



东塔网络安全学院

DoTa Cyber Security College

网络安全检测与防御技术国家地方联合工程技术研究中心

网络安全检测与防护技术国家地方联合工程研究中心

National Joint Engineering Research Center of Network Security Detection and Protection Technology



经国家发展改革委员会批准成立，由暨南大学牵头51位代表国际一流科研力量的院士、国家千人、长江学者、ACMFellow、IEEEFellow、教育部新世纪优秀人才、全国网络安全优秀教师等多名尖端学者成立“网络安全检测与防护技术国家地方联合工程中心”。



为解决我国网络空间安全人才紧缺、缺口巨大的问题，成立“网络安全检测与防护技术国家地方联合工程中心深圳分中心”。主要负责研究制定国家网络安全人才的教育与培养体系，开发出专门针对零基础人员的职业化实战训练课程以及一体化教学体系。



深圳分中心以网络安全检测与防护技术的研究成果为基础，设立“东塔网络安全学院”，通过培养大量的零基础人员加入网络安全人才大军，形成我国网络空间安全人才职业化等级梯队，铸造国家网络空间安全的“镇东之塔”。

WEB安全-弱口令、验证码安全、暴力破解



第二阶段 OWASP常见WEB漏洞利用及防御



强调声明

本次直播及相关资料仅用于信息防御技术教学，旨在培养白帽子安全工程师，请勿用于其他用途；

在未得到网站授权前提下，禁止对政府、事业单位、企业或其他单位网站及系统进行渗透测试；

技术是把双刃剑，请遵纪守法，做一名合格的白帽子安全专家，为国家的网络安全事业做出贡献。

本次直播及相关资料仅用于信息防御技术教学 请勿用于其他用途

- 1、了解OWASP常见的WEB漏洞的原理；
- 2、掌握弱口令相关概念、实战；
- 3、掌握验证码常见的漏洞原理、利用及防御；
- 4、掌握暴力破解常见的工具、原理；

第一章 OWASP常见漏洞

第一节 OWASP组织介绍

第二节 常见WEB漏洞介绍

第二章 弱口令漏洞

第一节 Kali下字典介绍

第三节 常见弱口令介绍

第四节 弱口令防范

第三章 验证码相关漏洞

第一节 验证码安全介绍

第二节 验证码绕过

第三节 验证码识别工具

第四章 暴力破解

第一节 暴力破解漏洞原理

第二节 字典生成工具介绍

第三节 彩虹表和撞库介绍

第四节 在线、离线暴力破解

第五节 暴力破解漏洞防御

开放式Web应用程序安全项目（OWASP, Open Web Application Security Project）是一个组织，它提供有关计算机和互联网应用程序的公正、实际、有成本效益的信息。其目的是协助个人、企业和机构来发现和使用可信赖软件。

OWASP是一个**非营利组织**，不隶属于任何企业或财团。因此，由OWASP提供和开发的所有设施和文件都不受商业因素的影响。OWASP支持商业安全技术的合理使用，它有一个论坛，在论坛里信息技术专业人员可以发表和传授专业知识和技能

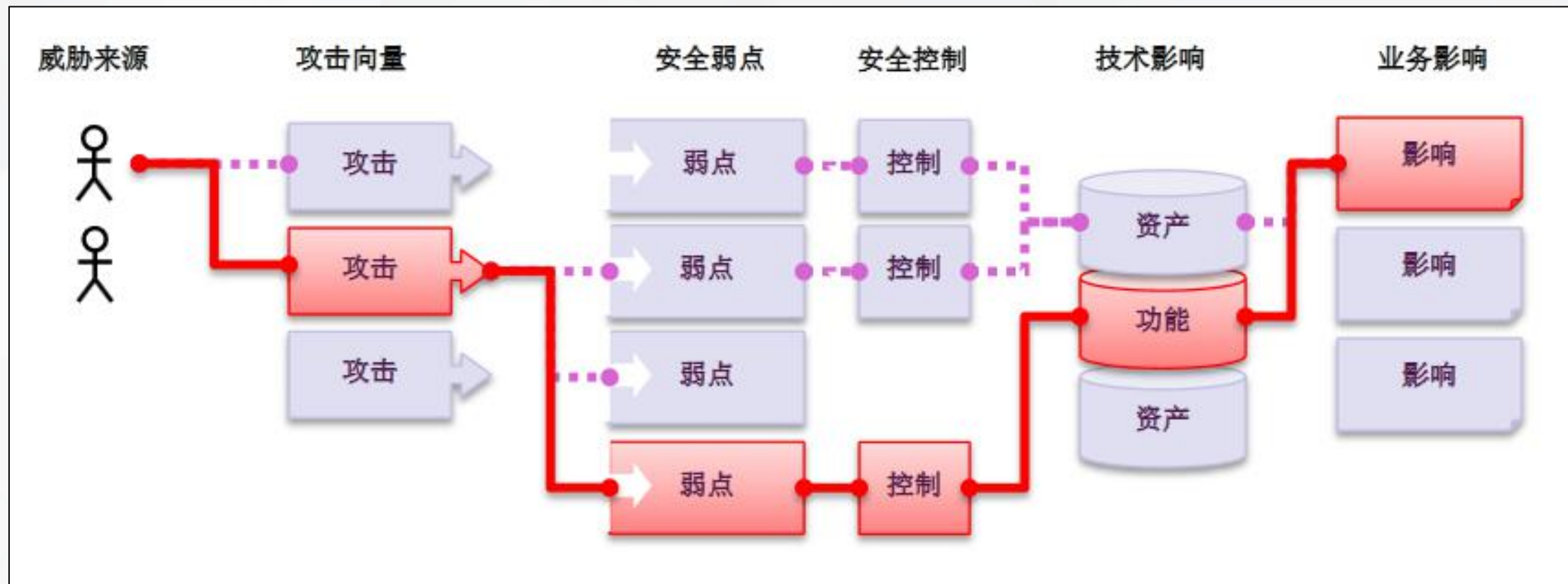


OWASP

Open Web Application
Security Project

<https://owasp.org/>
<http://www.owasp.org.cn/>

什么是应用程序安全风险



OWASP涉及的领域

- OWASP SAMM
- OWASP十大隐私风险 (OWASP_Top_10_Privacy_Countermeasures_v1.0)
- OWASP API 安全 TOP 10 项目
- 反勒索软件指南
- 应用软件安全测试技术
- OWASP ProActive Controls 中文项目
- OWASP无服务器应用安全风险TOP 10
- 区块链安全TOP10 2019
- 数据库审计系统测评基准
- 2010年OWASP Top 10项目
- 2013年OWASP Top 10项目
- 2017年OWASP Top 10项目
- Top 10 mobile controls and design principles

OWASP十大漏洞



OWASP Top 10 2017		change	OWASP Top 10 2021 proposal	
A1	Injections	as is	A1	Injections
A2	Broken Authentication	as is	A2	Broken Authentication
A3	Sensitive Data Exposure	down 1	A3	Cross-Site Scripting (XSS)
A4	XML eXternal Entities (XXE)	down 1 + A8	A4	Sensitive Data Exposure
A5	Broken Access Control	down 1	A5	Insecure Deserialization (merged with XXE)
A6	Security Misconfiguration	down 4	A6	Broken Access Control
A7	Cross-Site Scripting (XSS)	up 4	A7	Insufficient Logging & Monitoring
A8	Insecure Deserialization	up 3 + A4	A8	NEW: Server Side Request Forgery (SSRF)
A9	Known Vulnerabilities	as is	A9	Known Vulnerabilities
A10	Insufficient Logging & Monitoring	up 3	A10	Security Misconfiguration

OWASP十大漏洞

2013年版《OWASP Top 10》	➔	2017年版《OWASP Top 10》
A1 – 注入	➔	A1:2017 – 注入
A2 – 失效的身份认证和会话管理	➔	A2:2017 – 失效的身份认证
A3 – 跨站脚本 (XSS)	➔	A3:2017 – 敏感信息泄漏
A4 – 不安全的直接对象引用 [与A7合并]	U	A4:2017 – XML外部实体 (XXE) [新]
A5 – 安全配置错误	➔	A5:2017 – 失效的访问控制 [合并]
A6 – 敏感信息泄漏	➔	A6:2017 – 安全配置错误
A7 – 功能级访问控制缺失 [与A4合并]	U	A7:2017 – 跨站脚本 (XSS)
A8 – 跨站请求伪造 (CSRF)	☒	A8:2017 – 不安全的反序列化 [新, 来自于社区]
A9 – 使用含有已知漏洞的组件	➔	A9:2017 – 使用含有已知漏洞的组件
A10 – 未验证的重定向和转发	☒	A10:2017 – 不足的日志记录和监控 [新, 来自于社区]

A1:2017-注入

将不受信任的数据作为命令或查询的一部分发送到解析器时，会产生诸如SQL注入、NoSQL注入、OS注入和LDAP注入的注入缺陷。攻击者的恶意数据可以诱使解析器在没有适当授权的情况下执行非预期命令或访问数据。

A2:2017-失效的身份认证

通常，通过错误使用应用程序的身份认证和会话管理功能，攻击者能够破译密码、密钥或会话令牌，或者利用其它开发缺陷来暂时性或永久性冒充其他用户的身份。

A3:2017-敏感数据泄露

许多Web应用程序和API都无法正确保护敏感数据，例如：财务数据、医疗数据和PII数据。攻击者可以通过窃取或修改未加密的数据来实施信用卡诈骗、身份盗窃或其他犯罪行为。未加密的敏感数据容易受到破坏，因此，我们需要对敏感数据加密，这些数据包括：传输过程中的数据、存储的数据以及浏览器的交互数据。

A4:2017-XML 外部实体 (XXE)

许多较早的或配置错误的XML处理器评估了XML文件中的外部实体引用。攻击者可以利用外部实体窃取使用URI文件处理器的内部文件和共享文件、监听内部扫描端口、执行远程代码和实施拒绝服务攻击。

A5:2017-失效的访问控制

未对通过身份验证的用户实施恰当的访问控制。攻击者可以利用这些缺陷访问未经授权的功能或数据，例如：访问其他用户的帐户、查看敏感文件、修改其他用户的数据、更改访问权限等。

A6:2017-安全配置错误

安全配置错误是最常见的安全问题，这通常是由于不安全的默认配置、不完整的临时配置、开源云存储、错误的 HTTP 标头配置以及包含敏感信息的详细错误信息所造成的。因此，我们不仅需要对所有的操作系统、框架、库和应用程序进行安全配置，而且必须及时修补和升级它们。

A7:2017-跨站脚本 (XSS)

当应用程序的新网页中包含不受信任的、未经恰当验证或转义的数据时，或者使用可以创建 HTML 或 JavaScript 的浏览器 API 更新现有的网页时，就会出现 XSS 缺陷。XSS 让攻击者能够在受害者的浏览器中执行脚本，并劫持用户会话、破坏网站或将用户重定向到恶意站点。

A8:2017-不安全的反序列化

不安全的反序列化会导致远程代码执行。即使反序列化缺陷不会导致远程代码执行，攻击者也可以利用它们来执行攻击，包括：重播攻击、注入攻击和特权升级攻击。

A9:2017-使用含有已知漏洞的组件

组件（例如：库、框架和其他软件模块）拥有和应用程序相同的权限。如果应用程序中含有已知漏洞的组件被攻击者利用，可能会造成严重的数据丢失或服务器接管。同时，使用含有已知漏洞的组件的应用程序和 API 可能会破坏应用程序防御、造成各种攻击并产生严重影响。

A10:2017-不足的日志记录和监控

不足的日志记录和监控，以及事件响应缺失或无效的集成，使攻击者能够进一步攻击系统、保持持续性或转向更多系统，以及篡改、提取或销毁数据。大多数缺陷研究显示，缺陷被检测出的时间超过 200 天，且通常通过外部检测方检测，而不是通过内部流程或监控检测。

第一章 OWASP常见漏洞

第一节 OWASP组织介绍

第二节 常见WEB漏洞介绍

第二章 弱口令漏洞

第一节 Kali下字典介绍

第三节 常见弱口令介绍

第四节 弱口令防范

第三章 验证码相关漏洞

第一节 验证码安全介绍

第二节 验证码绕过

第三节 验证码识别工具

第四章 暴力破解

第一节 暴力破解漏洞原理

第二节 字典生成工具介绍

第三节 彩虹表和撞库介绍

第四节 在线、离线暴力破解

第五节 暴力破解漏洞防御

[illegible]

1、弱口令产生原因

与个人习惯和安全意识相关，为了避免忘记密码，使用一个非常容易记住的密码，或者是直接采用系统的默认密码等。

2、弱口令的危害

通过弱口令，攻击者可以进入后台修改资料，进入金融系统盗取钱财，进入OA系统可以获取企业内部资料，进入监控系统可以进行实时监控等等。



1、普通型

普通型弱口令就是常见的密码，比如，目前网络上也有人特地整理了常用的弱口令（Top 100）；对于网站后台而言，一般为：admin、admin123、admin666、admin888、manager...

```
123456 a123456 123456a 5201314 111111 woaini1314 qq123456 123123 000000 1qaz2wsx 1q2w3e4r  
qwe123 7758521 123qwe a123123 123456aa woaini520 woaini 100200 1314520 woaini123 123321  
q123456 123456789 123456789a 5211314 asd123 a123456789 z123456 asd123456 a5201314 aa123456  
zhang123 aptx4869 123123a 1q2w3e4r5t 1qazxsw2 5201314a 1q2w3e aini1314 31415926 q1w2e3r4  
123456qq woaini521 1234qwer a111111 520520 iloveyou abc123 110110 111111a 123456abc w123456  
7758258 123qweasd 159753 qwer1234 a000000 qq123123 zxc123 123654 abc123456 123456q qq5201314  
12345678 000000a 456852 as123456 1314521 112233 521521 qazwsx123 zxc123456 abcd1234 asdasd  
666666 love1314 QAZ123 aaa123 q1w2e3 aaaaaa a123321 123000 1111111 12qwaszx 5845201314  
s123456 nihao123 caonima123 zxcvbnm123 wang123 159357 1A2B3C4D asdasd123 584520 753951 147258  
1123581321 110120 qq1314520
```

1、普通型

具体来说，不同的后台类型拥有不同的弱密码：

- 数据库

账号：root

密码：root、root123、123456

- tomcat

账号：admin、tomcat、manager

密码：admin、tomcat、admin123、123456、manager

- jboss

账号：admin、jboss、manager

密码：admin、jboss、manager、123456

- weblogic

账号：weblogic、admin、manager

密码：weblogic、admin、manager、123456

2、条件型

条件型弱口令就是和用户信息相关的密码，比如生日+手机号、姓名首字母+生日、爱人姓名首字母+生日+常用字母（520、1314 等），可以使用一些社工软件，利用人性的弱点，生成密码字典；

安全牛-爱安全safe6.cn 社工爆破密码生成器v1.0

菜单 帮助

个人信息

姓(拼音):

名字第一个字

名(拼音):

名字第二个字

名(拼音):

名字第三个字

出生年:

出生日期:

年月日全写

邮箱:

手机号:

首字母缩写

名字缩写:

不用加http

网址:

非主流就别写了

网名(拼音):

QQ:

常用密码:

特殊年份:

配偶信息

姓(拼音):

名字第一个字

名(拼音):

名字第二个字

名(拼音):

名字第三个字

出生年:

出生日期:

年月日全写

邮箱:

手机号:

首字母缩写

名字缩写:

不用加http

网址:

非主流就别写了

网名(拼音):

QQ:

常用密码:

特殊年份:

其他信息

当前年:

下一年:

上一年:

使用说明: 填的东西越多, 你爆破成功几率越大,

手机号和姓名生日这三个可以算是必填的,

这三个都没填你就等着翻车吧, 或许弱口令还能救你。

发车区

☐ 混合弱口令

☐ 加入弱口令

☐ 大小写组合

☐ 加入符号

发车

官网



弱口令生成和收集

1、互联网搜索

在搜索引擎中搜索常见弱密码
top1000, top10000。

2、信息泄露

重要互联网企业、平台泄露的敏感数据，根据数据统计频率较高的密码。

3、工具生成

Pydictor、社工爆破密码生成器等。

中国版25个“弱密码”			
*本项统计基于国内流行的密码字典软件破解列表			
*标红密码同时也是国外网民常用的“弱密码”			
简单数字组合	顺序字符组合	临近字符组合	特殊含义组合
000000	abcdef	123qwe	admin
111111	abcabc	qwerty	password
11111111	abc123	qweasd	p@ssword
112233	a1b2c3		passwd
123123	aaa111		iloveyou
123321			5201314
123456			
12345678			
654321			
666666			
888888			

TXT	1w弱密码字典	立即下载
	1w常见弱密码，与大家共享，多一份人品，多一分幸运。	
	上传者: kkdelong 时间: 2019-02-11	
TXT	密码爆破字典	立即下载
	【爆破字典，常用密码，弱口令，5.6M，】	
	上传者: qq_43483233 时间: 2019-04-21	
RAR	弱口令字典，700万左右，分为了5个文件	立即下载
	弱口令字典，700万左右，分为了5个文件，适合暴力破解。比较全了。如果...	
	上传者: tsyang36 时间: 2018-10-30	
RAR	世界级弱口令TOP50000个、	立即下载
	世界级弱口令TOP50000个、	
	上传者: sonbyn001 时间: 2017-04-24	
ZIP	国人常用400万密码字典	立即下载
	国人常用400万密码字典，破解密码必备。	
	上传者: cwt0531 时间: 2013-08-03	
?.?	使用频率最高的密码字典top500	立即下载
	全球使用频率最高的500个密码字典密码字典，用于安全部门检查常见弱口令...	
	上传者: mulakejueshi 时间: 2013-07-30	
ZIP	弱口令字典(400W常用密码).zip	立即下载
	包含TOP10000\TOP300000\400W常用密码	
	上传者: qq_41848933 时间: 2019-08-27	
RAR	弱口令top10000.rar	立即下载
	常用弱口令top10000，ctf便捷方便，burpsuite直接爆破，好用！考弱口令...	
	上传者: lasedy3 时间: 2019-11-18	
TXT	top10000.txt	立即下载
	暴力破解top10000密码: 234 wangkai 5215211314 gordon 19871127...	
	上传者: qq_43700130 时间: 2020-05-18	

Kali系统下的字典介绍

路径: **/usr/share/wordlists**

```
root@kali: /usr/share/wordlists# ls
dirb          dnsmap.txt    fern-wifi     nmap.lst      sqlmap.txt
dirbuster     fasttrack.txt metasploit    rockyou.txt.gz wfuzz
```

1) dirb↓

big.txt #大的字典↓

small.txt #小的字典↓

catala.txt #项目配置字典↓

common.txt #公共字典↓

euskera.txt #数据目录字典↓

extensions_common.txt #常用文件扩展名字典↓

indexes.txt #首页字典↓

mutations_common.txt #备份扩展名↓

spanish.txt #方法名或库目录↓

others #扩展目录, 默认用户名等↓

stress #压力测试↓

vulns #漏洞测试↵

2) dirbuster↓

apache-user-enum-** #apache 用户枚举↓

directories.jbrofuzz #目录枚举↓

directory-list-1.0.txt #目录列表大, 中, 小 big, medium, small↵

3) fern-wifi↓

common.txt #公共 wifi 账户密码↵

4) metasploit↓

... #各种类型的字典↵

5) webslayer↓

general #普通字典目录↓

admin-panels.txt #后台路径 字典↵

Injection #注入字典目录↓

All_attack.txt #全部攻击↓

bad_chars.txt #字符注入↓

SQL.txt #sql 注入↓

7) others #扩展目录↓

common_pass.txt #通用密码字典↓

names.txt #用户名字典↵

stress #压力测试目录↵

vulns #漏洞测试目录↓

apache、iis、cgis...↵

webservices #web 服务目录↓

ws-dirs.txt #路径测试↓

ws-files.txt #文件测试↵

wfuzz ↵

#模糊测试, 各种字典...↵

其他字典介绍

名称	
400W常用密码	1,979,
wordlist	200,
WPA英文字典	2,312,
超级字典	6,210,
弱口令集	16,
生日1980-2010年	1,073,
真空密码字典生成器 2.5 绿色版	4,511,
(1-100W).TXT	10,709,
(101W-200W).TXT	10,204,
(201W-300W).TXT	9,946,
(301W-400W).TXT	9,876,
(401W-500W).TXT	10,330,
0-9.8位纯数密码.txt	1,000,00
3+sr.txt	1,547,52
123.txt	13,723,
133127.txt	200,
142183.txt	8,537,
14365003.txt	170,876
all_birth(vip).txt	2,516,
Beini-1.1 中的新字典.txt	2,624,
bir.txt	127,
DICT 213560 条记录.TXT	2,312,
fcicq-dict-unidict-20100410.txt	2,624,

弱口令如何利用

思路：

1、如果无法绕过验证码情况

直接利用常见的TOP10或者TOP100手动尝试；

2、能够爆破情况

利用Burp等工具调低进程和时间间隔，利用弱口令字典进行爆破

设置密码通常遵循以下原则：

- (1) 不使用空口令或系统缺省的口令，为典型的弱口令；
- (2) 口令长度不小于8 个字符；
- (3) 口令不应该为连续的某个字符（例如：AAAAAAAAA）或重复某些字符的组合（例如：tzf.tzf.）。
- (4) 口令应该为以下四类字符的组合；

大写字母(A-Z)、小写字母(a-z)、数字(0-9)和特殊字符。每类字符至少包含一个。如果某类字符只包含一个，那么该字符不应为首字符或尾字符。

- (5) 口令中不应包含特殊内容；

如本人、父母、子女和配偶的姓名和出生日期、纪念日期、登录名、E-mail 地址等等与本人有关的信息，以及字典中的单词。

- (6) 口令不应该为用数字或符号代替某些字母的单词。
- (7) 口令应该易记且可以快速输入，防止他人从你身后看到你的输入。
- (8) 至少90 天内更换一次口令，防止未被发现的入侵者继续使用该口令。

弱口令相关注意事项

- 1.在笔记本或其它地方不要记录口令。
- 2.向他人透露口令，包括管理员和维护人员。当有人打电话来向你索要口令时，你就该保持警惕了。
- 3.在e-mail或即时通讯工具中不透露口令。
- 4.离开电脑前，启动有口令保护的屏幕保护。
- 5.在多个帐户之间使用不相同的口令。
- 6.在公共电脑不要选择程序中可保存口令的功能选项。

切记，不要使用弱口令，以及保护好你的口令。

同时要注意，改过的口令一定要牢记。很多人因常改口令而遗忘，造成很多不必要的麻烦。

第一章 OWASP常见漏洞

第一节 OWASP组织介绍

第二节 常见WEB漏洞介绍

第二章 弱口令漏洞

第一节 Kali下字典介绍

第三节 常见弱口令介绍

第四节 弱口令防范

第三章 验证码相关漏洞

第一节 验证码安全介绍

第二节 验证码绕过

第三节 验证码识别工具

第四章 暴力破解

第一节 暴力破解漏洞原理

第二节 字典生成工具介绍

第三节 彩虹表和撞库介绍

第四节 在线、离线暴力破解

第五节 暴力破解漏洞防御

验证码绕过

- 1、验证码前端绕过
- 2、验证码后端绕过
- 3、后端TOKEN认证绕过
- 4、验证码识别思路



验证码绕过-前端验证绕过

原理：前端验证码绕过一般是前端JavaScript脚本生成验证码，验证的工作在前端进行；

思路：直接删除相对应的部份的代码即可，要求能够大概看懂前端的代码；

实战：东塔攻防世界-前端验证码绕过

[首页](#) / [在线靶场](#) / [前端验证码绕过](#)

Web安全

暴力破解
前端验证码绕过

Work hard and improve daily

初级
2 积分

前端验证码绕过

消耗 **2.00** 积分

人气: 靶场有1949人完成/2078人尝试

时间: 30分钟

收藏: ☆

启动靶场

验证码绕过-后端验证绕过

原理：后端绕过情况1：后端代码在逻辑上存在问题，验证失败时，验证码不过期，可以继续做认证（也算作逻辑漏洞）；

思路：这类情况需要Burp抓包测试验证；

实战：东塔攻防世界-后端验证码绕过

[首页](#) / [在线靶场](#) / 后端验证码绕过

Web安全

暴力破解
后端验证码绕过

Work hard and improve daily

中级
3 积分

后端验证码绕过

消耗 **3.00** 积分

人气: 靶场有2614人完成/4085人尝试

时间: 30分钟

收藏: ☆

启动靶场

后端验证代码

```
if(isset($_POST['submit'])) {  
    if (empty($_POST['username'])) {  
        $html .= "<p class='notice'>用户名不能为空</p>";  
    } else {  
        if (empty($_POST['password'])) {  
            $html .= "<p class='notice'>密码不能为空</p>";  
        } else {  
            if (empty($_POST['vcode'])) {  
                $html .= "<p class='notice'>验证码不能为空哦! </p>";  
            } else {  
                // 验证验证码是否正确  
                if (strtolower($_POST['vcode']) != strtolower($_SESSION['vcode'])) {  
                    $html .= "<p class='notice'>验证码输入错误哦! </p>";  
                    //应该在验证完成后,销毁该$_SESSION['vcode']  
                }else{  
  
                    $username = $_POST['username'];  
                    $password = $_POST['password'];  
                    $vcode = $_POST['vcode'];  
  
                    $sql = "select * from users where username=? and password=md5(?)";  
                    $line_pre = $link->prepare($sql);  
  
                    $line_pre->bind_param('ss',$username,$password);  
  
                    if($line_pre->execute()){  
                        $line_pre->store_result();  
                        //虽然前面做了为空判断,但最后,却没有验证验证码!!!  
                        if($line_pre->num_rows()==1){  
                            $html.='<p> login success</p>';  
                        }else{  
                            $html.= '<p> username or password is not exists~</p>';  
                        }  
                    }else{  
                        $html.= '<p>执行错误:'.$line_pre->errno.'错误信息:'.$line_pre->error.'</p>';  
                    }  
                }  
            }  
        }  
    }  
}
```

1、Token的引入

Token是在客户端频繁向服务端请求数据，服务端频繁的去数据库查询用户名和密码并进行对比，判断用户名和密码正确与否，并作出相应提示，在这样的背景下，Token便应运而生。

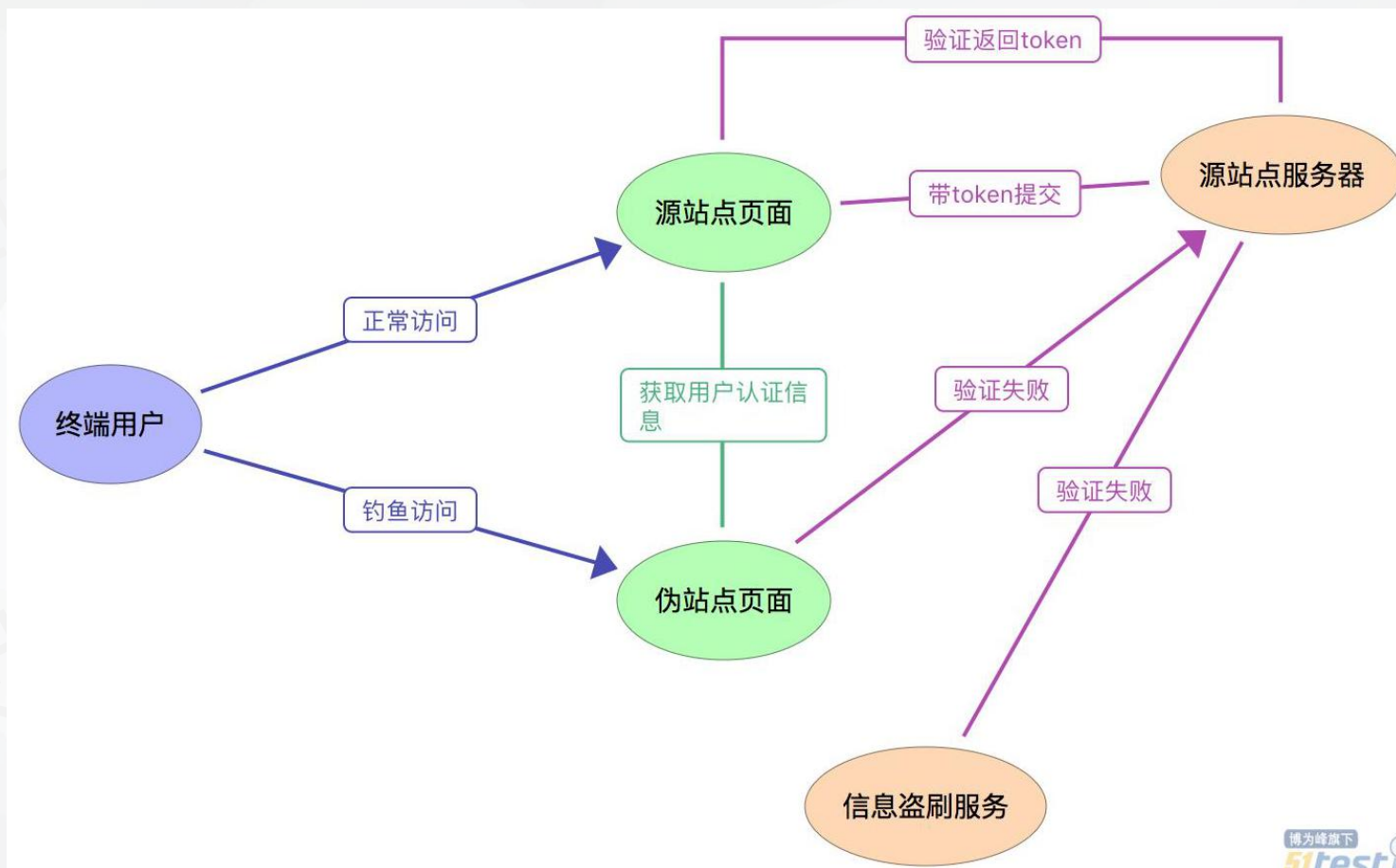
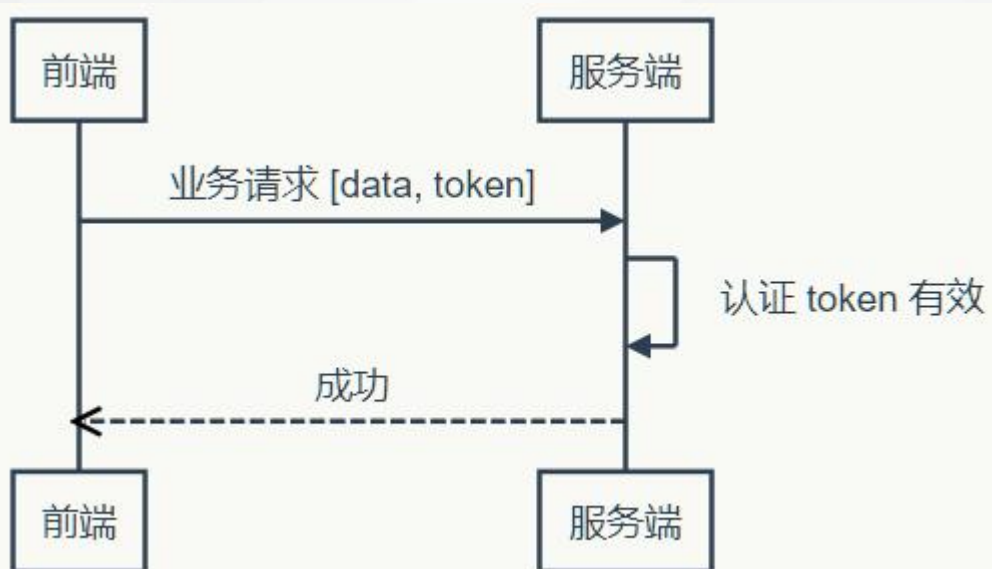
2、Token的定义

Token是服务端生成的一串字符串，以作客户端进行请求的一个令牌，当第一次登录后，服务器生成一个Token便将此Token返回给客户端，以后客户端只需带上这个Token前来请求数据即可，无需再次带上用户名和密码。

3、使用Token的目的

Token的目的是为了减轻服务器的压力，减少频繁的查询数据库，使服务器更加健壮。

验证码绕过-TOKEN爆破绕过



验证码绕过-TOKEN爆破绕过

思路：利用burp工具，可以每次自动提取后台返回的token值，用于下一次的爆破使用；

实战：东塔攻防世界-TOKEN绕过

首页 / 在线靶场 / Token验证绕过


Web安全

暴力破解

Token验证绕过

Work hard and improve daily

高级
4 积分



Token验证绕过

消耗 **4.00** 积分

人气: 靶场有2394人完成/2968人尝试

时间: 30分钟

收藏: ☆

启动靶场

验证码爆破工具

难点:

目前验证码识别难度比较大，主要是目前的验证码类别太多，针对每一类都需要优化算法，且需要有一定的编程和图像识别基础；

思路:

通过编写脚本、插件、工具等方式解决验证码识别，可找专业的人员解决该问题；



第一章 OWASP常见漏洞

第一节 OWASP组织介绍

第二节 常见WEB漏洞介绍

第二章 弱口令漏洞

第一节 Kali下字典介绍

第三节 常见弱口令介绍

第四节 弱口令防范

第三章 验证码相关漏洞

第一节 验证码安全介绍

第二节 验证码绕过

第三节 验证码识别工具

第四章 暴力破解

第一节 暴力破解漏洞原理

第二节 字典生成工具介绍

第三节 彩虹表和撞库介绍

第四节 在线、离线暴力破解

第五节 暴力破解漏洞防御

1、字典准备

收集的弱口令、常用应用密码、制作社工字典、网上泄露的字典、pydictor工具生成等;

2、暴力破解类别

1) 常见的网站前后台登录窗口, 可利用Burp进行爆破;

主要是http、https协议;

2) 常见的可爆破应用

hydra、medusa等支持POP3/SMB/RDP/SSH/FTP/POP3/Telnet/MYSQL常见的几十种协议爆破;

3) 操作系统登录爆破

操作系统远程登录爆破主要是RDP和SSH协议, 也可利用Hydra, John等工具爆破;

4) 离线爆破

编写相应的python脚本进行本地爆破, 一般适用于拿到密文hash值情况;

字典生成工具Pydictor介绍

pydictor

build Python 2.7&3.4 release License

README.md 中文版

pydictor — A powerful and useful hacker dictionary builder for a brute-force attack



Email: LandGrey@qq.com

```
usage:
pydictor.py [options]
    -base [type]
    -char [custom_char]
    -chunk [chunk1] [chunk2] ...
    -extend [string_or_file]
    -plug [birthday,pid6,ftp,pid8,pid4,scratch]
    --conf [expression_or_file]
    --sedb
    -o,--output [directory]
    -tool [shredder,uniqbiner,handler,uniqifer,comparer,hybr
    --len [minlen] [maxlen]
    --head [prefix_string]
    --tail [suffix_string]
    --encode [none,sha1,b64,url,execjs,des,rsa,b32,b16,test,sha
    --occur [letter] [digital] [special]
    --types [letter] [digital] [special]
    --repeat [letter] [digital] [special]
    --regex [regex]
    --level [code]
    --leet [code]
    --dmy
```

另外通过git 2.1.4.1#dev下载

```
git clone --depth=1 --branch=
https://www.github.com/landgre
cd pydictor/
chmod 755 pydictor.py
python pydictor.py
```

下载后修改pydictor目录下的文件，设置初

3、工具使用

工具学习方法:

- 1、利用Kali系统下的命令提示进行学习，先学习基本命令，然后再提升复杂命令，切记死记硬背。

```
root@kali:/# hydra
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS]
] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISou
vVd46] [service://server[:PORT][/OPT]]

Options:
-l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE  try password PASS, or load several passwords from FILE
-C FILE             colon separated "login:pass" format, instead of -L/-P options
-M FILE            list of servers to attack, one entry per line, ':' to specify port
-t TASKS           run TASKS number of connects in parallel per target (default: 16)
-U                 service module usage details
-h                 more command line options (COMPLETE HELP)
server             the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service            the service to crack (see below for supported protocols)
OPT                some service modules support additional input (-U for module help)
```



Hydra爆破工具学习-xHydra

xHydra

退出(Q)

Target Passwords Tuning Specific Start

Username

☒ Username

☐ Username List

☐ Loop around users ☐ Protocol does not require usernames

Password

☒ Password

☐ Password List

☐ Generate

Colon separated file

☐ Use Colon separated file

☐ Try login as password ☐ Try empty password ☐ Try reversed login

hydra -l yourname -p yourpass -t 16 127.0.0.1 adam6500



```
root@kali:/home/kali/www# medusa
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ALERT: Host information must be supplied.

Syntax: Medusa [-h host|-H file] [-u username|-U file] [-p password|-P file] [-C file] -M module [OPT]
-h [TEXT]      : Target hostname or IP address
-H [FILE]      : File containing target hostnames or IP addresses
-u [TEXT]      : Username to test
-U [FILE]      : File containing usernames to test
-p [TEXT]      : Password to test
-P [FILE]      : File containing passwords to test
-C [FILE]      : File containing combo entries. See README for more information.
-O [FILE]      : File to append log information to
-e [n/s/ns]    : Additional password checks ([n] No Password, [s] Password = Username)
-M [TEXT]      : Name of the module to execute (without the .mod extension)
-m [TEXT]      : Parameter to pass to the module. This can be passed multiple times with a
                  different parameter each time and they will all be sent to the module (i.e.
                  -m Param1 -m Param2, etc.)
-d            : Dump all known modules
-n [NUM]       : Use for non-default TCP port number
```



medusa -h 192.168.2.102 -u root -p root -v 6 -M ssh

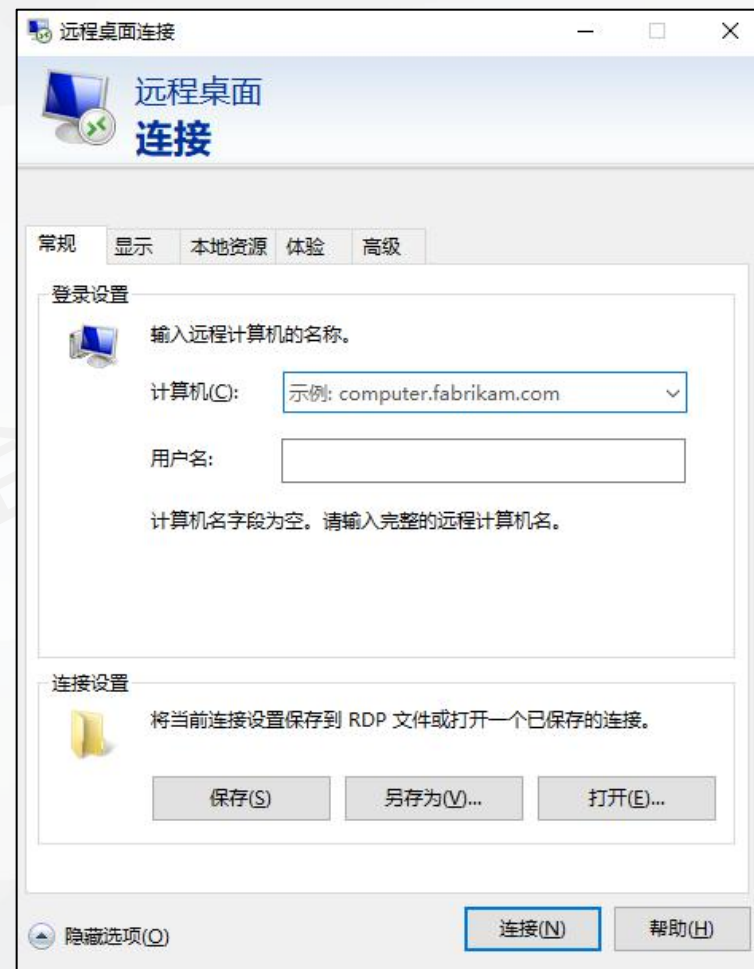
medusa -h 192.168.57.133 -u cxt -P 密码字典表 -v 6 -M ssh

什么是远程桌面协议 (RDP)

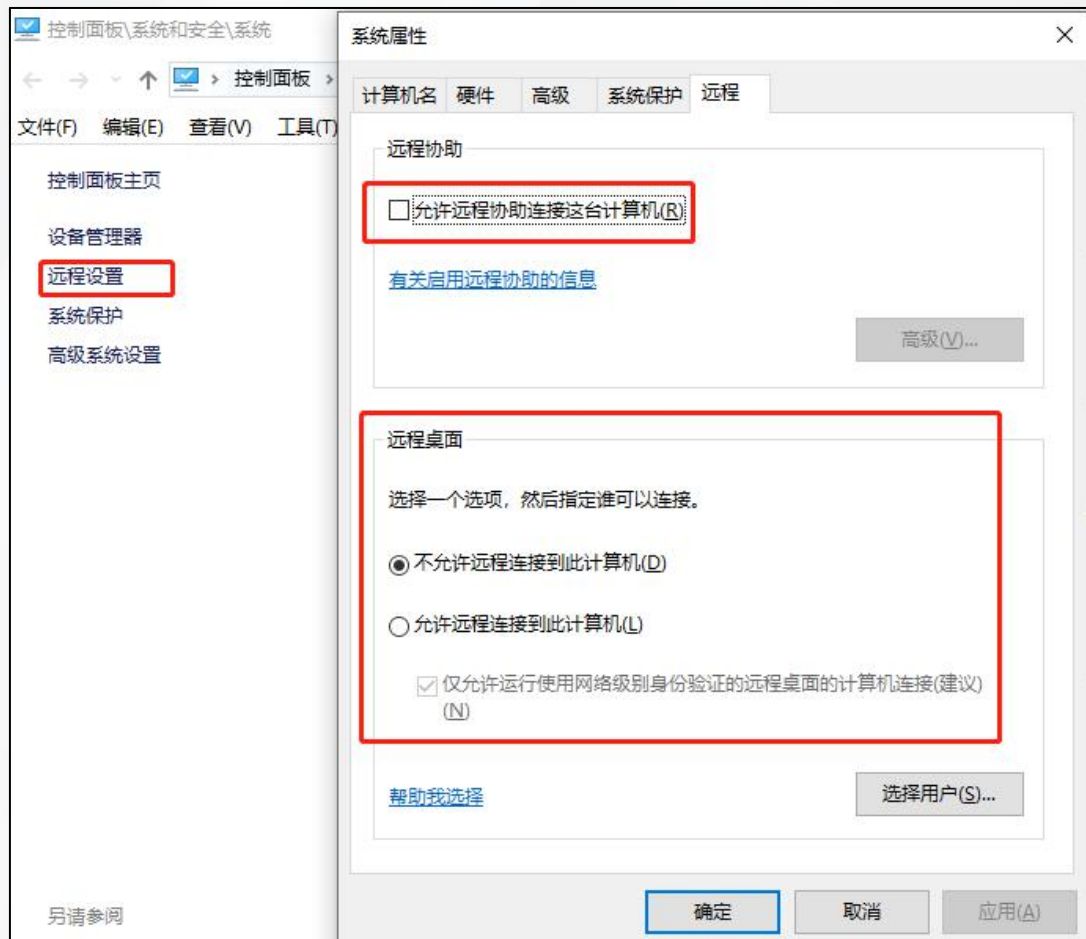
远程桌面协议 (RDP) 指的是用于远程使用桌面计算机的协议或技术标准。远程桌面软件可以使用几种不同的协议，如 RDP、独立计算架构 (ICA) 和虚拟网络计算 (VNC) 等，但 RDP 是最常用的协议。RDP 最初由微软公司发布，可用于大多数 Windows 操作系统，但 Mac 操作系统也提供相应的支持。

“远程桌面”是什么意思

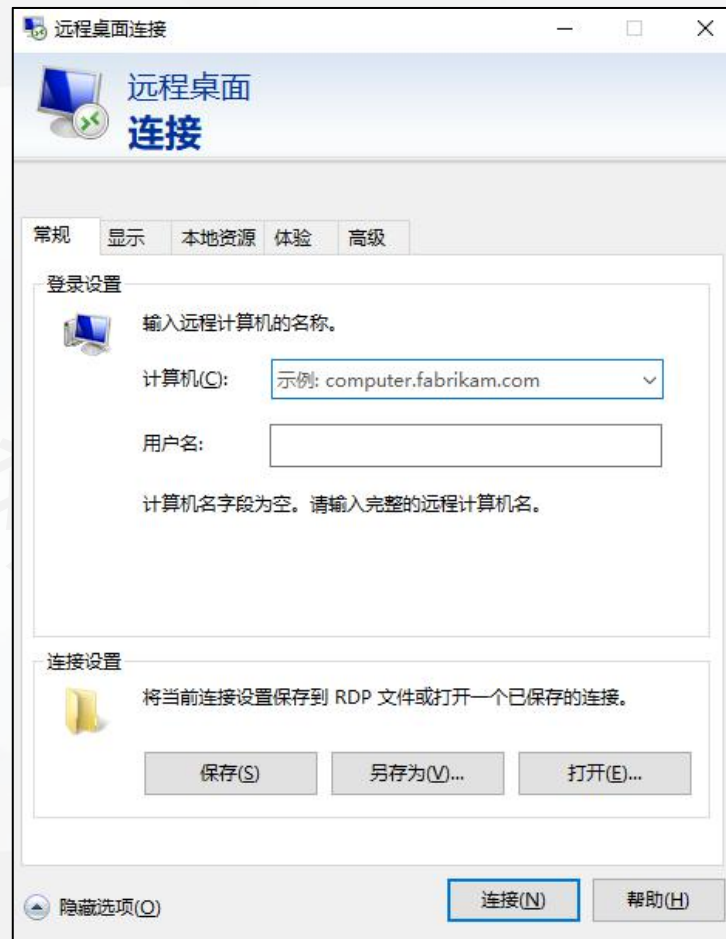
远程桌面是从另外一台计算机连接并使用远方的桌面计算机的功能。远程桌面用户可以访问其桌面，打开和编辑文件，并使用各种应用程序，就如实际坐在桌面计算机前一样。员工在出差期间或居家办公时，通常使用远程桌面软件访问其办公用计算机。



RDP协议设置



net start termervice



cmd->mstsc

RDPScan工具学习



[7] [7kbScan]-RDP-Sniper [铸剑实战靶场内部版]

OpenCount: LoginCount: About

IP: 192.168.1.1 Mask: 255.255.255.0 Port: 3389 ScanPortThread: 100 BurteThread: 5 OneIpBruteThread: 5 Timeout: 4 ☒ ScanPort ☒ SaveLog ☐ Admin GO

<http://www.7kb.org>



➤ john the ripper是一款本地密码破解工具

● 爆破后的结果

```
(root@kali)-[/home/kali]
# john --wordlist=password.lst pass.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6
)
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 3 candidates left, minimum 32 needed for performance.
123456          (root)
123456          (wangliang)
```


➤ Linux下用来爆破shadow文件的步骤:

```
(root@kali)-[/home/kali]  
# unshadow passwd shadow >pass.txt
```

把两个文件写入到一个文件

```
(root@kali)-[/home/kali]  
# cat pass.txt
```

查看写入的文件

```
(root@kali)-[/home/kali]  
# vim password.lst
```

编辑一个密码字典

使用密码字典

```
(root@kali)-[/home/kali]  
# john --wordlist=password.lst pass.txt
```

开始爆破

➤ 查看这个文件的结果

```
(root@kali)-[/home/kali]  
# john --show pass.txt  
root:123456:0:0:root:/root:/bin/bash  
wangliang:123456:1000:1000:wangliang:/home/wangliang:/bin/bash
```

什么是彩虹表?

彩虹表 (Rainbow Table) 是一种破解哈希算法的技术，是一款跨平台密码破解器，主要可以破解MD5、HASH等多种密码。它的性能非常让人震惊，在一台普通PC上辅以NVidia CUDA技术，对于NTLM算法可以达到最高每秒103,820,000,000次明文尝试（超过一千亿次），对于广泛使用的MD5也接近一千亿次。更神奇的是，彩虹表技术并非针对某种哈希算法的漏洞进行攻击，而是类似暴力破解，对于任何哈希算法都有效。

狭义上，彩虹表一般是指以“**hash值:原始值**”为行组成的文件，如下图所示。广义上，只要能从hash值找到对应原始如，形式怎么变都能称为彩虹表；如果要我将彩虹表写入数据库，那表字段应该：

password、md5_value、sha1_value、sha256_value...

hash算法，可以是标准的md5、sha1、sha256、sha512；也可以是其他混合变种，如mysql、md5(upper(\$pass))、md5(md5(\$pass))等等。

1	e7df7cd2ca07f4f1ab415d457a6e1c13:1234
2	d577273ff885c3f84dadb8578bb41399:12345
3	f447b20a7fcfb53a5d5be013ea0b15af:123456
4	f5ac8127b3b6b85cdc13f237c6005d80:abcd
5	e19d5cd5af0378da05f63f891c7467af:abcd1234

在线加解密网站

Md5加解密

<https://www.cmd5.com/>

综合类型加解密

<https://www.sojson.com/encrypt/>

<http://tools.bugscaner.com/encodeanddecode/>

<http://encode.chahuo.com/>

<http://tools.jb51.net/password/>

<http://www.metools.info/code/c28.html>

凯撒密码加密解密

<https://www.qqxiuzi.cn/bianma/kaisamima.php>

MD5加解密(注意查看解密范围)

<https://www.cmd5.com/>

CMD5 本站针对md5、sha1等全球通用公开的加密算法进行反向查询，通过穷举字符组合的方式，创建了明文密文对应查询数据库，创建的记录约90万亿条，占用硬盘超过500TB，查询成功率95%以上，很多复杂密文只有本站才可查询。自2006年已稳定运行十余年，国内外享有盛誉。

[首页](#) [解密范围](#) [批注](#)

密文:

类型: 自动 [\[帮助\]](#)

查询结果:

MD5		
收录内容	说明	数量
1-6位大小写字母+数字+特殊字符	收录100%	大于 1400亿
7位小写字母+数字	收录100%	大于 783亿
8位小写字母+数字	收录100%	大于28211亿
9位小写字母	已收录30%，正在添加	大于14000亿
8-11位数字	收录100%	大于 1000亿
1-15位其它数据	部分收录	大于28000亿
1-20位	900G独家超大字典	大于 910亿

本站支持的密文类型及格式说明

密文类型	格式举例	说明
md5	e10adc3949ba59abbe56e057f20f883e49ba59abbe56e057	标准md5，32位或16位
md5(md5(\$pass))	b80c9c5f86de74f0090fc1a88b27ef34	第一次加密后，结果转换成小写，对结果再加密一次
md5(md5(md5(\$pass)))	e57941ff9000aedb44eb2fa13f6e3e3c	第一次加密后，结果转换成小写，对结果再加密一次,结果转换成小写，对结果再加密一次
MD5(MD5(\$pass))	bb7ff6177ee612ef9dc6acd3a9ea7ea9	第一次加密后，结果转换成大写，对结果再加密一次
MD5(MD5(MD5(\$pass)))	36d627bd562e83ab995fb1fdf59c95d9	第一次加密后，结果转换成大写，对结果再加密一次,结果转换成大写，对结果再加密一次
sha1	f03e8a370aa8dc80f63a6d67401a692ae72fa530	密文长度必须为40位
md4	c0a27f801162b8b862cd5f5a1a66e85a	32位
mysql	29596332026fd206	老MYSQL数据库用的，16位，且第1位和第7位必须为0-8
mysql5	b34c662f720236babfc1b3f75203a80e1009844a	新版本MySQL数据库用的
md5(\$pass.\$salt)	9393dc56f0c683b7bba9b3751d0f6a46:OTD6v4c8I3Zid2AL	在密码后附加一个字符串再加密。
md5(\$salt.\$pass)	5610604c157ef1d0fb33911542e5b06f:zg	在密码前附加一个字符串再加密。
md5(md5(\$pass).\$salt); VB;DZ	30e23a848506770eca92faed1bd9f3ec:gM5cd1a0b2de38cc1d7d796b1d2ba6a954f:dc2bcead5f538296c0e05c26b85451fef9ea95:To!@35B%QS@)]U.DTy%fDm;SLwW58w	用于dz,vB等论坛程序，discuz的salt长度是6位，vBulletin的salt长度是3位或30位。
md5(md5(\$salt).md5(\$pass)) IPB	ac8dfc54ba110487b86ad6514328fd49:m@kZ}	salt长度5位
sha1(\$salt.\$pass)	9cea8c041ce88e0b2066343d819113005b80421c:23919cea8c041ce88e0b2066343d819113005b80421c 2391	用于SMF
Md5(Phpbb3)	\$H\$912345678Mw/BjmincvnSS94/STawW/	Linux
Md5 Wordpress)	\$P\$B12345678/c7bOMfLdQB9B/ypks8iB/	Linux
Md5(Unix)	\$1\$12345678\$kbapHduhijieYIUP66Xt/	Linux
Des(Unix)	af.kPXROLU9uY	Linux
ntlm	71dd0709187df68befd20973fc23f973	Windows
Domain Cached Credentials	1aefd85a507965a6f1719e951b81d0f7	Windows
sha256	8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918	
sha256(\$pass.\$salt)	1ec82d9b57403e53fafcf0ad8a86db196d135ef7513443a985385d7c20bdbfbfd:abcdabcd	
sha256(\$salt.\$pass)	a6a4ccd14c6b21c63b8a0d38cfb7ead3e5032c58fdea7cd8a4da901db9462088:abcdabcd\$sha256\$abcdabcd\$a6a4ccd14c6b21c63b8a0d38cfb7ead3e5032c58fdea7cd8a4da901db9462088	

注：

1) 如果你不知道密文类型，在首页查询时，密文类型选择"自动"即可，将尝试所有的密文类型，多试几条，解密成功提示真正的密文类型，除此以外则无法从一个32位等字符串判断密文类型。

2) 除了按以上直观方法判断密文类型，再无其它办法，请不要用任何方式咨询我们关于密文类型的问题。

解密举例：

感谢各位的用心聆听!

网络安全国家工程研究中心
——东塔网络安全学院