bugku题解-web



12 篇文章 1 订阅 订阅专栏

1.滑稽



打开题目进去发现很多滑稽脸,直接f12开发者,就能看到flag



2. Simple_SSTI_1

打开题目

您需要传入一个名为 flag 的参数。



CSDN @桔于

f12查看源代码发现线索

	<pre>r <nead></nead></pre>	
	▼ <body></body>	
	<pre>/font style="vertical-align: inherit;">/font>///font>///font>///font>///font>///font>///font>///font>///font>///font>///font>///font>///font>///font>///font>///font>///font>////font>///font>///font>////font>///font>////font>////font>////font>////font>////font>////font>///font>///font>////font>////font>////font>////font>////font>////font>////font>/////font>/////font>//////font>/////font>//////font>////////font>/////////font>/////font>/////////font>/////////font>////////////////////////////////////</pre>	
•••	You know, in the flask, We often set a secret_key ariable == \$0	
	<pre>div id="goog-gt-tt" class="skiptranslate" dir="ltr"></pre>	
	<pre>div class="goog-te-spinner-pos"></pre>	
		CSDN @桔于

flag在secret_key下,最下面说在flask里

• Flask/Jinja2

- {{ config.items() }}
- {{''.__class__.__mro__[-1].__subclasses_____}}

选择get的传入方式,一般secret-key中存在有价值的东西,或者说在config中,从而构建url: http://114.67.246.176:12152/?flag={{config}}, 看到secret_key中存在着flag



config的用法, config 也是 Flask模版中的一个全局对象,它包含了所有应用程序的配置值,所以可以使用 **config.xxx** 来查看该对象的属性值。

理解了题目的含义,直接构建如下url: http://114.67.246.176:12152/?flag={{config.SECRET_KEY}} 得到flag

\leftarrow	- → C 🔺 不安全 114.67.246.176:12152/?flag={{config.SECRET_KEY}}										
	应用	٢	攻防世界	2	ctftools	6	CTF在线工具-CTF	C csdn	📩 kelatv	100	Bugku CTF
flag	{a52a	a3fa	a4a9733	879	7894cd	a1c	l02df410}				
											CSDN @桔于

python和jinja 2的的ssti模板注入题目,需了解基础的jinja语法和网页页面渲染方式

3.计算器

打开题目看到有一个算式,但是发现只能输入一位数



In top ▼ G ittië

发现长度是1,所以右键修改属性,改为2

<pre>e" class="code" style="background:</pre>	rgb(171,	77,	240);	co]
<pre>text" class="input" maxlength="2"></pre>	== \$0			
neck">验证				
put				
唐 羊 索		CSDI	1 @ 稿·	j

再次输入答案即可得到flag

/ max	······································	THE R PERCENT AND THE REPORT OF	
← → C ▲ 不安全 114.67.246.176	12122		
👯 应用 🛞 攻防世界 🚨 ctftools 🥥 CTF&	総工具-CTF C 114.67.246.1	76:12122 显示	
7744=? 81 验证	flag(9a731ee1	e2752bef825f99ce4c3bcd42}	織定

CSDN @桔于

4.GET

Get是从服务器上获取数据,Get是把参数数据队列加到提交表单的Action属性所指的URL中,值和表单内各 个字段一一对应,在URL中可以看到。



CSDN @桔于

根据提示, 传入?what=flag即可



5.POST

Post是向服务器传送数据。 Post是通过HTTP post机制,将表单内各个字段与其内容放置在HTML header内一 起传送到Action属性所指向的URL地址。用户看不到这个过程。

打开题目,用POST请求方法可知只要传递相应参数即可获得相应内容



CSDN @桔于

方法一: hacbar直接输入what=flag

方法二: bp抓包



打开bp软件抓包

ctrl +r 发送,然后变更请求方式为post

● ●	Burp Project 测试器 重发器 窗口 帮助							
アメート 目前: http://14.67.246.176.13899 ② ③ 第次 日前: http://14.67.246.176.13899 ② ③ ③ 第二 日前: http://14.67.246.176.13899 ② ③ ③ ③ 第二 日前: http://14.67.246.176.13899 ③	(父表盘) 目标 代理 测试器 重发器 定序器 编码器	副 对比器 插件扩展	项目选项	用户选项				
● 図画 ()))) ()) ()) () () () () () () ()	7 × 8 ×							
	发递 取消 < v > v					目标: http://114.67.246.176:13899 🖉 ?		
Rem Hax DET/HTP/1 DET/HTP/1 DetT/HTP/1 DET/HTP/1	请求				响应			
ET / 11 / 17 / 24 / 176 1389 Cache-Corrol: max-agee0 Uggrade-inscere: Requests: 1 User-Agent: Mozilla50 (Window KT 10.0: Winds, x64) AppleWebk/2637.36 (V0HML, like Gecko) Chormed/4 - Loft 5 Salark573 - 26 Accept: glicatining/genetice/u/time+xml.application/xml.q=0.3 (mage) glicatining/genetice/u/time+xml.application/xml.q=0.3 glicatining/genetice/u/time/genetice/u	Raw 头 Hex				Raw			
Heat: 1145:246.766 13699 Capache Control: maragen0 Upgrade Instrume 244.06657 State 527.36 Accept. Accept. Accept.Language: the NLT100; Win64; x63 AppleWebKit6537.36 (OHTML, like Gecke) ExtMind appleatation/html+xml appleatation/html=0.9.mage/ Accept.Language: the OL:th:v=0.9 Zeame-tion: class	GET / HTTP/1.1			A		4		
Uggrafik instrume Regiments: 1 Uggrafik instrume Regiments: 1 Ugerand instrume Regiments: 1 Accept. Exatorial application/indire-0.9 imagef Page Lation/Signed-Accept.Emology appl Connection: close 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Host: 114.67.246.176:13899							
User Agent Macrille ⁵ Q (Mindex NT 100, Winde, x64) AppleWebkid537.36 (HTML, like Gecko) Chormo940 Lock 7 Sahak53.73 gg, dista Accept: Accept: Acception accent a	Upgrade-Insecure-Requests: 1							
Chormady 40, 406 f71 Safaria57.36 Accept: backtiming page, databa Accept:Encoding, gap, databa Accept:Encoding, gap, databa Cacept:Accept:Acception (Safaria) Camection: class Camection: class	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Apple	WebKit/537.36 (KHTML	, like Gecko)				
i sostini generalization/html application/marken/application/space/ generalization/html application/space/ generalization/html application/space/ generalization/html application/space/ generalization/html application/space/ generalization/html application/space/ generalization/html application/space/ generalization/space/ generalization/html application/space/ generalization/space/ generalization/space/ generalization/space/ generalization/space/ generalization/space/ generalization/space/ generalization/space/ generalization/space/ generalization/space/ generalization/space/ space/ generalization/space/ space/ generalization/space/ space/ generalization/space/ space/ generalization/space/ space/ generalization/space/ space/ generalization/space/ space/ generalization/space/ space/ generalization/ gener	Chrome/94.0.4606.71 Safari/537.36							
pp(catin/signed-exchange-wtb) 유민 3 Accept-Excoding 20p, defails Accept-Language, th CN, th 국민 9 Come-clion: close 전문체 2000 2000 2000 2000 2000 2000 2000 20	text/html.application/xhtml+xml.application/xml:a=0.9.image/	扫描		la				
AcceptEncoding gzp, defile AcceptEncoding zp, defile Connection: close Connection: close UEBROPHIC Connection: close UEBROPHIC UEBROPHI	pplication/signed-exchange;v=b3;q=0.9	发送给Intruder	Ctrl+I					
Accepted anguage an ULEAR #0.9 Connection: Claim # 2 能够Connection: Claim # 2	Accept-Encoding: gzip, deflate	发送给Repeater	Ctrl+R					
	Accept-Language: zn-UN,zn;q=0.9 Connection: close	发送给Sequencer						
发生的Decoder 日 世社(対応)告诉术 ▶ 世生) 世生) 日 (新 新 新 ★) 日 (新 新 新 ★) 日 (新 新 新 ★) 日 (新 新 ★) 日 (新 ★) 1 (新		发送给Comparer						
		发送给Decoder						
世代工作		通过浏览器请求	•					
		相关工具	· ·					
神術和の次 置動回知 置動回知 置動到定律 人文件私給 作称項目 律等項入項目 特項加入規定現代 形式以も認力資源米 洗面對化合地器		受更请不万法						
		對体销的以及 冒創回日						
		复制curl命令						
人 52件 秘涵 作 存所回 作 存所回 作 存 前、力反 22 承 将 20 L 税助力請求 注 次 19 好心 地間 10 日 10		复制到文件						
住存项目 (存存執)、历史记录 将ULLH品力请求 次因到后。他图		从文件粘贴						
律存輸入历史记录 特URL 484次为课来 这般到估点地图		保存项目						
将URL相限为请求 添加到站后她摺		保存输入历史记录						
添加到站点她蹭		将URL粘贴为请求						
		添加到站点地图						
转换选择 ▶		转换选择	•					
いれ、原母組入		URL编码输入	0.1.7					
		初計	Ctrl+X			CON ONT		
et CSDN @ 括于 kknit CN4V		at the	CtrlaV			CSDN @桔子		

然后输入what=flag(与上面空一行)



最后发送即可得到flag

6.alert

打开题目发现一直有弹窗

🖗 alert - Bugku CTF	× S BKCTF-WEB6	× C 写文章-CSDN博客 ×	+
\leftarrow \rightarrow C A 不安全	114.67.246.176:13022		
🗰 应用 😢 攻防世界 🛓	ctftools	C 114.67.246.176:13022 显示 来找找吧	CTF
			·····································

直接bp抓包

🖗 alert - Bugku CTF	× O BKCTF-WEB6	× C 写文章-CSDN博客	× +					
← → X ▲ 不弱	民全 114.67.246.176:13022							
👬 应用 🛞 攻防世界	🌲 ctftools 🧕 CTF在线工具-CTF 🕻	114.67.246.176:13022 显示						
	Burp Suite Professional v2.0.11beta - Temporary Project - licensed to surferxyz By:LianZhang							
	Burp Project 测试器 重发器 窗口 帮助							
	仪表盘 目标 代理 测试器 重发器 定序器 编码器	对比器 插件扩展 项目选项 用户选项						
	★●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●							
放包 廣包 拦颤请求 行动								
	Raw 头 Hex							
	GET / HTTP/1.1							
	Host: 114.67.246.176:13022 Cache-Control: max-age=0							
Upgrade-Insecure-Requests: 1								
userAgent: moziuma-u (vrinnovs ni i uu, vrinnet; too), AppleWeb/Mib/J.s/b (VHIML, like Gecko) Chrome/AU.4bb,/T Statub.5/, be Accept: texthmin.application/thmiret.ma.application/thmice-09.jmage/ar/ii.mage/web/ii.mage/application/signet-exchange,v=b3.q=0.9								
Accept-Encoding: gzip, deflate Accept-Language: zh-CN zh-c=0.9								
	Connection: close							
			CSDN @桔于					

查看源码(利用了alert()函数跳出弹窗)



发现最低端有一串字符



了解知识点:末尾存在一些以&#开头;号结尾的东西,是html实体

用burp解码得到flag

alert("00000¥0");	发送给Intruder	Ctrl+I	
alert("flag000000");	发送给Repeater	Ctrl+R	
alert("00000¥0");	发送给Sequencer		
alert("flagDDDDDDDD");	安连给Comparer		
alert("00000¥0");	2012 Sel Comparen		
alert("flag0000000");	久达hDecouer		
alert("0000¥0");	在浏览器中显示响应		
alert("flag000000");	通过浏览器请求	•	
alert("0000140"); •	相关工具	►	
</td <td>复制网址</td> <td></td> <td></td>	复制网址		
flag{496f5164d2	复制curl命令		
7;9813c2195339c190	気 (h)Culling マ 気 わ)の(か)(h)		
7;e893}>	复利到义计		
	保存项目		
	保存输入历史记录		
	将URL粘贴为请求		
	添加到站占地图		
	杜 按 注 招		
	我供应性	- Co	DN @#
	切割	Ctrl+X	

🚯 Burp Suite Professional v2.0.11beta - Temporary Project - licensed to surferxyz By:LianZhang —	\Box \times
Burp Project 测试器 重发器 窗口 帮助	
仪表盘 目标 代理 剥试器 重发器 定席器 编码器 对比器 插件扩展 项目违项 用户违项	
f,l,a,g,{,4,9,6f,5,1,64,d,2,a,9,8,1,3,3,3,9,c,1,&# - -</td><td>● Text ○ Hex ? 解码▼</td></tr><tr><td>-t</td><td>编码▼ 哈希▼ 智能解码</td></tr><tr><td><! flag(496/5164d2a9013c2195339c190ae093)</td><td>● Text ○ Hex 解码</td></tr><tr><td></td><td>编码▼</td></tr><tr><td></td><td>智能解码 CSDN の結子</td></tr></tbody></table>	

7.你必须让他停下

打开题目,发现页面一直刷新

$\leftarrow \rightarrow \mathbf{x}$	< ▲ 不爹	安全 114.67	.246.176:13974					
👥 应用 🍯	攻防世界	a ctftools	€ CTF在线工具-CTF	C csdn	📩 kelatv	闷 🛛 Bugku CTF	C 安全-alert (Bugku	简 Bugku-CTF题解W
I want to play Dummy game with others£;But I can't stop! Stop at panda ! u will get flag							l can't stop!	

方法一:因为页面自动刷新,所以只需将burp收到的包发送repeater,查看响应,然后forward,如此反复,有一个响应有flag

CSDN @桔于

🚯 Burp Suite Professional v2.0.11 beta - Temporary Project - licensed to surferxyz By:LianZhang	_		×
Burp Project 测试器 重发器 窗口 帮助			
【			
★● HTTP历史记录 WebSocket历史 选项			
放包 廣包 拦戰请求 行动	评论这个项目		*
Raw + Hex			
GET / HTTP/1 1 HTTP/1 / HTTP/1			
Uggalaremacuterequesis. User-Agent: McSulfa O (Vindova J. ws NT 10.0; Win54; n.54) AppleWeb/dx537;36 (VirtINL, like Gecks) Chrome/94.0.4006;71 Safar(537;36 Accept: textfirml.application/shtml+xml.application/shtml;et=0.9;mage/awf;mage/webp;mage/app;?*;e=0.8,application/signed-exchanges;=0.9 Referen: http://11.472.246;176:13974/			
AcceptEncoding:gzip, dellate Accept⊥anguage: zh-Cit.ytape3 Connection: Cose			
	C	SDN @	桔子

发送查看响应,然后forward,如此反复,有一个响应有flag

Burp Project 测试器 重发器 窗口 帮助	
仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项	
1 × 2 × 3 × 4 ×	
发送 职清 < ▼ > ▼	目标: http://114.67.246.176:13974 🖉 ?
请求	响应
Raw A Hex	Raw 头 Hex HTML Render
GET / HTTP/1.1	HTTP/1.1 200 OK
Host: 114.67.246.176:13974	Date: Thu, 07 Oct 2021 06:48:15 GMT
Cache-Control: max-age=0	Server: Apache/2.4.7 (Ubuntu)
Upgrade-Insecure-Requests: 1	X-Powered-By: PHP/5.5.9-1 ubuntu4.6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Winb4; xb4) AppleWebKit/537.36 (KHTML, like Gecko) Chromo/94.0 4006 71 Seferi/E37.36	Vary: Accept-Encoding
Accent:	Connection: close
text/html.application/xhtml+xml.application/xml;g=0.9,image/avif.image/webp.image/apng;*/*;g=0.8,a	Content-Type: text/html
pplication/signed-exchange;v=b3;q=0.9	<i>"</i>
Referer: http://114.67.246.176:13974/	<html></html>
Accept-Encoding: gzip, deflate	<head></head>
Accept-Language: zh-CN,zh;q=0.9	<meta charset="utf-8"/>
Connection, close	<meta content-="" initial-scale-1.0="" name-="" viewponi="" widin-device-widin,=""/>
	<meta content="></td></tr><tr><td></td><td><title>Dummy game</title></td></tr><tr><td></td><td></head></td></tr><tr><td></td><td><script language=" javascript"="" name="description"/>
	function myrefresh(){
	window.location.reload();
	setTimeout('myrefresh()'.500):
	<body></body>
	<center>I want to play Dummy game with others£;But I can't stop!</center>
	<center>Stop at panda ! u will get flag</center>
	<center><dv>c/dv>+rcenter> <a< td=""></a<></dv></center>
	style= usplay.none anglas Hoostonezano to a subscrap so y as analys
	· · · · · · · · · · · · · · · · · · ·
	CSDN @結于
¥	C1014 64E11

方法二: crtl+u 查看源代码,一直刷新即可找到含有flag的页面源代码



8.网站被黑



打开题目进入一个网页



通过题目tips我们可以得知网站被黑之后,黑客留下了后门

使用御剑后台扫描工具 扫描到黑客留下的后门地址

域名	: http://114.67.246.176:10167/	开始	扫描	停止扫	描
线程 超时	: 20 - > (条 CPU核心 * 5最佳) DIR: 446889 ASP: 297812 : 3 - > (秒 超时的页面被丢弃) MDB: 9071	▲SPX: 42529 ✓ PHP: 52815 □ JSP: 19739		☑ 探测200 □ 探测403 □ 探测3XX	
描信	息:扫描完成	扫描线程	:0	扫描速度:()/秒
ID	地址			HTTPO	\overline{b}
	http://114.67.246.176:10167/index.php			200	
	http://114.67.246.176:10167/shell.php			200	
	http://114.67.246.176:10167/index.php?.php			200	
	http://114.67.246.176:10167/?.php			200	

通过扫描结果我们发现**shell.php**文件非常可疑

尝试访问,发现了一个需要密码的登录框

← → C ▲ 不安全 114.67.246.176:10167/shell.php	Se 🗘	🖽 O 🗯 😩 E
👬 应用 🛞 攻防世界 🌲 ctftools 🧕 CTF在线工具-CTF 🦲 csdn 🖄 kelatv 🏁 Bugku CTF 🔯 Bugku-CTF题解W		III 阅读清单
Walichall		
Websiteit		
PASS:		
登录		
		CSDN @措于

我们可以使用暴力破解的方式(我们使用Burpsuite进行抓包)



发送给intruder攻击(用burp暴力破解教程)BurpSuite系列(五)----Intruder模块(暴力破解)_fendo-CSDN博客

BugKu Web题《网站被黑》writeUp_CSDN_suuny的博客-CSDN博客

上面文章有爆破教程,学习后设置好开始爆破

Burp Project 測试器 重发器 窗口 鞣助	
化未盘 目标 代号 测试器 重发器 定序器 编码器 对比器 插件扩展 项目途项 用户选项	
目标 位置 有效载荷 逃顷	
	TT #4 viz.th
→ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	77 आ - २२ म
+ m . 144.67.046.476	
± 11, 11, 11, 242, 179	
яжц: 10167	
□ 使用HTTPS	
	CSDN @ 桔于

得到密码为hack,输入得到flag

攻击 1 (结果	保存 列 ┃目标 位置 有效载荷 逆	顷					
过滤器	· 显示所有项目						?
请求	有效载荷	状态	错误	超时	ĸ	评论	
173	hack	200			1203		
0		200			1200		
1	admin	200			1200		
2	admin12	200			1200		
3	admin888	200			1200		
4	admin8	200			1200		
5	admin123	200			1200		
6	sysadmin	200			1200		
7	adminxxx	200			1200		
9	6kadmin	200			1200		
8	adminx	200			1200		۷
							CSDN @桔干

	WebShell	
PASS		
17135.		
	啓司	

CSDN @桔于

9.本地管理员



打开题目



CSDN @桔于

尝试登陆: admin和admin账号密码,显示IP禁止访问,IP已经被记录,打开控制台,发现底部有个``



CSDN @桔于

很明显的base64编码,解码得到: test123,猜测账号: admin,密码: test123

€ 在线工具	买SSL证书	SSL在线工具	工具网	
base编码				
base16、base32、base64	ļ.			
dGVzdDEyMw==				
编码 base64	ţ	▼ 字	符集 utf8(unicode编码) ▼	
			编 码	解 码
test123				CSDN @桔于

应该就不是爆用户名和密码的问题了

又题目描述本地管理员,联系本地管理员登陆,burp抓包伪造XFF头

IP欺骗(XFF头等)_weixin_30466421的博客-CSDN博客(知识点)

1.X-Forwarded-For:(转载上面链接)

简称XFF头,它代表客户端,也就是HTTP的请求端真实的IP,只有在通过了HTTP代理或者负载均衡服务器时 才会添加该项。它不是RFC中定义的标准请求头信息,在squid缓存代理服务器开发文档中可以找到该项的详细 介绍。标准格式如下:X-Forwarded-For: client1, proxy1, proxy2。

这一HTTP头一般格式如下:

X-Forwarded-For: client1, proxy1, proxy2, proxy3

其中的值通过一个 逗号+空格 把多个IP地址区分开,最左边(client1)是最原始客户端的IP地址,代理服务器每成功 收到一个请求,就把**请求来源IP地址**添加到右边。在上面这个例子中,这个请求成功通过了三台代理服务器: proxy1, proxy2 及 proxy3。请求由client1发出,到达了proxy3(proxy3可能是请求的终点)。请求刚从client1中发 出时,XFF是空的,请求被发往proxy1;通过proxy1的时候,client1被添加到XFF中,之后请求被发往proxy2;通 过proxy2的时候,proxy1被添加到XFF中,之后请求被发往proxy3;通过proxy3时,proxy2被添加到XFF中,之后请求的的去向不明,如果proxy3不是请求终点,请求会被继续转发。

如果一个 HTTP 请求到达服务器之前,经过了三个代理 Proxy1、Proxy2、Proxy3, IP 分别为 IP1、IP2、IP3, 用户真实 IP 为 IP0, 那么按照 XFF 标准,服务端最终会收到这样信息:X-Forwarded-For: IP0, IP1, IP2

鉴于伪造这一字段非常容易,应该谨慎使用X-Forwarded-For字段。正常情况下XFF中最后一个IP地址是最后一个代理服务器的IP地址,这通常是一个比较可靠的信息来源。burp抓包伪造XFF头

直接burp抓包伪造XFF头

Burn Project 测试器 郵送器 窗口 帮助								
以衣盖 曰外 19世 羽氏器 里久器 正序器 獨同器 31比器 加什扩展 坝目透映 用户透映								
■ ■ HTTP历史记录 WebSocket历史 选项								
✓ http://114.67.246.176:12453 请求								
放包 廣包 拦截清求 行动								
Raw 参数 头 Hex								
POST / HTTP/1.1								
Host: 114.67.246.176:12453								
Content-Length: 23								
Cache-Control: max-age=0								
Upgrade-Insecure-Requests: 1								
Origin: http://114.67.246.176:12453								
Content-Type: application/x-www-form-urlencoded								
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.71 Safari/537.36								
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9								
Referer: http://114.67.246.176:12453/								
Accept-Encoding: gzip, deflate								
Accept-Language: zh-CN,zh;q=0.9								
Connection: close								
user=admin&pass=test123	CSDN @桔于							

伪造

X-Forwarded-For 127.0.0.1 (空格再输入127.0.01)

得到flag

Burp Project 测试器 重发器 窗	口 帮助					
(重发器 定序器	\$│编码器│对比器	插件扩展	项目选项	用户选项	
1 × 2 ×				-		·
发送 取消 く 🔻	$> \mathbf{v} $					目标: http://114.67.246.176:12453 🖉 ?
请求						响应
Raw 参数 头 Hex						Raw 🔆 Hex HTML Render
名 Cache-Control Upgrade-Insecure-Requests Origin Content-Type User-Agent Accept Referer Accept-Encoding Accept-Language Connection XFrorwardel-For µser=admin&pass=test123	(<u>fi</u> max-age=0 1 http://114.67.24 application/x-wn Mozilla/5.0 (Wi text/html.applic http://114.67.24 gzip, deflate zh-CN.zh;q=0.9 close 127.0.0.1	6.176:12453 ww-form-urlencoded adows NT 10.0, Winf ation/xhtml+xml,app 6.176:12453/	i4; x64) Appl ication/xml;o	eW	ata (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	HTTP/1.1200 OK ATTP:/1.200 OK ATTP:/1.200 OK Date: Fini @ 00 t2021 02:54:31 GMT Server: Apache/2.4.7 (Ubuntu) X-Powerad-By: PHP/5.5.9-1ubuntu4.6 Vary: Accept Encoding Content-Length: 5506 Contention: loss Co
? < + > 輸入的	皇家宁词			ž	2有比赛	парадаралараларалараларалараларалараларал