从零学习CTF

原创

即将成为大佬的菜鸡 于 2018-12-21 18:35:54 发布 2385 收藏 58

分类专栏： CTF 文章标签： 初学 CTF

本文链接：https://blog.csdn.net/weixin_44147777/article/details/85160125

从零学习CTF

本人大一小白一枚，对信息安全颇感兴趣，就将我的学习作为博客。若我日后成为大佬，我的博客是不是也会对以后的小白有所帮助呢，想想都有点小激动，哈哈哈哈。

我是分界线

首先

什么是CTF

CTF(夺旗赛)简介：

CTF（Capture The Flag）中文一般译作夺旗赛，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。

竞赛模式

解题模式

攻防模式（Attack-Defense）

混合模式（mix）

题目类别

WEB（网络安全）

MISC（安全杂项）

Crypto（密码学）

Reverse（逆向工程）

PPC（编程类题目）

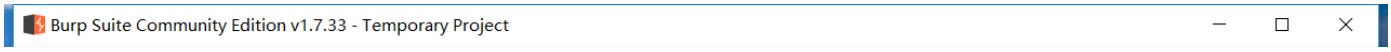
PWN（二进制安全）

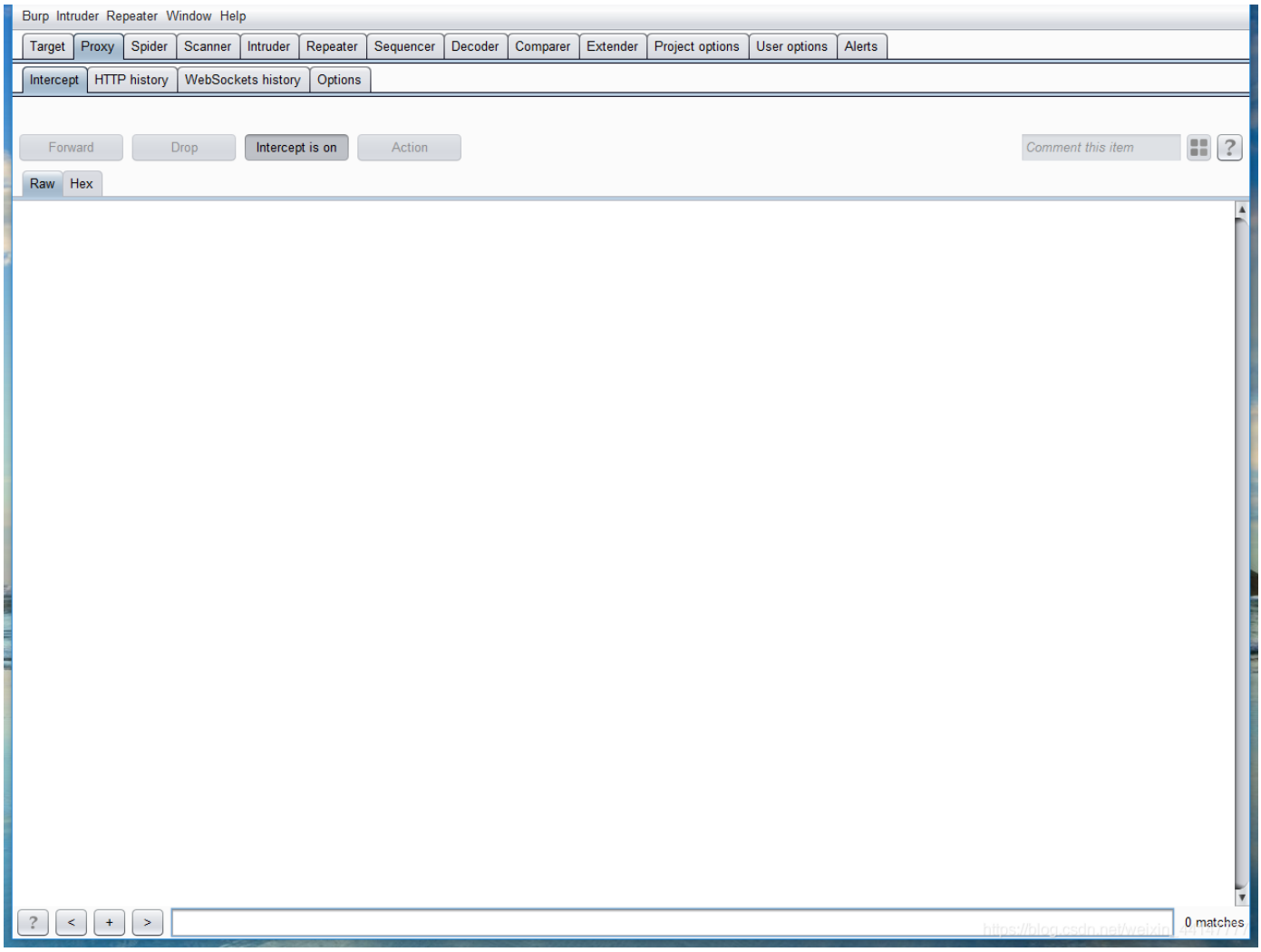
Burpsuit：

• BurpSuite 是用于攻击web 应用程序的集成平台。它包含了许多工具，并为这些工具设计了许多接口，以促进加快攻击应用程序的过程。

•所有的工具都共享一个能处理并显示HTTP 消息，持久性，认证，代理，日志，警报的一个强大的可扩展的框架。

•可以用于抓包，改包，数据爆破等多种功能





Proxy——是一个拦截HTTP/S的代理服务器，作为一个在浏览器和目标应用程序之间的中间人，允许你拦截，查看，修改在两个方向上的原始数据流。

Spider——是一个应用智能感应的网络爬虫，它能完整的枚举应用程序的内容和功能。

Scanner[仅限专业版]——是一个高级的工具，执行后，它能自动地发现web 应用程序的安全漏洞。

Intruder——是一个定制的高度可配置的工具，对web应用程序进行自动化攻击，如：枚举标识符，收集有用的数据，以及使用fuzzing 技术探测常规漏洞。

Repeater——是一个靠手动操作来补发单独的HTTP 请求，并分析应用程序响应的工具。

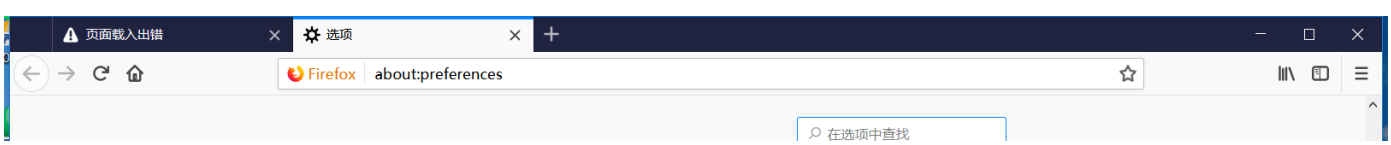
Sequencer——是一个用来分析那些不可预知的应用程序会话令牌和重要数据项的随机性的工具。

Decoder——是一个进行手动执行或对应用程序数据者智能解码编码的工具。

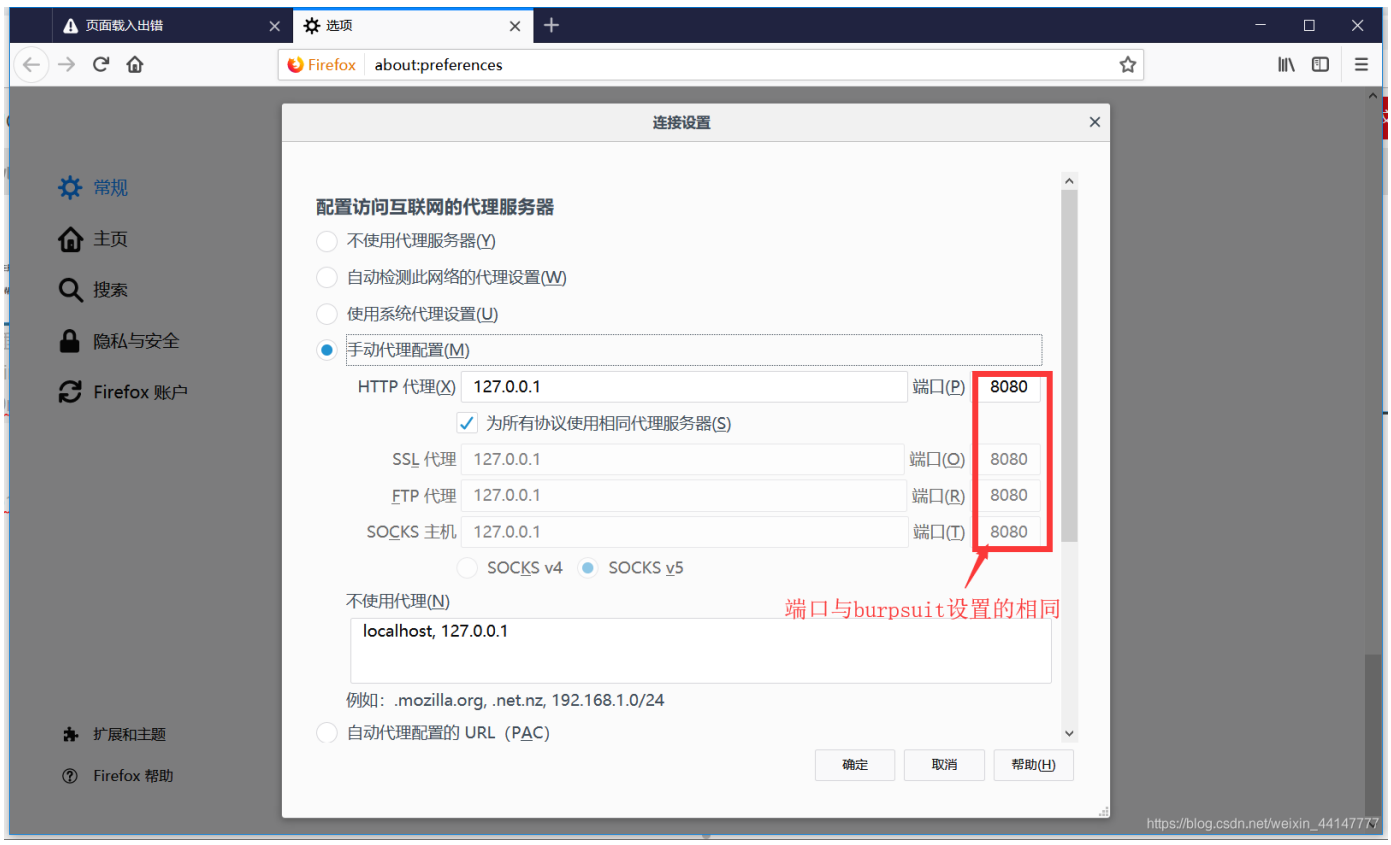
Comparer——是一个实用的工具，通常是通过一些相关的请求和响应得到两项数据的一个可视化的“差异”。

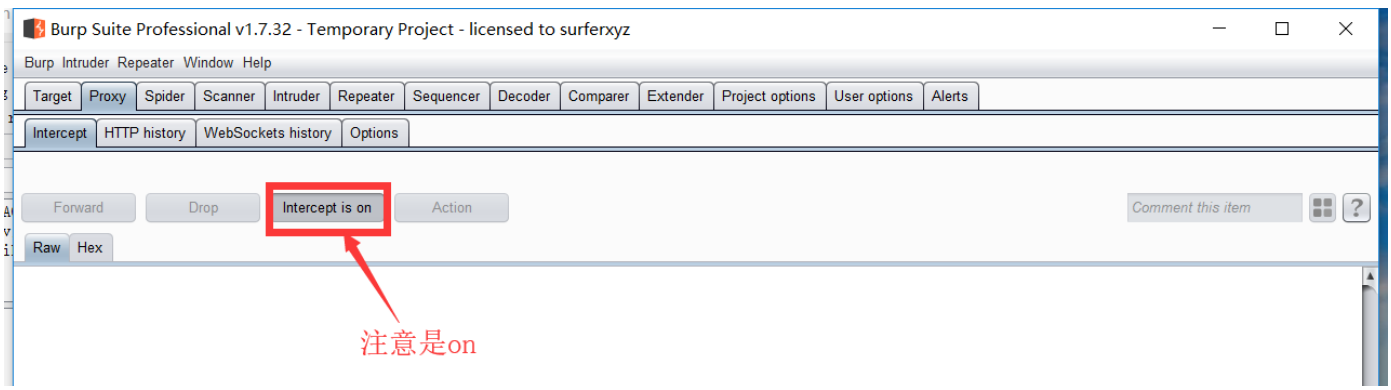
Burpsuit安装可见我一个学姐的博客

浏览器配置
火狐浏览器 选项–>>网络设置




常规
主页
搜索
隐私与安全
Firefox 账户
使用推荐的性能设置(U) 详细了解
自动选择适合此电脑配置的设置。
浏览
使用自动滚屏(A)
使用平滑滚动(M)
在需要时显示触摸键盘(K)
始终使用方向键在页面内导航(C)
若在文本框外输入，则在页面中查找文本(X)
在您浏览时推荐扩展(R) 详细了解
网络设置
配置 Firefox 如何连接互联网。 详细了解
设置(E)...
扩展和主题
Firefox 帮助


页面载入出错
选项
Firefox about:preferences
连接设置
配置访问互联网的代理服务器
不使用代理服务器(Y)
自动检测此网络的代理设置(W)
使用系统代理设置(U)
手动代理配置(M)
HTTP 代理(X) 127.0.0.1 端口(P) 8080
为所有协议使用相同代理服务器(S)
SSL 代理 127.0.0.1 端口(O) 8080
FTP 代理 127.0.0.1 端口(R) 8080
SOCKS 主机 127.0.0.1 端口(T) 8080
SOCKS v4 SOCKS v5
不使用代理(N)
localhost, 127.0.0.1
例如：.mozilla.org, .net.nz, 192.168.1.0/24
自动代理配置的 URL（PAC）
确定 取消 帮助(H)
端口与burpsuit设置的相同
常规
主页
搜索
隐私与安全
Firefox 账户
扩展和主题
Firefox 帮助


Burp Suite Professional v1.7.32 - Temporary Project - licensed to surferxyz
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
Raw Hex
注意是on

就可以抓包了。

http协议

•什么是 HTTP？
•超文本传输协议（HTTP）的设计目的是保证客户机与服务器之间的通信。
•HTTP 的工作方式是客户机与服务器之间的请求-应答协议。
•web
浏览器可能是客户端，而计算机上的网络应用程序也可能作为服务器端。
•举例：客户端（浏览器）向服务器提交
HTTP 请求；服务器向客户端返回响应。响应包含关于请求的状态信息以及可能被请求的内容。

两种 HTTP 请求方法：GET和 POST
•在客户机和服务器之间进行请求-响应时，两种最常被用到的方法是：GET 和
POST。
•GET - 从指定的资源请求数据。
•POST - 向指定的资源提交要被处理的数据
请求报文，响应报文

2.2 常见状态码的含义

200---OK/请求已经正常处理完毕

301---/请求永久重定向

302---/请求临时重定向

304---/请求被重定向到客户端本地缓存

400---/客户端请求存在语法错误

401---/客户端请求没有经过授权

403---/客户端的请求被服务器拒绝，一般为客户端没有访问权限

404---/客户端请求的URL在服务端不存在

500---/服务端永久错误

503---/服务端发生临时错误

- CTF中常见的编码和加密
  1.ASCII编码
  •ASCII编码大致可以分作三部分组成：

•第一部分是：ASCII非打印控制字符（参详ASCII码表中0-31）；

•第二部分是：ASCII打印字符，也就是CTF中常用到的转换;

•第三部分是：扩展ASCII打印字符

十进制	二进制	符号	十进制	二进制	符号	十进制	二进制	符号	十进制	二进制	符号
0	0000 0000	NUL	32	0010 0000	[空格]	64	0100 0000	@	96	0110 0000	`
1	0000 0001	SOH	33	0010 0001	!	65	0100 0001	A	97	0110 0001	a
2	0000 0010	STX	34	0010 0010	"	66	0100 0010	B	98	0110 0010	b
3	0000 0011	ETX	35	0010 0011	#	67	0100 0011	C	99	0110 0011	c
4	0000 0100	EOT	36	0010 0100	$	68	0100 0100	D	100	0110 0100	d
5	0000 0101	ENQ	37	0010 0101	%	69	0100 0101	E	101	0110 0101	e
6	0000 0110	ACK	38	0010 0110	&	70	0100 0110	F	102	0110 0110	f
7	0000 0111	BEL	39	0010 0111	'	71	0100 0111	G	103	0110 0111	g
8	0000 1000	BS	40	0010 1000	(	72	0100 1000	H	104	0110 1000	h
9	0000 1001	HT	41	0010 1001	)	73	0100 1001	I	105	0110 1001	i
10	0000 1010	LF	42	0010 1010	*	74	0100 1010	J	106	0110 1010	j
11	0000 1011	VT	43	0010 1011	+	75	0100 1011	K	107	0110 1011	k
12	0000 1100	FF	44	0010 1100	,	76	0100 1100	L	108	0110 1100	l
13	0000 1101	CR	45	0010 1101	-	77	0100 1101	M	109	0110 1101	m
14	0000 1110	SO	46	0010 1110	.	78	0100 1110	N	110	0110 1110	n
15	0000 1111	SI	47	0010 1111	/	79	0100 1111	O	111	0110 1111	o
16	0001 0000	DLE	48	0011 0000	0	80	0101 0000	P	112	0111 0000	p
17	0001 0001	DC1	49	0011 0001	1	81	0101 0001	Q	113	0111 0001	q
18	0001 0010	DC2	50	0011 0010	2	82	0101 0010	R	114	0111 0010	r
19	0001 0011	DC3	51	0011 0011	3	83	0101 0011	S	115	0111 0011	s
20	0001 0100	DC4	52	0011 0100	4	84	0101 0100	T	116	0111 0100	t
21	0001 0101	NAK	53	0011 0101	5	85	0101 0101	U	117	0111 0101	u
22	0001 0110	SYN	54	0011 0110	6	86	0101 0110	V	118	0111 0110	v
23	0001 0111	ETB	55	0011 0111	7	87	0101 0111	W	119	0111 0111	w
24	0001 1000	CAN	56	0011 1000	8	88	0101 1000	X	120	0111 1000	x
25	0001 1001	EM	57	0011 1001	9	89	0101 1001	Y	121	0111 1001	y
26	0001 1010	SUB	58	0011 1010	:	90	0101 1010	Z	122	0111 1010	z
27	0001 1011	ESC	59	0011 1011	;	91	0101 1011	[	123	0111 1011	{
28	0001 1100	FS	60	0011 1100	<	92	0101 1100	\	124	0111 1100	|
29	0001 1101	GS	61	0011 1101	=	93	0101 1101	]	125	0111 1101	}
30	0001 1110	RS	62	0011 1110	>	94	0101 1110	^	126	0111 1110	~
31	0001 1111	US	63	0011 1111	?	95	0101 1111	_	127	0111 1111	DEL

Base64/32/16编码

•base64、base32、base16可以分别编码转化8位字节为6位、5位、4位。16,32,64分别表示用多少个字符来编码，这里我注重介绍base64。Base64常用于在通常处理文本数据的场合，表示、传输、存储一些二进制数据。包括MIME的email，email via MIME,在XML中存储复杂数据。

•i love CTF

•aSBsb3ZlIENURg==

•重要特征，大部分base64后面有1-2个等号

原因：

• Base64编码要求把3个8位字节（3*8=24*）转化为4个6位的字节（*4*6=24），之后在6位的前面补两个0，形成8位一个字节的形式。

如果剩下的字符不足3个字节，则用0填充，输出字符使用'='，因此编码后输出的文本末尾可能会出现1或2个'='。

URL编码

•url编码又叫百分号编码，是统一资源定位(URL)编码方式。URL地址（常说网址）规定了常用地数字，字母可以直接使用，另外一批作为特殊用户字符也可以直接用（/,:@等），剩下的其它所有字符必须通过%xx编码处理。

现在已经成为一种规范了，基本所有程序语言都有这种编码，

•编码方法很简单，在该字节ascii码的的16进制字符前面加%. 如

空格字符，ascii码是32，对应16进制是'20'，那么urlencode编码结果是:%20。

•源文本：

The

quick brown fox jumps over the lazy dog

•编码后：

•%54%68%65%20%71%75%69%63%6b%20%62%72%6f%77%6e%20%66%6f%78%20%6a%75%6d%70%73%20%6f%76%65%72%20%74%68%65%20%6c%61%7a%79%20%64%6f%67

MD5

•Message

Digest Algorithm MD5（中文名为消息摘要算法第五版）为计算机安全领域广泛使用的一种散列函数，用以提供消息的完整性保护

•结果都是一个定长：16 、32、64。

•MD5

(“message digest”) = f96b697d7cb7938d525a2f31aaf161d0

等等

怕篇幅太长，下一篇继续，嘿嘿。

分享几个好的论坛（网站）：

freebuf

看雪

春秋