ctf和DVWA靶场

原创

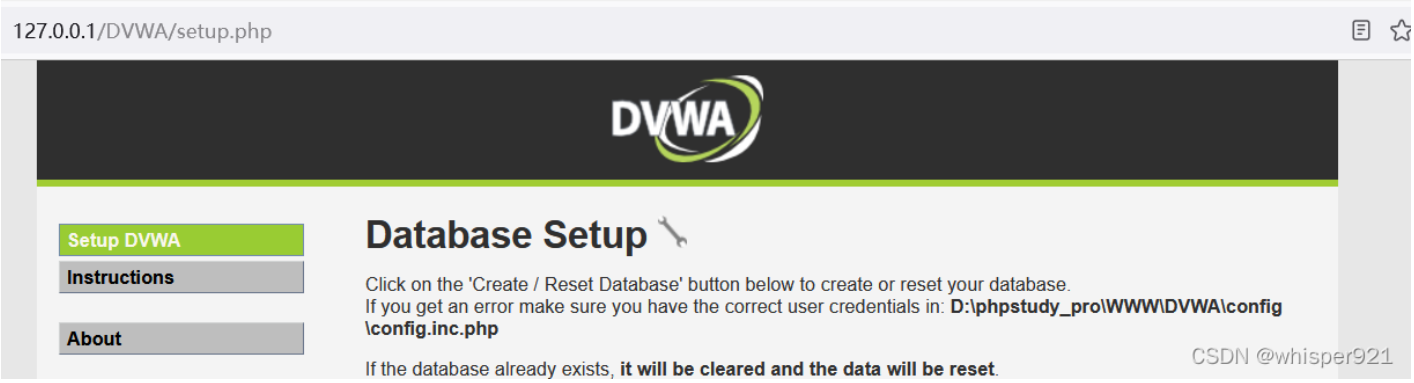
whisper921 于 2022-01-15 19:25:31 发布 2195 收藏
文章标签： 安全 sql web安全

一.ctf-web-第三题

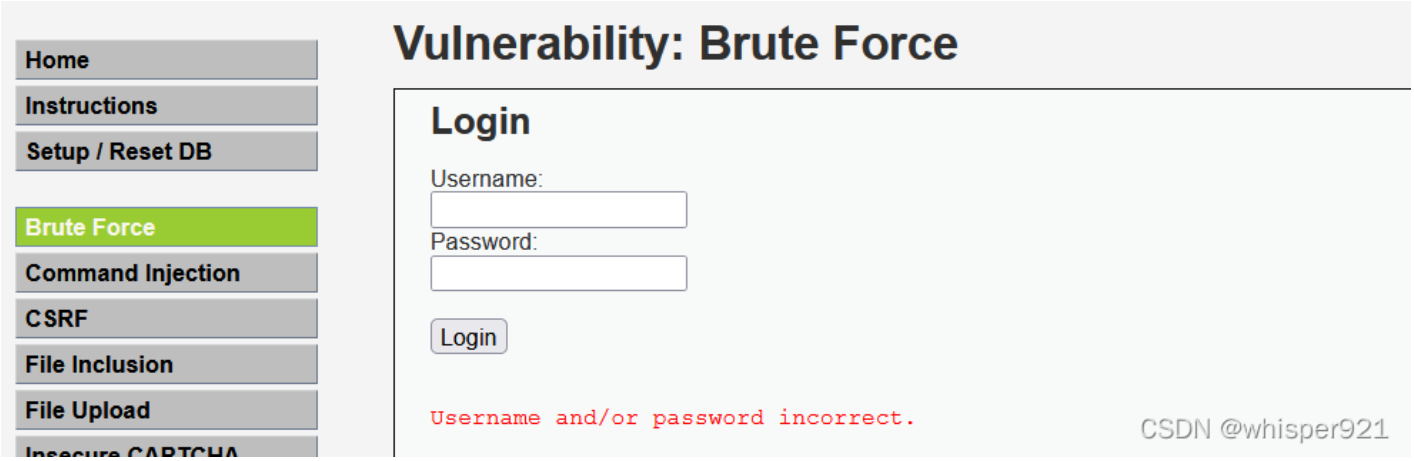
通过bp抓包即可获得flag

二.DVWA靶场

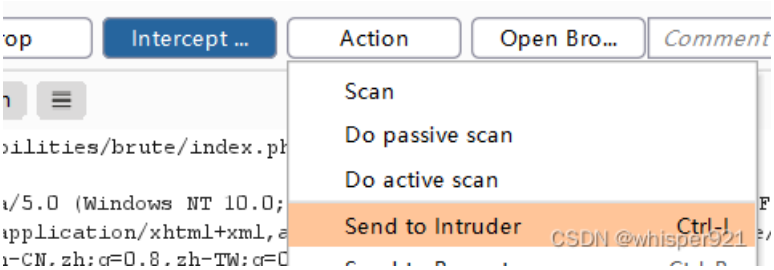
先使用PHP创建靶场

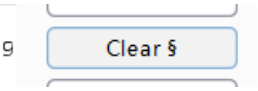


第一题Brute Force（爆破）low



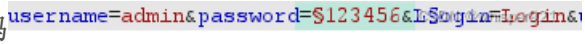
先随便输入账号密码，使用BP抓包



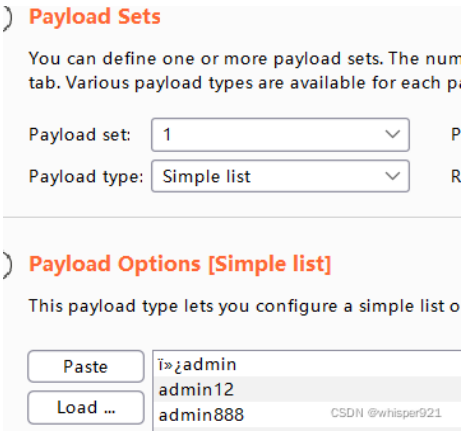


按清除

选中密码



load选择常用密码

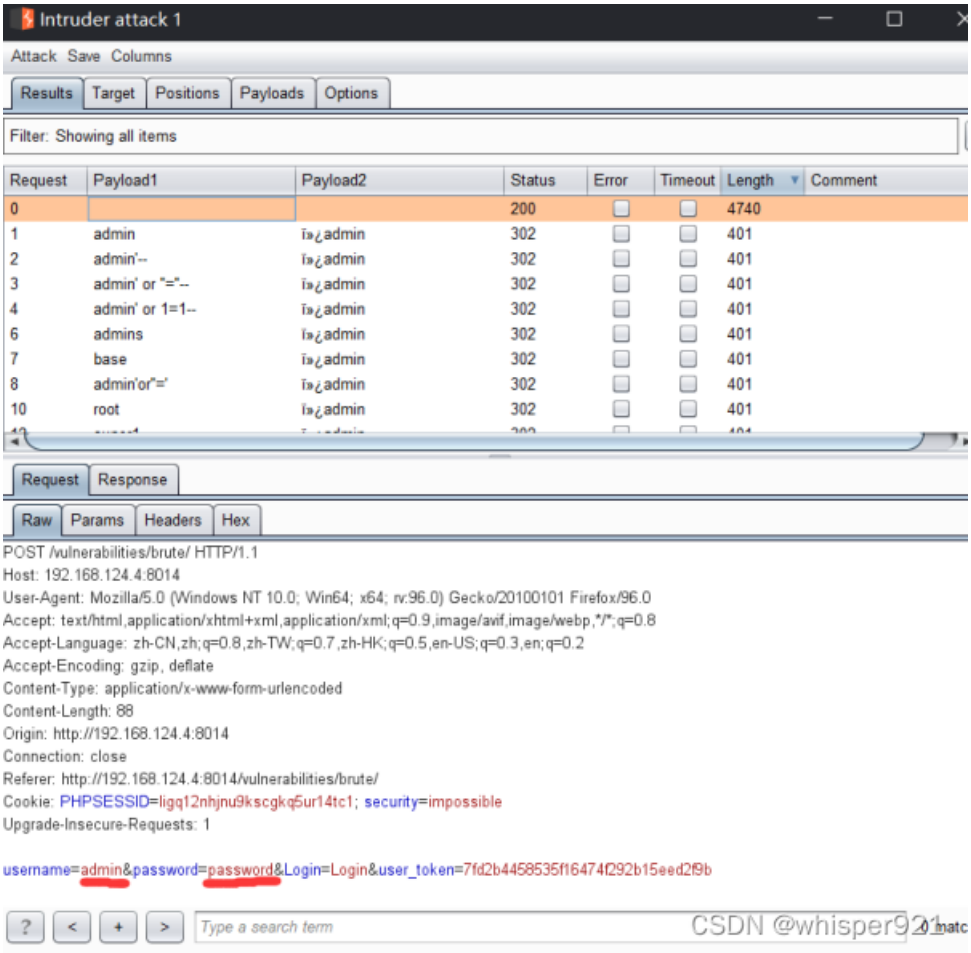


开始爆破

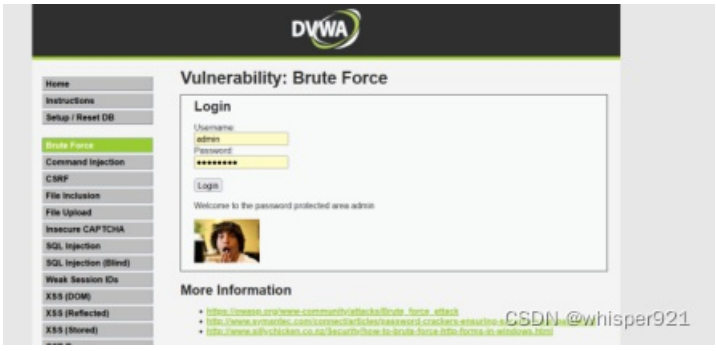
Request	Payload	Status	Error	Timeout	Length	Comment
0		302			376	
1	ï»¿admin	200			4640	
2	admin12	200			4640	
3	admin888	200			4640	
4	admin8	200			4721	
5	admin123	200			4640	
6	sysadmin	200			4640	
7	adminxxx	200			4640	
8	adminx	200			4640	
9	6kadmin	200			4640	
10	base	200			4640	
11	feitium	200			4640	

长度不一样一般即为密码

开始爆破，发现当payload1和payload2分别为admin和password时返回值长度与其他数据不同



分析该组数据为正确用户名与密码，输入登录成功



2、Command Injection

命令注入，是指通过提交恶意构造的参数破坏命令语句结构，从而达到执行恶意命令的目的。PHP命令注入攻击漏洞是PHP应用程序中常见的脚本漏洞之一，国内著名的Web应用程序Discuz!、DedeCMS等都曾经存在过该类型漏洞。

DVWA中就是让输入一个IP地址，然后去ping这个IP地址
题目需要我们输入一个ip进行ping

分析源码发现对于不同的系统会进行不同的ping操作，但没有进行注释，直接调用cmd，因此可以直接利用ping指令获得服务器ip

DOS中&&用法

&& Usage：第一条命令 && 第二条命令 [&& 第三条命令…]

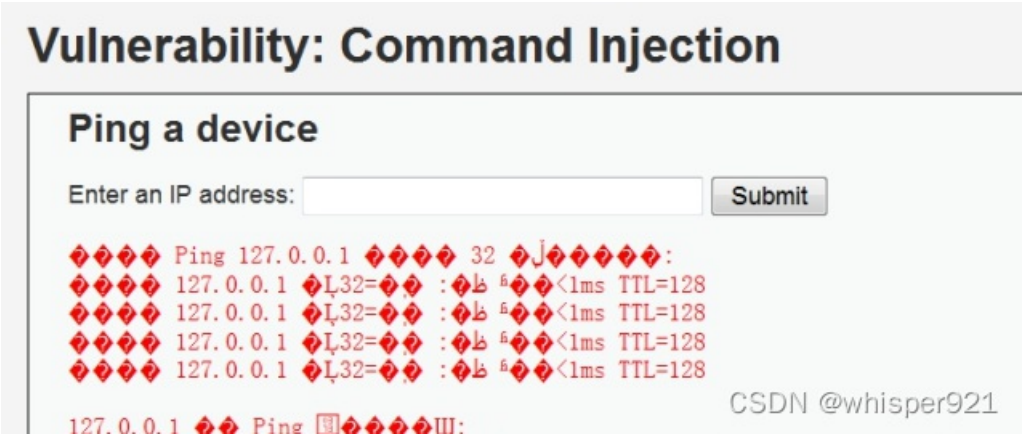
当碰到执行出错的命令后将不执行后面的命令，如果一直没有出错则一直执行完所有命令；

ping自己

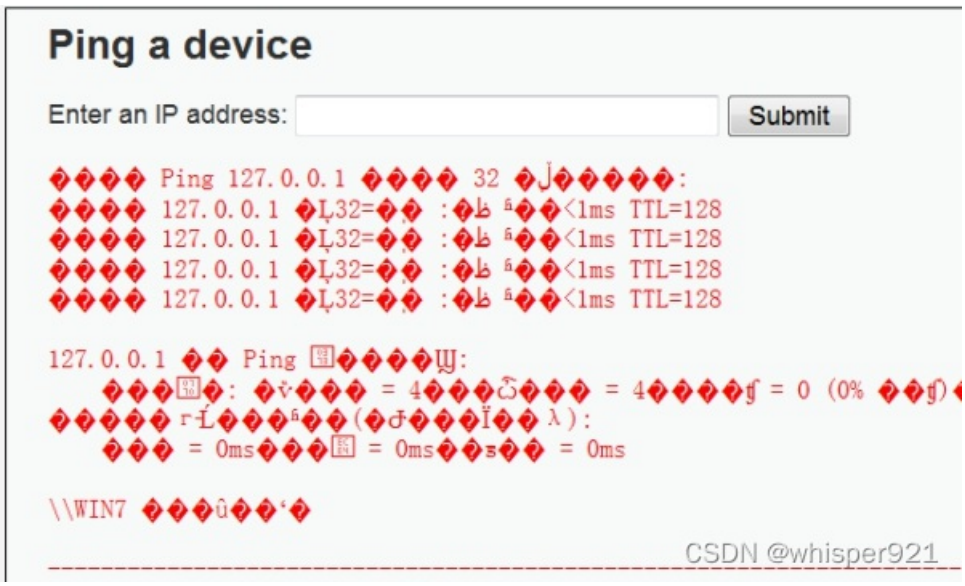
输入127.0.0.1

那么我们就是用&& 127.0.0.1&&net user

127.0.0.1&&net user zzyy 111 /add

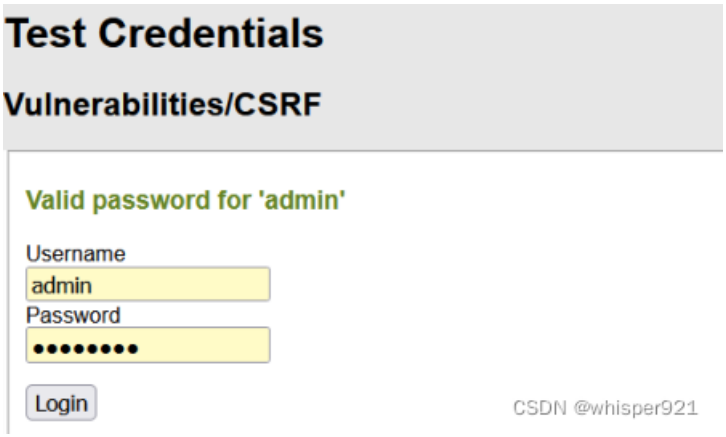


127.0.0.1&&net user

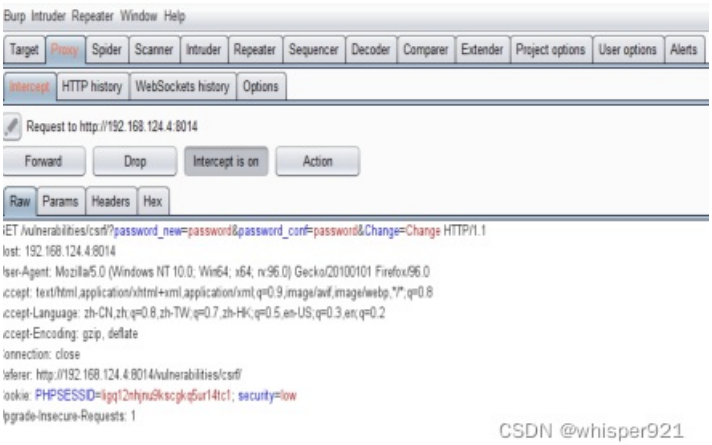


3.CSRF

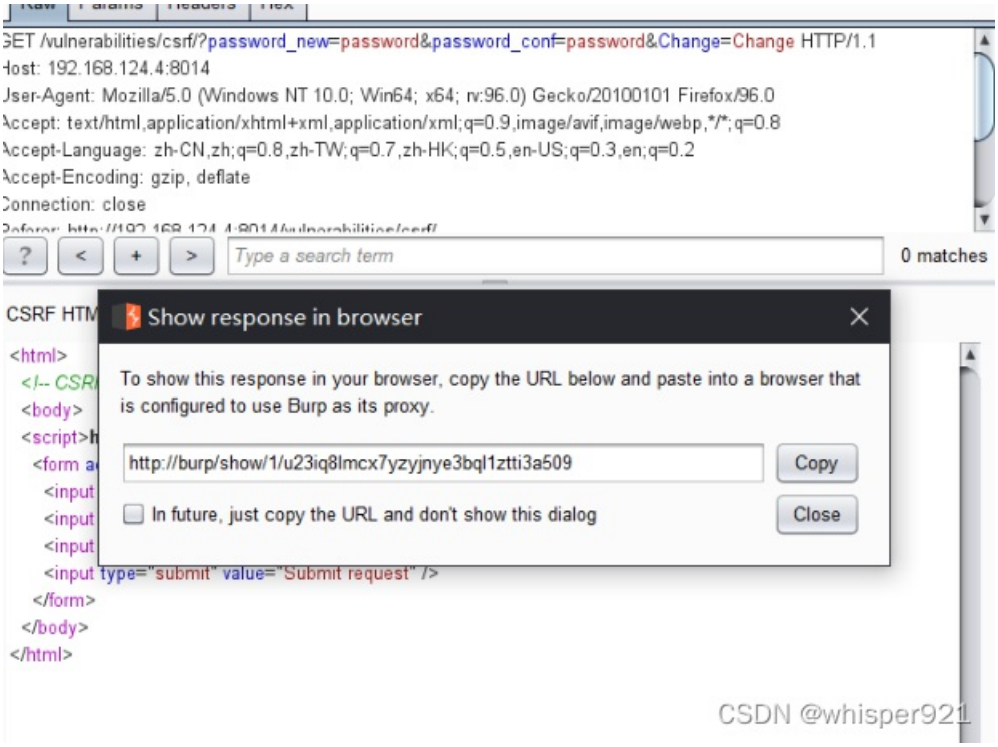
CSRF是跨站请求伪造，攻击者盗用合法的用户身份，以合法用户的名义去发出恶意请求，但这对服务器来说确识完全合法的，通过CSRF可以完成密码重置，管理员账户添加，转账等高位操作。
题目是一个密码修改界面，尝试修改密码并验证



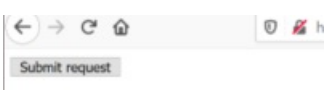
发现验证成功，接下来尝试使用BP抓包



点击test in browser



在浏览器中打开，得到如下界面



单击submit request，返回页面出现password changed，说明存在CSRF漏洞，利用成功