CTF基础知识及web

原创

m0_60484735 已于 2022-04-26 09:58:40 修改 28 收藏

文章标签： 人工智能

于 2022-04-21 09:44:09 首次发布

本文链接：https://blog.csdn.net/m0_60484735/article/details/124312716

> 提示：文章写完后，目录可以自动生成，如何生成可参考右边的帮助文档

文章目录

CTF基础知识

一、CTF简介

CTF（Capture The Flag）夺旗比赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。CTF起源于1996年DEFCON全球黑客大会，以代替之前黑客们通过互相发起真实攻击进行技术比拼的方式。发展至今，已经成为全球范围网络安全圈流行的竞赛形式，2013年全球举办了超过五十场国际性CTF赛事。而DEFCON作为CTF赛制的发源地，DEFCON CTF也成为了目前全球最高技术水平和影响力的CTF竞赛，类似于CTF赛场中的“世界杯”。

二、CTF赛事介绍

CTF是一种流行的信息安全竞赛形式，其英文名可直译为“夺得Flag”，也可意译为“夺旗赛”。其大致流程是，参赛团队之间通过进行攻防对抗、程序分析等形式，率先从主办方给出的比赛环境中得到一串具有一定格式的字符串或其他内容，并将其提交给主办方，从而夺得分数。为了方便称呼，我们把这样的内容称之为“Flag”。

三、CTF竞赛模式

1.解题模式（Jeopardy）

在解题模式CTF赛制中，参赛队伍可以通过互联网或者现场网络参与，这种模式的CTF竞赛与ACM编程竞赛、信息学奥赛比较类似，以解决网络安全技术挑战题目的分值和时间来排名，通常用于在线选拔赛。题目主要包含逆向、漏洞挖掘与利用、Web渗透、密码、取证、隐写、安全编程等类别。

2.攻防模式（Attack-Defense）

在攻防模式CTF赛制中，参赛队伍在网络空间互相进行攻击和防守，挖掘网络服务漏洞并攻击对手服务来得分，修补自身服务漏洞进行防御来避免丢分。攻防模式CTF赛制可以实时通过得分反映出比赛情况，最终也以得分直接分出胜负，是一种竞争激烈，具有很强观赏性和高度透明性的网络安全赛制。在这种赛制中，不仅仅是比参赛队员的智力和技术，也比体力（因为比赛一般都会持续48小时及以上），同时也比团队之间的分工配合与合作。

3.混合模式（Mix）

结合了解题模式与攻防模式的CTF赛制，比如参赛队伍通过解题可以获取一些初始分数，然后通过攻防对抗进行得分增减的零和游戏，最终以得分高低分出胜负。采用混合模式CTF赛制的典型代表如iCTF国际CTF竞赛。

四、CTF竞赛内容

不管是国内外，目前主流的CTF比赛内容主要涉及以下多个方面：
Web 应用漏洞挖掘利用
Crypto 密码学
Pwn 程序的逻辑分析，漏洞利用windows、linux、小型机、固件设备等
Misc 杂项，隐写，数据还原，脑洞、社会工程、与信息安全相关的大数据等
Reverse 二进制程序逆向，逆向windows、linux、移动设备类等
Ppc 编程类

国内外著名赛事

1、国际知名CTF赛事

· DEFCON CTF：CTF赛事中的“世界杯”

· UCSB iCTF：来自UCSB的面向世界高校的CTF

· Plaid CTF：包揽多项赛事冠军的CMU的PPP团队举办的在线解题赛

· Boston Key Party：近年来崛起的在线解题赛

· Codegate CTF：韩国首尔“大奖赛”，冠军奖金3000万韩元

· Secuinside CTF：韩国首尔“大奖赛”，冠军奖金3000万韩元

· XXC3 CTF：欧洲历史最悠久CCC黑客大会举办的CTF

· SIGINT CTF：德国CCCAC协会另一场解题模式竞赛

· Hack.lu CTF：卢森堡黑客会议同期举办的CTF

· EBCTF：荷兰老牌强队Eindbazen组织的在线解题赛

· Ghost in the Shellcode：由Marauders和Men in Black Hats共同组织的在线解题赛

· RwthCTF：由德国0ldEur0pe组织的在线攻防赛

· RuCTF：由俄罗斯Hackerdom组织，解题模式资格赛面向全球参赛，解题攻防混合模式的决赛面向俄罗斯队伍的国家级竞赛

· RuCTFe：由俄罗斯Hackerdom组织面向全球参赛队伍的在线攻防赛

· PHD CTF：俄罗斯Positive Hacking Day会议同期举办的CTF

国际重要CTF赛事分布图：红色为解题模式选拔赛+攻防模式现场决赛，黑色为混合模式在线赛，紫色为解题模式CTF赛，橘色为在攻防模式在线赛。

2、国内知名CTF赛事

· XCTF全国联赛

中国网络空间安全协会竞评演练工作组主办、南京赛宁承办的全国性网络安全赛事平台，2014-2015赛季五站选拔赛分别由清华、上交、浙大、杭电和成信技术团队组织（包括杭电HCTF、成信SCTF、清华BCTF、上交0CTF和浙大ACTF），XCTF联赛总决赛由蓝莲花战队组织。XCTF联赛是国内最权威、最高技术水平与最大影响力的网络安全CTF赛事平台。

· AliCTF

由阿里巴巴公司组织，面向在校学生的CTF竞赛，冠军奖金10万元加BlackHat全程费用。

· KCTF

看雪CTF（简称KCTF）是圈内知名度最高的技术竞技，从原CrackMe攻防大赛中发展而来，采取线上PK的方式，规则设置严格周全，题目涵盖Windows、Android、iOS、Pwn、智能设备、Web等众多领域。
看雪CTF比赛历史悠久、影响广泛。自2007年以来，看雪已经举办十多个比赛，与包括金山、360、腾讯、阿里等在内的各大公司共同合作举办赛事。比赛吸引了国内一大批安全人士的广泛关注，历年来CTF中人才辈出，汇聚了来自国内众多安全人才，高手对决，精彩异常，成为安全圈的一次比赛盛宴，突出了看雪论坛复合型人才多的优势，成为企业挑选人才的重要途径，在社会安全事业发展中产生了巨大的影响力。

· XDCTF
2015年之前由西安电子科技大学信息安全协会与西安电子科技大学组织的CTF竞赛，其特点是偏向于渗透实战经验。2016年之后由西安电子科技大学组织举办。

· HCTF

由杭州电子科技大学信息安全协会承办组织的CTF

杭州电子科技大学信息安全协会由杭州电子科技大学通信工程学院组织建立，协会已有七年历史，曾经出征DEFCON,BCTF等大型比赛并取得优异成绩，同时协会还有大量有影响力的软件作品。协会内部成员由热爱黑客技术和计算机技术的一些在校大学生组成，有多个研究方向，主要有渗透，逆向，内核，web等多个研究方向。至今已经成功举办6次CTF比赛。

· ISCC

由北理工组织的传统网络安全竞赛，最近两年逐渐转向CTF赛制。

· LCTF

由L-Team战队组织的CTF竞赛。
· TCTF

TCTF由中国网络空间安全协会竞评演练工作委员会指导、腾讯安全发起、腾讯安全联合实验室主办，0ops战队和北京邮电大学协办的CTF竞赛。

· Real World CTF

Real World CTF 是由长亭科技主办的国际级 CTF 大赛，全球首创 CTF 夺旗赛和 Pwn 赛结合的全新赛制，赛题全部基于 现实世界软件的修改或二次开发，首届即吸引了 5 大洲，15 个国家地 区顶尖战队参赛。

· 百度杯CTF夺旗大战

由百度安全应急响应中心和i春秋联合举办的CTF比赛，国内现今为止首次历时最长（半年）、频次最高的CTF大赛。赛题丰富且突破了技术和网络的限制。

· 全国大学生信息安全竞赛创新实践能力赛线上赛

由教育部高等学校信息安全专业教学指导委员会主办，西安电子科技大学、永信至诚、国卫信安等承办;百度安全中心、阿里安全应急响应中心、腾讯安全平台方舟计划、360企业安全集团赞助支持的CTF竞赛，覆盖面广，质量级别最高，被参赛选手称作CTF的国赛。

五、如何学习CTF

1、分析赛题情况(属于哪一类涉及哪些知识点等)
2、分析自身能力，自己最适合哪个方向？(方向很重要，建议3、兴趣所致，有时也需为团队牺牲！！！)
4、选择更适合的入手(从低到高、由易入难)
5、研究历年经典的wp(writeup)

1、分析赛题

PWN、Reverse：偏重对汇编、逆向及底层核心的理解

Crypto：偏重对数学、算法的学习，密码学要深入学习

Web：偏重对技巧沉淀、快速搜索能力的挑战、发散性思维，对底层、代码原理只需要了解，相关漏洞知识的积累

Misc：偏重则更复杂，所有与计算机安全挑战有关的都在其中，隐写、图片数据分析还原、流量分析、大数据、游戏逆向分析等等

2、常规操作

A方向：PWN+Reverse+Crypto 随机搭配

B方向：Web+Misc组合

Misc所有人都可以做

3、入门知识

团队要学的内容：linux基础、计算机组成原理、操作系统原理、网络协议分析

A方向：IDA工具使用（fs插件）、逆向工程、密码学、缓冲区溢出等

B方向：Web安全、网络安全、内网渗透、数据库安全、top10的安全漏洞等

推荐书籍

A方向：

RE for Beginners
IDA Pro权威指南
揭秘家庭路由器0day漏洞挖掘技术
自己定操作系统
黑客攻防技术宝典：系统实战篇 有各种系统的逆向讲解
B方向：

Web应用安全权威指南 最推荐小白，宏观web安全
Web前端黑客技术揭秘
黑客秘籍—渗透测试实用指南
黑客攻防技术宝典 web实战篇 web安全的所有核心基础点，有挑战性，最常规，最全，学好会直线上升
代码审计：企业级web代码安全架构

六、备份文件下载

1、目录遍历

点开下方链接，开启题目

逐个点开文件，直到找到flag

Index of /flag_in_here

Name	Last modified	Size	Description
Parent Directory		-	
1/	2022-04-22 01:04	-	
2/	2022-04-22 01:04	-	
3/	2022-04-22 01:04	-	
4/	2022-04-22 01:04	-	

Apache/2.4.38 (Debian) Server at challenge-2c702831fe852557.sandbox.ctfhub.com Port 10800

Index of /flag_in_here/3/4

Name	Last modified	Size	Description
Parent Directory		-	
flag.txt	2022-04-22 01:04	33	

Apache/2.4.38 (Debian) Server at challenge-2c702831fe852557.sandbox.ctfhub.com Port 10800

粘贴flag到题目下方提交flag即可

```
ctfhub{d703d89cb1cc176d85d9c1c4}
```

2、PHPINFO

点开链接，开启题目


PHPINFO
所需金币：30
题目状态：已解出
解题奖励：金币:50 经验:10
http://challenge-b9549a3656796aad.sandbox.ctfhub.com:10800
00:29:24
环境续期
停止并销毁环境
每分钟需要1个金币,请根据个人需求
Flag{.....}
提交Flag
WriteUp

phpinfo

点击查看phpinfo

ZLib Support	enabled
Stream Wrapper	compress.zlib://
Stream Filter	zlib.inflate, zlib.deflate
Compiled Version	1.2.11
Linked Version	1.2.11

Directive	Local Value	Master Value
zlib.output_compression	Off	Off
zlib.output_compression_level	-1	-1
zlib.output_handler	*no value*	*no value*

Additional Modules

Module Name

Environment

Variable	Value
APACHE_RUN_DIR	/var/run/apache2
APACHE_PID_FILE	/var/run/apache2/apache2.pid
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
APACHE_LOCK_DIR	/var/lock/apache2
LANG	C
APACHE_RUN_USER	www-data
APACHE_RUN_GROUP	www-data
APACHE_LOG_DIR	/var/log/apache2
PWD	/
FLAG	ctfhub{cb6373af775cabd22144090a}

PHP Variables

Variable	Value
$_REQUEST['UM_distinctid']	18049ba2ffa4bb-05bace738c87f3-7b422e27-1fa400-18049ba2ffb60e
$_COOKIE['UM_distinctid']	18049ba2ffa4bb-05bace738c87f3-7b422e27-1fa400-18049ba2ffb60e
$_SERVER['HTTP_HOST']	challenge-b9549a3656796aad.sandbox.ctfhub.com:10800
$_SERVER['HTTP_X_REAL_IP']	112.115.169.197
$_SERVER['HTTP_X_FORWARDED_FOR']	112.115.169.197
$_SERVER['HTTP_CONNECTION']	close
$_SERVER['HTTP_UPGRADE_INSECURE_REQUESTS']	1
$_SERVER['HTTP_USER_AGENT']	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36 Edg/100.0.1185.44

粘贴flag到下方，提交flag即可解开题目

3、网站源码

开启题目

点开链接后，进入环境，可以看到常见网站源码备份文件的后缀和备份文件名

备份文件下载 - 网站源码

可能有点用的提示

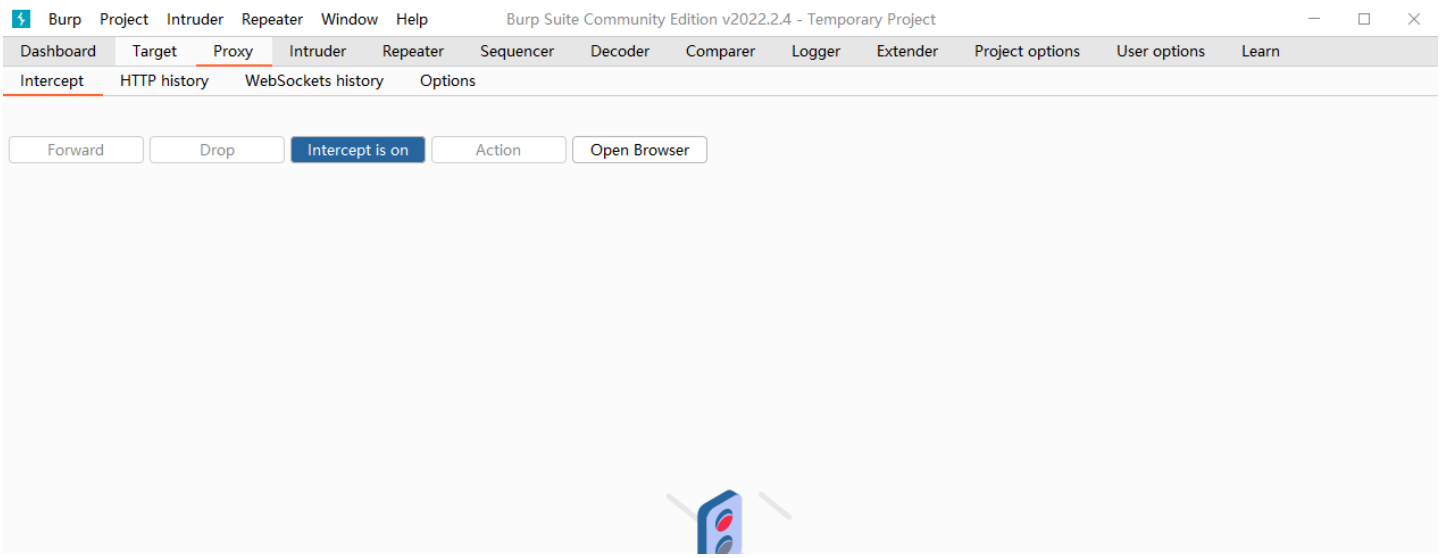
常见的网站源码备份文件后缀

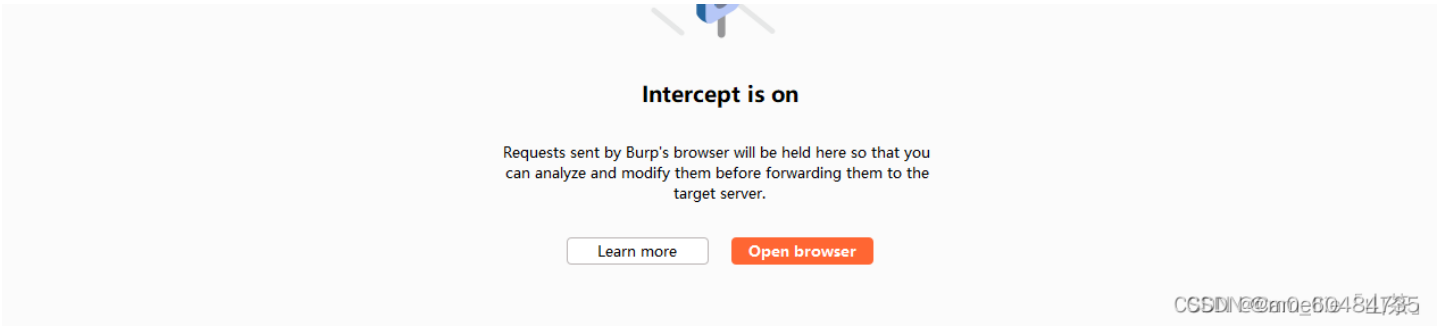
- tar
- tar.gz
- zip
- rar

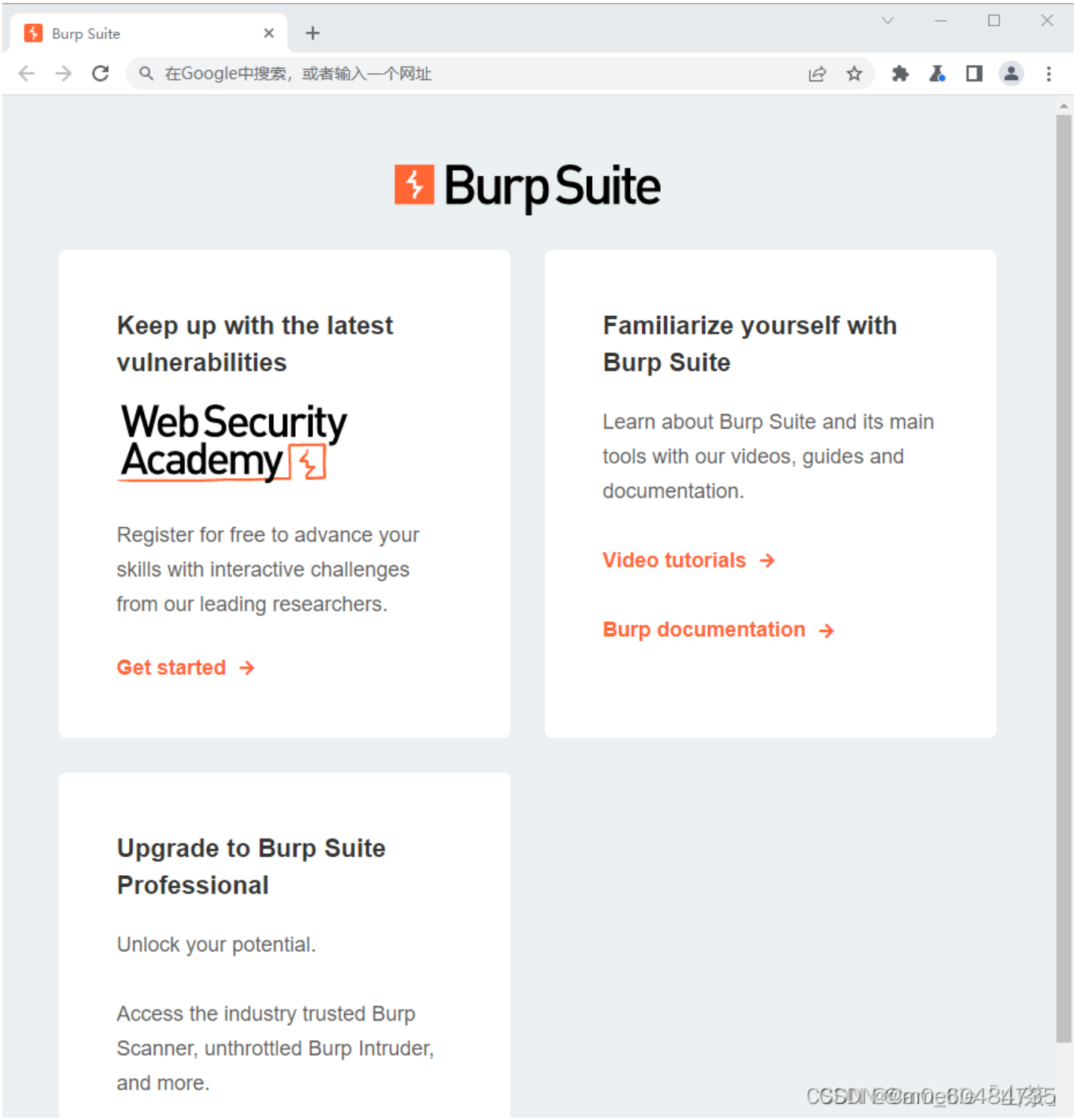
常见的网站源码备份文件名

- web
- website
- backup
- back
- www
- wwwroot
- temp

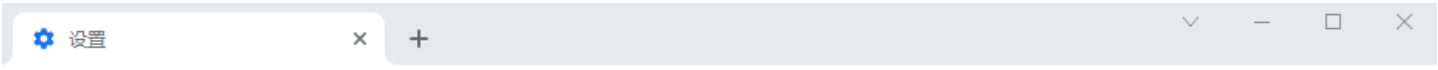
打开burp暴力破解flag

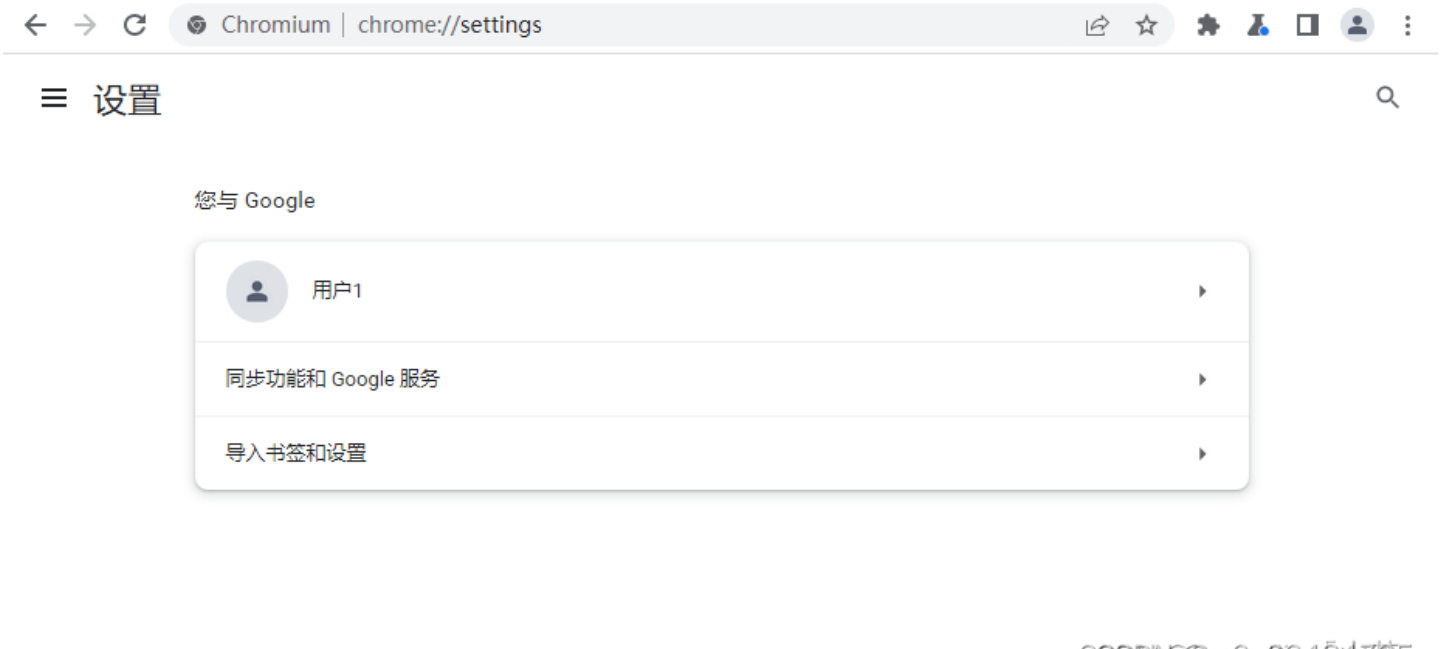


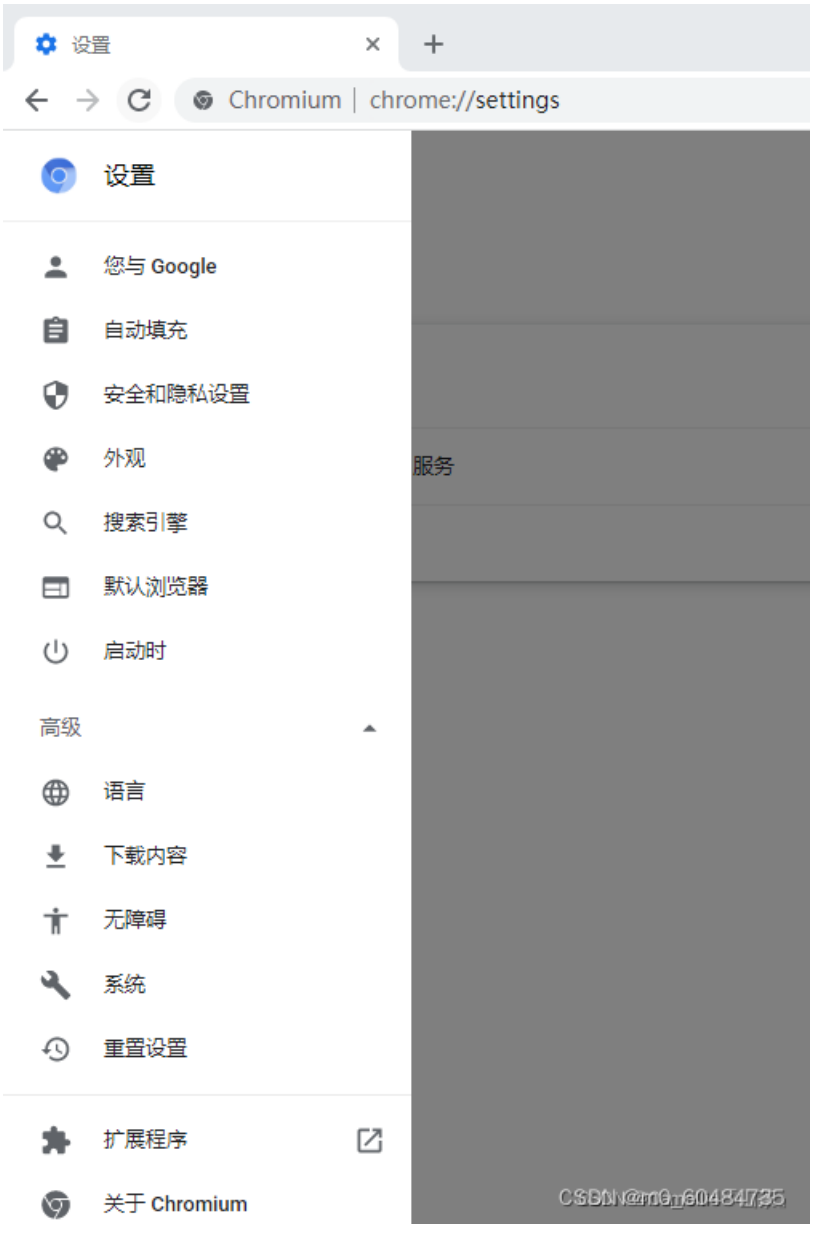

Intercept is on
Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.
Learn more
Open browser


Burp Suite
在Google中搜索，或者输入一个网址
Burp Suite
Keep up with the latest vulnerabilities
Web Security Academy
Register for free to advance your skills with interactive challenges from our leading researchers.
Get started
Familiarize yourself with Burp Suite
Learn about Burp Suite and its main tools with our videos, guides and documentation.
Video tutorials
Burp documentation
Upgrade to Burp Suite Professional
Unlock your potential.
Access the industry trusted Burp Scanner, unthrottled Burp Intruder, and more.

设置打开代理


设置





代理

自动设置代理

获取帮助

提供反馈

将代理服务器用于以太网或 Wi-Fi 连接。这些设置不适用于 VPN 连接。

自动检测设置

开

使用设置脚本

关

脚本地址

保存

手动设置代理

将代理服务器用于以太网或 Wi-Fi 连接。这些设置不适用于 VPN 连接。

使用代理服务器

开

地址 127.0.0.1

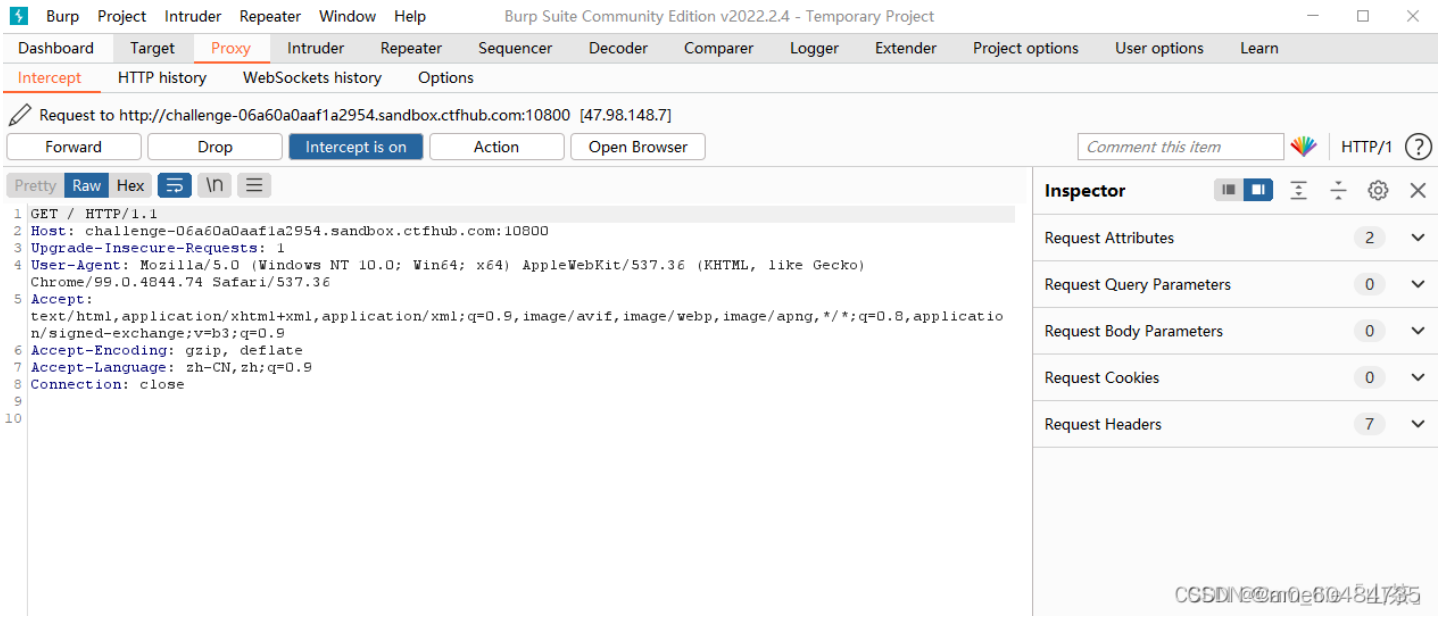
端口 8080

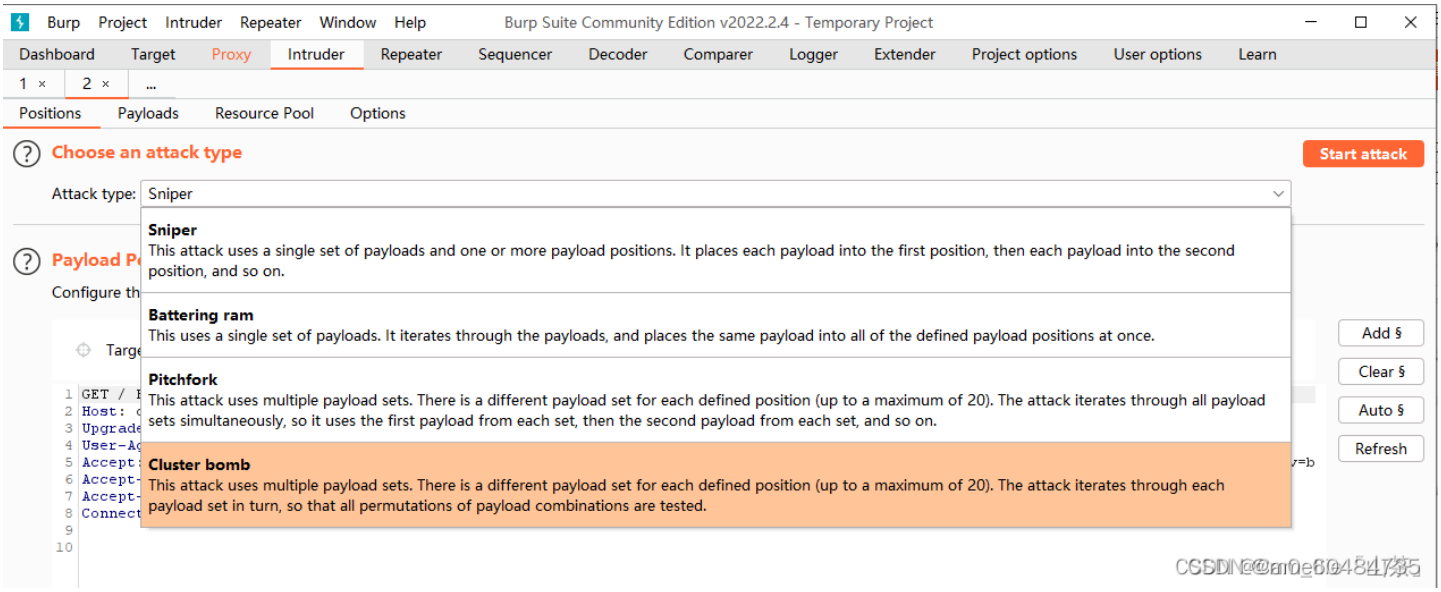
请勿对以下列条目开头的地址使用代理服务器。若有多个条目，请使用英文分号 (;) 来分隔。

请勿将代理服务器用于本地(Intranet)地址

保存

开始抓包





Positions | Payloads | Resource Pool | Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positio
payload type can be customized in different ways.

Payload set: 1 — Payload count: 0

Payload type: Simple list — Request count: 0

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste
Load ...
Remove
Clear
Deduplicate

Add — *Enter a new item*

Add from list ... [Pro version only]

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add
Edit
Remove
Up
Down

Enabled	Rule

Positions | Payloads | Resource Pool | Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in t
payload type can be customized in different ways.

Payload set: 2 — Payload count: 1

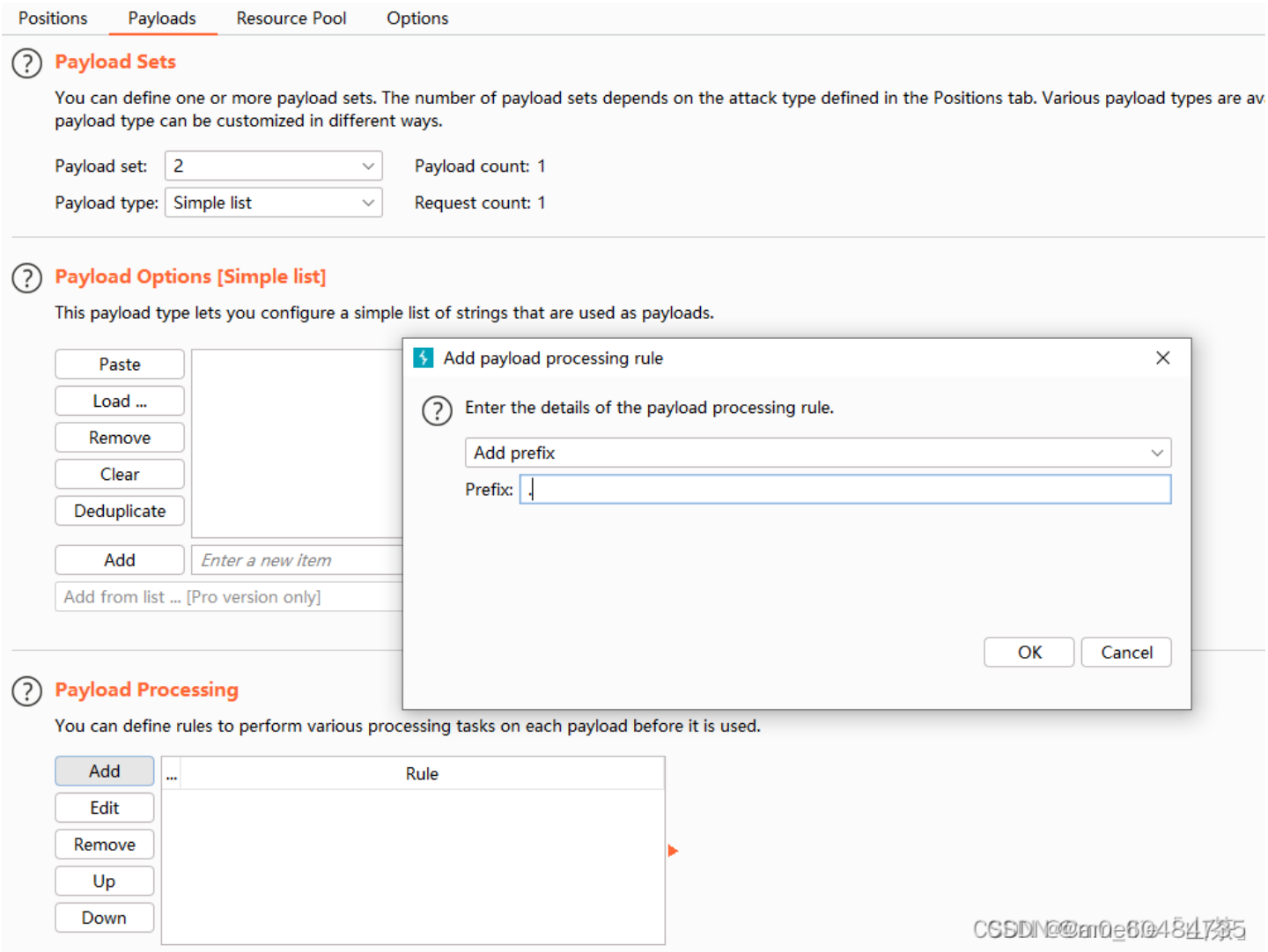
Payload type: Simple list — Request count: 1

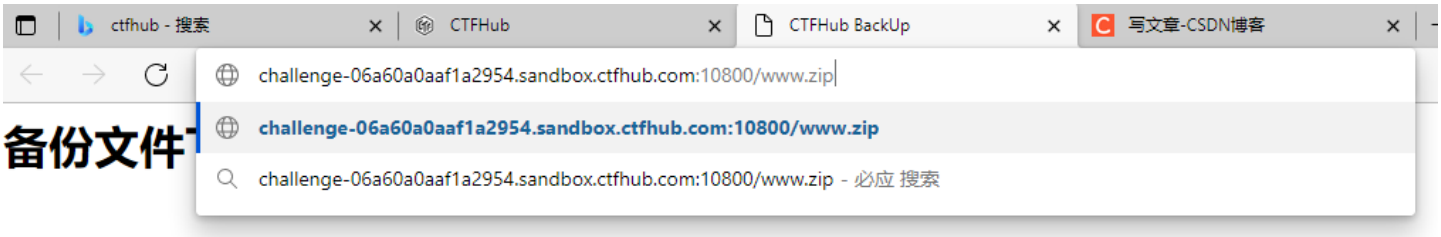
Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste
Load ...
Remove
Clear
Deduplicate
Add

Add from lis — Add the specified item





备份文件

可能有点用的提示

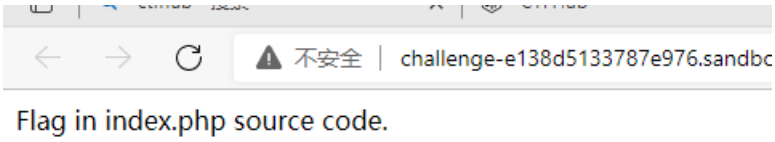
常见的网站源码备份文件后缀

- tar
- tar.gz
- zip
- rar

2.bak文件

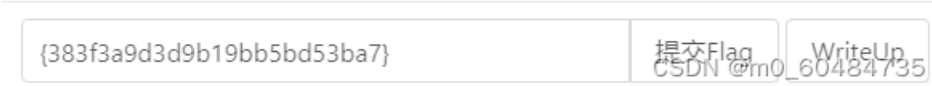
开启bak题目

点开链接，进入环境，出现这个界面



打开文件，找到flag

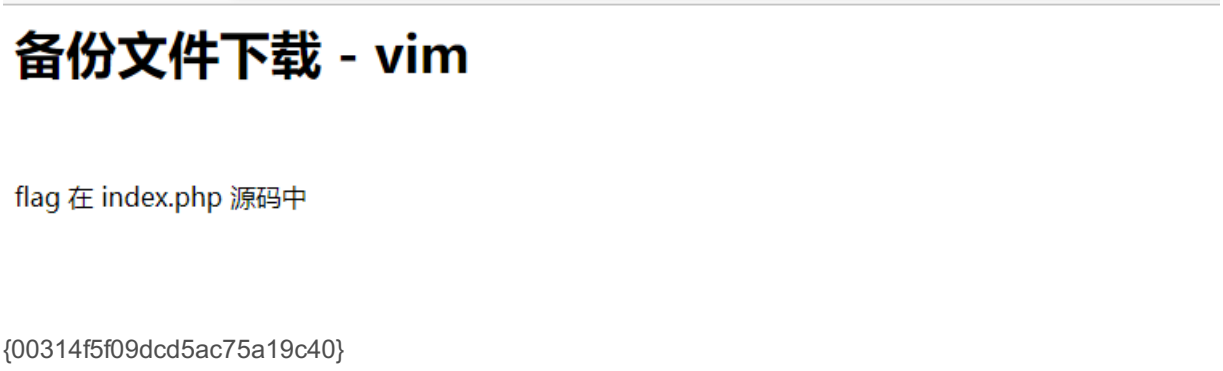
提交即可解开题目



3、vim缓存

开启题目

点开链接后，在网址后输入/index.php.swp，跳转到打开文件，找到flag即可解开题目



{00314f5f09dcd5ac75a19c40}

返回题目，提交flag即可

4、.DS_Store

开启题目，点开链接

打开下载的文件，寻找flag

找到flag之后提交即可解开题目，注意：不可有空格

点击提交即可