Suite	1.4.1.4
Cobalt Strike	1.4.1.5
Nessus	1.4.1.6
ZAP	1.4.1.7

其他	1.4.1.8
NetSparker	1.4.1.8.1
Nikto	1.4.1.8.2
N-Stalker	1.4.1.8.3
Whisker	1.4.1.8.4
Sn1per	1.4.1.8.5
WebScarab	1.4.1.8.6
Webinspect	1.4.1.8.7
Wikto	1.4.1.8.8
端口扫描类	1.4.2
nmap	1.4.2.1
Layer	1.4.2.2
注入类	1.4.3
sqlmap	1.4.3.1
模糊测试类	1.4.4
渗透测试阶段	1.5
渗透前	1.5.1
渗透中	1.5.2
后渗透	1.5.3
相关	1.6
安全分析	1.6.1
安全日志分析	1.6.1.1
网络分析工具	1.6.1.2
网络和安全证书	1.6.2
附录	1.7
参考资料	1.7.1

# 潜入你的网络：渗透测试

- 最新版本: v0.8
- 更新时间: 20210526

## 简介

先对渗透测试进行宏观概述，属于安全方向的哪个子领域。再介绍基本的渗透测试和攻击的大体流程和涉及内容，再整理出网络攻击和防御的全流程和涉及的方方面面的内容。总结各种渗透测试的手段，包括Web前端的代码注入类的XSS跨站脚本攻击、CSRF跨站请求伪造，后端的SQL注入、RCE远程代码执行、SSRF服务端请求伪造、CORS跨域资源共享、越权访问，后端语言比如Java的反序列号、struts2等，以及文件类的文件包含、文件上传、目录浏览、任意文件读取和下载、XML文件的XXE等；以及其他渗透测试工具，比如漏洞扫描类的Metasploit、AppScan、AWVS、BurpSuite、Cobalt Strike、Nessus、ZAP和其他一些不常见的工具；以及端口扫描类的nmap、Layer等，注入类的sqlmap等以及模糊测试相关工具；然后根据渗透测试阶段，分渗透前、渗透中、渗透后；以及相关的玩网络安全，包括安全日志分析、网络分析工具等内容。

## 源码+浏览+下载

本书的各种源码、在线浏览地址、多种格式文件下载如下：

### Gitbook源码

- [crifan/infiltrate\\_your\\_net\\_penetration\\_testing: 潜入你的网络：渗透测试](#)

### 如何使用此Gitbook源码去生成发布为电子书

详见：[crifan/gitbook\\_template: demo how to use crifan gitbook template and demo](#)

### 在线浏览

- [潜入你的网络：渗透测试 book.crifan.com](#)
- [潜入你的网络：渗透测试 crifan.github.io](#)

### 离线下载阅读

- [潜入你的网络：渗透测试 PDF](#)
- [潜入你的网络：渗透测试 ePub](#)
- [潜入你的网络：渗透测试 Mobi](#)

## 版权说明

此电子书教程的全部内容，如无特别说明，均为本人原创和整理。其中部分内容参考自网络，均已备注了出处。如有发现侵犯您版权，请通过邮箱联系我 admin 艾特 crifan.com，我会尽快删除。谢谢合作。

## 鸣谢

感谢我的老婆陈雪的包容理解和悉心照料，才使得我 crifan 有更多精力去专注技术专研和整理归纳出这些电子书和技术教程，特此鸣谢。

## 更多其他电子书

本人 crifan 还写了其他 100+ 本电子书教程，感兴趣可移步至：

[crifan/crifan\\_ebook\\_readme: Crifan的电子书的使用说明](#)

crifan.com，使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2021-05-26 22:19:37

# 渗透测试概述

如之前在[信息安全概览](#)中所总结的，信息安全领域内有几个大的方向：

- 线上或线下
  - 侧重线下的
    - 侧重windows系统的： 漏洞和安全
  - 侧重线上的
    - 侧重远程Web网络的： 渗透测试
    - 侧重远程工控设备的： 工控安全  $\sim=$  物联网安全
- 设备和端
  - 侧重移动端： 移动端 安全和破解
    - 安卓 的安全和破解
    - iOS 安全和破解

而此处主要介绍涉及到线上的，尤其是[Web网络](#)端的 渗透测试

## 概述

- 渗透测试  $\sim=$  渗透攻击  $\sim=$  网络攻击  $\sim=$  Web安全  $\sim=$  网络安全
  - 含义
    - 模拟一种网络攻击，在真正的黑客入侵之前，模拟黑客入侵企业网络来发现薄弱之处
    - 渗透测试工程师完全模拟黑客可能使用的攻击技术和漏洞发现技术，对目标网络、主机、应用的安全作深入的探测，发现系统最脆弱的环节
  - 目的
    - 发现目标系统潜在的业务漏洞风险
  - 标准
    - PTES = Penetration Testing Execution Standard = 渗透测试执行标准
      - 包含
        1. Pre-engagement Interactions 前期交互
        2. Intelligence Gathering 信息收集
        3. Threat Modeling 威胁建模
        4. Vulnerability Analysis 漏洞分析
        5. Exploitation 渗透利用
        6. Post Exploitation 后渗透
        7. Reporting 报告
    - 输出
      - 渗透测试报告
        - 几类
          - 只提供一份测试报告，报告主体内容是 漏洞列表，漏洞详情
          - 提供简单的 checklist，一般是以附录的形式写在测试报告中
          - 提供来测试计划，以及测试报告
    - 常用工具
      - 扫描
        - 漏洞扫描 = Web漏洞扫描 = Vulnerability Scanning

- AwVS
- appscan
- Metasploit
- Burp = Burp Suite = Burpsuite
- Metasploit = MSF = Metasploit Framework
- CS = Cobalt Strike
- 端口扫描
  - nmap
- 注入类
  - SQL
    - sqlmap
- 相关
  - 模糊测试
    - 名词: 模糊测试 = fuzz = fuzz testing = fuzzing
    - 工具
      - PEACH = Peach = Peach Fuzzer
      - Sulley
      - AutoDafe

## 概念对比

### 安全检测 vs 渗透测试

- 安全检测
  - 横向 地毯式 自动化扫描
- 渗透测试
  - 纵向 深度 人工化入侵

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:10:58

# 渗透测试和攻击

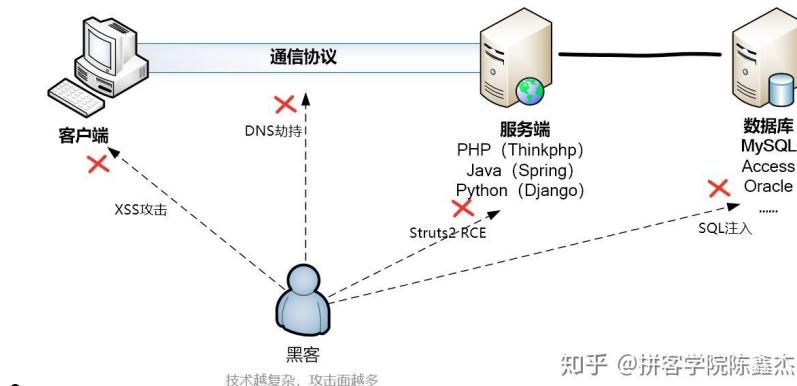
- 普通用户：上网 = 访问网络
  - 基本流程



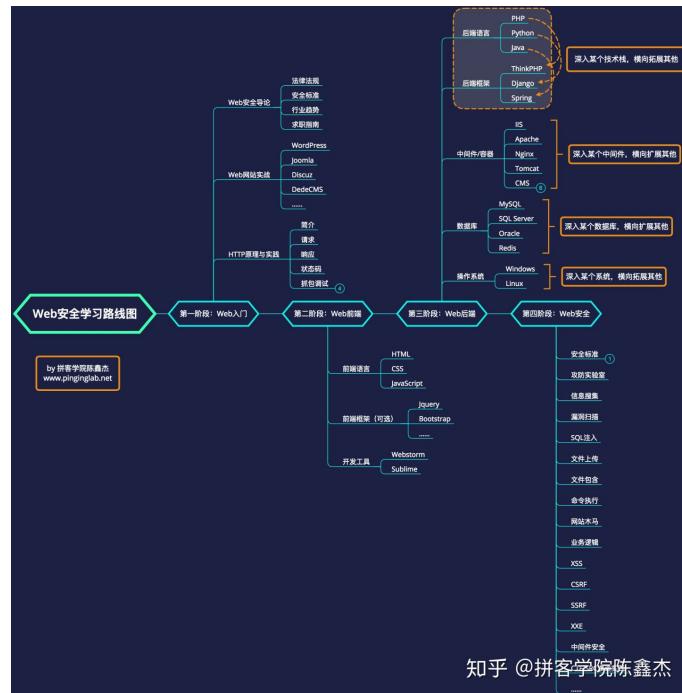
- 详细过程



- 渗透测试 ~= 渗透攻击



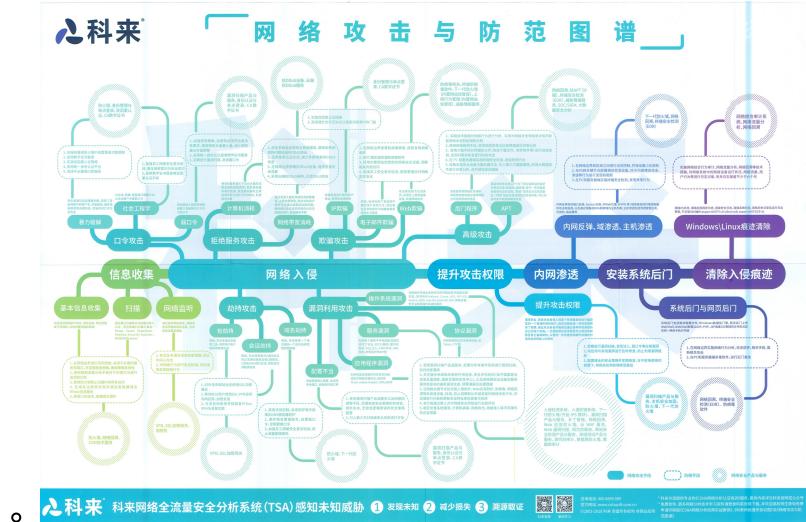
- (对应的、可能的) 学习路线



crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2021-05-26 22:11:07

# 网络攻击和防御

- 网络攻击与防御图谱



- 有助于从大体上了解网络攻击的宏观流程和具体涉及内容

crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2021-05-26 22:14:31

# 渗透测试手段

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:16:20

# Web前端

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:13:12

# 代码注入类

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:12:05

# XSS跨站脚本

- 前端安全
  - 背景
    - 移动互联网
    - 前端的攻击
  - 攻击手段 = 安全问题
    - 传统
      - XSS
      - CSRF
    - 新型
      - 网络劫持
      - 非法调用 Hybrid API
  - 防护手段
    - 浏览器
      - CSP
      - Same-Site Cookies
- XSS
  - XSS = Cross-Site Scripting = 跨站脚本 -> 跨站脚本攻击 = 跨站攻击
    - 为何缩写成XSS而不是CSS?
      - 已有缩写CSS, 表示网页领域的层叠样式表 (Cascading Style Sheets)
      - 所以改用XCS, 其中X表示Cross的交叉的含义
  - 是什么: 网站应用程序的安全漏洞攻击手段之一
    - 攻击者通过在目标网站上注入(恶意)脚本, 使之在用户的浏览器上运行, 从而引发潜在风险
      - 利用这些恶意脚本, 攻击者可获取用户的敏感信息如 Cookie、SessionID 等, 进而危害数据安全
  - 类型: 代码注入 攻击
  - 本质
    - 恶意代码未经过滤, 与网站正常的代码混在一起
      - 浏览器无法分辨哪些脚本是可信的, 导致恶意脚本被执行
  - 相关
    - CSRF
      - = 跨站请求伪造
  - 原理
    - 利用网页开发时留下的漏洞
    - 通过巧妙的方法注入恶意指令代码到网页
      - 恶意指令的语言
        - 常是: JavaScript
        - 其他
          - Java
          - VBScript
          - ActiveX
          - Flash
          - HTML

- 使用用户加载并执行攻击者恶意制造的网页程序
- 攻击策略
  - 在部分情况下，由于输入的限制，注入的恶意脚本比较短
  - 但可以通过引入外部的脚本，并由浏览器执行，来完成比较复杂的攻击策略
- (恶意代码) 注入来源
  - 来自用户的 UGC 信息
  - 来自第三方的链接
  - URL 参数
  - POST 参数
  - Referer (可能来自不可信的来源)
  - Cookie (可能来自其他子域注入)
- 攻击类型
  - 按攻击来源分
    - 存储型：经过后端，经过数据库
    - 反射型：经过后端，不经过数据库
    - DOM 型：通过前端，不经过后端
      - DOM-based XSS漏洞
        - 基于文档对象模型Document Object Model,DOM)的一种漏洞
        - dom - xss是通过url传入参数去控制触发的
  - 按是否持久分
    - 非持久型xss攻击
      - 顾名思义，非持久型xss攻击是一次性的，仅对当次的页面访问产生影响。非持久型xss攻击要求用户访问一个被攻击者篡改后的链接，用户访问该链接时，被植入的攻击脚本被用户浏览器执行，从而达到攻击目的。
    - 持久型xss攻击
      - 持久型xss，会把攻击者的数据存储在服务器端，攻击行为将伴随着攻击数据一直存在。
- 结果效果
  - 获取到
    - 更高权限
      - 提权
        - 利用植入Flash，通过crossdomain权限设置进一步获取更高权限
      - 私密网页内容
      - 会话
      - Cookie
        - 盗用cookie，获取敏感信息
  - 攻击
    - 利用以获取的用户信息冒充用户向网站发起攻击者定义的请求
    - 举例
      - 利用可被攻击的域受到其他域信任的特点，以受信任来源的身份请求一些平时不允许的操作，如进行不当的投票活动
      - 利用iframe、frame、XMLHttpRequest或上述Flash等方式，以（被攻击）用户的身份执行一些管理动作，或

- 执行一些一般的如发微博、加好友、发私信等操作
- 在访问量极大的一些页面上的XSS可以攻击一些小型网站，实现DoS攻击的效果
- 防护手段
  - 后端（开发期间）
    - HTML 转义 = 过滤特殊字符
    - 使用HTTP头指定类型

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:10:56

# CSRF跨站请求伪造

- CSRF
  - 名称
    - CSRF = Cross-Site Request Forger = 跨站请求伪造
    - 缩写：
      - CSRF
      - XSRF
    - 又称： One Click Attack = Session Riding
  - 含义：一种对网站的恶意利用
    - 攻击者盗用了你的身份，以你的名义进行某些非法操作
      - CSRF能够使用你的账户发送邮件，获取你的敏感信息，甚至盗走你的账户
  - 说明
    - 听起来像跨站脚本（XSS），但它与XSS非常不同，并且攻击方式几乎相左
      - XSS 利用站点内的受信任用户
      - CSRF 则通过 伪装 来自受信任用户的请求来利用受信任的网站
        - 与XSS攻击相比，CSRF攻击往往不大流行（因此对其进行防范的资源也相当稀少）和难以防范，所以被认为比XSS更具危险性
  - 扫描是否存在CSRF漏洞
    - 自动化扫描工具
      - netspark
      - AwVS
      - appscan
    - 半自动检测工具
      - CSRFTester

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新：2021-05-26 22:11:31

# 后端

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:16:49

# SQL注入

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:14:44

# RCE远程代码执行

- RCE
  - = Remote Code Execution = 远程命令执行 -> RCE漏洞
    - = RCI = Remote Code Injection
  - 用途：用户通过浏览器提交执行命令，由于服务器端没有针对执行函数做过滤，导致在没有指定绝对路径的情况下就执行命令，可能会允许攻击者通过改变 \$PATH 或程序执行环境的其他方面来执行一个恶意构造的代码

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新：2021-05-26 22:08:09

# SSRF服务端请求伪造

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:14:44

# CORS跨域资源共享

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:10:30

# 越权访问

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:17:03

# 后端语言

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:17:59

# Java

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:12:59

# JAVA反序列化

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:10:02

## struts2

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:14:55

# 文件

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:15:16

## 文件包含

- 文件包含 -> 文件包含漏洞
  - LFI = Local File Inclusion
  - RFI = Remote File Inclusion

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:16:01

# 文件上传

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:12:43

# 目录浏览

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:16:08

# 任意文件读取和下载

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:10:43

# XML文件

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:11:22

# XXE

- XML

- 基础知识

- XML中可以引入外部文件
      - DTD（文档类型定义）的作用是定义 XML 文档的合法构建模块。DTD 可以在 XML 文档内声明，也可以外部引用
      - 引用外部DTD
        - <!DOCTYPE 根元素 SYSTEM "文件名">
        - 或者
          - <!DOCTYPE 根元素 PUBLIC "public\_ID" "文件名">
      - 引用外部实体
        - <!ENTITY 实体名称 SYSTEM "URI">
        - 或者
          - <!ENTITY 实体名称 PUBLIC "public\_ID""URI">
      - 当允许引用外部实体时，通过构造恶意内容，可导致读取任意文件、执行系统命令、探测内网端口、攻击内网网站等危害
        - 不同程序支持的协议不一样

libxml2	PHP	Java	.NET
file	file	http	file
http	http	https	http
ftp	ftp	ftp	https
	php	file	ftp
	compress.zlib	jar	
	compress.bzip2	netdoc	
	data	mailto	
	glob	gopher	*
	phar		

- XXE = XML eXternal Entity = XML外部实体 -> XML外部实体注入 -> XXE漏洞

- 2017年的 OWASP 10之一

- 含义：

- 一种针对解析XML输入的应用程序的攻击。
    - 它实质上是另一种注入类型攻击
    - 如果正确利用，可能非常严重。
      - 当包含对外部实体的引用的XML输入是由弱配置的XML解析器处理时该攻击就会发生。
      - 这种攻击可能导致从解析器所在机器泄漏机密数据，拒绝服务，服务器端请求伪造，端口扫描，以及其他一些系统影响，如亿笑-Dos攻击

- XXE漏洞利用举例

```
http://192.168.0.145:65412/?xml=<!DOCTYPE example [<!ENTITY xxe SYSTEM
```

- 对策

- 举例

- PHP

- 禁用外部实体: `libxml_disable_entity_loader` 设置为 TRUE

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:17:39

# 渗透测试工具

- 渗透测试常见工具
  - 漏洞扫描类
    - AppScan : IBM的一款安全扫描软件
    - AWVS : 一款知名的网络漏洞扫描工具
    - Burp Suite : 一款信息安全从业人员必备的集成型的Web渗透测试工具, 价格昂贵的收费软件
    - Cobalt Strike : 一款基于java的渗透测试神器, 常被业界人称为CS神器
    - Nessus : 目前全世界最多人使用的Web漏洞扫描与分析软件
    - NetSparker : 一款综合型的web应用安全漏洞扫描工具
    - Nikto : 一个开源的Web服务器扫描器, 漏洞扫描神器
    - WebScarab : 一个用来分析使用HTTP和HTTPS协议的应用程序框架
    - Whisker : 一款非常好的HTTP服务器缺陷扫描软件, 基于libwhisker
    - ZAP : OWASP的集成渗透测试和漏洞工具, 免费开源跨平台
  - 端口扫描
    - nmap : 网络端口扫描嗅探工具
  - SQL注入
    - Sqlmap : 数据库注入神器

更新细节详见后续解释。

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:11:18

## 漏洞扫描类

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:17:38

# Metasploit

- Metasploit
  - Metasploit = MSF = Metasploit Framework = Metasploit框架 = Metasploit项目
  - 简介
    - 世界上使用最广泛的渗透测试框架
    - Metasploit项目是一个旨在提供安全漏洞信息计算机安全项目，可以协助安全工程师进行渗透测试及入侵检测系统签名开发。Metasploit项目最为知名的子项目是开源的Metasploit框架，一套针对远程主机进行开发和执行"exploit代码"的工具
  - 使用
    - 像是一把弓箭
      - 瞄准目标，选择漏洞，选择有效载荷，然后发射

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新：2021-05-26 22:15:19

# AppScan

- AppScan
  - = IBM AppScan
  - 一句话介绍：IBM公司开发的用于扫描web应用的基础架构，也是安全渗透行业扛把子的产品

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新：2021-05-26 22:15:45

## AWVS

- AWVS
  - = Acunetix Web Vulnerability Scanner
  - 一句话描述：一款知名的全能的Web安全漏洞扫描器，并附带有很多实用的工具
    - 通过网络爬虫测试你的网站安全，检测流行安全漏洞

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新：2021-05-26 22:12:04

# Burp Suite

- Burp Suite = BurpSuite
  - 简介
    - 一款信息安全从业人员必备的集成型的渗透测试工具，它采用自动测试和半自动测试的方式
    - 一款专业人员常用的昂贵的工具
  - 特点
    - 收费
    - 有免费的社区版
      - 但功能有限
      - 功能全面
  - 用途
    - 个人常用于暴破，抓包，CSRF测试等等

crifan.com，使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新：2021-05-26 22:17:30

## Cobalt Strike

- Cobalt Strike
  - = CobaltStrike
    - 别称: CS神器
  - 一款基于java的渗透测试神器

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:17:51

# Nessus

- Nessus
  - 一句话介绍：Nessus 是目前全世界最多人使用的Web漏洞扫描与分析软件
    - 总共有超过75,000个机构使用Nessus 作为扫描该机构电脑系统的软件
  - 竞品
    - Burp Suite

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新：2021-05-26 22:10:46

# ZAP

- ZAP
  - 名称
    - ZAP = Zed Attack Proxy
    - ZAP = OWASP ZAP = Owasp-Zap
  - 简介
    - 一款开源的Web安全扫描软件
  - 原理
    - ZAP置于浏览器和测试网站之间（又名中间人），允许拦截流量进行检查和修改
  - 竞品
    - Arachni、Wfuzz、Nikto

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:10:14

## 其他

此处整理不太出名的其他的渗透测试领域的漏洞扫描相关工具。

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:17:47

## NetSparker

- NetSparker
  - 一款综合型的web应用安全漏洞扫描工具
  - 对SQL注入， XSS， LFI等漏洞扫描效果不错的漏洞扫描器

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:13:40

## Nikto

- Nikto
  - 一款开源的（GPL）网页服务器扫描器，它可以对网页服务器进行全面的多种扫描

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:17:37

## N-Stalker

- N-Stalker
  - 旧称: N-Stealth
  - 是什么: 一款商业级的Web服务器安全扫描程序

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:17:12

## Whisker

- Whisker
  - Whisker是一款基于libwhisker的扫描器，但是现在大家都趋向于使用Nikto，它也是基于libwhisker的

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:14:11

## Sn1per

- Sn1per
  - 擅长枚举以及扫描已知漏洞
  - 建议这个工具与Metasploit或Nessus一起使用

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:10:27

## WebScarab

- WebScarab
  - 一个用来分析使用HTTP和HTTPS协议的应用程序框架
    - WebScarab记录它检测到的会话内容，使用者可以通过多种形式来查看记录

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:10:58

# Webinspect

- Webinspect
  - = HP Webinspect
  - 惠普公司的安全渗透产品，运行起来占用大量内存，小家碧玉的就慎用了

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:15:26

## Wikto

- Wikto
  - Wikto是一款基于C#编写的Web漏洞扫描工具

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:08:55

## 端口扫描类

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:12:44

## nmap

TODO:

- 【记录】尝试用nmap去扫描局域网内的计算机的ip和其他详细信息 – 在路上
- nmap
  - =网络扫描仪
  - GUI 版本: Zenmap
    - 包了一个可视化的皮
  - 功能: 扫描端口
    - 就像: 敲门看看你家是否有人
    - 扫描看你开了哪些端口
    - 猜测端口用于何种用途
  - 介绍
    - 不少黑客爱用的工具, 黑客会利用nmap来搜集目标电脑的网络设定, 从而计划攻击的方法
  - 竞品
    - masscan

\* 扫全球的时候用

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:13:49

# Layer

TODO:

待整理

[子域名搜集思路与技巧梳理 - SecPulse.COM | 安全脉搏](#)

- Layer
  - 简介：一款域名查询工具，可提供网站子域名查询服务
    - 子域名/IP段收集
  - 被称为：Layer子域名挖掘机
  - 作用和特点：
    - 拥有简洁的界面、简单的操作模式
    - 支持服务接口、暴力搜索、同服挖掘三种模式
    - 支持打开网站、复制域名、复制IP、复制CDN、导出域名、导出IP、导出域名+IP、导出域名+IP+WEB服务器以及导出存活网站！
      - 可过滤过出存活主机
  - GitHub
    - euphrat1ca/LayerDomainFinder: Layer子域名挖掘机
      - <https://github.com/euphrat1ca/LayerDomainFinder>

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新：2021-05-26 22:09:05

# 注入类

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:16:46

## Sqlmap

- Sqlmap
  - 数据库注入神器
  - 自动执行检测，利用SQL注入漏洞并接管数据库服务器的过程
  - 支持
    - MySQL
    - Oracle
    - PostgreSQL
    - Microsoft SQL Server
    - Microsoft Access
    - IBM DB2
    - SQLite
    - Firebird
    - Sybase
    - SAP MaxDB
    - Informix
    - HSQLDB
    - H2

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:15:33

## 模糊测试类

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:14:17

## 渗透测试阶段

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:17:56

## 渗透前

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:15:29

# 渗透中

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:08:52

## 后渗透

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:14:17

## 相关

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:17:25

# 安全分析

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:08:48

# 安全日志分析

- 安全日志分析
  - 工作所需技能
    - **40%的渗透测试**: 了解渗透攻击相关逻辑和相关日志规则
    - **40%大数据技术**: 处理数据, 包括先提取日志中有用数据
    - **20%的人工智能技术**: 用机器学习和AI, 根据数据建模和分析、聚类, 找出逻辑关联
  - 最终实现: 态势感知、攻击溯源

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:17:35

# 网络分析工具

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:17:07

# 网络和安全证书

从事网络安全领域相关工作，有些需要相关证书

关于证书的背景知识：

- 证书类型
  - 三类
    - 厂商认证
      - 依托厂商在行业的影响力、产品垄断等优势而推出的认证，由厂商对认证进行背书
      - 举例：思科的各种认证
    - 行业认证
      - 同样依托行业影响力或相关标准的制定等提供认证的背书
    - 政府(机构)认证
      - 有政府背景的机构来提供认证

此处主要涉及到2大类的证书：

- 网络证书 和 安全证书
  - 概述
    - 目前行业内受认可的信息安全认证主要有 CISP 和 CISSP
    - 国内外的网络安全人员认证
      - 比较综合性的国外认证品牌  
有： CISSP 、 GIAC 、 Security+ 、 CISA / CISM 等
      - 这些国外的认证品牌的专业水平很高，在全球都有很大的影响力，但因为各种原因（诸如费用较高、英文培训和考试、无国内培训班或考点等），在国内的发展有限
    - 国内比较主流的认证品牌有： CISP 、 CCSRP 、 CISAW 等
    - 随着我国国内网络安全从业人员社会化技能认证的日益推进，国内的认证品牌将会进一步发展壮大
  - 作用
    - 找（安全相关）工作 = 求职的敲门砖 = 招聘时标注有 XX 认证的优先考虑
    - 升职加薪 = 镀金以提高身价
    - 项目投标（时候报人员）

## 安全证书

### 国内

#### CISP

- CISP = Certified Information Security Professional = 注册信息安全专业人员
  - 证书类型：政府(机构)认证
  - 发证机构：中国信息安全测评中心
    - CISP 系经 中国信息安全测评中心 实施国家认证
  - 考证要求：需要工作经验

- 考取难度: ★★★☆☆
- 适应类型: 国有企业、政府、军工、8+2行业信息安全主管及为国内提供信息安全服务的安全公司从业人员
- 费用: 培训、考试费为12800 人民币
  - 包括两次补考费用
    - 也就是说有三次考试机会, 再考就每次500考试费
- 认证要求
  - 注册要求
    - 教育与工作经历
      - 硕士及以上: 具有1年工作经历
      - 本科毕业: 具有2年工作经历
      - 大专毕业: 具有4年工作经历
    - 专业工作经历
      - 至少具备1年从事信息安全有关的工作经历
  - 培训资格
    - 在申请注册前, 成功地完成了CNITSEC或其授权培训机构组织的注册信息安全专业人员培训课程相应资质所需的分类课程, 并取得培训合格证书
    - 通过由CNITSEC举行的注册信息安全专业人员考试
    - 能力要求
      - 具备一定的信息安全基础知识, 了解并掌握 GB/T 18336 、 ISO 15408 、 ISO 17799 等有关信息安全标准, 具有进行信息安全服务的能力
- 认证说明
  - 概述
    - CISP是认证类型总称
    - 实际上分为四项认证证书
      - CISE = Certified Information Security Engineer = 注册信息安全工程师
        - 工程师
      - CISO = Certified Information Security Officer = 注册信息安全管理人員
        - 管理员
      - CISP-A = 注册信息安全审核员 = 注册信息安全审计师
        - 审计师
      - CISD = CISP-DRP = 注册信息安全灾难恢复工程师
        - 开发人员
    - 面向对象不同, 适用面也不同
  - 详解
    - CISE / CISO
      - 概述: 侧重安全技术和安全管理, 教材一样, 课程一样, 同班上课, 只是考卷不同而已
      - 详解
        - CISE
          - 如果一直干技术工作的, 建议选CISE
          - 主要从事信息安全技术领域的工作, 具有从事信息系统安全集成、安全技术测试、安全加固和安全运维的基本知识和能力
        - CISO

- 一直干管理或咨询的，建议选CISO
  - 主要从事信息安全管理领域的工作，具有组织信息安全风险评估、信息安全总体规划编制、信息安全策略制度制定和监督落实的基本知识和能力
- CISPA = CISPAudit
  - 侧重安全审计方面的知识
    - 主要从事信息安全审计工作，在全面掌握信息安全基本知识技能的基础上，具有较强的信息安全风险评估、安全检查实践能力
- CISD
  - 面向软件开发人员，侧重软件安全开发
    - 申请中国信息安全测评中心软件安全开发企业认证绑定的是个证书，所以要申请开发类企业认证的，注意要考的是CISD
    - 主要从事信息系统灾难恢复工作，在全面掌握信息安全基本知识技能的基础上，具有较强的信息系统灾难恢复建设和管理的实践能力
- 最新情况
  - 近几年该认证体系不断丰富，引入了更多认证：
    - CISPCSE：对应云安全
    - CISPBDSA：大数据安全
    - CISPICSSE：工控安全
    - CISPPTE/PTS：渗透测试
    - CISPIRE：应急响应
    - CISPDSG：数据治理
    - CISPPIP：个人信息保护
    - CISPF：调查取证
- 注意
  - CISP为强制培训，也就是说不能直接考试，必须报一个授权培训机构（培训也采取授权制，必须有授权才能培训和考试）接受8天的培训后才能参加考试（2018年起调整为五天）
    - 未来会逐步结合在线学习等，降低培训时间要求
  - 报考时要选择考试类型，根据自己能力和擅长方向选择。不要因为听谁说哪个好考就考哪个

### CCSRP = 网络与信息安全应急人员认证

- CCSRPA = 网络与信息安全应急人员认证
  - 发证机构：国家计算机网络应急技术处理协调中心
    - 简称：国家互联网应急中心
    - 是中共中央网络安全和信息化委员会办公室（以下简称中央网信办）的直属事业单位

### CISAW = 信息安全保障人员认证

- CISAW = 信息安全保障人员认证
  - 发证机构：中国网络安全审查技术与认证中心
    - 原中国信息安全认证中心

- 是国家市场监督管理总局直属事业单位，同时在业务上接受中央网信办的指导

## 国外

### CISSP = 信息系统安全专业认证

- CISSP = 信息系统安全专业认证
  - 证书类型：行业认证
  - 发证机构：ISC
    - ISC = 国际信息系统安全认证协会 = International Information Systems Security Certification Consortium
  - 考证要求：需要工作经验
  - 考取难度：★★★★☆
    - 比CISP难度多一星
    - 因为英语和6小时的考试时间，比较摧残人
  - 适应类型：外企、涉外服务、大型企业（包括国有企业，有不少国企也比认CISSP）如银行等信息安全主管和信息安全从业者
  - 费用：
    - 培训：不强制 -> 无需培训也可直接考试
    - 国内很多培训公司都提供
    - 考试：考试费 599美元
      - 这是一次考试的费用，如果没通过，下次还要交考试费
  - 证书



- 作用：代表国际信息系统安全从业人员的权威认证
- 认证对象
  - 面向从事商业环境安全体系建构、设计、管理或控制的专业人员
    - 对从业人员的技术及知识积累进行测试
- ISC 共有9项认证
  - CISSP = 注册信息系统安全师
  - 8个延伸出来的系列认证
    - CSSLP = 注册软件生命周期安全师
    - CCFPSM = 注册网络取证师
    - CAP = 注册信息安全许可师
    - SSCP = 注册系统安全员
    - HCISPPSM = 医疗信息与隐私安全员
    - CISSP专项加强认证
      - CISSP-ISSAP = Information Systems Security Architecture Professional = 信息系统安全架构专家

- CISSP-ISSEP = Information Systems Security Engineering Professional = 信息系统安全工程专家
- CISSP-ISSMP = Information System Security Management Professional = 信息系统安全管理专家
- 考试内容=领域：8个
  - 安全和风险管理
  - 资产安全
  - 安全架构和安全模型
  - 通信和网络安全
  - 身份和访问管理
  - 安全评估和测试
  - 安全操作
  - 软件开发安全
- 要求
  - 在两个或两个以上CISSP领域有五年相关工作经验
- 现状
  - 根据Global Knowledge的数据
    - 到2020年，持证人员的平均工资为141452美元
    - CISSP证书持有者
      - 平均年龄为48.1岁
      - 从事安全工程师或分析师工作
      - 普遍拥有6.1项证书
- 评价
  - CISSP因为推出比较早，所以相对比较知名
    - 目前认证中也就CISSP因为资格老，比较多人知道，所以考的较多，其他的嘛，屈指可数
  - CISSP考试相对难些
    - CISSP考试难点在于两个地方，一是英文考试，二是考试时间。
      - 考题
        - 考卷250道题，其中50道是不计分的（哪50道题都不知道）
      - 考试时间
        - 6小时，也就是360分钟
        - 平均不到一分半要答一道题
          - 中间还需要上厕所，吃东西，所以每道题时间就一分钟多
    - 英文
      - 对英语的要求不是一点点的高
      - 后来改成中英文都有
        - 愿意看中文的看中文，不愿意看中文的看英文
      - 不过根据之前参加考试的反馈，中文题翻译的质量实在不咋的，很多人题都读不懂，还不如用英文
      - 并且六个小时的考试，大脑高度紧张，压力是真不小的

## 安全证书对比

CISP VS CISSP

- CISP VS CISSP

- 相同点

- CISP 和 CISSP : 都是偏重信息安全管理的 = 信息安全类认证
    - 技术知识讲的宽泛且浅显, 考试都是一带而过 = 特点: 一英里宽一英寸深
    - 这两个认证证明持证人员对信息安全知识了解比较全面
    - 两者没本质区别
    - CISSP从2011年就开始谋求在中国与CISP互认, 互认的备忘录都签了
    - 当时双方还做了知识体系的对比, 知识体系没太多差别, 基本都是一致的
    - 主要差别在法律法规上。所以双方没有本质区别
  - 不同点
  - CISSP
    - 要求持证人员的信息安全工作经验都要5年以上
    - 特点
      - 由于 CISSP 推出时间较早, 目前已经国际化运作, 因此被称为国际认证
  - CISP
    - 要求大专学历4年以上工作经验
    - 特点
      - CISP 是中国信息安全测评中心推出, 有政府背景给认证做背书

## 网络证书

### CCIE = 思科认证互联网专家

- CCIE = 思科认证互联网专家
  - 概述: 美国Cisco公司于1993年开始推出的专家级认证考试, 被全球公认为IT业最权威的认证
  - 作用: 证书持有者被认为是具有专业网络技术知识和丰富工作经验的最好证明
  - 证书



- 认证领域：6个
  - 路由和交换认证
  - 服务提供商认证
  - 安全认证
  - 协作认证
  - 数据中心认证
  - 无线认证

**CISA**

**CCNP**

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新：2021-05-26 22:13:10

## 附录

下面列出相关参考资料。

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:10:12

## 参考资料

- [3 Phases of Penetration of Pathogenesis in Plants](#)
- [Phenomenon of infection – pre-penetration, penetration and post penetration](#)
- [第六十一课：高级持续渗透-第五季关于后门 - Micro8](#)
- [记一次完整的渗透测试流程-技术圈](#)
- [Web 安全渗透方面的学习路线? - 知乎](#)
- [黑客以50万美元价格出售Zoom的远程代码执行漏洞](#)
- [rce漏洞 远程代码执行 简介\\_Java\\_whatday的专栏-CSDN博客](#)
- [远程代码执行漏洞 - Mannix的博客 | Mannix](#)
- [从XML到RCE（远程代码执行） - 安全客，安全资讯平台](#)
- [XXE漏洞挖掘分享 - 云+社区 - 腾讯云](#)
- [WEB安全入门系列之CSRF漏洞详解 - SecPulse.COM | 安全脉搏](#)
- [跨站脚本 - 维基百科，自由的百科全书](#)
- [前端安全系列（一）：如何防止XSS攻击？ - 美团技术团队 \(meituan.com\)](#)
- [【渗透实例】记录一次XSS渗透过程 - 知乎 \(zhihu.com\)](#)
- [渗透测试之XSS漏洞详细使用教程【攻防演练】 - 知乎 \(zhihu.com\)](#)
- [渗透测试技巧之一个XSS引发的漏洞利用与思考 - 先知社区 \(aliyun.com\)](#)
- [渗透测试XSS前端漏洞 - 红日攻防实验室 \(sec-redclub.com\)](#)
- [Web Vulnerabilities](#)
- [资深漏洞猎人谈：漏洞赏金 vs 渗透测试，谁更适合企业？ - 安全内参 | 决策者的网络安全知识库](#)
- [Web渗透测试3个要点（信息收集→漏洞发现→漏洞利用） - 简书](#)
- [浅谈Web渗透测试 - FreeBuf专栏·kali渗透测试笔记](#)
- [渗透测试及漏洞挖掘技巧干货分享——客户端JavaScript静态分析 - 知乎](#)
- [Index of /sec-chart/APT 攻击](#)
- [你离IT大佬还差11个认证 | SDNLAB | 专注网络创新技术](#)
- [信息安全从业人员的薪酬水平是怎样的？ - 知乎](#)
- [「安全服务工程师（渗透） 郑州\(J12726\)招聘」\\_绿盟科技招聘-BOSS直聘](#)
- [招聘 | 【阿里系】 【长亭科技】 【安全工程师】 【北京海淀】](#)
- [你离IT大佬还差11个认证 | SDNLAB | 专注网络创新技术](#)
- [漫谈信息安全认证\(CISP与CISSP\) - 知乎](#)
- [考CISP认证，需要哪些条件？ - 知乎](#)
- [国内网络安全人员认证品牌大盘点：CISP、CCSRP和CISAW - 安全内参 | 决策者的网络安全知识库](#)
- [Index of /sec-chart/APT 攻击](#)

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-26 22:10:05